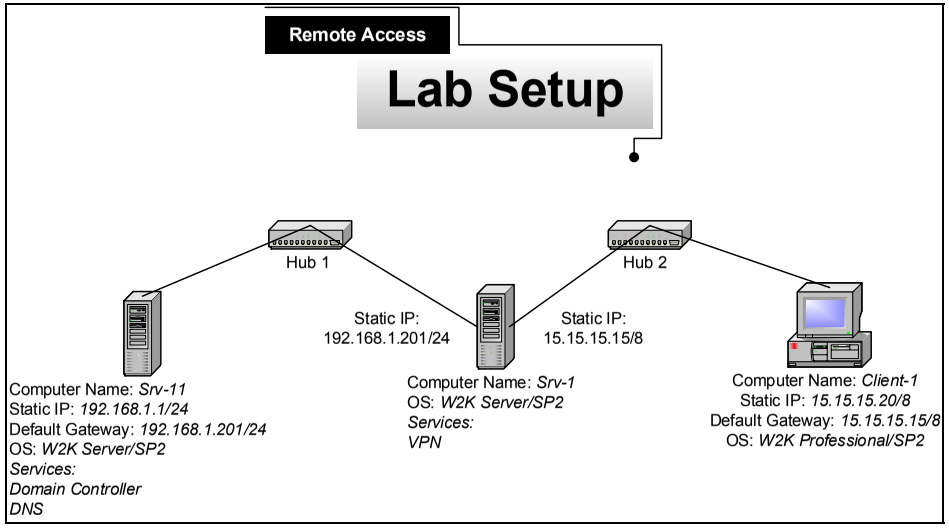
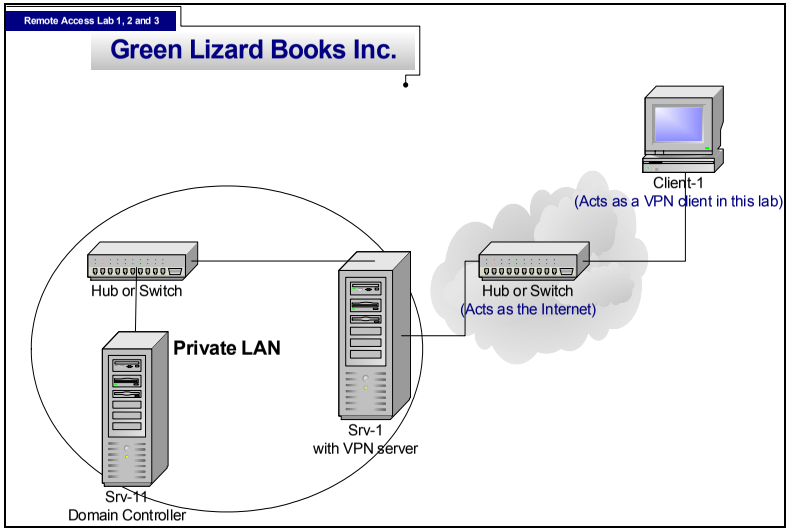
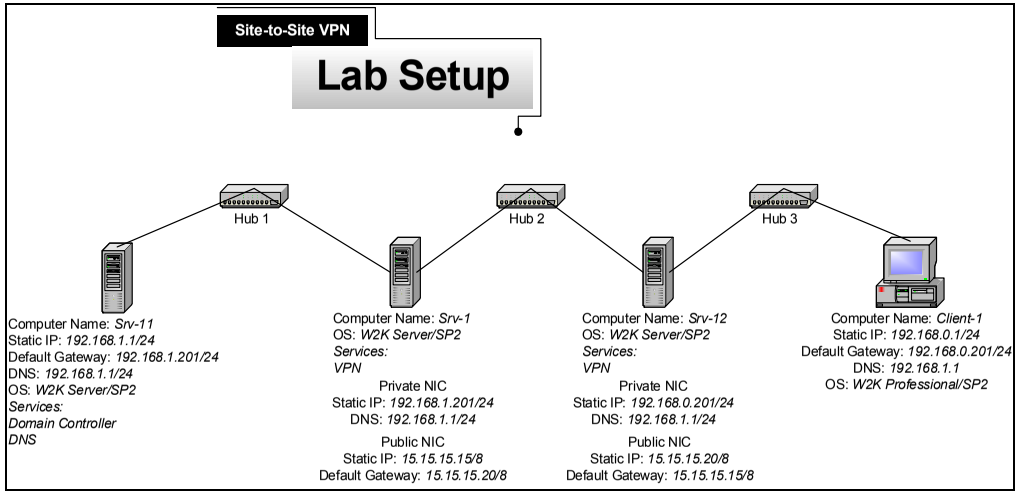
Installing Virtual Private Networks (VPNs) using
PPTP & L2TP for Green Lizard Books, Inc.

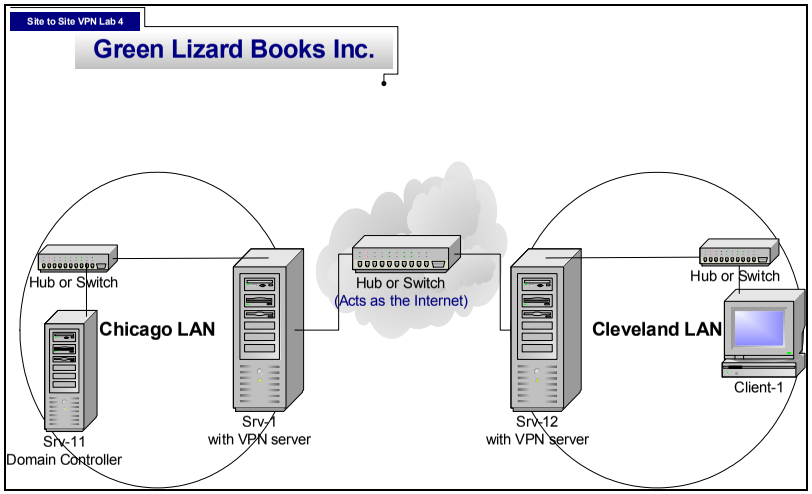
Mega Lab 8

Part 2 of 3 in the Windows 2000/2003
Routing & Remote Access Series

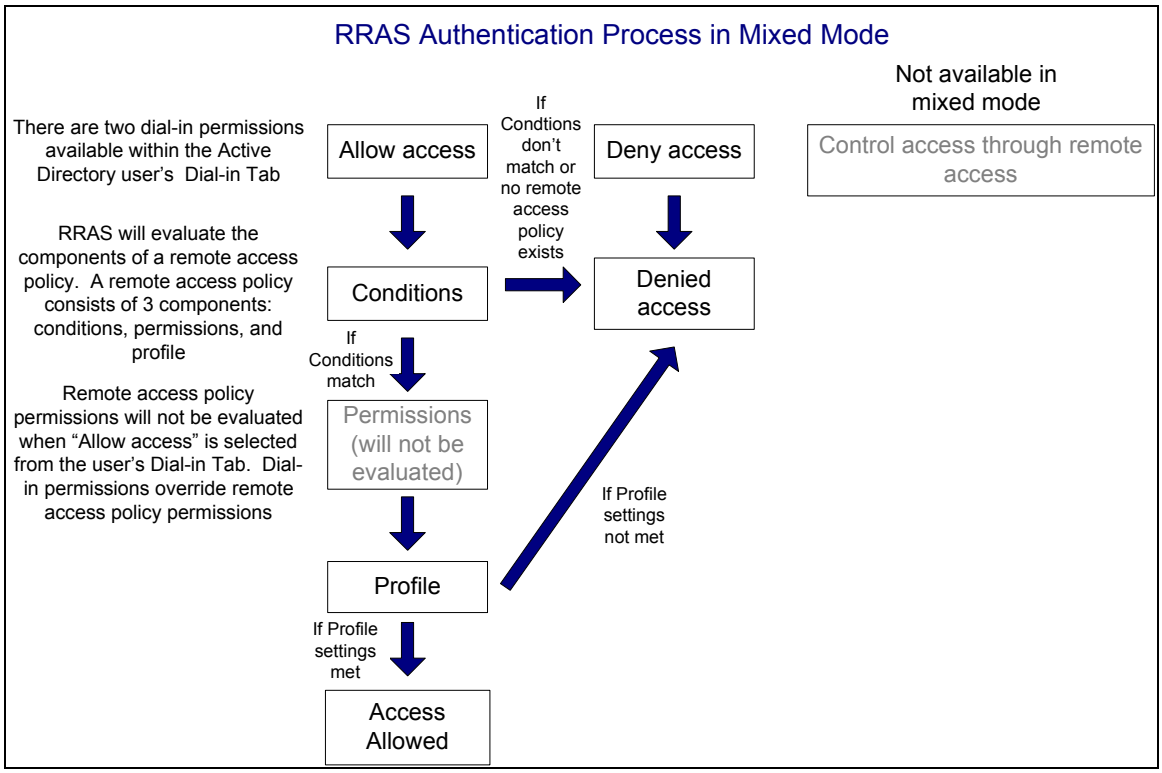


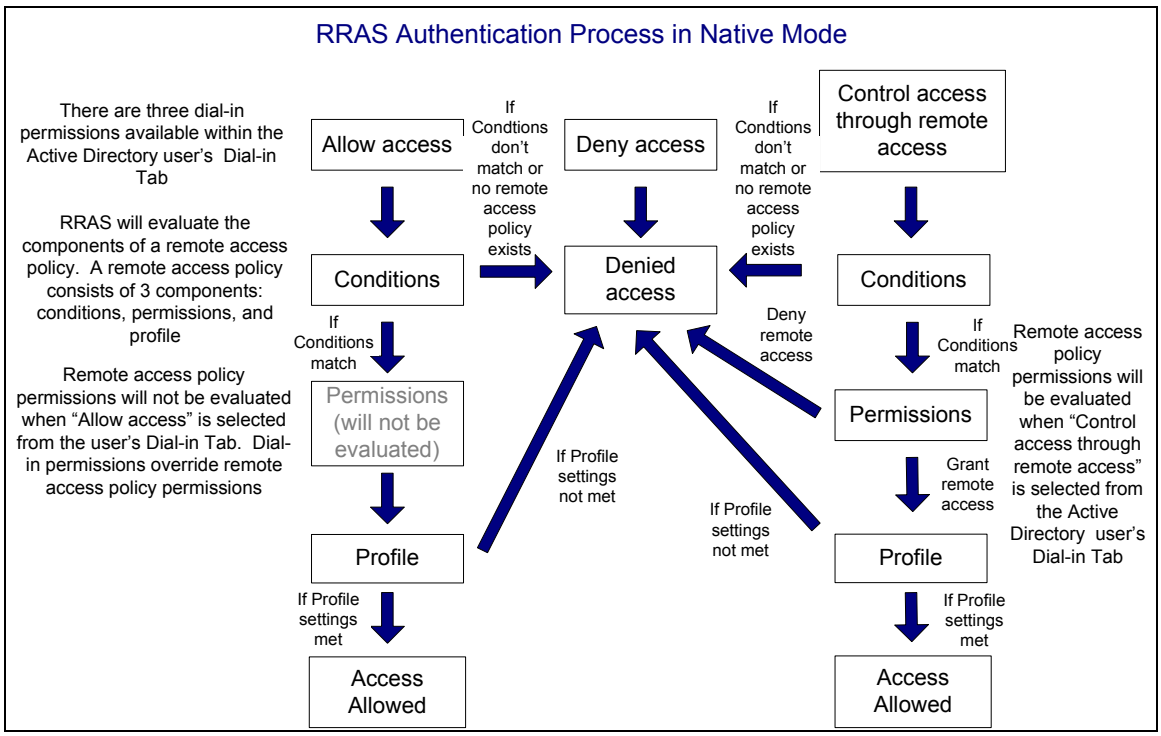






© Train Signal, Inc, 2003





© Train Signal, Inc, 2003

Installing Virtual Private Networks (VPNs) using PPTP & L2TP for Green Lizard Books, Inc.

Mega Lab 8

Part 2 of 3 in the Windows 2000/2003
Routing & Remote Access Series

© Train Signal, Inc., 2002-2003

© Train Signal, Inc., 2002-2003

About the Authors

Scott Skinger (MCSE, CNE, CCNP, A+) is the owner of Train Signal, Inc. and is an experienced Windows 2000 instructor. He has also worked in the trenches as a Network Engineer, Director of Technology and currently as an Independent Consultant through his own company, SAS Technology Advisors. As an instructor, he has taught over 50 courses, covering topics such as Windows 2000, NT 4, Novell NetWare, Cisco Routers and security.

Wilson Chan (MCSA) is responsible for content development for the Routing and Remote Access Mega Lab Series. He also does network support, computer hardware repair and software support for a computer consulting company.

Train Signal, Inc.
400 West Dundee Road
Suite #106
Buffalo Grove, IL 60089
Phone - (847) 229-8780
Fax – (847) 229-8760
www.trainsignal.com

Copyright and other Intellectual Property Information

© Train Signal, Inc., 2002-2003. All rights are reserved. No part of this publication, including written work, videos and on-screen demonstrations (together called "the Information" or "THE INFORMATION"), may be reproduced or distributed in any form or by any means without the prior written permission of the copyright holder.

Products and company names, including but not limited to, Microsoft, Novell and Cisco, are the trademarks, registered trademarks and service marks of their respective owners.

Disclaimer and Limitation of Liability

Although the publishers and authors of the Information have made every effort to ensure that the information within it was correct at the time of publication, the publishers and the authors do not assume and hereby disclaim any liability to any party for any loss or damage caused by errors, omissions, or misleading information.

TRAIN SIGNAL, INC. PROVIDES THE INFORMATION "AS-IS." NEITHER TRAIN SIGNAL, INC. NOR ANY OF ITS SUPPLIERS MAKES ANY WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. TRAIN SIGNAL, INC. AND ITS SUPPLIERS SPECIFICALLY DISCLAIM THE IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THERE IS NO WARRANTY OR GUARANTEE THAT THE OPERATION OF THE INFORMATION WILL BE UNINTERRUPTED, ERROR-FREE, VIRUS-FREE, OR THAT THE INFORMATION WILL MEET ANY PARTICULAR CRITERIA OF PERFORMANCE OR QUALITY. YOU ASSUME THE ENTIRE RISK OF SELECTION, INSTALLATION AND USE OF THE INFORMATION.
IN NO EVENT AND UNDER NO LEGAL THEORY, INCLUDING WITHOUT LIMITATION, TORT, CONTRACT, OR STRICT PRODUCTS LIABILITY, SHALL TRAIN SIGNAL, INC. OR ANY OF ITS SUPPLIERS BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER MALFUNCTION, OR ANY OTHER KIND OF DAMAGE, EVEN IF TRAIN SIGNAL, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL TRAIN SIGNAL, INC. BE LIABLE FOR DAMAGES IN EXCESS OF TRAIN SIGNAL, INC.'S LIST PRICE FOR THE INFORMATION.

To the extent that this Limitation is inconsistent with the locality where You use the Software, the Limitation shall be deemed to be modified consistent with such local law.

Choice of Law:

You agree that any and all claims, suits or other disputes arising from your use of the Information shall be determined in accordance with the laws of the State of Illinois, in the event Train Signal, Inc. is made a party thereto. You agree to submit to the jurisdiction of the state and federal courts in Cook County, Illinois for all actions, whether in contract or in tort, arising from your use or purchase of the Information.

© Train Signal, Inc., 2002-2003

TABLE OF CONTENTS

© Train Signal, Inc., 2002-2003

© Train Signal, Inc., 2002-2003

Introduction

Welcome to Train Signal!

This series of labs on Windows 2000/2003 is designed to give you detailed, hands-on experience working with Windows 2000/2003. Train Signal's Audio-Visual Lab courses are targeted towards the serious learner, those who want to know more than just the answers to the test questions. We have gone to great lengths to make this series appealing to both those who are seeking Microsoft certification and to those who want an excellent overall knowledge of Windows 2000/2003.

Each of our courses puts you in the driver's seat, working for different fictitious companies, deploying complex configurations and then modifying them as your company grows. They are not designed to be a "cookbook lab," where you follow the steps of the "recipe" until you have completed the lab and have learned nothing. Instead, we recommend that you perform each step and then analyze the results of your actions in detail.

To complete these labs yourself, you will need at least three computers equipped as described in the Lab Setup section. You also need to have a foundation in Windows 2000 and TCP/IP concepts. You should be comfortable with installing Windows 2000 Professional or Server and getting the basic operating system up and running. Each of the labs in this series will start from a default installation of Windows 2000 and will then run you through the basic configurations and settings that you must use for the labs to be successful. It is very important that you follow these guidelines **exactly**, in order to get the best results from this course.

The course also includes a CD-ROM that features an audio-visual walk-through of all of the labs in the course. In the walk-through, you will be shown all of the details from start to finish on each step, for every lab in the course. During the instruction, you will also benefit from live training that discusses the current topic in great detail, making you aware of many of the associated fine points.

Thank you for choosing Train Signal!

© Train Signal, Inc., 2002-2003

© Train Signal, Inc., 2002-2003

Lab Setup

© Train Signal, Inc., 2002-2003

Setting up the Lab

1. Computer Equipment Needed

Item	Minimum	Recommended
Computers	(3) Pentium I 133 MHz	(4) Pentium II 300MHz or greater -a 4th system is needed for Lab 4 only
Memory	128 MB	256 MB
Hard Drive	2 GB	4 GB or larger
NIC	1/machine (2 computers) 2 for the VPN server machine	1/machine (2computers) 2/VPN server (2 computers)
Hubs	2	2 (3 are needed for Lab 4)
Network Cable	(4) Category 5 cables	(5) Category 5 cables

I strongly urge you to acquire all of the recommended equipment in the list above. It can all be easily purchased from eBay or another source, for around $400 (less if you already have some of the equipment). This same equipment is used over and over again in all of Train Signal's labs and will also work great in all sorts of other network configurations that you may want to set up in the future. It will be an excellent investment in your education. You may also want to look into a disk-imaging product such as Norton Ghost. Disk imaging software will save you a tremendous amount of time when it comes to reinstalling Windows 2000 for future labs. Many vendors offer trial versions or personal versions of their products that are very inexpensive.

© Train Signal, Inc., 2002-2003

2. Computer Configuration Overview

Computer Number	1	2	3
Computer Name	SRV-1	Client-1	SRV-11
IP Address	NIC #1 192.168.1.201/24 NIC #2 15.15.15.15/8	15.15.15.20/8	192.168.1.1/24
Default Gateway	N/A	15.15.15.15	192.168.1.201
OS	W2K Server	W2K Pro	W2K Server
Additional Configurations	SP2	SP2	SP2

3. Detailed Lab Configuration

*****Important Note*****
This lab should NOT be performed on a live production network. You should only use computer equipment that is not part of a business network AND is not connected to a business network. Train Signal Inc. is not responsible for any damages. Refer to the full disclaimer and limitation of liability, which appears at the beginning of this document and on our Website at: http://www.trainsignal.com/legalinfo.html

© Train Signal, Inc., 2002-2003

Computer 1

Computer 1 will be named SRV-1 and the operating system on this computer will be Windows 2000 Server or Advanced Server. You should also install Service Pack 2 to avoid any unforeseen problems. If you do not have a copy of Windows 2000 Server you can obtain an evaluation copy of Windows 2000 Advanced Server within the Microsoft Press series of books, and Service Pack 2 is available for download on Microsoft's Website.

SRV-1 will have 2 network cards, each with a static IP address. One NIC will have an IP address of 192.168.1.201, with a 255.255.255.0 subnet mask and it should be renamed as **private**. The default gateway can be left blank. Configure the preferred DNS server setting to point to SRV-11, 192.168.1.1, and leave the alternate DNS setting blank. The second NIC will have an IP address of 15.15.15.15 with a 255.0.0.0 subnet mask. This NIC should be named **public**. The default gateway field and the DNS Server field should be left blank. You will need to make this computer a member server of the greenlizardbooks.com domain, by simply right clicking on the "**My Computer**" icon on the desktop and selecting **Properties**. Select the **Network identification** tab, select **Properties**, select **domain** and type in the domain name of the domain it will join, which is **greenlizardbooks.com** or its NetBIOS name, **greenlizardbook.** Note: NetBIOS names are a single label (no periods) up to 15 characters in length. Then click **OK**. Windows 2000 will then ask for a username and password. Use the administrator account name and password **from the greenlizardbooks.com domain.** When it has joined successfully, it will "welcome you to the domain" and then tell you that it needs to restart in order for the changes to take effect. After restarting the computer, make sure you change the "Log on to" dialog box to the domain rather than "this computer". See figure 1, next page.

*****Important Note*****
This last step (joining SRV-1 to the domain) cannot be performed until after you have created the greenlizard.com domain by running dcpromo on SRV-11 in the Computer 3 setup below.

Computer 2

Computer 2 will be named Client-1 and Windows 2000 Professional will be installed on this computer along with Service Pack 2. Client-1 will be joined to the greenlizardbooks.com domain. Client-1 will eventually be a VPN client, but initially will have a static IP address of 15.15.15.20 with a 255.0.0.0 subnet mask. The default gateway should be configured to point to SRV-1, 15.15.15.15, and the DNS Server field should be left blank. See figure 1, next page.

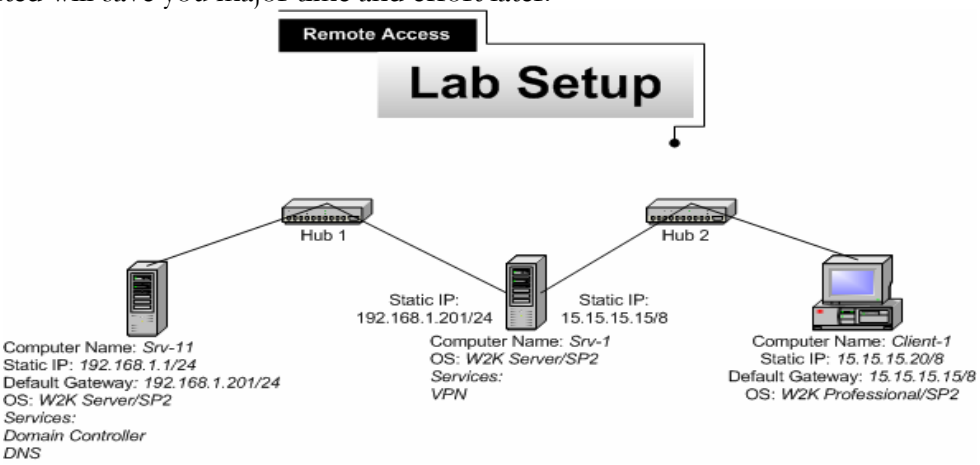
Computer 3

Computer 3 will be named SRV-11 and will have Windows 2000 Server or Advanced Server installed as the operating system. SRV-11 will have a static IP address of 192.168.1.1 with a 255.255.255.0 subnet mask. The default gateway should be configured to point to SRV-1, 192.168.1.201, and the DNS server field should be left blank. See figure 1, next page.

© Train Signal, Inc., 2002-2003

SRV-11 will be setup as the domain controller for Green Lizard Books Inc., called greenlizardbooks.com by using the dcpromo.exe program. In order to make this machine a domain controller, DNS will need to be installed as well. There are 2 ways to install DNS – automatically when you run dcpromo.exe or manually when you install it through Add/Remove Programs in Control Panel. For our purposes, we are going to install DNS automatically. To run dcpromo.exe on this machine go to the desktop, click on **Start → Run**, then type in **DCPROMO** in the run command and click **OK**. Make the following selections as you are prompted: **Domain controller for a new domain; Create a new domain tree; Create a new forest of domain trees**. The DNS domain name for the scenario is greenlizardbooks.com. The NetBIOS name will be greenlizardbook. Notice that there is no "s" at the end of greenlizardbook. This is because NetBIOS names can be a maximum of 15 characters long and the "s" would have been the 16th character. Leave all the other settings at their defaults. When the wizard asks if you would like to install and configure DNS on this computer, select **Yes, install and configure DNS on this computer**. Also choose permissions compatible with pre-Windows 2000 servers. In the next step, you will be asked for an AD password - for our purposes, we will leave this blank. Active Directory installation should then take place and you can restart the computer when you are prompted. **MAKE SURE** that the network card is plugged into a hub or into another computer with a crossover cable before you run dcpromo. Otherwise, Active Directory installation will fail, without giving you a clear cause. See figure 1.

Important - You should test the network connections (using the PING command) between each of these machines to ensure that your network is set up properly. Testing before you get started will save you major time and effort later.



(figure 1)

*****Important Note*****

This lab should NOT be performed on a live production network. You should only use computer equipment that is not part of a business network AND that is not connected to a business network. Train Signal Inc. is not responsible for any damages. Refer to the full disclaimer and limitation of liability which appears at the beginning of this document and on our web site, www.trainsignal.com

© Train Signal, Inc., 2002-2003

© Train Signal, Inc., 2002-2003

Lab 1

Setting up a Virtual Private Network for Green Lizard Books, Inc.

You will learn how to:

- Install a VPN Server using the RRAS setup wizard
- Manually configure a VPN Server
- Examine and Configure the properties of a VPN Server
- Set up a VPN client and configure its properties
- Test the VPN Server using different tunneling protocols
- Test the VPN Server using different authentication protocols

© Train Signal, Inc., 2002-2003

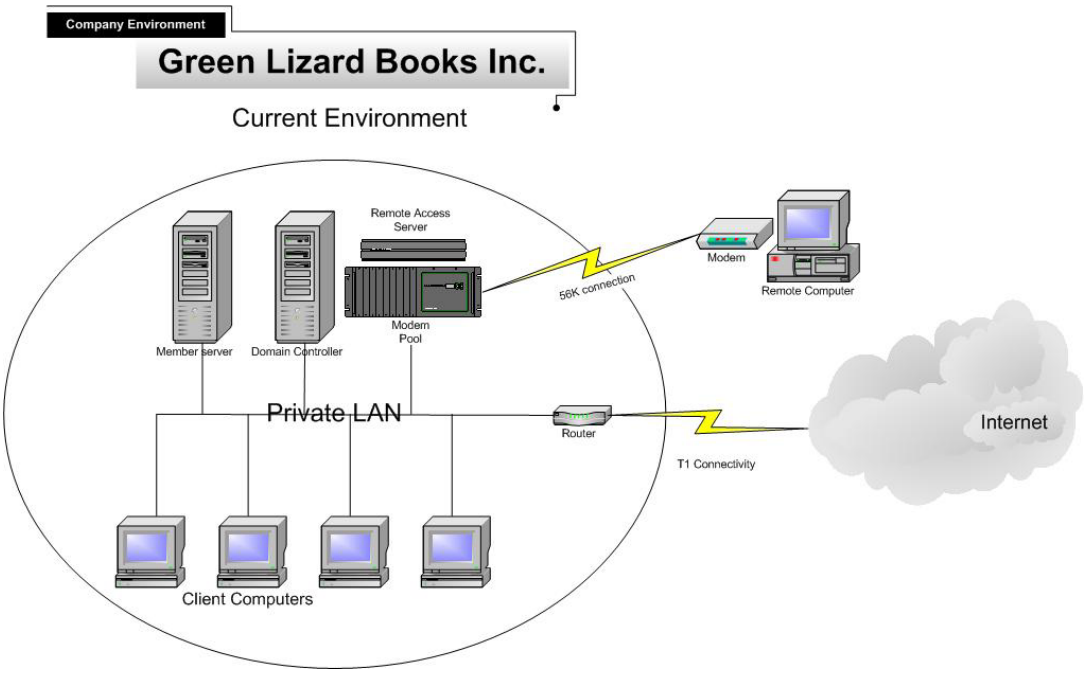
Scenario

Green Lizard Books Inc. is a book publishing company located in Chicago, IL. Green Lizard deals with authors, publishers and retail stores throughout the US and sometimes internationally. While traveling, Green Lizard executives and sales representatives must be able to use the company's private network in order to access contracts, sales leads and the customer database. Green Lizard is currently using a dial-up remote access solution to provide access to their employees. This solution has worked adequately for several years, but lately it has proven to be unreliable. In addition, it has always been slow and the monthly long distance expenses have been substantial, due to employees dialing in from locations that are not local to Chicago. The owner, Bill, is looking for a more reliable solution that will reduce the current long distance expense. You have been hired as an independent computer consultant to assist Green Lizard in finding a replacement to their current dial-up solution.

Since Green Lizard already has a dedicated connection (T1, operating at 1.5 Mbps) to the Internet, you suggest that they should consider deploying a Virtual Private Network (VPN). You inform him that a VPN would be an ideal remote access solution for his current situation. "A VPN," you explain, "will allow Green Lizard's employees to access the company network utilizing a secure connection over the Internet. Users will simply need to dial into a local ISP first, in order to connect to the company LAN. This will tremendously reduce the cost of long distance charges due to remote access connections." Bill likes your idea and wants you to start on it immediately.

In this lab, you will install a VPN Server using both the RRAS wizard and manual setup for Green Lizard Books Inc. You will then configure the VPN Server's properties and modify its available port settings. You will also set up a VPN client and test the VPN connection. Finally, you will test the VPN connection using L2TP and different remote authentication protocols.

© Train Signal, Inc., 2002-2003

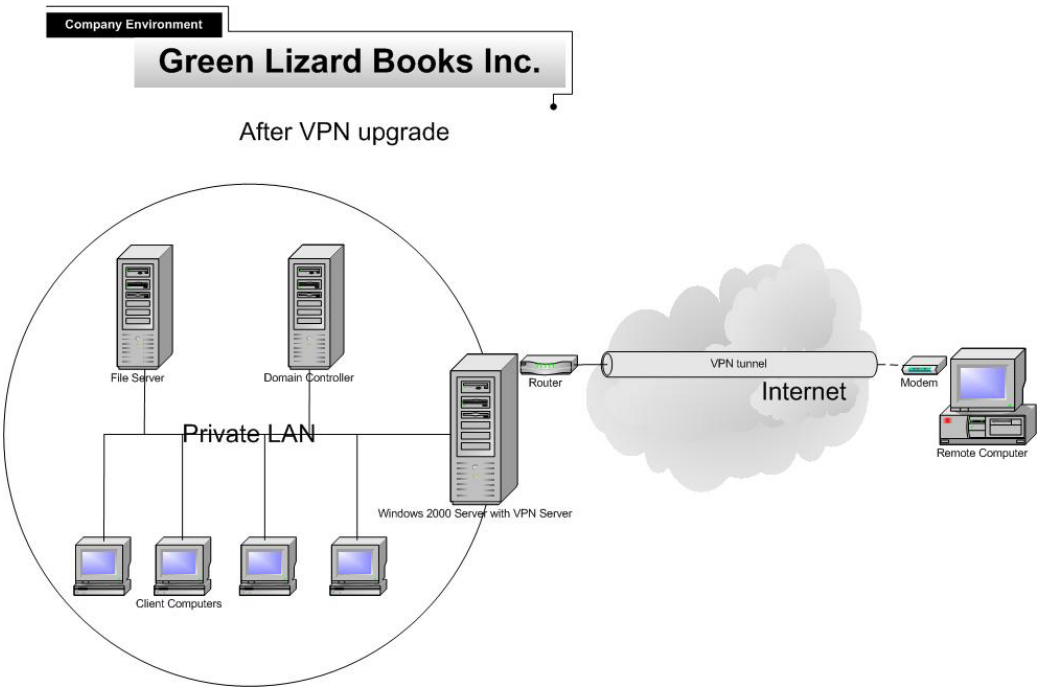


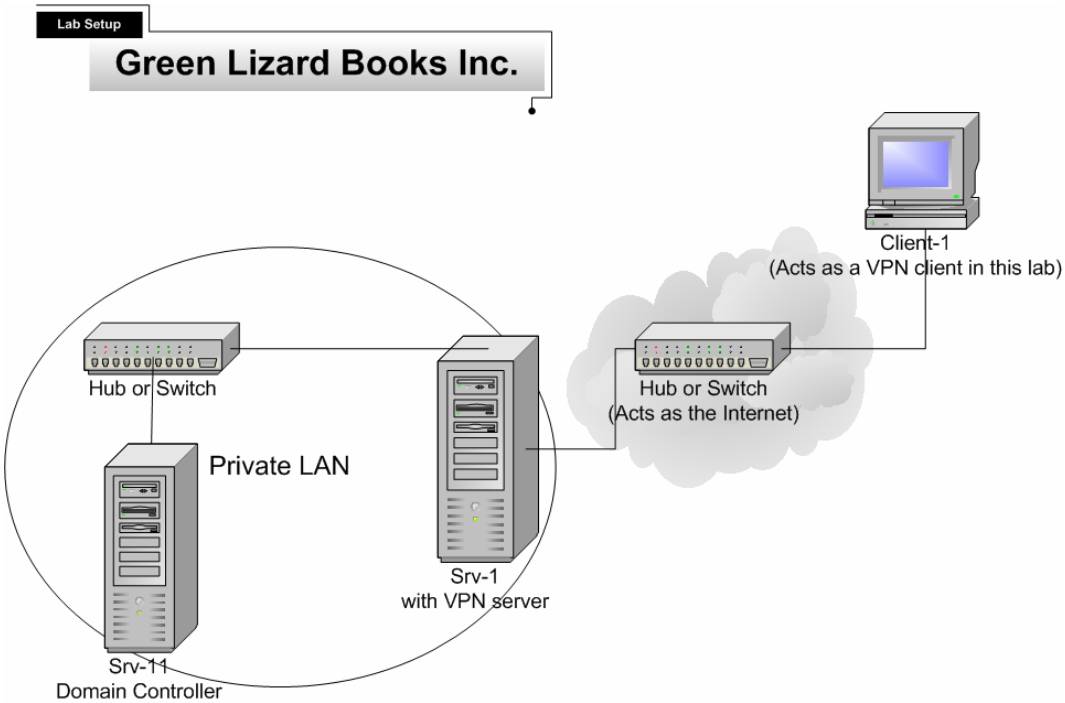
Windows 2000 Remote Access Solutions

VPN connections vs. Dial-up connections

	VPN connections	Dial-up connections
Connection Methods	VPN client establishes a local connection to the Internet and connects to the LAN through a VPN server. This connection provides secure remote access through the Internet over a TCP/IP connection.	Dial-up client uses common phone lines over the Public Switched Telephone Network (PSTN) to create a physical connection to a modem on a remote access server on the company LAN.
Cost	Requires remote clients to connect to the Internet through a local Internet service provider (ISP) only. It can reduce long-distance telephone charges and toll calls.	Requires expensive long-distance telephone charges or toll calls if there is a large number of remote clients traveling to far away locations.
Telecommunication/ Hardware requirement	Requires an existing connection to the Internet and a VPN server on the LAN	Requires many incoming telephone lines and hardware devices in-house (such as remote access servers, modem pools, etc.)

© Train Signal, Inc., 2002-2003



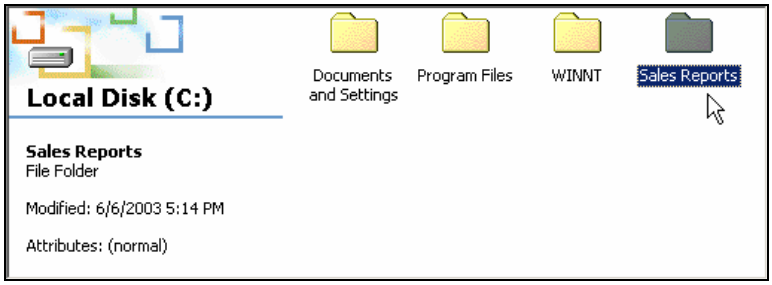


© Train Signal, Inc., 2002-2003

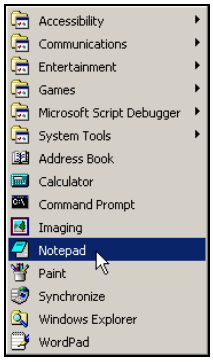
Creating a share to test remote access

Before you install the VPN Server, you will create a file in a shared folder on the domain controller, SRV-11. This file will be used to test access from Client-1, your VPN client, to the internal network through the VPN Server.

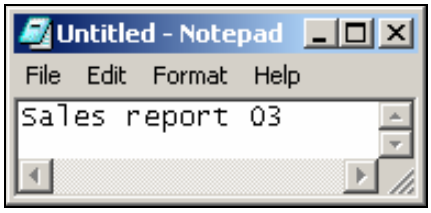
1. Log on to **SRV-11**, open **Windows Explorer**, and then open the **C: drive**. Create a new folder named **Sales Reports**. This can be done by right clicking on an empty space within the C: drive and selecting **New Folder** from the shortcut menu. You should now have a folder in the C: drive named Sales Reports. Close **Windows Explorer** when you are finished.



2. Next, use Notepad to create a simple text file that will be stored within the Sales Reports folder. Go to **Start→Programs→Accessories→Notepad**.

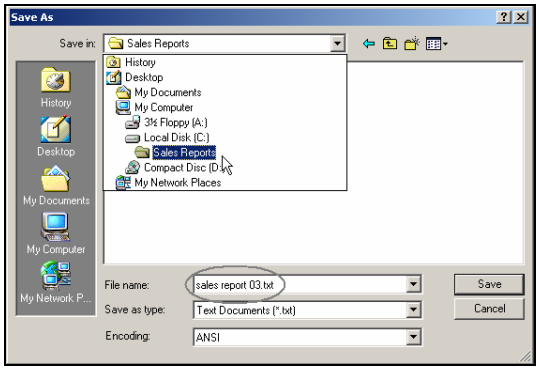


3. In Notepad, type in **Sales Report 03** and then select **File→Save As** from the menu.

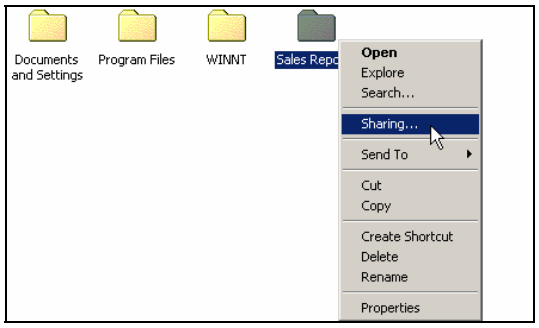


© Train Signal, Inc., 2002-2003

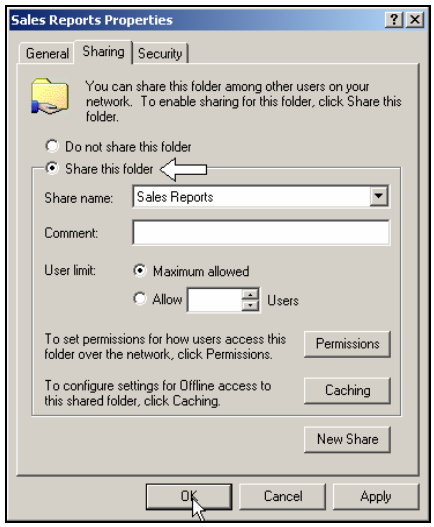
4. On the Save As screen, open the **Save in** drop down menu and select the **Sales Reports** folder that you created earlier as the location to save this file. Once you have selected the folder, enter the filename **sales report 03.txt**. Then click on the **Save** button and close **Notepad**.



5. Within Windows Explorer, right click on the **Sales Reports** folder and select **Sharing**.

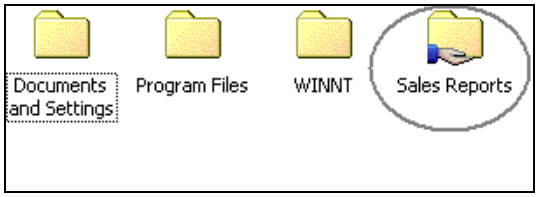


6. On the Sharing tab, select **Share this folder** and click **OK** to apply your changes.



© Train Signal, Inc., 2002-2003

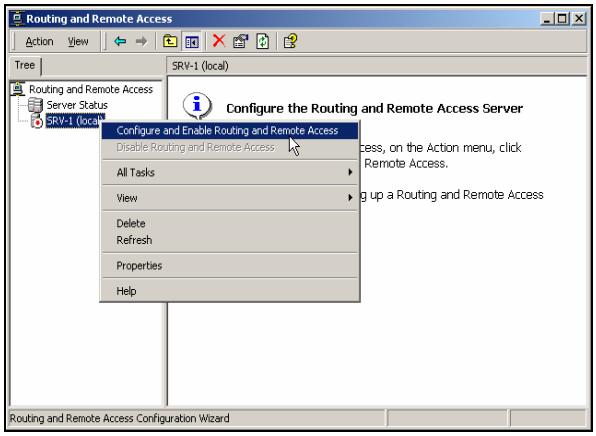
7. Notice that there is now a hand holding the Sales Reports folder, meaning that this folder is being shared on the network.

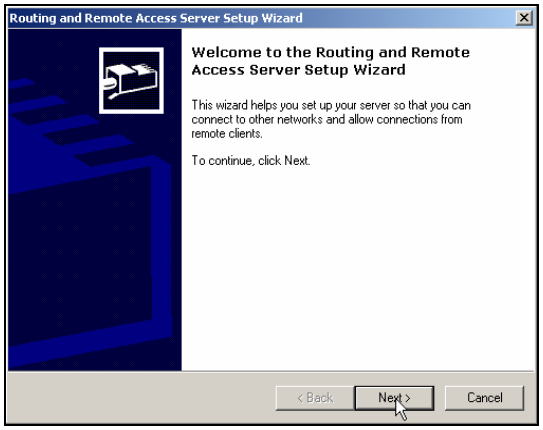


Installing a VPN Server through the RRAS setup wizard

SRV-1 has one NIC that is directly attached to the Internet that will be configured as Green Lizard's VPN Server. This NIC will serve as the public side of the VPN Server and will allow VPN clients to find SRV-1 across the Internet.

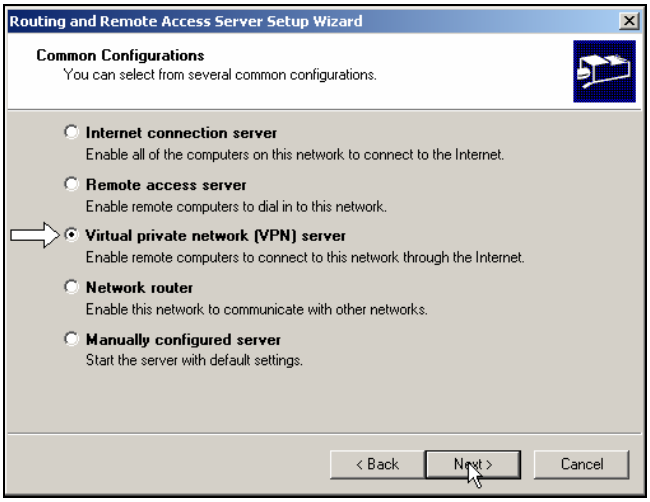
1. Log on to **SRV-1**. In order for you to install SRV-1 as a VPN server, you will need to configure and enable the Routing and Remote Access Server (RRAS) first. Notice that RRAS is installed as part of the Windows 2000 server installation. It is located under Administrative Tools. On SRV-1, go to **Start→Programs→Administrative Tools** and click on **Routing and Remote Access**. Right click **SRV-1** and then click **Configure and Enable Routing And Remote Access**. This will bring up the **Routing and Remote Access Server Setup Wizard**, just click **Next** to continue.



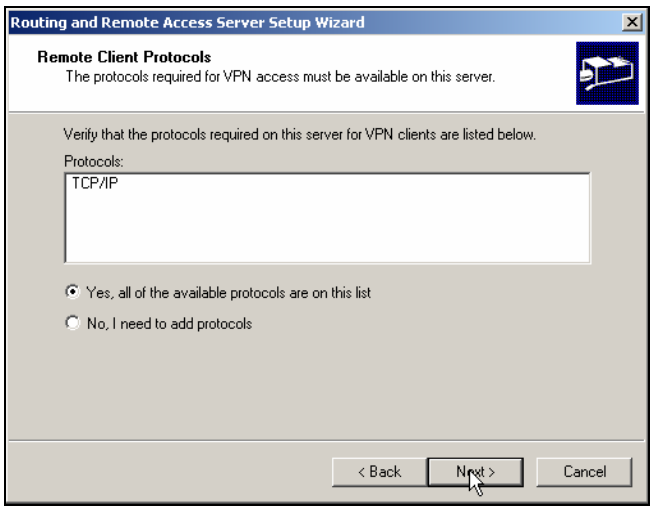


© Train Signal, Inc., 2002-2003

2. On the Common Configurations page, there are 5 common configurations for you to choose from. Within RRAS, there are many services that you can choose from other than just a VPN server. You can turn your computer into a NAT server or a Network router, to name a few. These other services are covered in great detail in both Lab 7 and Lab 9. For now, select the **Virtual private network (VPN) server** and click **Next** to continue with the installation.



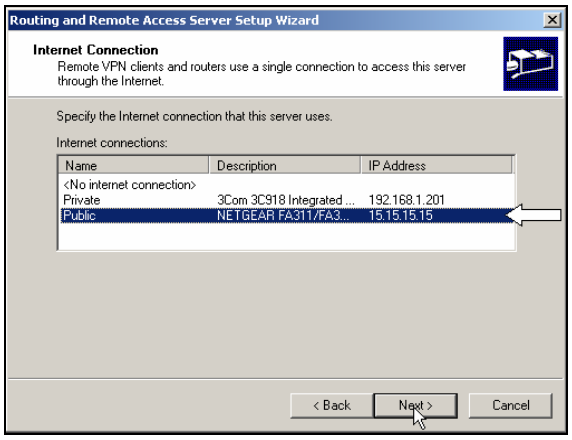
3. This will bring you to the Remote Client Protocols screen. For Green Lizard's VPN, TCP/IP is the only protocol that is required for remote access through the VPN server. This protocol should be installed by default. Just verify that TCP/IP is listed in the Protocols list and click **Next** to continue.



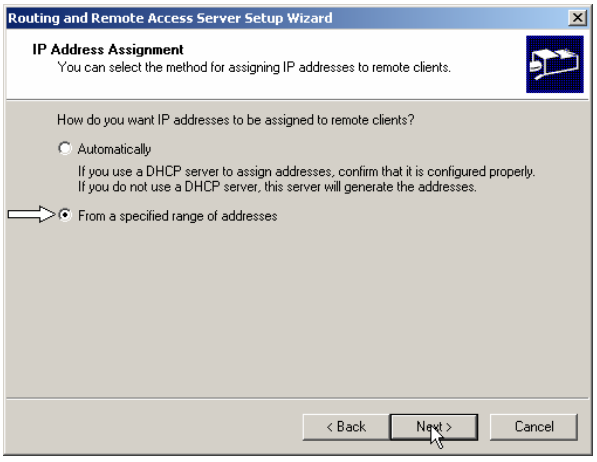
© Train Signal, Inc., 2002-2003

4. The next screen of the wizard will ask you to specify the Internet connection that the VPN server uses. In most real world cases, you will be connecting your VPN server's 2nd network card (public network card) to the device supplying you with the Internet connection (i.e. DSL Router, Cable Modem or T-1 Router).

   Under Internet connections, there are 2 network interfaces for you to choose from. **MAKE SURE** that you select the interface with the public IP address. In the lab, this interface should be marked **public,** with the IP address of 15.15.15.15. Remember, in a real world scenario, your Internet Service Provider provides this address to you and the interface would be connected to the public side of your network. Therefore, highlight **Public** and click **Next**.

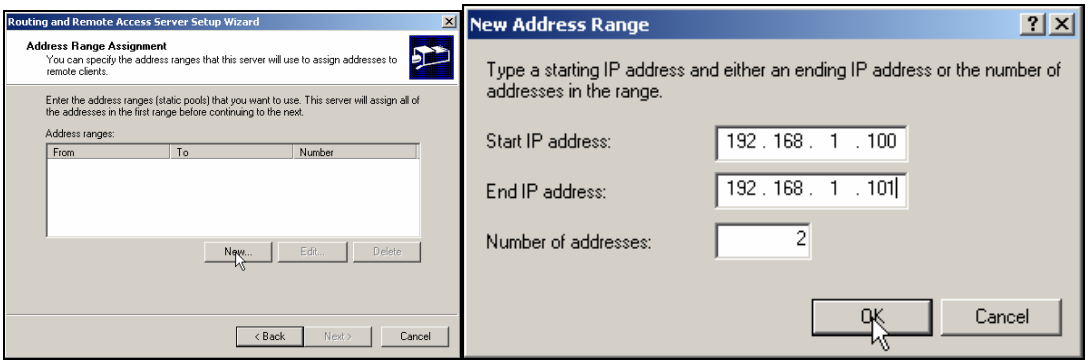


5. On the next screen, you will be asked to either select to **Automatically** assign IP addresses to your remote users or to assign their IP address **From a specified range of addresses**. Since you do not have a DHCP server setup on your network that handles IP address assignment, you will select **From a specified range of addresses** and click **Next**.

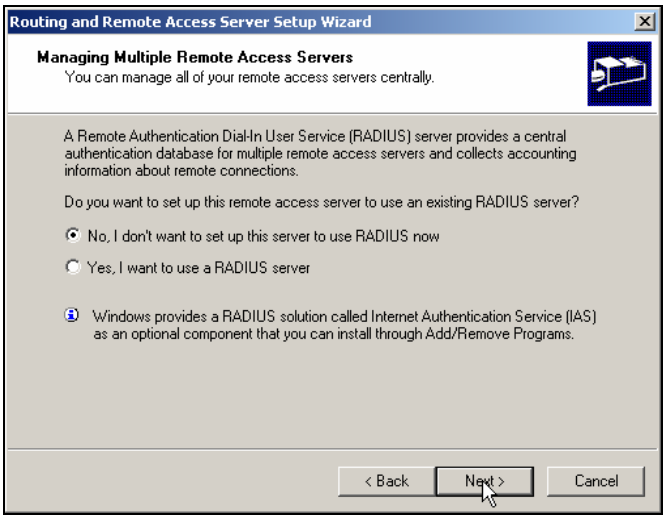


© Train Signal, Inc., 2002-2003

6. This will bring you to the Address Range Assignment screen. Click on **New** to specify the address range. For this lab, you will enter **192.168.1.100** as the Start IP address and **192.168.1.101** as the End IP address, click **OK** and **Next** to continue. This will give you a total of 2 IP addresses for your remote access client to lease. These IP addresses will be returned to this static address pool as soon as your remote access client is done with its VPN session. On a production VPN server it is very important that you specify enough addresses to handle all of your remote access clients at once **AND** that the addresses you specify are not in use anywhere else on the network.

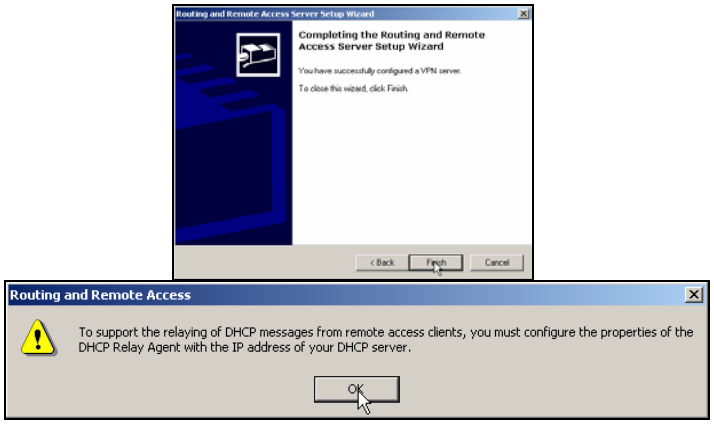


7. On the next screen, you will be asked if you want to use a RADIUS server. For this lab, just select **No, I don't want to set up this server to use RADIUS now** and click **Next**.



© Train Signal, Inc., 2002-2003

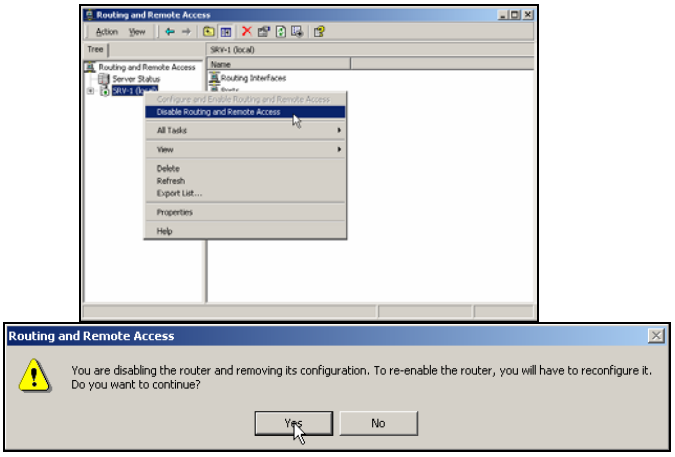
8. On the last screen of the wizard, click **Finish** and then **OK** on the DHCP Relay Agent message. This is just a reminder about setting up a DHCP Relay Agent properly, if you have a DHCP server located on a different subnet. You are now finished installing the VPN server using the wizard.



Manually configuring RRAS as a VPN server

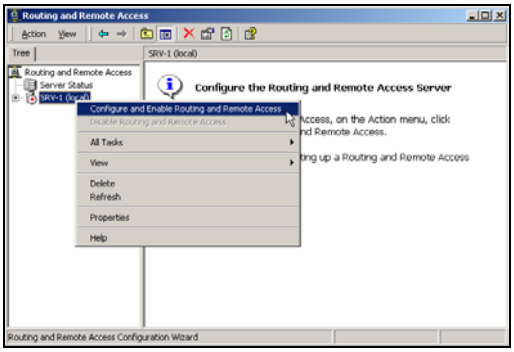
The proceeding steps showed you how to setup up a VPN server using the RRAS wizard but it is important to know how to setup the VPN server manually (without the wizard) as well. From the previous installation, you have already enabled RRAS. In order to show you the alternative way, you have to disable RRAS first. Disabling RRAS will result in all of your current settings being reset.

1. Open **RRAS**, right click **SRV-1** and click **Disable Routing and Remote Access**. Also click **Yes** to continue disabling the router and removing its configuration.

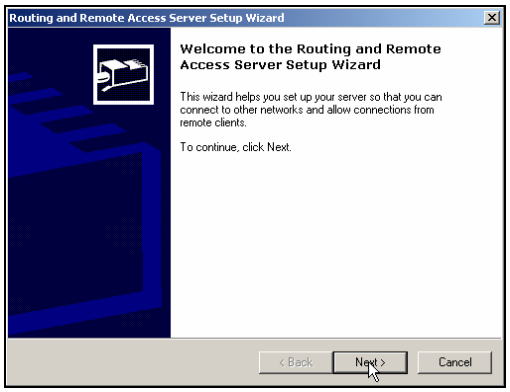


© Train Signal, Inc., 2002-2003

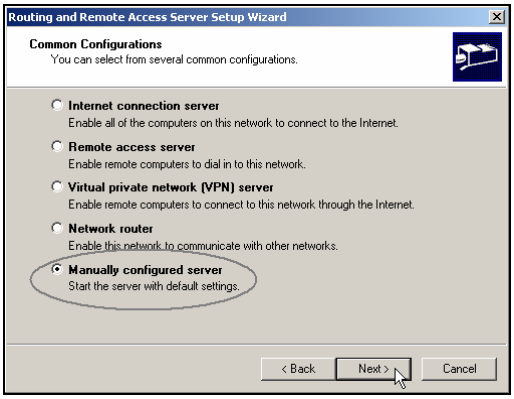
2. After you see the red down arrow, indicating that RRAS is disabled, right click **SRV-1** again and click **Configure and Enable Routing And Remote Access**.



3. This will bring up the Routing and Remote Access Server Setup Wizard, just click **Next** to continue.

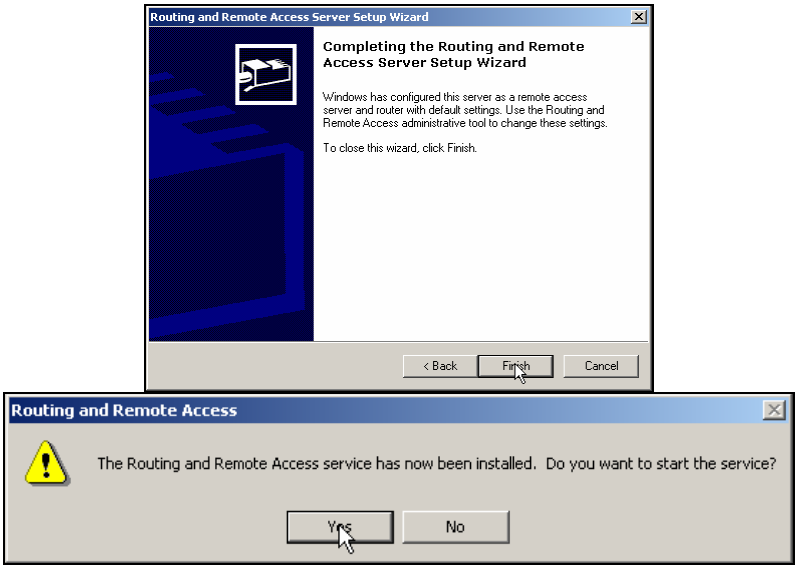


4. Again, on the Common Configurations page, there are 5 common configurations for you to choose from. This time, you will select **Manually configured server** to start the server with default settings. Just click **Next** to continue with the installation.



© Train Signal, Inc., 2002-2003

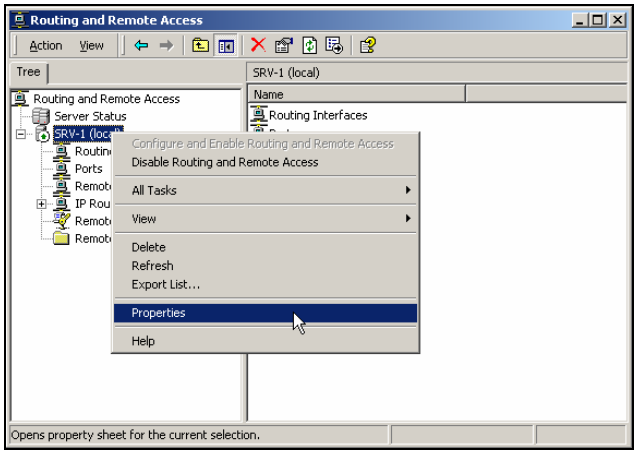
5. Click **Finish** and you will complete the installation. Also, click **Yes** to start the RRAS service. You have now enabled the Routing and Remote Access service, but you still need to configure the properties of the VPN.



Configuring the VPN properties

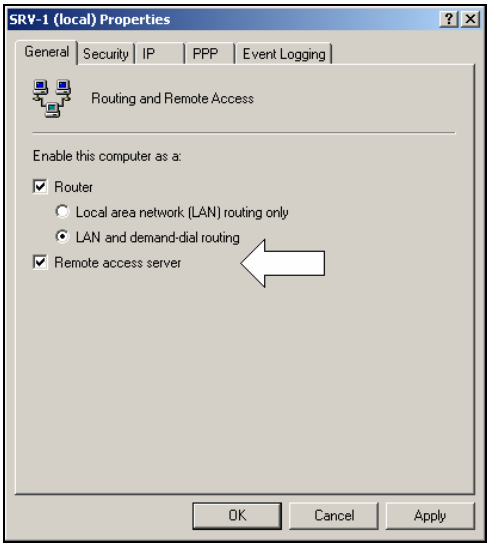
There are many different configurable properties for the VPN Server. To configure the VPN server, you will first have to open the Routing and Remote Access properties.

1. To do this just right click on **SRV-1** and select **Properties**.

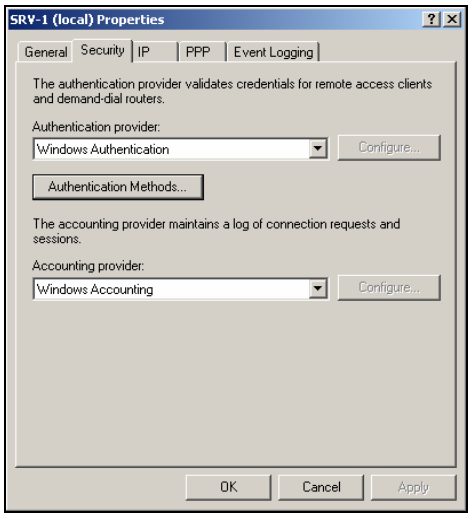


© Train Signal, Inc., 2002-2003

2. This will bring up the SRV-1 Properties dialog box, where you configure Routing and Remote Access. There are 5 tabs for you to select from (General, Security, IP, PPP and Event Logging) and many options to configure. The General tab allows you to enable the RRAS role that this computer will take on. In order for SRV-1 to act as a remote access server, you will have to make sure that the **Remote access server** option is checked. For now, leave the **Router** option checked and **LAN and demand-dial routing** selected as they are default settings. We will cover these options later in the lab.

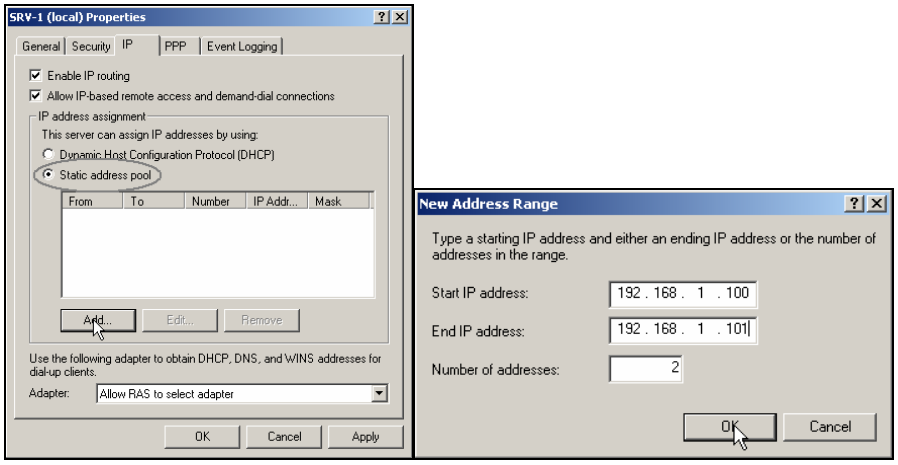


3. The next tab is the Security tab. It allows you to choose different Authentication methods for the VPN Server, which we will cover in greater detail later in this lab. This tab also allows you to select an Accounting provider, which specifies where to save log files.

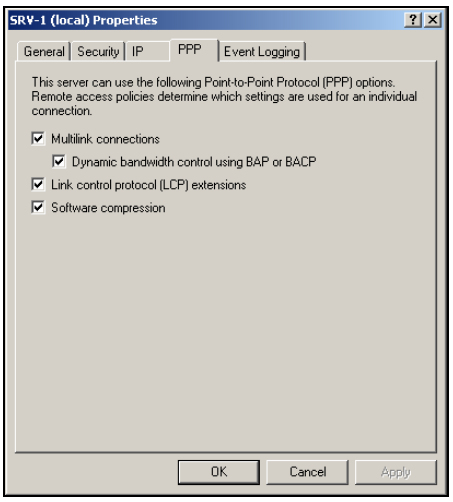


© Train Signal, Inc., 2002-2003

4. The third tab is the IP tab. This is where you can configure how IP address assignments for your clients are handled. You can either choose to automatically assign IP addresses using DHCP or you can create your own address pool. Since there is no DHCP server setup on your network, you will select **Static address pool** and click **Add** to add to your address range. In this lab you will enter **192.168.1.100** as the Start IP address and **192.168.1.101** as the End IP address and click **OK**.

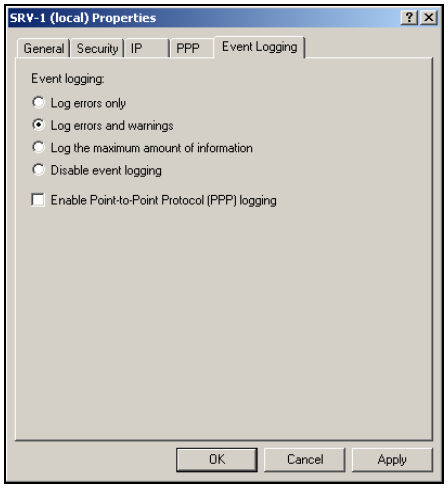


5. The fourth tab is the PPP, or Point-to-Point Protocol, tab. The PPP settings are enabled by default and can be left alone. They are not necessary for a VPN connection using a dedicated connection to the Internet (i.e. DSL, T1, etc.). So, for Green Lizard, leave these settings as they are.

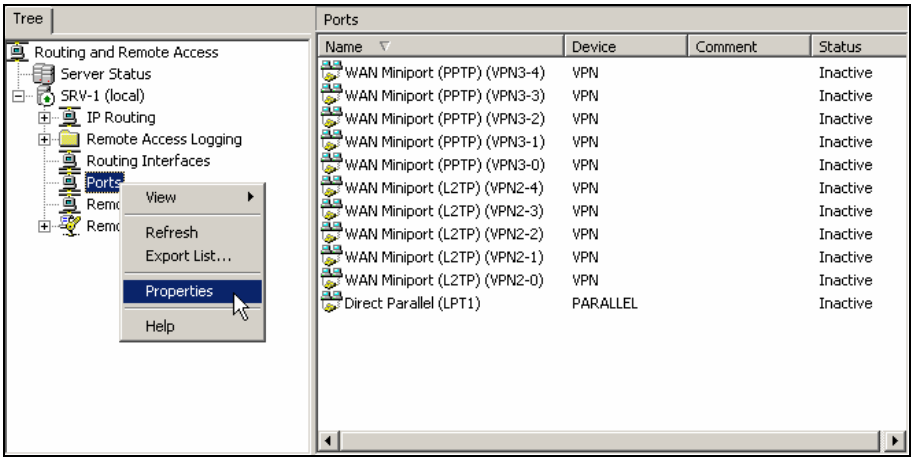


© Train Signal, Inc., 2002-2003

6. The last tab is the Event Logging tab. This tab allows you to choose different logging options. All events are logged in the system log of the event viewer. The default is set on **Log errors and warnings**.

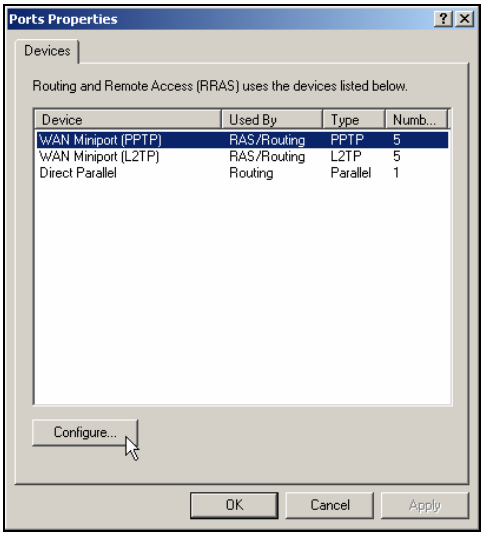


7. When you install the VPN server through the Routing and Remote Access Setup wizard 128 PPTP and 128 L2TP ports are typically created. However, when you install the VPN Server using the manual setup just 5 PPTP and 5 L2TP ports are typically created. Regardless of the number of ports created initially, you have complete control over the number of ports that are available to your remote access users. Keep in mind that each port represents one "opening" through your VPN server - so each connected user will use one port. You should set the number of ports to a number that is great enough to support all of your remote access users at any one given time while not opening up excess ports, creating a security issue. To configure the number of ports, right click **Ports** and select **Properties**.

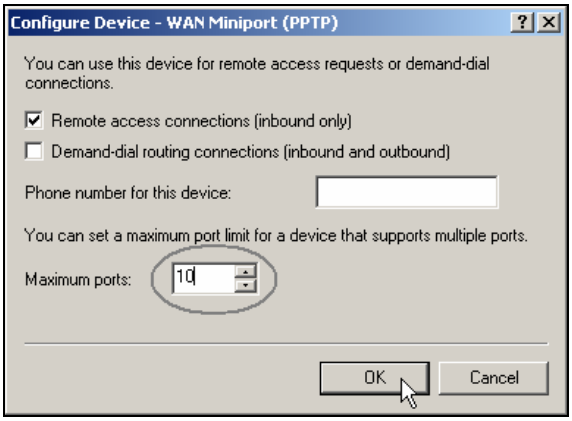


© Train Signal, Inc., 2002-2003

8. This will bring up the Ports Properties dialog box. There are 2 types of VPN ports, WAN Miniport (PPTP) and WAN Miniport (L2TP). Select **WAN Miniport (PPTP)** and click **Configure**.

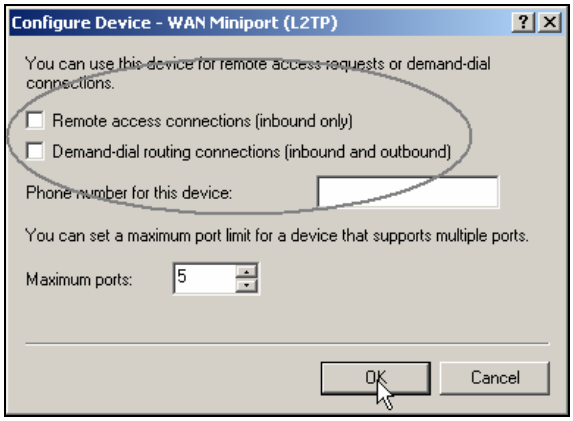


9. This will open the Configure Device – WAN Miniport (PPTP) dialog box. From here, you can specify the function of the PPTP ports and the number of virtual ports to create. Enter **10** as the maximum number of PPTP ports and verify that the Remote access (inbound) is selected for inbound connections. This will enable remote access through PPTP ports. Since this is not a modem port, just leave the phone number field blank and click **OK**.

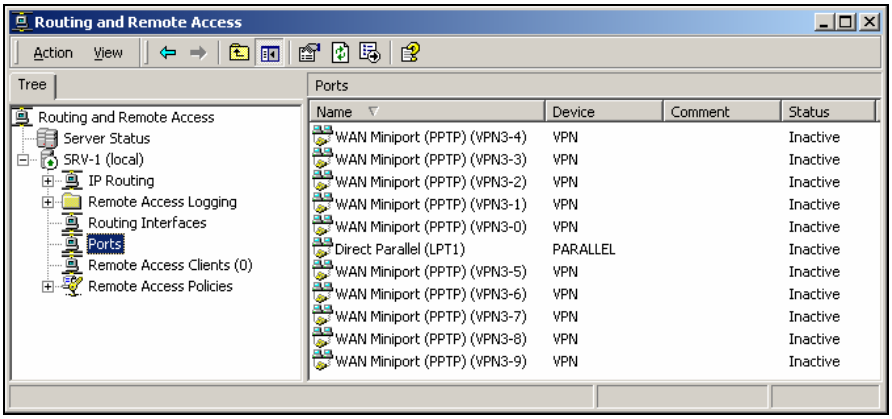


© Train Signal, Inc., 2002-2003

10. Select **WAN Miniport (L2TP)** in the Ports Properties dialog box and click **Configure**. This time you will disable all of the L2TP ports. Uncheck **Remote access connections (inbound only)** and uncheck the **Demand-dial routing connections (inbound and outbound)**. Click **OK** and then click **OK** on the Ports Properties dialog box to complete the configuration.



11. As you can see from the right pane of the RRAS console, you now have 10 PPTP ports and no L2TP ports available for your VPN clients.

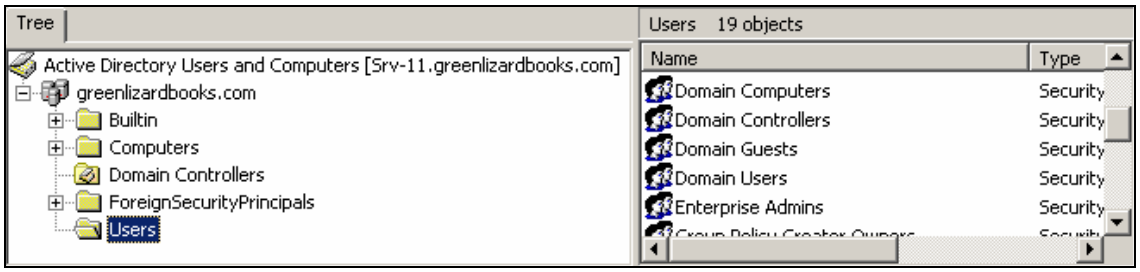


© Train Signal, Inc., 2002-2003

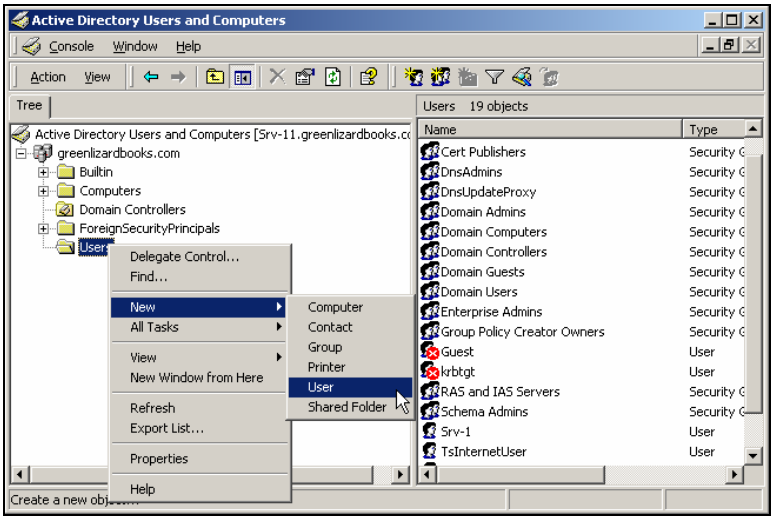
Setting up a VPN client on Client-1

To setup a VPN client on Client-1, you will have to create a user account within your domain. You will create a user account named *John Stacey* for your remote access user account.

1. Log on to **SRV-11** and open the Active Directory Users and Computers console by going to **Start→Programs→Administrative Tools→Active Directory Users and Computers**. In the left pane of the console, open the container named **Users**.

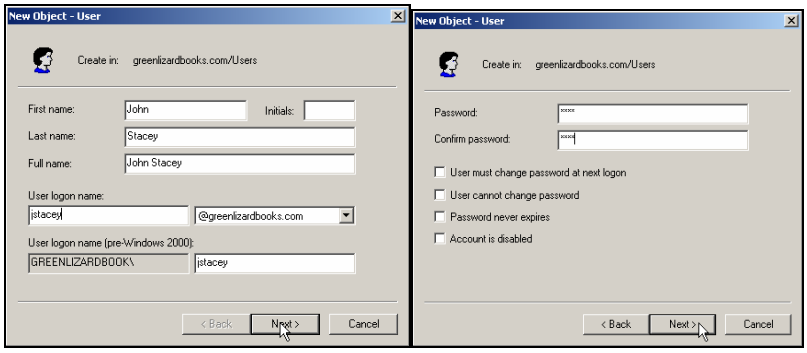


2. To create a user account, right click on the **Users** container in the left pane and select **New→User**.

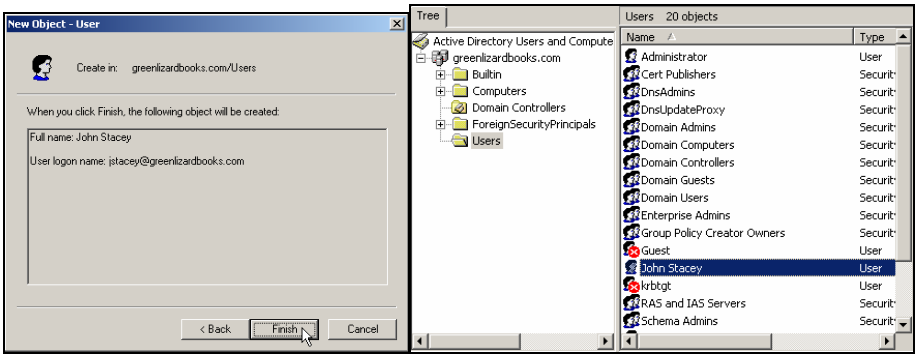


© Train Signal, Inc., 2002-2003

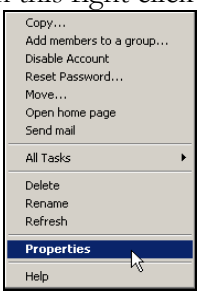
3. This will bring up a wizard for creating a new user. On the first screen, type in the first and last name for the user (***John Stacey***) and, for the logon name, type in the first initial of the first name and the full last name (***jstacey***) and click **Next**. On the next screen you must enter a password for this new user account. Type in **mega** as the password and click **Next**.



4. The final screen is just a summary of all the information that you entered in the wizard. Confirm that the information is correct and click **Finish**. Now, within the Active Directory Users and Computers console, you should see a user account named *John Stacey* located in the Users container.

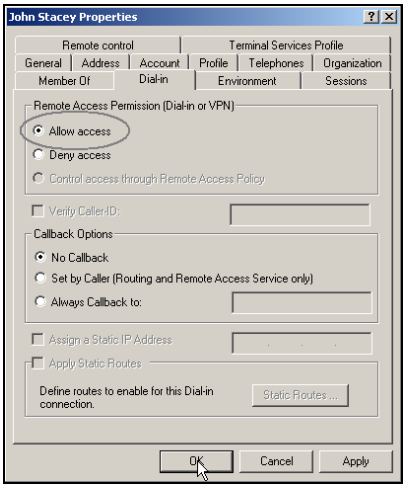


5. In order for *John Stacey* to gain remote access to the network, he must be given remote access permissions. To accomplish this right click on *John Stacey* and select **Properties**.



© Train Signal, Inc., 2002-2003

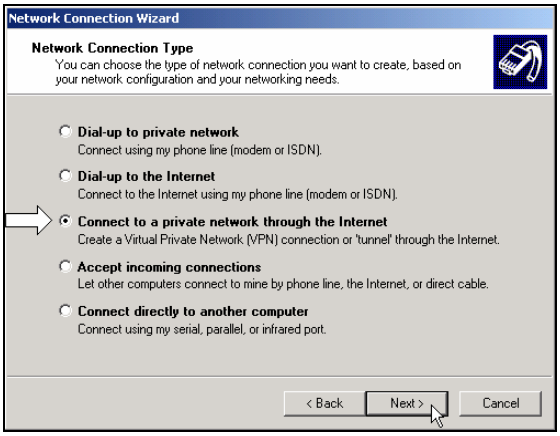
6. This will bring you to the John Stacey Properties dialog box. There are 3 different options you can set for Remote Access Permission: Allow access, Deny access, and Control access through Remote Access Policy. Notice that the last option is grayed out at the moment. This is because your domain is currently in mixed mode, which we will cover later in the next lab. For now, select the **Dial-in** tab and select **Allow access** under Remote Access Permission (Dial-in or VPN). This will give John the remote access permission necessary for either a dial-up or VPN connection. Click **OK** when you are done with this configuration.



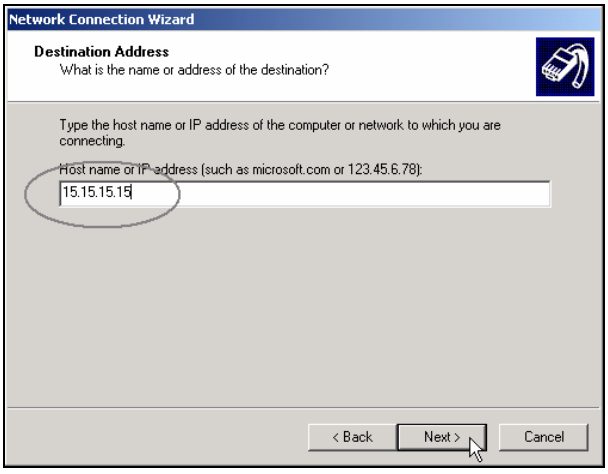
7. Next, to setup a VPN client, log on to **Client-1** and go to **Start→Settings→Network and Dial-up Connections** and click on **Make New Connection**. This will bring up the Network Connection Wizard. Click **Next** to continue.

© Train Signal, Inc., 2002-2003

8. On the Network Connection Type page, there are 5 network connection types for you to choose from, including setting up your computer as a VPN client. You can set up your computer to dial-up to a LAN, to the Internet, to accept incoming connections, or to connect directly to another computer. For now, select **Connect to a private network through the Internet** and click **Next** to continue.

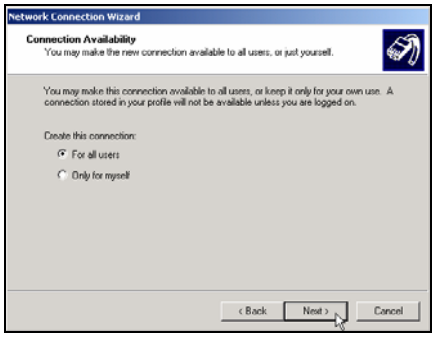


9. The next screen of the wizard will ask you to enter the Destination Address. This is the public IP address of your VPN server. For this lab, the destination IP address will be **15.15.15.15**. Click **Next** to continue.



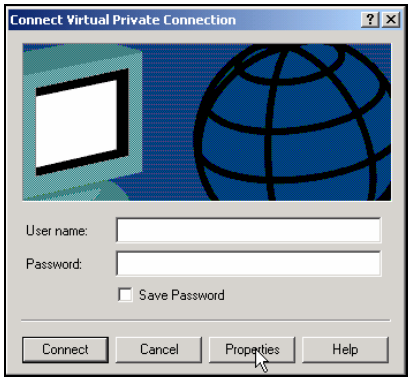
© Train Signal, Inc., 2002-2003

10. This will bring you to the Connection Availability screen. On this screen, you have the choice to setup this new connection so that it is available to all users of Client-1 or just yourself. In this lab, you will set it up for all users of Client-1. Select **For all users** and click **Next** to continue.



11. On the last screen of the wizard, you can give your VPN connection any name that you like. The default name is Virtual Private Connection. Click **Finish** and your VPN client setup is complete.

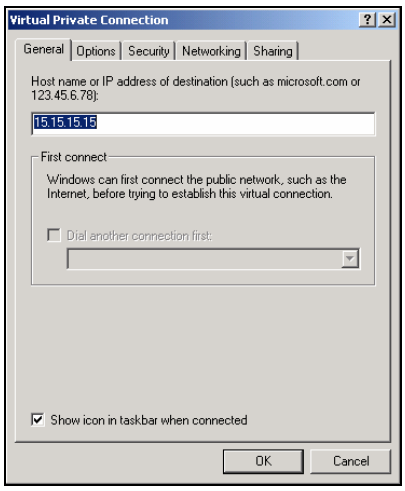
12. Once you are done setting up your VPN client, you will immediately get the Connect Virtual Private Connection dialog box. This is where you will initiate your VPN connection. Before you connect to your LAN, click on the **Properties** button to see what settings are configurable for the VPN client.



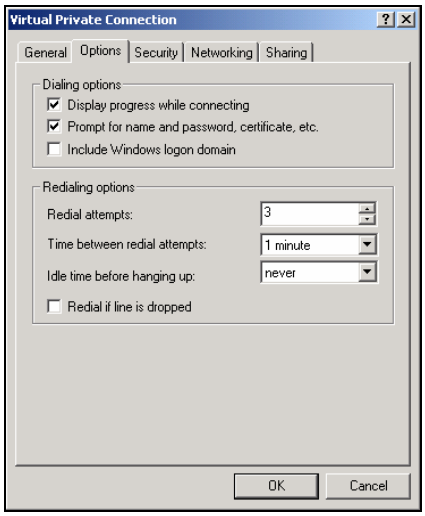
© Train Signal, Inc., 2002-2003

Configuring the VPN client properties

1. Clicking the **Properties** button brings up the Virtual Private Connection dialog box. There are 5 tabs (General, Options, Security, Networking and Sharing) for you to select and many options to configure. The General tab is where you specify the public IP address of the remote VPN server that you want to connect to. The First connect option allows you to specify a dial-up connection to automatically connect to before you attempt to access the VPN Server. This would be your normal connection to the Internet, typically a dial-up connection.

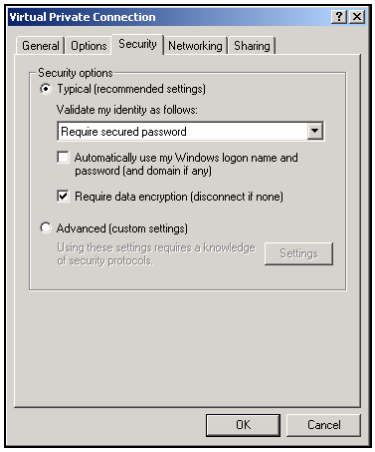


2. The next tab is the Options tab. Most of these settings are self-explanatory and, by default, none of these settings have to be changed in order to connect to the VPN Server

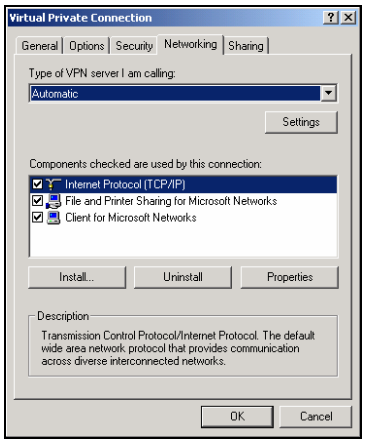


© Train Signal, Inc., 2002-2003

3. The third tab is the Security tab, which allows you to fine tune the security for your VPN connection. You can choose either Typical or Advanced. Typical, the default, only allows you to control basic options. In this case you have the ability to disable encryption over the VPN connection and choose whether or not to automatically log you in to the VPN Server. The Advanced option allows you to choose exactly which remote authentication protocols you want to allow, including the use of smart cards. We will take a closer look at remote authentication protocols later in this lab.

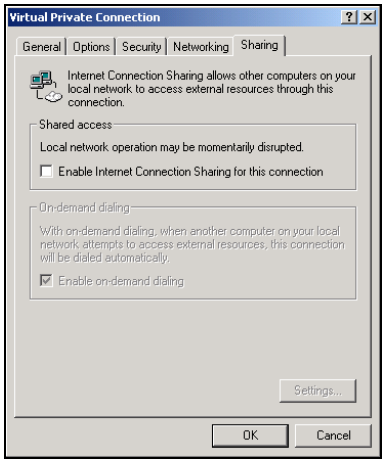


4. The forth tab is the Networking tab. It allows you to select which VPN protocol (L2TP or PPTP) you want to use for the connection. The default setting is set to Automatic. The automatic setting will have your computer attempt to use L2TP first and then use PPTP if L2TP is not available on the VPN Server. You can also install or uninstall any network components that you want to use for this connection. The default components are typically left in place, as they allow for "normal" usage of the Windows 2000 network that the VPN client is connected to. You can configure these components individually by highlighting them and clicking on **Properties**.



© Train Signal, Inc., 2002-2003

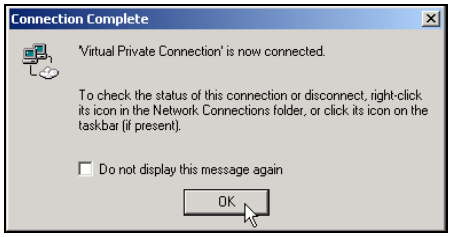
5. The last tab is the Sharing tab. It allows you to enable Internet Connection Sharing (ICS) for the VPN connection. If, for example, you have other computers on Client-1's LAN, enabling ICS will allow these computers to access external resources through the VPN connection as well. For security reasons, enabling this setting on a VPN client that connects to a corporate network is not a good idea. Leave ICS disabled (unchecked) and click **OK** to close the Virtual Private Connection dialog box.



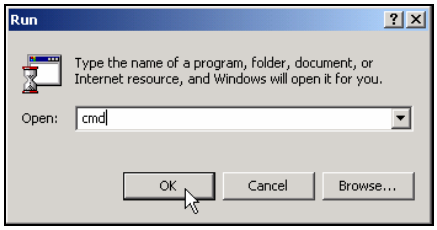
6. Alright, now let's attempt to access the VPN server. Type in ***jstacey*** as the user name and ***mega*** as the password. Remember, this is the new user you added to the Users container in Active Directory Users and Computers in SRV-11 earlier. Click **Connect** to establish the VPN connection.

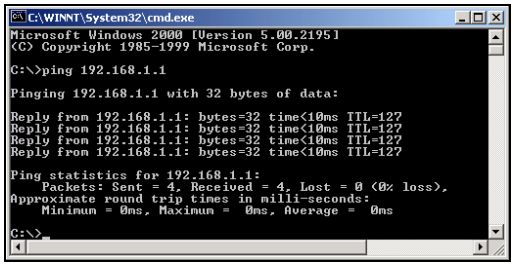
© Train Signal, Inc., 2002-2003

7. The first time you establish a Virtual Private Connection, you will get this Connection Complete dialog box. You can either check or uncheck **the Do not display this message again** box. Just click **OK** to close the dialog box.

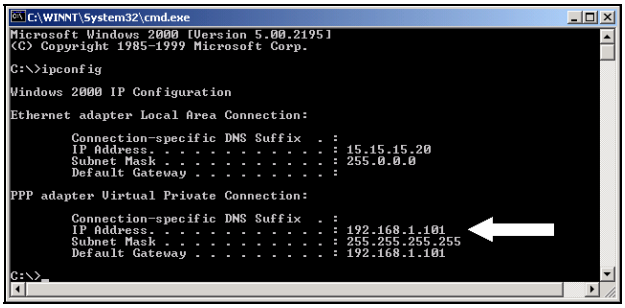


8. In order to test access to your internal network, you can use the ping utility to ping SRV-11. Go to **Start→Run**, type in **cmd** and click **OK** to open the command prompt. Within the command prompt, type in **ping 192.168.1.1,** which is the domain controller on your network, and press **Enter**. If you receive four replies from 192.168.1.1, then you are able to communicate with SRV-11 through your VPN server.





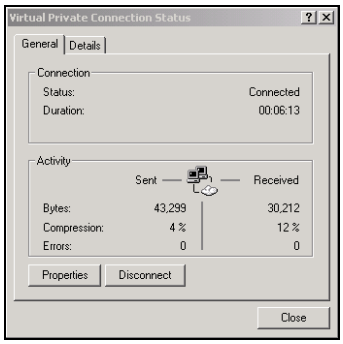
9. To check Client-1's virtual address information, type in **ipconfig** and press **Enter** at the command prompt. The IPCONFIG utility gives you some basic output about the IP configuration of the network interface on Client-1. Client-1's virtual address should be an IP address from the range of 192.168.1.100 to 192.168.1.101. This IP address is randomly selected from the IP address range that you setup earlier in the static address pool on your VPN server. Therefore, you should have either 192.168.1.100 or 192.168.1.101 as your virtual IP address. After verifying this configuration, type in **exit** and press **Enter** to close the command prompt.



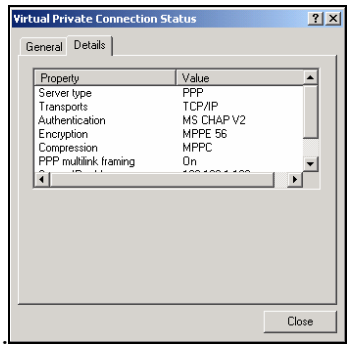
© Train Signal, Inc., 2002-2003

10. Also, click on the **2 computers icon** in the lower right corner of your taskbar that indicates that your Virtual Private Connection is active.

11. Double clicking this **icon** will bring up the Virtual Private Connection Status dialog box. There are 2 tabs (General and Details) for you to select. The General tab provides you with connection status and activity information. You can also click on the **disconnect button** to disconnect the VPN session or on the Properties button to configure your VPN client, which is the Virtual Private Connection dialog box that you were in earlier.



12. The Details tab provides information on how you have connected your VPN session, including which authentication and encryption methods the VPN connection is using. As you see, PPP is the remote access protocol being used to establish this connection. The LAN protocol is TCP/IP and MS-CHAP V2 was used to authenticate the remote access client. Further down, you should also see that 56-bit Microsoft Point-to-Point Encryption (MPPE) is being used for data encryption and that Microsoft Point-to-Point Compression (MPPC) is the compression method. If you scroll down further, you will see the server and client IP addresses that are used during this VPN session. Click on the **Close** button after you have verified this information.



© Train Signal, Inc., 2002-2003

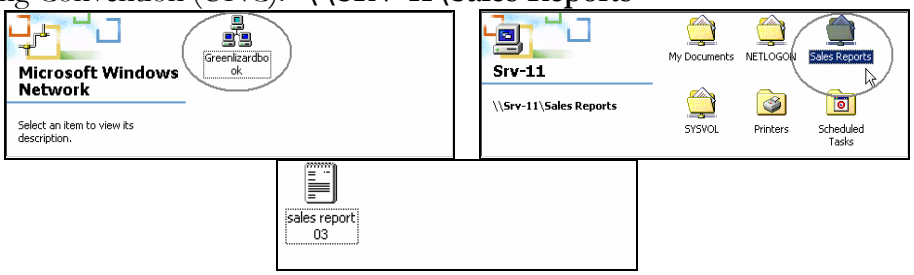
Join Client-1 to the Greenlizard.com Domain

Joining Client-1 to the domain is not a technical requirement of setting up a VPN, but it better simulates a company environment. Joining a computer to a domain will provide centralized authentication, policy and security. In a real world situation, your computer (the user's computer) most likely would have been joined to the domain when it was first deployed to the end user and not after the user has taken the computer home and formed a VPN connection.

1. To join Client-1 to the domain, simply right click the **"My Computer"** icon on the desktop and select **Properties**. From here, select the **Network identification tab**, select **Properties**, select **Domain** and then type in the domain name of the domain Client-1 will join. You can use the DNS Host name, greenlizardbooks.com, or the NetBIOS name, greenlizardbook. Remember, NetBIOS names are a single label (no periods) and can be up to 15 characters in length. Click **OK** after entering the domain name. You will then be asked for a username and password. Use **jstacey** as the account name and **mega** as the password from the greenlizardbooks.com domain. When the computer account has been successfully joined to the domain, it will "welcome you to the domain" and you should then **restart the computer.**
2. After restarting the computer log back on to **Client-1**. Next, go to **Start → Settings → Network and Dial-up Connections** and double click on the **Virtual Private Connection**. Just type in **jstacey** as the user name, **mega** as the password and click **Connect** to establish the VPN connection again.

Accessing the share through the VPN server

1. Next, see if you can access the sales report file that you shared on the network from SRV-11 earlier. Browse the network for this resource by double clicking on **My Network Places,** clicking on **Entire Network,** clicking on **entire contents** and then on **Microsoft Windows Network.** From here, double click on the **Greenlizardbooks domain,** double click **SRV-11** and double click the **Sales Reports** folder. This final double click should reveal the sales report 03 file that you created earlier. You can also access this shared folder by going to **Start→Run** and then entering the Universal Naming Convention (UNC): **\\SRV-11\Sales Reports**

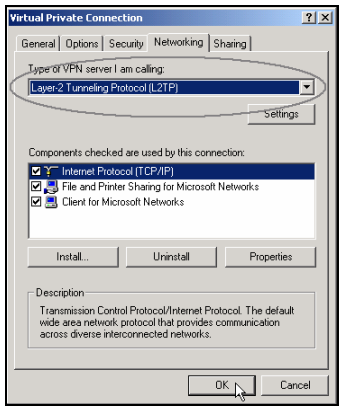


© Train Signal, Inc., 2002-2003

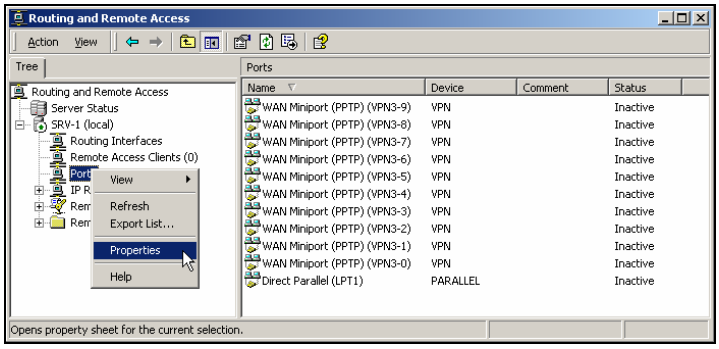
Troubleshooting tunneling protocols between SRV-1 and Client-1

In this section you will examine the interaction between a L2TP client session and your current VPN server, which is setup to serve PPTP VPN clients.

1. First, to form a L2TP session, you will have to disconnect your current VPN session and configure your VPN client properties. To do this click on the **Disconnect** button in the General tab. Next, go to **Start→Settings→ Network and Dial-up Connections**, click on **Virtual Private Connection**. This will bring you to the Connect Virtual Private Connection dialog box again, click on the **Properties** button and select the **Networking** tab. Click on the **down arrow** and select **Layer 2 Tunneling Protocol (L2TP)** as the type of VPN server you are connecting to. Click **OK** to complete this configuration.

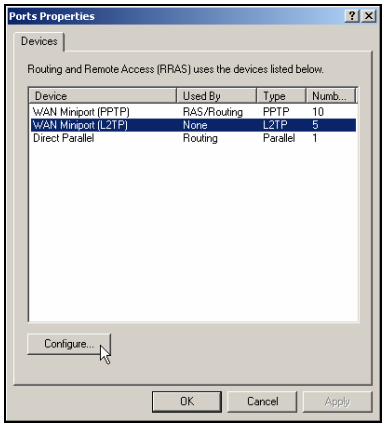


2. Next, in order to support L2TP on the VPN Server, you will have to increase the number of available L2TP ports (they are currently disabled) on SRV-1. Log on to **SRV-1**, go to **Start→Programs→Administrative Tools** and click on **Routing and Remote Access**. Right click **Ports** and select **Properties**.

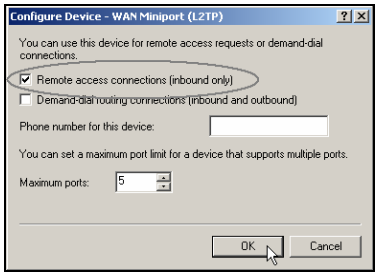


© Train Signal, Inc., 2002-2003

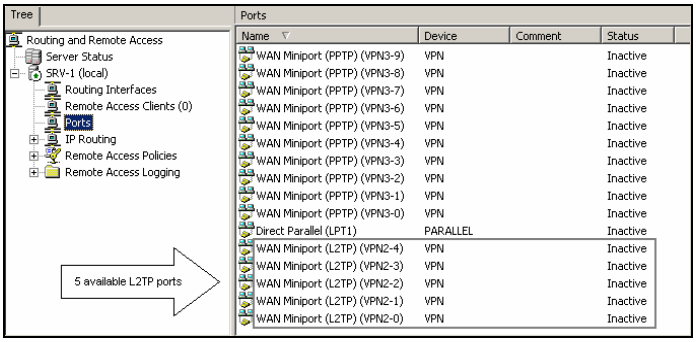
3. This will bring up the Ports Properties dialog box. Again, there are 2 types of VPN ports, WAN Miniport (PPTP) and WAN Miniport (L2TP). Select **WAN Miniport (L2TP)** and click **Configure**.



4. Within the Configure Device – WAN Miniport (L2TP) dialog box, you can specify the function of the L2TP ports and the number of virtual ports available. Leave the maximum L2TP ports as is and check the **Remote access connections (inbound only)**. This will enable remote access through the L2TP ports. Leave the Demand dial-routing connections (inbound and outbound) unchecked and the phone number field blank. Click **OK**.



5. After you click **OK** you should see that, along with the 10 available PPTP ports, you also have 5 L2TP ports currently available for your VPN clients.



© Train Signal, Inc., 2002-2003

6. You are now ready to attempt to establish your VPN session using L2TP on Client-1. Type in ***jstacey*** as the user name and ***mega*** as the password in the Connect Virtual Private Connection dialog box. Click **Connect** to establish the VPN connection. Almost immediately, you should get an error message. This error message indicates that there is no valid machine certificate found on Client-1. Your VPN client will not be able to connect to the VPN server using L2TP until a machine certificate is installed. Certificate services and L2TP connections will be explored in more depth in the next lab. For now, your VPN clients will only be able to use PPTP to establish VPN sessions. Click **Cancel** on the error message and go back to the **Networking** tab in the Virtual Private Connection dialog box. Change the type of VPN server that you are calling back to **Automatic**. This setting allows your VPN client to negotiate the most secure protocol, L2TP, first. Since the VPN server currently doesn't support L2TP, it will use PPTP instead.

Remote Authentication Protocols

Remote access servers use authentication to identify a user who wants to remotely access the LAN. Routing and Remote Access offers many standard authentication protocols to perform this authentication. These include Password Authentication Protocol (PAP), Shiva Password Authentication Protocol (SPAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), and MS-CHAP v2. MS-CHAP and MS-CHAP v2 are the default authentication protocols enabled within Windows 2000. RRAS also allows the use of Extensible Authentication Protocols (EAP), which are used with smart cards and to allow you to load additional third-party protocols. A closer look at each of these Remote Authentication Protocols follows:

Password Authentication Protocol (PAP) - This is the least secure authentication protocol of all. It sends clear-text passwords and provides very little protection against unauthorized access.

Shiva Password Authentication Protocol (SPAP) - This protocol is a 2-way reversible encryption authentication protocol. It encrypts password data sent between the remote client and the server. Regardless of this encryption, this protocol is still not a secure protocol.

© Train Signal, Inc., 2002-2003

Challenge Handshake Authentication Protocol (CHAP) - This protocol allows clients running non-Microsoft operating systems to communicate with a Windows 2000 server using encryption. It uses the Message Digest 5 (MD5) one-way encryption scheme to encrypt the response. It provides a medium level of protection against unauthorized access.

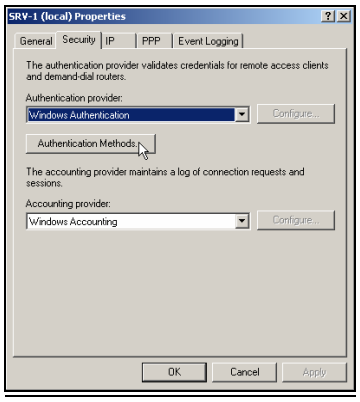
Microsoft CHAP (MS-CHAP) - This protocol is enabled by default on RRAS Servers and Window 2000 remote access clients. It allows clients running NT version 4.0 and later, or Windows 95 and later, to communicate with a Windows 2000 server using Microsoft Point-to-Point Encryption (MPPE). It is also only offers one-way authentication.

MS-CHAP v2 – This protocol is the most secure of all the standard protocols. It is enabled by default on RRAS servers and Windows 2000 remote access clients. It provides mutual authentication, stronger data encryption keys, and uses different encryption keys for sending and receiving. It can be configured on dial-up clients running Windows 2000. It can also be configured on VPN clients running Windows 2000, Windows NT 4.0 or Windows 98.

Troubleshooting Remote Authentication Protocol settings on SRV-1 and Client-1

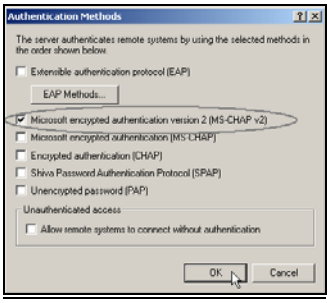
In this section you will examine the interaction between a VPN server and Client-1 when using different Remote Authentication Protocols on each of them.

1. To demonstrate these settings, you have to first log on to **SRV-1**. From there, go to **Start → Programs → Administrative Tools → Routing and Remote Access** and open SRV-1 Properties. Right click on **SRV-1** and click on **Properties**. Select the **Security** tab and click on the **Authentication Methods** button.

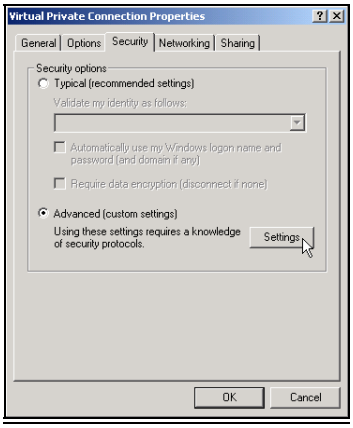


© Train Signal, Inc., 2002-2003

2. Clicking on the **Authentication Methods** button will bring up the Authentication Methods dialog box. From here, you can enable and disable the standard authentication protocols used on your VPN server. Only those protocols that are checked will be allowed for client authentication. Microsoft encrypted authentication version 2 (MS-CHAP v2) and Microsoft encrypted authentication (MS-CHAP) are enabled by default. In order to test these settings, un-check **MS-CHAP** and leave MS-CHAP v2 checked, as the only authentication protocol your VPN server will accept. Click **OK** and **OK** again on the Security tab to complete the configuration.

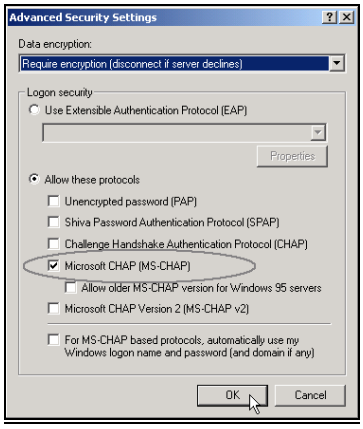


3. Next, log on to **Client-1**, go to **Start→Settings→Network and Dial-up Connections**, and click on the **Virtual Private Connection**. This will bring you to the **Connect Virtual Private Connection** dialog box**,** click on the **Properties** button and select the **Security** tab. Select **Advanced (custom settings)** and click on the **Settings** button.



© Train Signal, Inc., 2002-2003

4. This will bring up the Advanced Security Settings dialog box. From here you can configure Client-1's VPN security settings. Just like the VPN server, Microsoft encrypted authentication version 2 (MS-CHAP v2) and Microsoft encrypted authentication (MS-CHAP) are enabled by default. Un-check **MS-CHAP v2** and leave MS-CHAP checked, as the only authentication protocol that Client-1 will use for authentication. Click **OK** and **OK** again on the Security tab to complete the configuration.



5. You can now test the interaction between SRV-1 and Client-1 using different authentication protocols. From Client-1, type in ***jstacey*** as the user name, ***mega*** as the password and click **Connect** to try to establish a VPN session. You should immediately get an error message. This error message indicates that SRV-1 refused the connection based on a non-matching authentication protocol. In order to establish a VPN session successfully, you will have to enable MS-CHAP v2 on Client-1 and reconnect to the VPN server.

© Train Signal, Inc., 2002-2003

© Train Signal, Inc., 2002-2003

Lab 2

Configuring a Virtual Private Network for Green Lizard Books, Inc. using the Layer Two Tunneling Protocol (L2TP)

You will learn how to:

- Install Certificate Services
- Install machine certificates on a VPN server and client
- Configure a VPN server to accept L2TP connections
- Establish a VPN session using L2TP
- Monitor security on the link using ipsecmon

© Train Signal, Inc., 2002-2003

Scenario

The VPN you setup for Green Lizard has been working fantastically. There have been no complaints from anybody and the users are impressed with the reliability and speed that their new solution offers them. Bill, the owner of Green Lizard, is even happier. His long distance phone bill charges have been cut drastically, and he has already recouped the investment he made in the new solution. The reason that you approach Bill today is to talk about security. Bill has been burnt once before for his lack of concern over the issue, so he is all ears. You spare him the technical details, but inform him that you have been doing some research on Microsoft's VPN offerings, and that you think that Green Lizard would be more secure if they used a different type of VPN. You ensure him that although current VPN connections are encrypted and secure with Point-to-Point Tunneling Protocol (PPTP), you are able to increase security even further for little to no additional cost. Your plan is to switch Green Lizard's current PPTP VPN setup to a solution that supports L2TP exclusively. L2TP is a joint venture that takes the best features of Microsoft's PPTP and combines them with Cisco's Layer Two Forwarding (L2F) to produce a more functional, secure and standardized protocol. The major differences between the two protocols are listed below:

	PPTP	L2TP
Supported Operating Systems	Windows 9x, NT 4.0, ME, Windows 2000, Windows XP, Windows 2003, UNIX	Windows 2000, XP/2003 and NT4/98/ME (with the L2TP/IPSec VPN client installed)
NAT Compatibility	Windows 2000 PPTP – Yes Windows 2003 PPTP – Yes	Windows 2000 L2TP VPNS – No Windows 2003 L2TP VPNS - Yes
User Authentication	Point-to-Point-Protocol (PPP)	Point-to-Point-Protocol (PPP)
Encryption	MS Point-to-Point (MPPE)	IPSec
Certificate Services	Not Necessary	Required

© Train Signal, Inc., 2002-2003

In this lab, you will modify your PPTP VPN server so that it will only support the more secure L2TP. In order for L2TP to work, you will need to install certificate services and then manually install machine certificates on both your VPN server and client. After the setup is complete, you will modify the VPN server to accept L2TP connections as well as make the necessary changes to the VPN client.

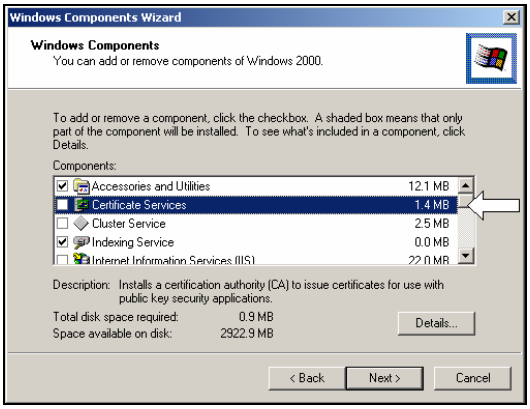
Certificate Services

Certificate Services allow information to be exchanged securely both on the Internet and within private networks through the use of PKI (Public Key Infrastructure) technology. PKI uses a pair of keys, a public encryption key and a private encryption key, to verify the identity of systems. A private encryption key always stays protected on the local client or server. The public encryption key, on the other hand, is distributed freely so others can engage in encrypted communication with the local machine. Certificate Servers, also known as Certificate Authorities (CAs), distribute keys by issuing certificates which contain the public key to the requesting clients.

Installing Certificate Services

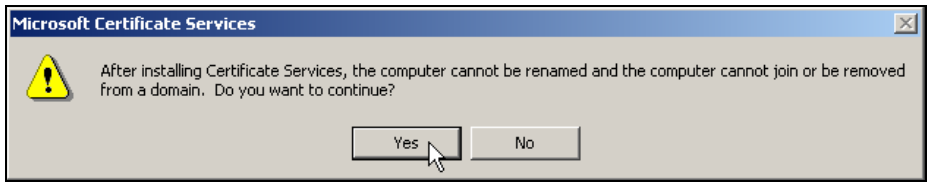
In order for L2TP VPN sessions to work properly, you will have to install machine certificates on both your VPN server and client. These will be obtained from a local Certificate Server on Green Lizard's network.

1. Log on to SRV-11 and go to **Start→Settings→Control Panel**. Double click on the **Add/Remove Programs** icon and click on **Add/Remove Windows Components** on the left column. This will bring up the Windows Components Wizard. Place a check mark in the box next to **Certificate Services** and click **Next** to continue.

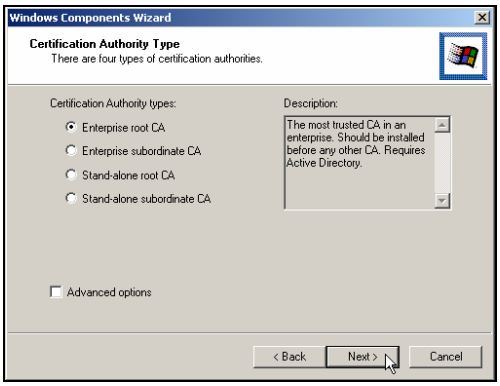


© Train Signal, Inc., 2002-2003

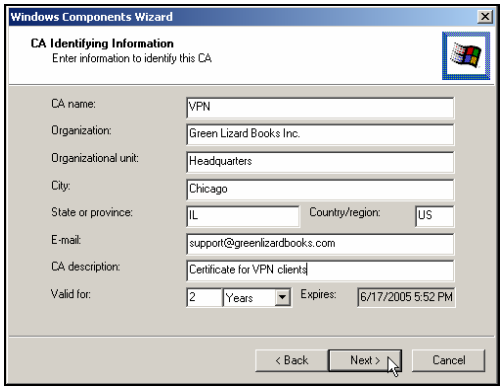
2. You will receive a message warning you that the server cannot be renamed or its domain membership has changed after the Certificate Services installation. Just click **Yes** to continue.



3. The next screen will give you 4 different Certification Authority types (Enterprise root CA, Enterprise subordinate CA, Stand-alone root CA and Stand-alone subordinate CA) to choose from. Certificates will only be distributed to users and computers within Green Lizard, so you will select **Enterprise root CA** and click **Next** to continue.

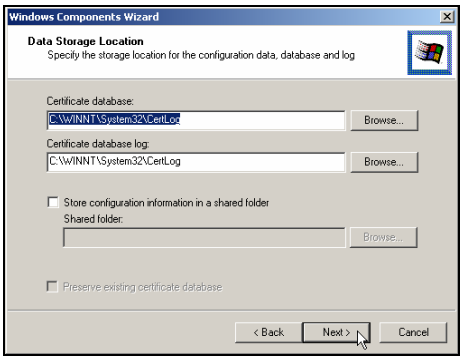


4. This will bring you to the CA Identifying Information screen. Fill this form out with all of the required information - don't worry about completeness or accuracy of information for this lab. Click Next to continue.

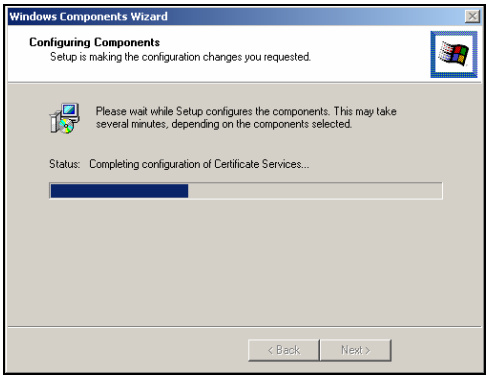


© Train Signal, Inc., 2002-2003

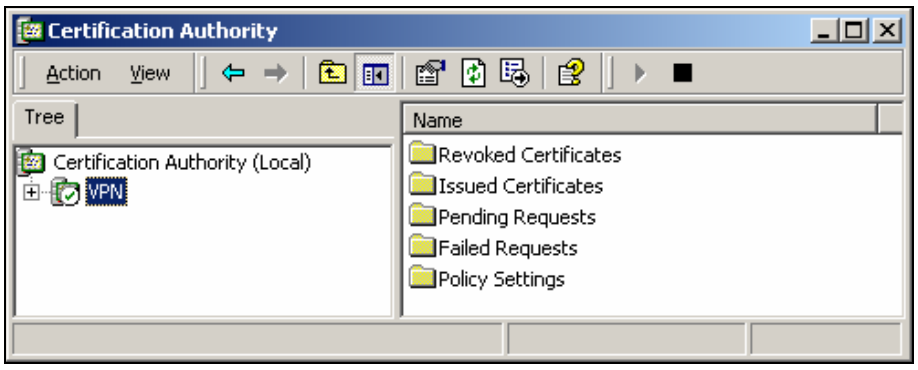
5. On the Data Storage Location screen, just confirm the certificate database location and click **Next**.



6. The installation takes about 5-10 minutes. You will eventually get a screen letting you know that the installation is done. Click on **Finish** to complete the installation.



7. To open Certificate Services, just go to **Start→Programs→Administrative Tools→Certification Authority**. As you can see, VPN, the Enterprise root CA that you named in the last step, is ready to issue certificates. **Reboot** SRV-11 once you have verified the installation of Certificate Services.



© Train Signal, Inc., 2002-2003

Installing machine certificates on both of your VPN server and client

There are several methods of installing certificates onto computers, including: automatic deployment, manual certificate deployment and Internet based deployment. For the purposes of this lab, you will install certificates manually.

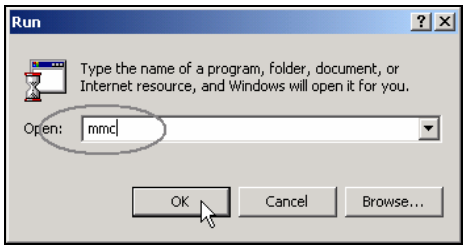
1. Before you can install a machine certificate on Client-1, you will have to connect Client-1 directly to Green Lizard's private LAN. To accomplish this, just **plug Client-1's network cable into the private LAN hub/switch**, and change its static IP address from 15.15.15.20 with 255.0.0.0 subnet mask to **192.168.1.2** with **255.255.255.0** subnet mask. Also, configure the preferred DNS server setting to point to **SRV-11, 192.168.1.1** and leave the alternate DNS setting blank. The default gateway should also now change to point to the private side of SRV-1, 192.168.1.201. You are now ready to install a certificate on Client-1.

*****Important Note*****

Reassigning Client-1's IP address is only temporary, in order to install the certificate without any problems. At the end of this procedure, Client-1's IP address will be re-assigned the IP address information it used originally.

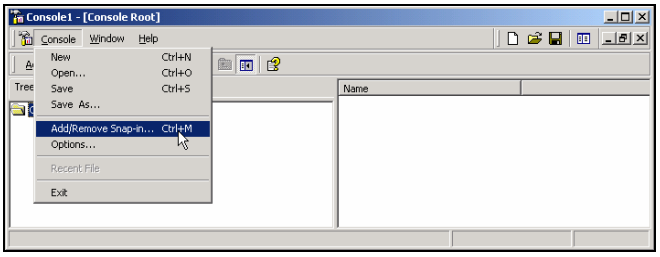
Client Certificate Installation

1. Log on to **Client-1** as the administrator, go to **Start→Run,** type in **mmc** and click **OK** to open the Microsoft Management Console (MMC).

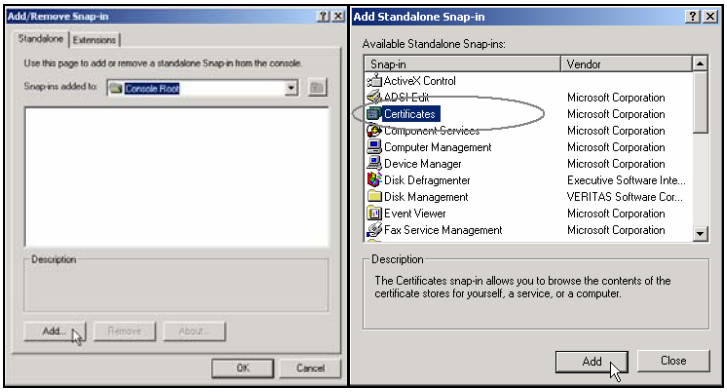


© Train Signal, Inc., 2002-2003

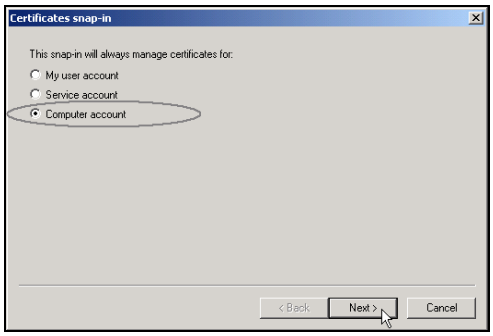
2. This will bring you to the Console 1 window. Select **Console→Add/Remove Snap-in** from the menu.



3. In this Add/Remove Snap-in screen, just click **Add** and you will see there are many Snap-ins available for you to add. Select **Certificates** to be the Standalone Snap-in and click **Add** to continue.

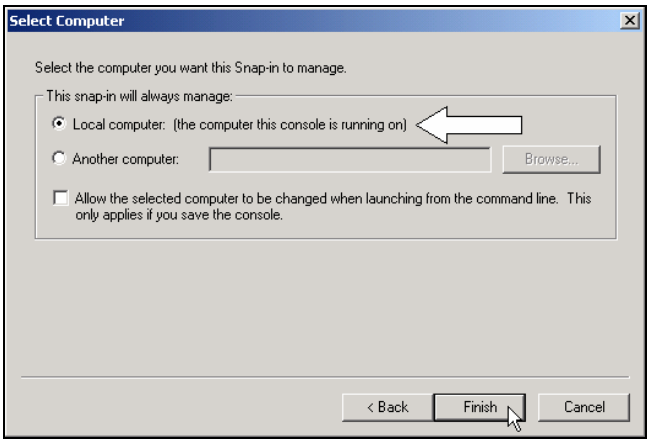


4. This will bring you to the Certificates snap-in dialog box. From here you can control what type of certificates will be managed within the Certificates snap-in. Since you will be installing a machine certificate on Client-1, you will want this snap-in to manage certificates for computer accounts. Therefore, just select **Computer account** and click **Next**.

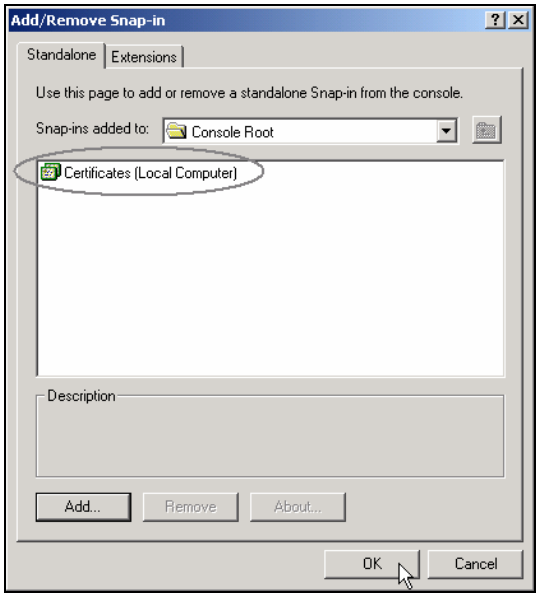


© Train Signal, Inc., 2002-2003

5. Within the Select Computer screen, you will need to select a computer for this snap-in to manage. You can either choose the local computer or another computer on your network. Since you only want this snap-in to manage Client-1, the local computer, you will select **Local computer**. Click **Finish** to close this screen. Then click **Close** in the Add Standalone snap-in window.



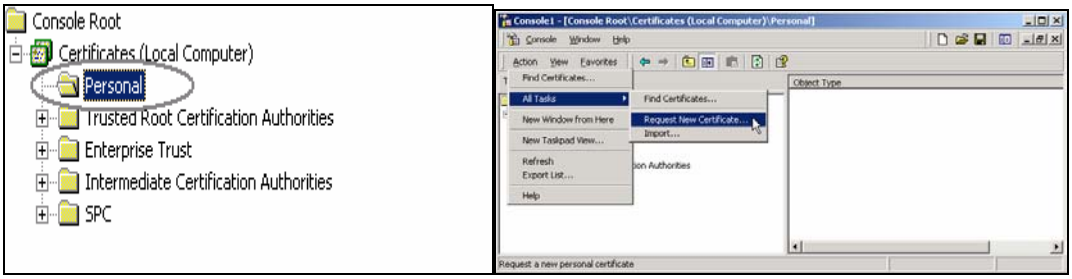
6. Next, verify that the Certificates (Local Computer) Snap-in has been added to the Console Root and click **OK** to close this Add/Remove Snap-in window.



© Train Signal, Inc., 2002-2003

Initiating a new Certificate request through the Certificates snap-in

1. Double click **Certificates (Local Computer)** under the Console Root in the left pane. It will bring you all of the certificate categories for Client-1. Next, select the **Personal** folder and then select **Action→All Tasks→Request New Certificate** from the menu above.

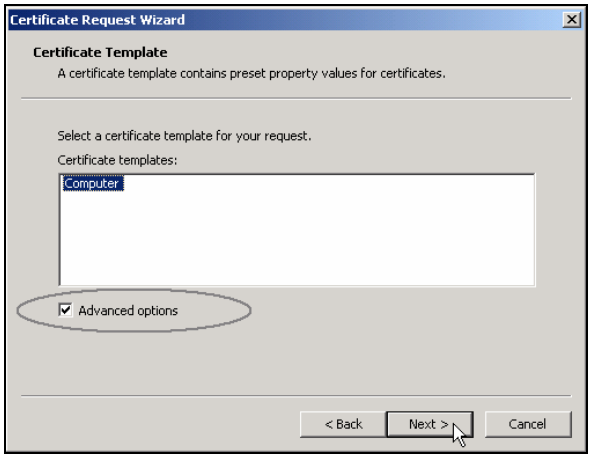


2. This will bring up the Certificate Request Wizard, click **Next** to continue. If this fails, reboot your computer and attempt to start the wizard again.

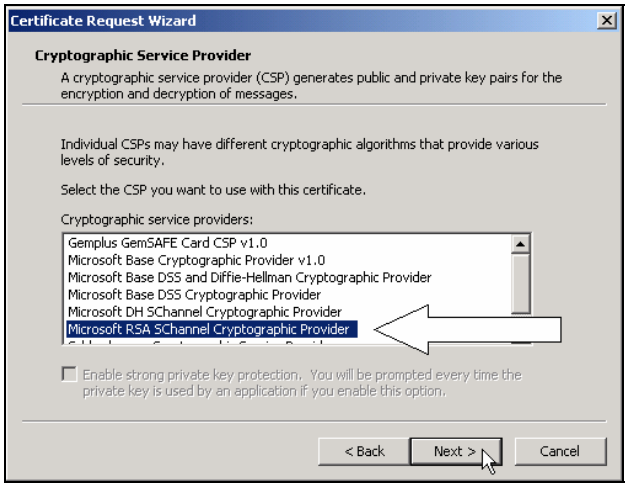
© Train Signal, Inc., 2002-2003

3. From within the Certificate Template page, you can select different certificate templates. Since you specified "computer account" earlier, the only template you will see is for computers. Highlight the **Computer template** and select the **Advanced** options checkbox. Click **Next** to continue.

.

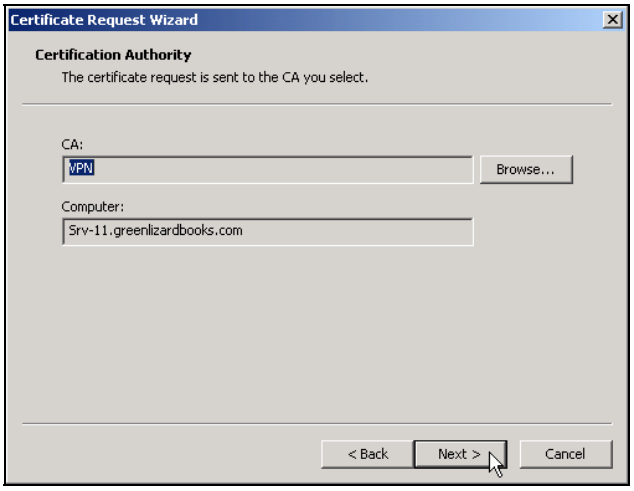


4. The Cryptographic Service Provider screen allows you to choose what type of algorithm to use in conjunction with your certificates. This can be adjusted based on security needs and other preferences. The default algorithm is fine, so leave Microsoft RSA Schannel Cryptographic Provide selected and click **Next** to continue.

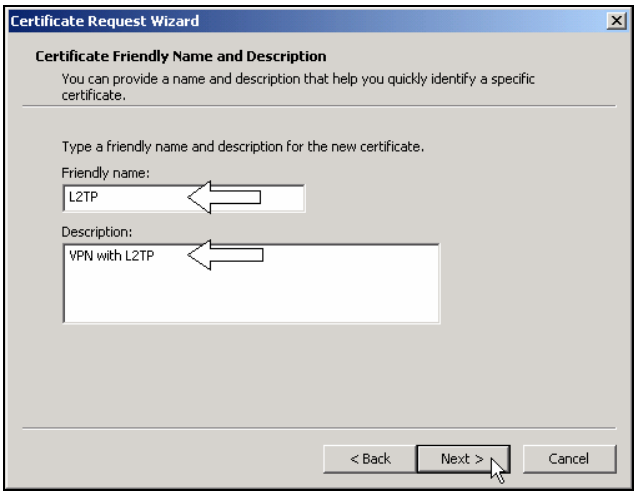


© Train Signal, Inc., 2002-2003

5. The Certificate Request Wizard then allows you to choose which Certificate Authority to send your request to. VPN, the enterprise root CA you installed earlier on SRV-11, should be highlighted. Click **Next** to continue.



6. This brings up the Certificate Friendly Name and Description screen where you can type in a friendly name and description to identify this certificate. The friendly name is locally significant to your computer and allows you to identify the purpose of the certificate on the local computer. Click **Next** to continue.

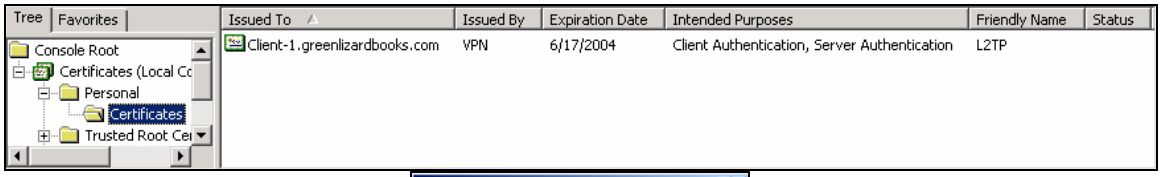


© Train Signal, Inc., 2002-2003

7. On the last screen of the wizard, verify all of the settings that you have specified. Click **Finish** and you will have completed the certificate request.

8. The wizard should then report a successful certificate request. Just click **OK** to close this dialog box.

9. You should now confirm the receipt of this certificate. In the Certificates snap-in, double click **Certificates (Local Computer)** under Console Root in the left pane, double click the **Personal** folder and click on the **Certificates** folder. As you see in the right pane, you can view information about this certificate. You can also view this information by double clicking on the certificate. Double clicking the certificate will bring up the Certificate dialog box and provide you with information about this certificate.



© Train Signal, Inc., 2002-2003

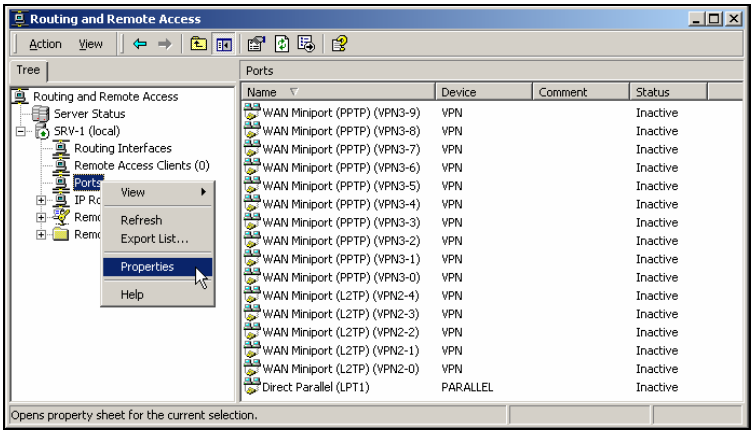
10. You now have successfully installed a machine certificate on Client-1, your VPN client. Make sure that you reboot **Client-1** to avoid any unforeseen problems. On SRV-1, your VPN server, you will install a certificate the same way by following the above procedures. Don't forget to restart **SRV-1** after you have completed the certificate request process. After you have finished this step, make sure that you reconnect **Client-1** back to the public side of your network and **make sure that all of the IP addresses are properly assigned as was originally specified**. Refer to Computer Configuration Overview, if you have any questions on this.

Establishing a VPN session using L2TP

VPN Server setup

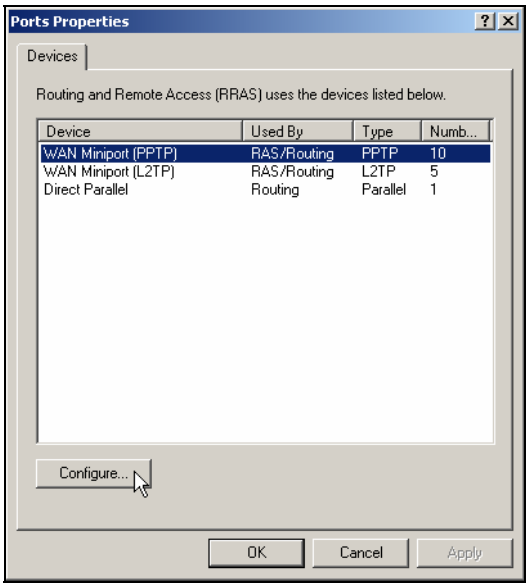
In Lab 1, you already setup 5 L2TP ports to be available on the VPN Server. In this lab, you now want SRV-1, your VPN server, to accept only L2TP connections, so you will want to disable all of the PPTP ports on SRV-1.

1. To do this, log on to **SRV-1**, go to **Start→Programs→Administrative Tools** and click on **Routing and Remote Access**. Right click **Ports** and select **Properties**.

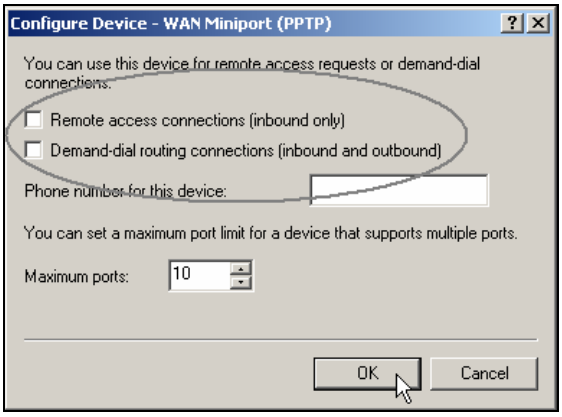


© Train Signal, Inc., 2002-2003

2. This will bring up the Ports Properties dialog box. Again, there are 2 types of VPN ports, WAN Miniport (PPTP) and WAN Miniport (L2TP). Select **WAN Miniport (PPTP)** and click **Configure**.

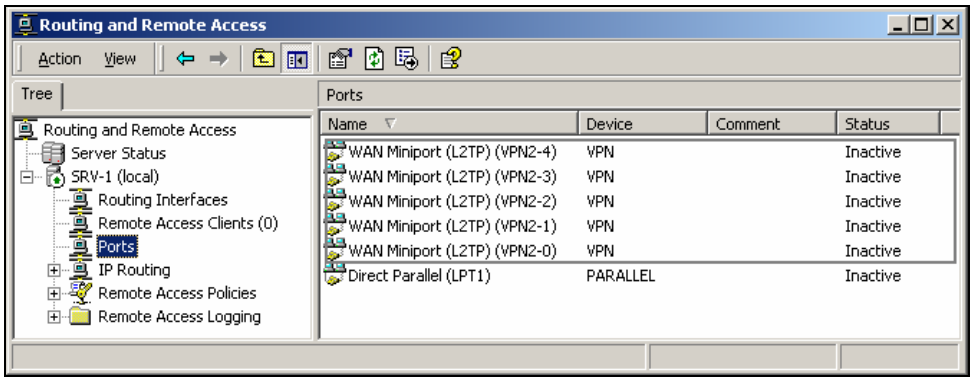


3. In the Configure Device – WAN Miniport (PPTP) dialog box, **uncheck Remote access connections (inbound only)** and uncheck **the Demand-dial routing connections (inbound and outbound)**. Click **OK** and then **OK** again on the Ports Properties dialog box to complete the configuration.



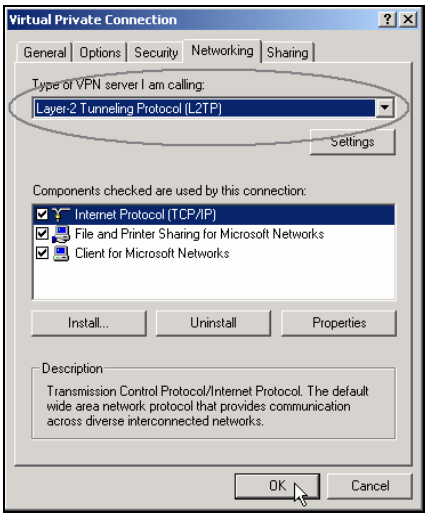
© Train Signal, Inc., 2002-2003

4. As you can see from the right pane of the RRAS console, you now have 5 L2TP ports and no PPTP ports available for your VPN clients to access.



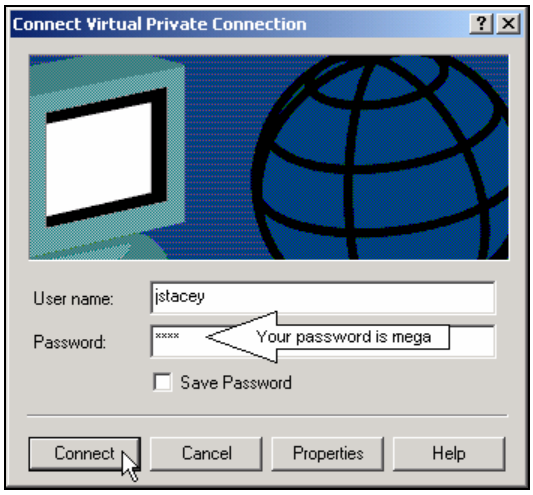
VPN Client setup

5. Log on to **Client-1**, go to **Start→Settings→Network and Dial-up Connections** and click on the **Virtual Private Connection** (which will be named whatever you set it at in the previous lab). This will bring you to the Connect Virtual Private Connection dialog box again, click on the **Properties** button and select the **Networking** tab. Click on the **down arrow** and select **Layer 2 Tunneling Protocol (L2TP)** as the type of the VPN server you are calling. Click **OK** to complete the configuration.



© Train Signal, Inc., 2002-2003

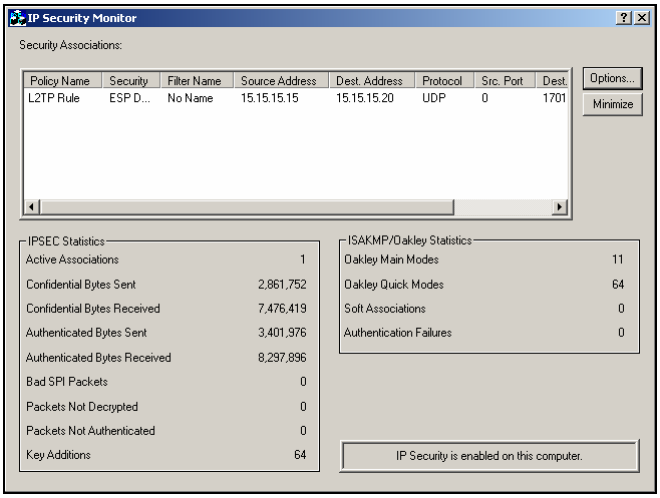
6. You are now ready to establish your VPN session using L2TP. From Client-1, just type in ***jstacey*** as the user name and ***mega*** as the password in the Connect Virtual Private Connection dialog box. Click **Connect** to establish the VPN connection with L2TP.



Monitoring security on the link using ipsecmon

After you have established your VPN session with L2TP, you can use ipsecmon to monitor the security on the link.

1. To do this, on either your VPN server or client, go to **Start→Run,** type in **ipsecmon** and click **OK** to open the IP Security Monitor. This IP Security Monitor screen provides you with information about the IPSec relationship between the 2 edges of your VPN tunnel.



© Train Signal, Inc., 2002-2003

Lab 3

Creating and configuring Remote Access policies for Green Lizard Books, Inc.

You will learn how to:

- Create a Remote Access Policy in Mixed Mode
- Create a Remote Access Policy in Native Mode
  - Modify the default policy
  - Set Remote Access Policy conditions
  - Set Remote Access Policy permissions
  - Create a Remote Access Policy profile

© Train Signal, Inc., 2002-2003

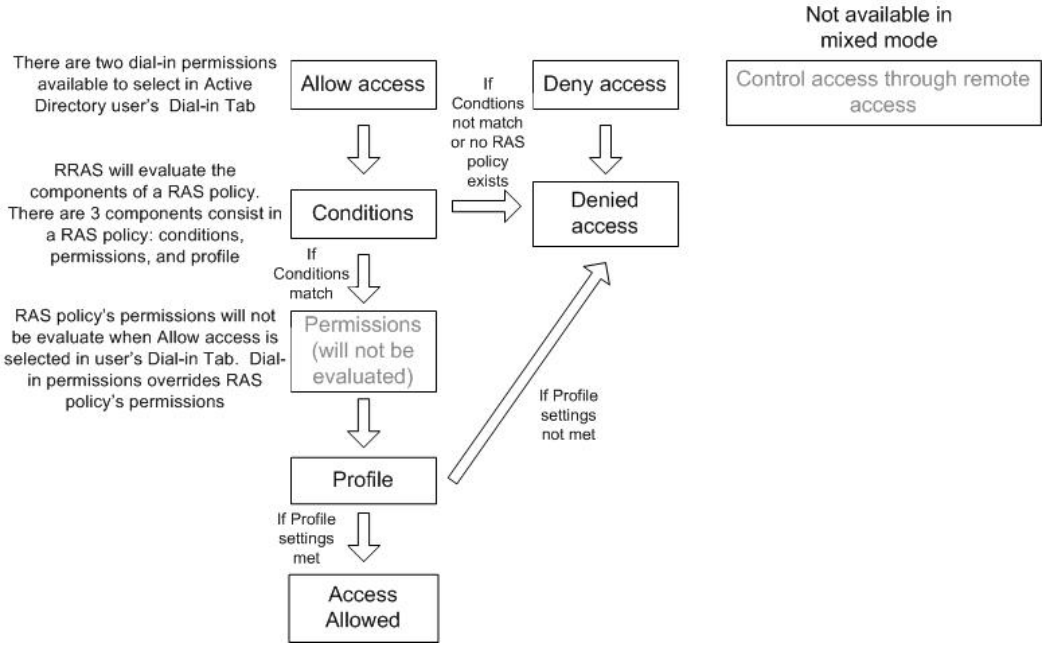
Scenario

Now that Green Lizard Books Inc. has a L2TP VPN Server in place for its remote access clients, you feel a lot more comfortable with the overall security of the remote access solution. In your weekly meeting with Bill, however, he brings up the issue of having more control over which of his employees have remote access to Green Lizard's LAN. He also mentions that he would like to control how and when these employees connect to the LAN. "What a great idea - why didn't I come up with that?" you think to yourself. "Well, right now," you say out loud, "the VPN solution has a policy that allows everyone to access the LAN 24 hours a day/7 days a week, so I will have to look at this a little closer and get back to you with an adequate solution. In the meantime, I will need for you (Bill) to come up with a list of users that should be granted remote access and the times that they should be allowed to connect to the network." He agrees and you both decide to meet again next week to discuss how to set policies on the VPN server.

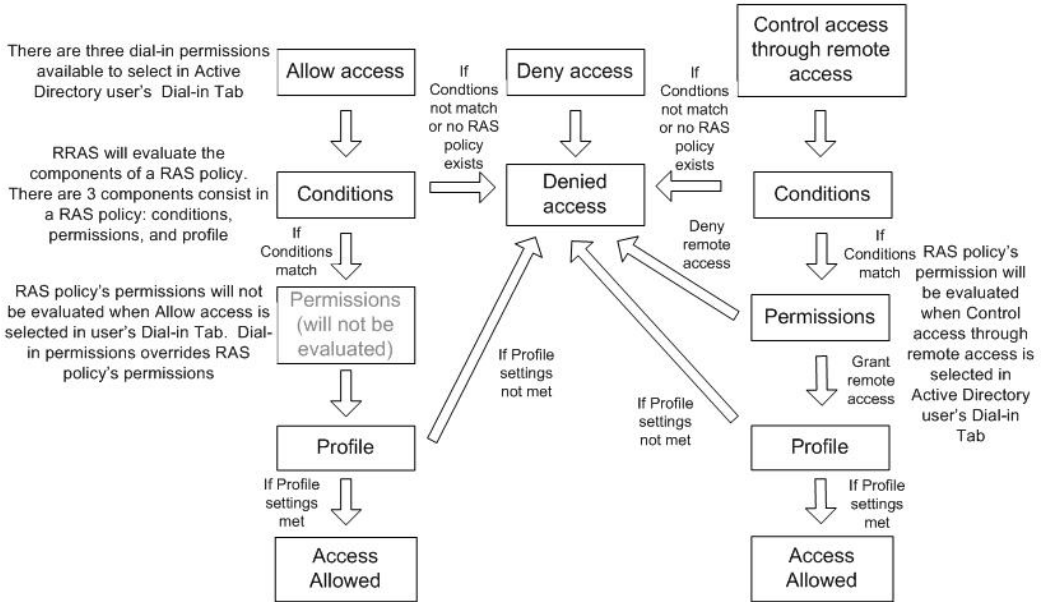
In this lab, you will examine the default state that a VPN server is in when you first enable remote access on the server. From there, you will learn how to decide which option for assigning remote access policy best suits your network. Finally, you will create, configure and implement several different remote access policies and examine how they interact with the VPN connection.

© Train Signal, Inc., 2002-2003

RRAS Authentication Process in Mixed Mode



RRAS Authentication Process in Native Mode

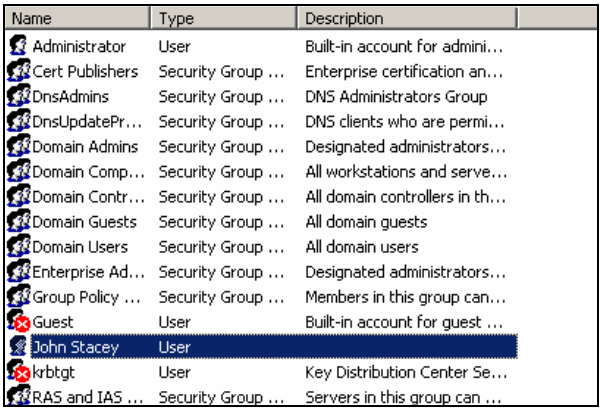


© Train Signal, Inc., 2002-2003

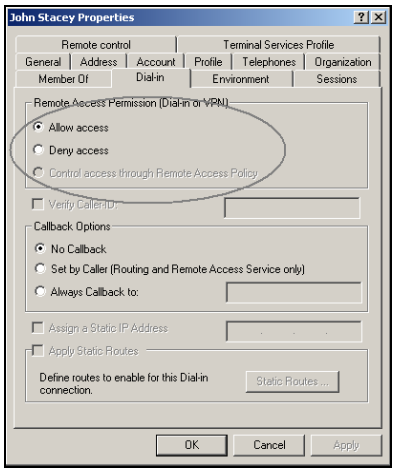
Reviewing the current remote access permissions

In Lab 1, the remote access permission was granted to allow access to your remote user, John Stacey. In this lab, you are going to take a closer look at how remote access permissions and policies interact.

1. Log on to **SRV-11** and open the **Active Directory Users and Computers** console by going to **Start→Programs→Administrative Tools→Active Directory Users and Computers**. In the right pane of console, select ***John Stacey*** and double click the **user**.



2. This will bring you to the John Stacey Properties dialog box. Select the **Dial-in** tab and notice that it gives you 3 different options you can set for Remote Access Permission: Allow access, Deny access and Control access through Remote Access Policy. By default, the last option, Control access through Remote Access Policy, should be grayed out. This option is not available when your domain is in mixed mode. Later in this lab you will switch your domain to native mode in order to make this option available.

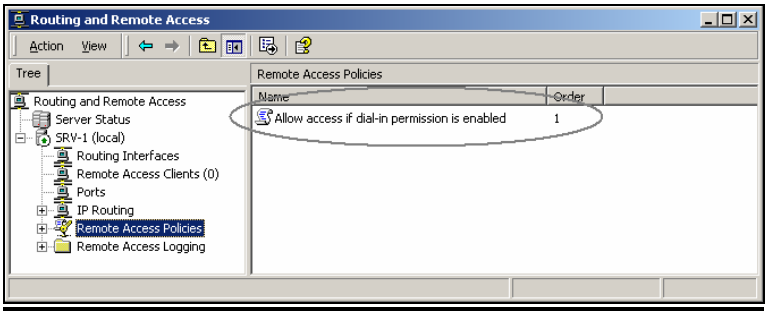


© Train Signal, Inc., 2002-2003

In Lab 1, the user account, John Stacey, was allowed remote access by selecting the Allow access option as John's remote access permission. But, according to the authentication process detailed on page 69, the RRAS server will also check to see if a remote access policy exists, which is exactly how this process works. If there is no remote access policy configured, John's access will be denied. By default however, there is a remote access policy that was automatically created when RRAS was enabled, and it contains a condition that specifies that anybody can access the VPN Server 24 hours a day, 7 days a week. If this condition is met, then the policy will check the profile settings before allowing John access to the VPN server.

Viewing the default RAS policy

1. To view this default RAS policy, log on to **SRV-1** and **open Routing and Remote Access** by going to **Start→Programs→Administrative Tools→Routing and Remote Access**. In the left pane of the console, click on **Remote Access Policies**. This will show all of the remote access policies in the right pane. There should only be one remote access policy present, named "Allow access if dial-in permission is enabled," which is created by default when you enabled RRAS.



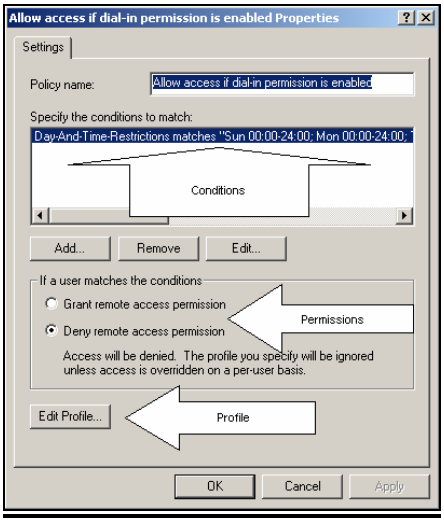
2. Double click the **policy** and it will bring you to its properties. From here, notice that there are 3 components present that make up the remote access policy: Condition(s), Permission and the Profile

   In this default policy, there is only one condition listed. This condition allows users to access the VPN server from Sunday at 00:00 to the following Saturday at 24:00. In other words, it allows access all of the time.

© Train Signal, Inc., 2002-2003

3. The next component is the permission, which you can set to either grant or deny access to the remote user, if the user matches the initial conditions. Although it is currently set at deny access, the permission of this RAS policy will **NOT** be under consideration, because you have selected Allow access as John Stacey's dial-in permission within Active Directory. In other words, according to the RRAS authentication process, the user's dial-in permission overrides the permission set within the RAS policy and the only time this permission will be considered is when the user's dial-in permission is set to "Control access through Remote Access Policy."

   The profile is the last component of a RAS policy. It contains 6 tabs with many configurable settings. We will go into each tab in great detail later in this lab.



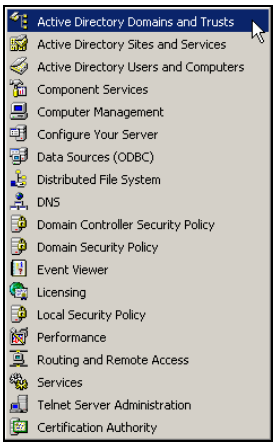
© Train Signal, Inc., 2002-2003

Switching to Native Mode

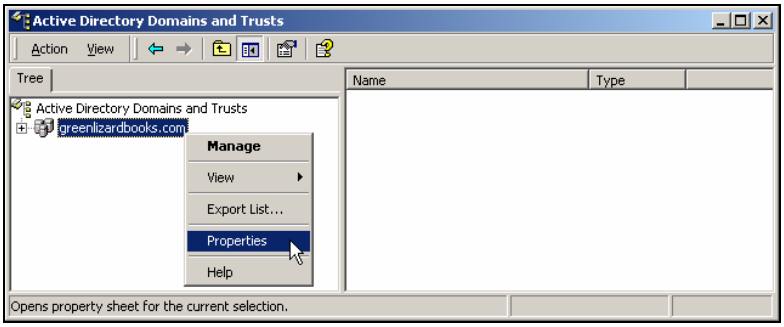
In order to have the third option, "Control access through Remote Access Policy," available on John Stacey's Dial-in tab, you will have to switch the domain mode from the default mixed mode to native mode. Mixed mode supports both Windows 2000 and NT 4 domain controllers. Once your domain is switched to Native mode, NT 4 domain controllers will no longer be supported. Also, even though NT 4 domain controllers may have never existed within your domain, your domain will still default to mixed mode and you are required to manually make the switch from mixed mode to native mode. Once you make the switch from mixed mode to native mode you can not go back without completely wiping out your Active Directory and starting from scratch.

Green Lizard's network only contains a Windows 2000 domain controller and they have no future plans on adding a NT 4 domain controller, so they can make the switch to native mode without any problems.

1. Log on to **SRV-11** and open the **Active Directory Domains and Trusts** console by going to **Start→Programs→Administrative Tools→Active Directory Domains and Trusts**.

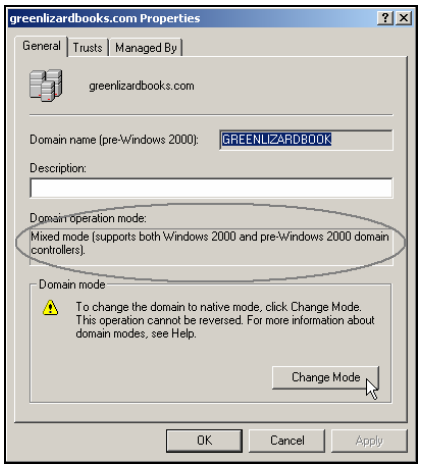


2. In the left pane of the console, right click on **greenlizardbooks.com** and choose **Properties**.

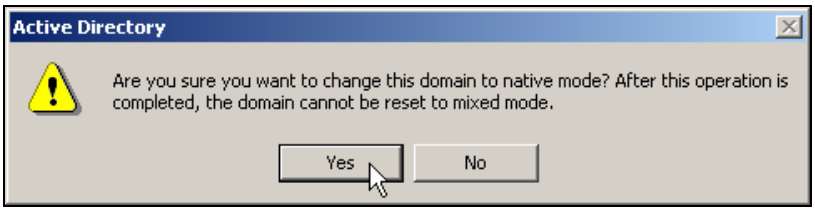


© Train Signal, Inc., 2002-2003

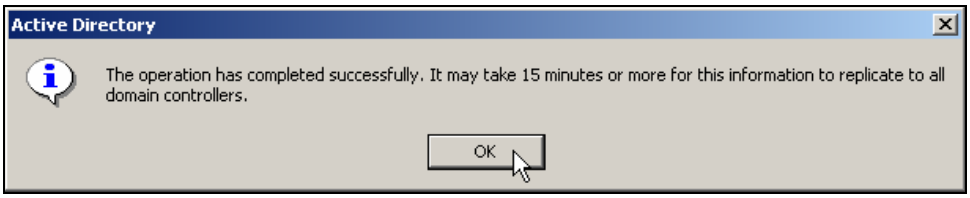
3. This will bring you to the greenlizardbooks.com properties dialog box. As you see, your domain is currently in mixed mode. In order for you to switch to the native mode, just click the **Change Mode** button.



4. You will get a message warning you that the domain will not be able to be reset to mixed mode after this operation. Just click **Yes** to continue.

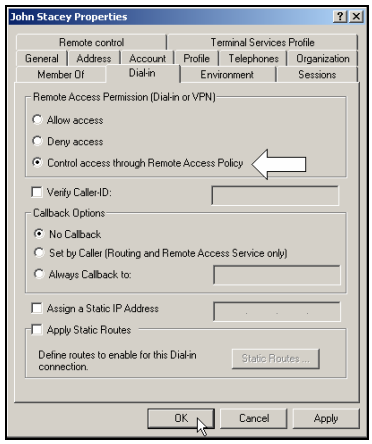


5. Click **OK** in the greenlizardbooks.com properties dialog box and also click **OK** in the confirmation message box to complete the operation. Also, it is a really good idea to **restart your computer** to avoid any unexpected potential problems after changing the domain mode.



© Train Signal, Inc., 2002-2003

6. Once your system has rebooted, log back on to **SRV-11** and open **the Active Directory Users and Computers** console by going to **Start→Programs→Administrative Tools→Active Directory Users and Computers**. In the right pane of console, select ***John Stacey*** and double click the object. Select the **Dial-in** tab again. Notice, that the third option is now available to select. Select **Control Access through Remote Access Policy** and click **OK**. You will be using this remote access permission to examine the RAS policy in the next section.



Examining the remote access policy

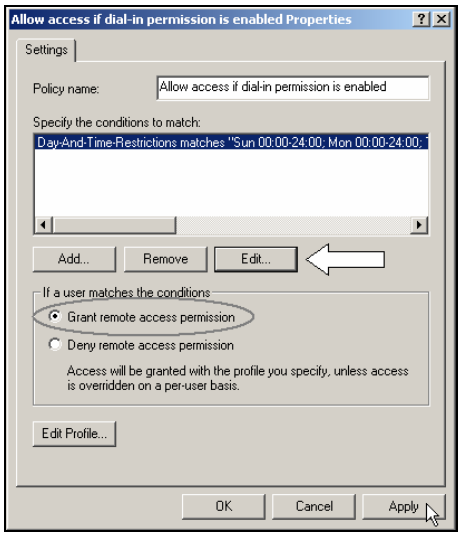
1. Log on to **Client-1**, go to **Start→Settings→Network and Dial-up Connections** and click on the **Virtual Private Connection**. This will bring you to the Connect Virtual Private Connection dialog box again, just type in ***jstacey*** as the user name and ***mega*** as the password and try to establish the VPN connection by clicking the **Connect** button. You will immediately get an error message indicating that John's account does not have permission to dial in. Remote access has been denied. This is due to the setting you changed in the last step when you selected "Control access through Remote Access Policy" from John's Dial-in tab. The permission from the default remote access policy is now being evaluated, and, as was pointed out in an earlier step, the permission of the default remote access policy is currently set for deny access. Therefore, John's access has been denied.

© Train Signal, Inc., 2002-2003

2. To modify the default remote access policy, log back on to **SRV-1** and open **Routing and Remote Access** by going to **Start → Programs → Administrative Tools → Routing and Remote Access**. Double click the default **remote access policy**, which will bring you to its properties. Select **Grant remote access permission** as the permission of this RAS policy and click **Apply**. After waiting a few seconds, you should now be able to establish a VPN connection from Client-1.

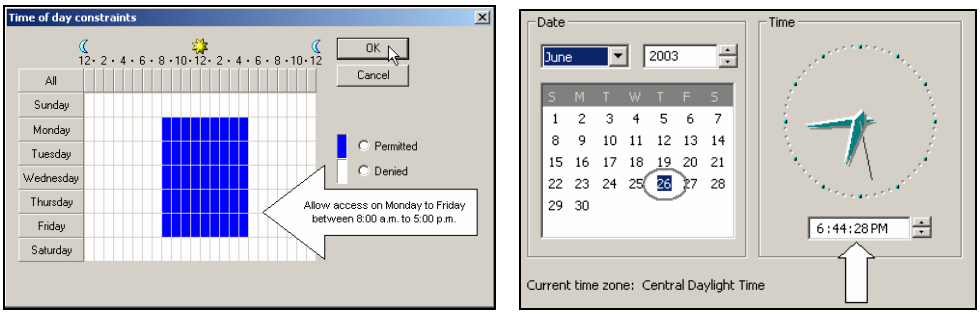
Conditions

1. Next, take a closer look at the remote access policy itself. First, start with understanding the conditions. The conditions are the first part of the remote access policy that is checked when a VPN client attempts to access a VPN server. If no condition is matched or no conditions exist, the VPN client is immediately denied access without any further consideration. The top portion of the interface shown below is used to edit current conditions or to add new ones. Click on the **Edit** button to modify the default condition.

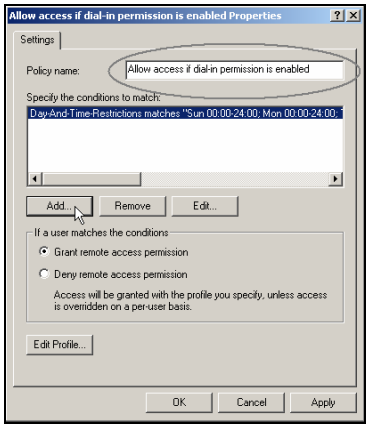


© Train Signal, Inc., 2002-2003

2. This will bring up the Time of day constraints dialog box. As you see, the default condition is set for 24/7 access. You can modify the day and the time to allow access. Below, the schedule has been modified to allow access from 8:00 a.m. to 5:00 p.m. on weekdays. As you see from the system clock, the time is now way past 5:00 p.m. on Thursday. Because this condition is not matched, the VPN client will be denied access to the VPN server once again. You can test this condition by setting different days and times. Don't forget to change this condition back to **24/7 access** (the default setting) after you finish testing.



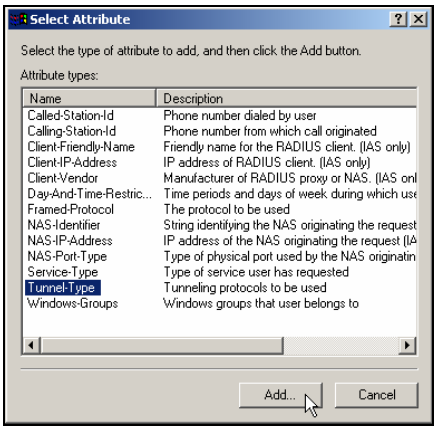
3. From within the Default remote access policy, the policy name can be changed to something that is meaningful on the network. You can also add multiple conditions to the remote access policy. Adding multiple conditions requires the VPN client to match **ALL** of the conditions that are present within the remote access policy. To add additional conditions, just click on the **Add** button.



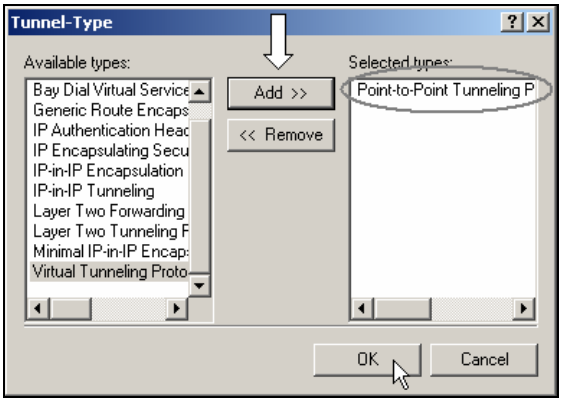
© Train Signal, Inc., 2002-2003

4. Clicking on the Add button brings you to the Select Attribute dialog box. There are many attributes listed but most of them are related to IAS (RADIUS), which you have not configured in this lab. You will specify a tunneling protocol to be used as a second condition for this RAS policy. Just select **Tunnel Type** and click **Add**.

   Windows-Groups is another common condition. Windows-Groups allows you to select specific group/groups for which you want to restrict or allow access. Do not select this condition right now.

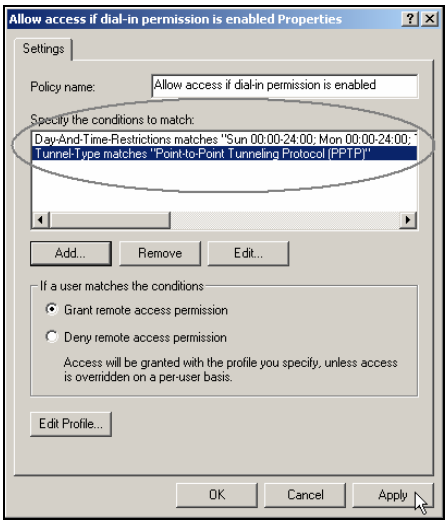


5. In the Tunnel Type dialog box, there are many different types of tunneling protocols to choose from. Select **Point-to-Point Tunneling Protocol (PPTP)**, and then click the **Add** button and the **OK** button to add this protocol as the required tunnel type for the second condition.



© Train Signal, Inc., 2002-2003

6. There are now two conditions within the default remote access policy and more can be added if desired. Just remember, your remote users will have to meet all of the conditions to gain access to the network. For this lab, the VPN client must meet the 24/7 condition (log on anytime) and also be using Point-to-Point Tunneling Protocol (PPTP) as the tunneling protocol for connection.

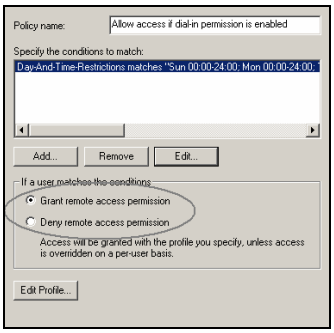


7. In Lab 2, you configured Client-1 to use Layer 2 Tunneling Protocol (L2TP) as the tunneling protocol. Assuming that this configuration is still in place, try to gain access to Green Lizard's network by using the VPN connection on Client-1. Once again, access should be denied, because Client-1 did not meet all of the conditions (Tunnel-Type should be PPTP) set forth in the default remote access policy. If you remove the Tunnel-Type condition Client-1 should be able to establish the VPN connection.

© Train Signal, Inc., 2002-2003

Permissions

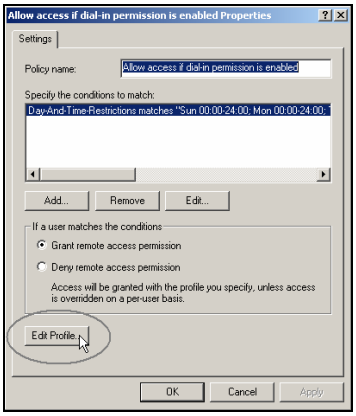
Permissions are the second component of a remote access policy. There are two permissions to choose in this component: **Grant access remote permission** and **Deny remote access permission**. Again, the permissions in a remote access policy will only be evaluated when the user's dial-in permission in Active Directory is set to Control access through remote access policy and all of the conditions are matched. In this lab, as you remember, John Stacey's dial-in permission is currently set to Control access through remote access policy. Permissions **will** be evaluated if the condition is matched



Profiles

The Profile is the third component of a remote access policy. The profile is checked once the remote user has met the conditions of the policy **AND** has been granted remote access permission (refer back to the diagram at the beginning of this lab). The profile is where you can fine tune your remote access policy and configure more advanced settings.

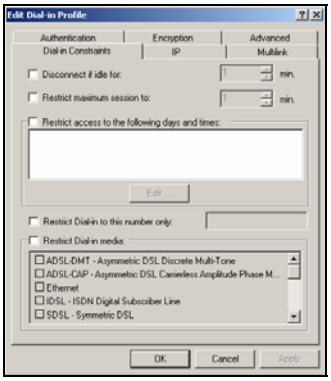
1. To configure the profile, just click on the **Edit Profile** button from within the default remote access policy properties dialog box.



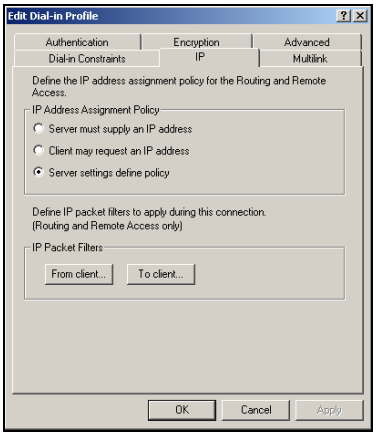
© Train Signal, Inc., 2002-2003

2. This will bring you to the Edit Dial-in Profile dialog box. As you can see, there are 6 tabs (Dial-in Constraints, IP, Multilink, Authentication, Encryption and Advanced) available with many settings for you to configure.

   The first tab is the Dial-in Constraints tab. This tab allows you to configure many dial-in restrictions such as the amount of idle time allowed, the maximum remote access session time allowed, the days and time specified for remote access (this setting is the same as the day and time restrictions setting available as the condition), the incoming telephone number allowed and Dial-in media types. No restrictions are set, by default, from the dial-in constraint tab.



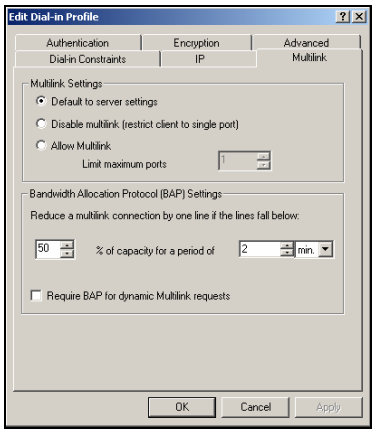
3. The next tab is the IP tab. This tab allows you to configure client IP Address Assignment Policy and IP packet filters. The default IP Address Assignment Policy is set on **Server settings define policy**. This means that the RRAS server settings will define how IP addresses are assigned. In this lab, the RRAS server will assign IP address from a static address pool. For IP packet filters settings, you can configure separate filters for inbound (from client) or outbound (to client) data packets.



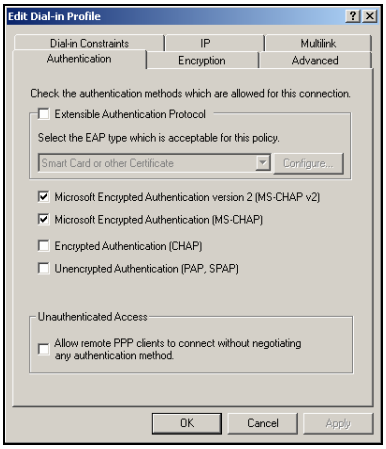
© Train Signal, Inc., 2002-2003

4. The third tab is the Multilink tab. This tab allows you to configure Multilink and Bandwidth Allocation Protocol (BAP). The default Multilink Setting is **Default to server settings**. Note: Multilink is a feature that allows remote users with multiple modems to connect to a multilink enabled RRAS server to improve speed performance.

   For Bandwidth Allocation Protocol (BAP) settings, you can configure a couple of options, including one to disconnect a line if the capacity of the multilink connection falls below a certain level for a given length of time that you define.

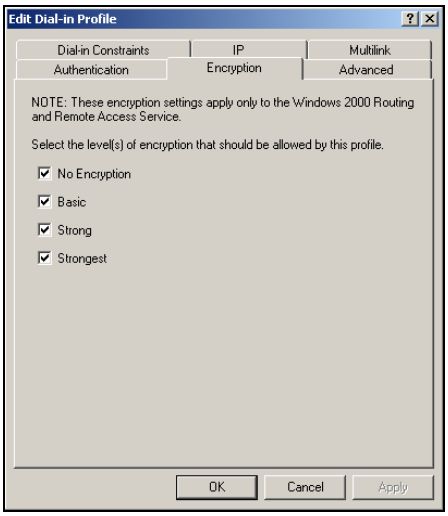


5. The forth tab is the Authentication tab. This tab allows you to define the type of authentication that is allowed for remote access. MS-CHAP versions 1 and 2 are enabled by default. Note that MS-CHAP v2 is the most secure authentication protocol and is a recommended protocol if your dial-up clients are running Windows 2000 or your VPN clients are running Windows 2000, Windows NT 4.0 or Windows 98. Remember that any protocols that you enable in this tab also need to be enabled in the RRAS server properties.

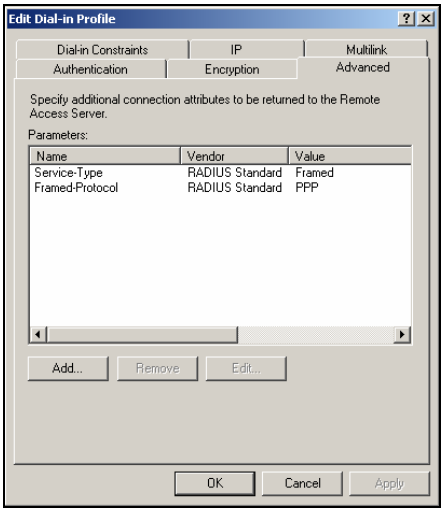


© Train Signal, Inc., 2002-2003

6. The fifth tab is the Encryption tab. This tab allows you to define the types of encryption that are required for the remote user to connect. There are 4 levels of encryption: No Encryption, Basic, Strong and Strongest. If there is more than one level of encryption enabled, your RRAS Server will use the most secure encryption that is supported by both your RRAS server and your remote user.



7. The last tab is the Advanced tab. This tab allows you to add connection attributes, include generic RADIUS attributes and many different vendor-specific attributes.

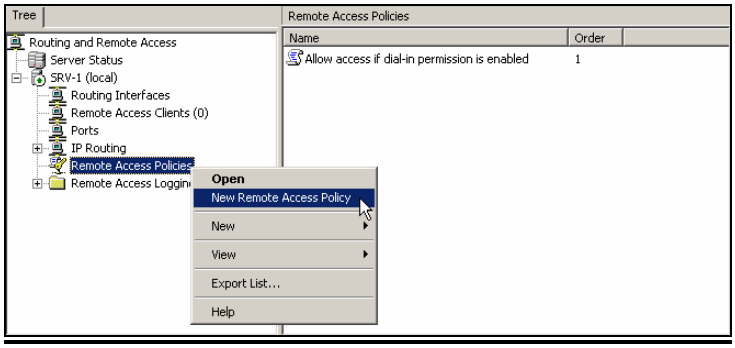


© Train Signal, Inc., 2002-2003

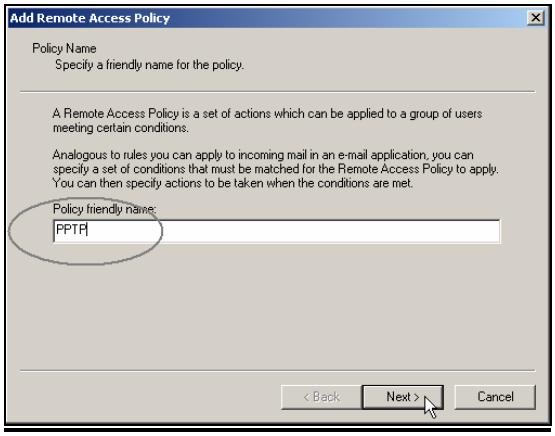
Adding a new Remote Access Policy

You can also add multiple remote access policies on your RRAS Server. The authentication process will become a little different with multiple policies. The order of your RAS policies in the RRAS console will be critical to the authentication process. We will go over that after adding a new RAS policy.

1. For now, in order for you to add a new RAS policy, just right click on **Remote Access Policies** in the left pane of the RRAS console and choose **New Remote Access Policy**.

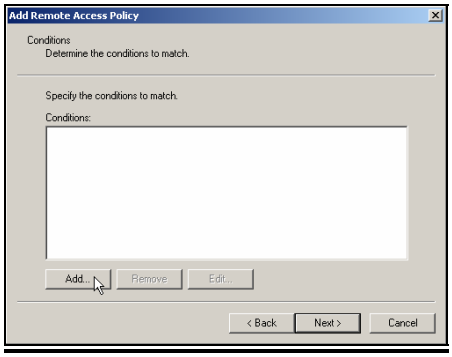


2. This will bring up the Policy Name dialog box. Just type in **PPTP** as the name of this new policy and click **Next** to continue.

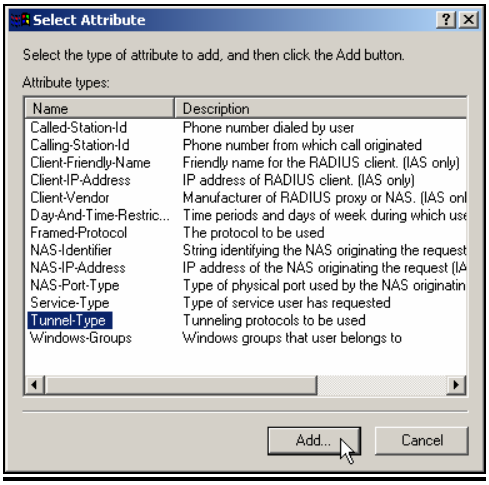


© Train Signal, Inc., 2002-2003

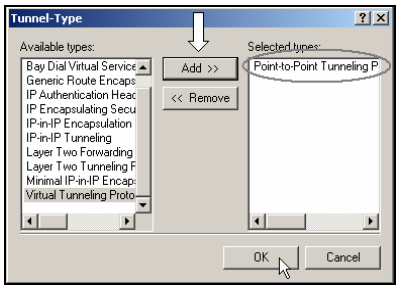
3. In the Conditions dialog box, just click the **Add** button to add a condition for this new RAS policy.



4. This will bring up to the Select Attribute dialog box. As before, there are many attributes listed. Again, for this lab, you will specify the type of tunneling protocol to be used as a condition for this new RAS policy. Select **Tunnel Type** and click **Add**.

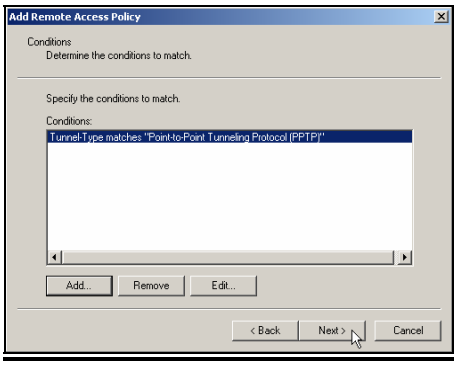


5. In this Tunnel Type dialog box, select **Point-to-Point Tunneling Protocol (PPTP)**. Click the **Add** button and the **OK** button to add this protocol as the required tunnel type for the condition in this new RAS policy.

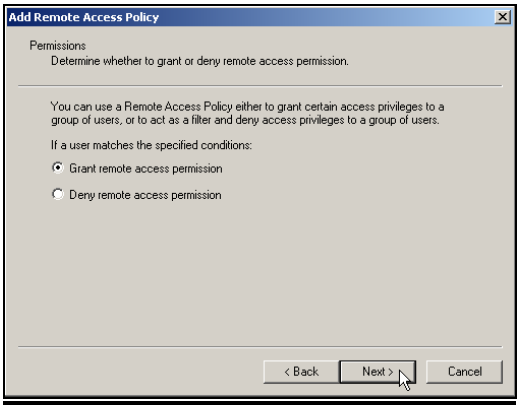


© Train Signal, Inc., 2002-2003

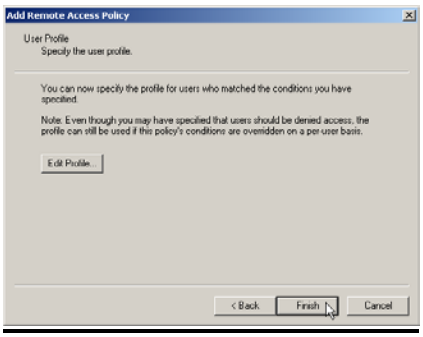
6. Verify the added condition and click **Next** to continue



7. This will bring up the Permissions dialog box. You can either grant remote access or deny remote access if your remote users met the condition that you just added. Select **Grant remote access permission** as the Permission when your users match the condition. Click **Next** to continue.



8. On the User Profile dialog box, you can configure the profile settings for this new remote access policy by clicking the **Edit Profile** button. But, for the purposes of this lab, leave all of the settings in this remote access profile at their default settings and click **Finish** to complete the addition of the remote access policy.

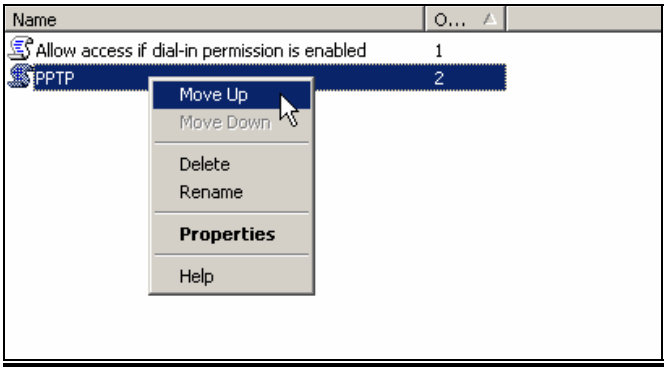


© Train Signal, Inc., 2002-2003

9. As you can see from the right pane of your RRAS console, you now have 2 RAS policies. One is named **Allow access if dial-in permission is enabled** and the other is named **PPTP**. The authentication process is going to be slightly more complicated. The process will start by first checking your remote user's dial-in permission in Active Directory. The RRAS server will then evaluate the first remote access policy in the list and determine if the remote user has either Allow access or Control access through remote access policy as their dial-in permission.

   If the condition of the first policy does not match, it will then check the next policy in the list until the RRAS server finds a remote access policy that does match the user's condition. Access will then be evaluated based on the determination of the permissions and profile settings of that remote access policy. If the remote user does not meet **all** of the conditions of **any** policy, then access will be denied.

   In this lab, your remote user will gain access no matter what order the two remote access policies are in. You can change the order of the policies by right clicking the **PPTP** policy and click **Move up** to move it to the top of the list. Although this policy was set for allowing PPTP traffic only, your default policy will always grant access to your remote user no matter which tunneling protocol they use.



© Train Signal, Inc., 2002-2003

© Train Signal, Inc., 2002-2003

Lab 4

Configuring a Site-to-Site VPN for Green Lizard Books, Inc.

You will learn how to:

- Plan for a Site-to-Site VPN
- Configure the Physical Setup
- Create Demand Dial Interfaces
- Configure Static Routes between locations
- Initiate a VPN connection between two locations

© Train Signal, Inc., 2002-2003

Scenario

Over the past year, business has been going extremely well for Green Lizard Books Inc. The owner, Bill, has opened another office in Cleveland, Ohio and he has sent his brother, Mike, to run this new branch office. About a week ago, Bill called you up and asked you to meet him and his brother in their Chicago office. They were looking for suggestions on how to connect the Chicago and the Cleveland offices together. Mike informed you that their initial plan was to set up the Cleveland network completely separate from the Chicago location and they had even hired a computer consultant in Cleveland, Nancy, to help out with basic administration there. After some thought was given to the subject, they have decided that there are a lot of company documents that need to be shared between the 2 networks. Mike would like to connect these two networks together so that users at both locations can exchange their documents. Right away, Nancy and you came up with several ideas to connect these networks together. The choices came down to:

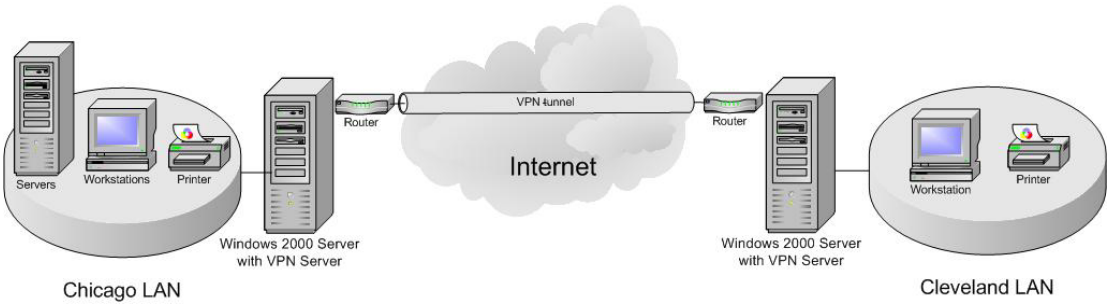
1. **Remote Access (dial up or VPN)** – Users from the two different networks would have to manually establish an individual connection to the remote location. This would be cheaper up front, but would cause a lot of headaches for the users and yourself (the administrator).
2. **Leased Lines (dedicated telecommunications line between the sites)** – Leased lines would work great for this solution. However, leased lines are expensive (dependent upon the two locations that are being connected) and they typically require contracts, locking you in with a provider. Also, you often have to wait from 4 to 6 weeks before they are installed.
3. **Site-to-Site VPN** – This solution requires some investment up front as you should have a dedicated Internet connection (56K modems are NOT recommended) as well as a VPN Server at each location. There are many quality VPN Server products on the market, but a Windows 2000 solution is a good choice for Windows 2000 administrators, because of its ease of use and integration with Active Directory.

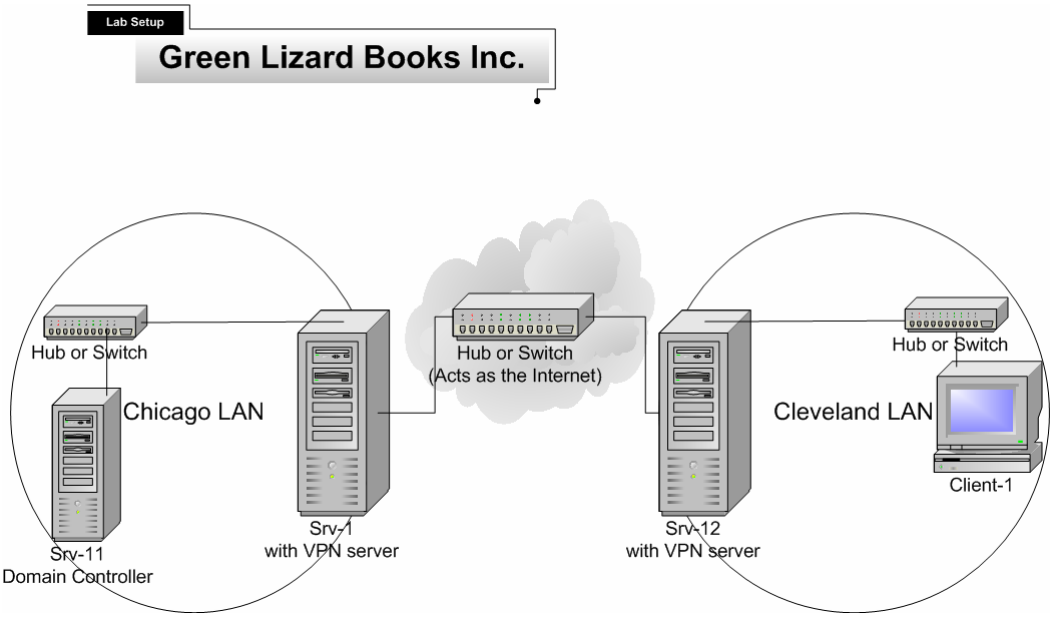
Nancy thought that remote access was good but only when an individual user is on the road and needs to connect to the remote network. Leased lines would be the ideal option, but you both thought that Bill and Mike would be unhappy about the big bill each month. Since each location has a dedicated connection to the Internet, Nancy and you agreed that a Site-to-Site VPN would be the best solution to connect the two networks together. Nancy and you have both planned your work and today it is time to work the plan. You will be implementing a site to site VPN to solve Green Lizard's problem.

In this lab, you will install a VPN server manually in the Cleveland site. You will also add demand-dial interfaces and create static routes on both VPN servers. After this, you will need to create VPN service accounts within Active Directory for these VPN servers, configure their dial-in permissions and verify permissions within the remote access policy. Finally, you will test the site to site VPN by attempting to gain access to a file in one location from the other.

© Train Signal, Inc., 2002-2003

Site to Site VPN Connection

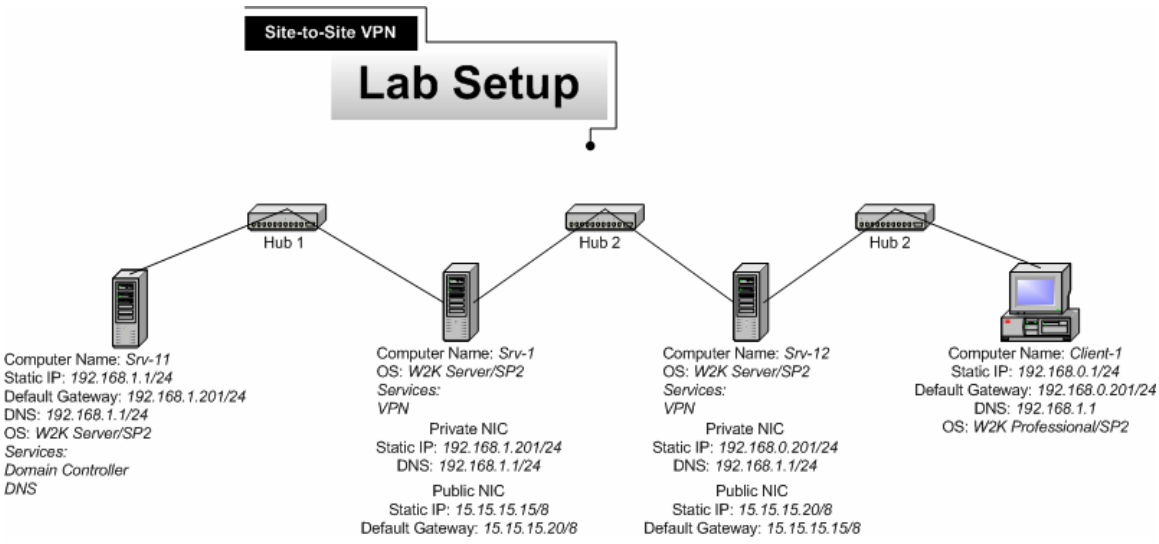




© Train Signal, Inc., 2002-2003

In order to setup the site to site VPN, an additional computer, hub, cable and NIC is required. Below are the computer configurations and lab diagram for this lab.

Computer Number	1	2	3	4
Computer Name	SRV-11	SRV-1	SRV-12	Client-1
IP Address	192.168.1.1/24	Private: 192.168.1.201/24 Public: 15.15.15.15/8	Private: 192.168.0.201/24 Public 15.15.15.20/8	192.168.0.1/24
Default Gateway	192.168.1.201/24	Public 15.15.15.20/8	Public 15.15.15.15/8	192.168.0.201/24
Preferred DNS server	192.168.1.1/24	Private 192.168.1.1/24	Private 192.168.1.1/24	192.168.1.1/24
OS	W2K Server	W2K Server	W2K Server	W2K Pro
	SP2	SP2	SP2	SP2

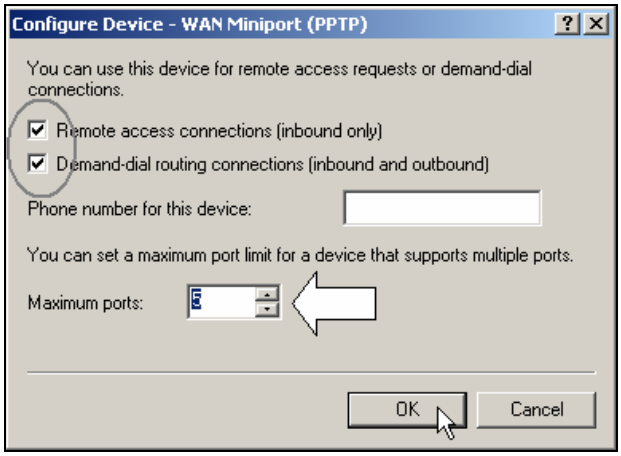


© Train Signal, Inc., 2002-2003

PPTP-based Site to Site VPN connection

In the pervious lab, you only have L2TP ports available on SRV-1 (the Chicago VPN server) that are accepting VPN connections. In this lab, you will be using PPTP as the tunneling protocol for the Site-to Site VPN connection instead. Therefore, you will need to have PPTP ports available in your Chicago VPN server for this lab.

1. To add PPTP ports to your Chicago VPN server, you will need to log on to **SRV-1**, go to **Start→Programs→Administrative Tools** and click on **Routing and Remote Access**. Right click **Ports** and select **Properties**. In the Ports Properties dialog box, select **WAN Miniport (PPTP)** and click **Configure**. In the Configure Device – WAN Miniport (PPTP) dialog box, check **Remote access connections (inbound only)** and check the **Demand-dial routing connections (inbound and outbound)**. Enter **5** as the number of available ports and click **OK** once and then again on the Ports Properties dialog box to complete the configuration. You should now have 5 PPTP ports available for your VPN connection.

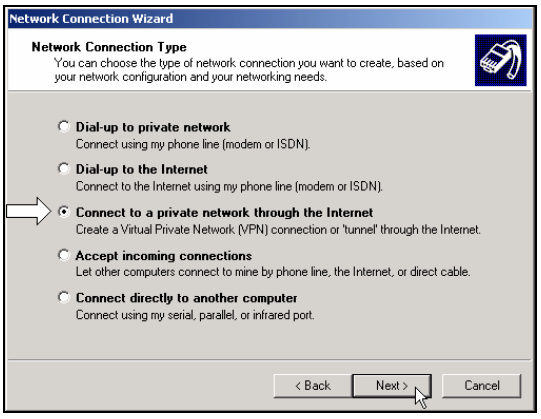


© Train Signal, Inc., 2002-2003

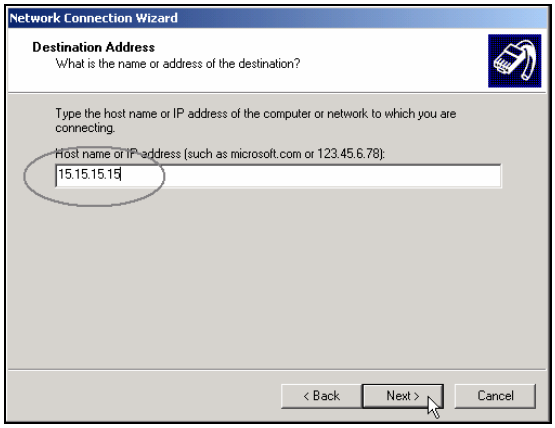
Configuring SRV-12 as a member server

Since this new Cleveland location will also be within the Green Lizard Books Inc. domain, you will want to make SRV-12 a member server within the greenlizardbooks.com domain. In order for SRV-12 to join the domain as a member server, a connection will have to be established over the simulated Internet. This can be accomplished by setting up SRV-12 as a VPN client temporarily.

1. Log on to **SRV-12** and go to **Start→Settings→Network and Dial-up Connections**, click on **Make New Connection**. This will bring up the Network Connection Wizard. Just click **Next** to continue. On the Network Connection Type page, select **Connect to a private network through the Internet** and click **Next** to continue.

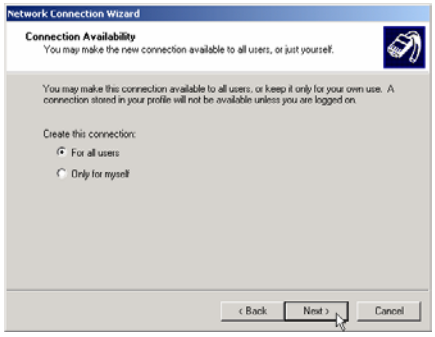


2. The next screen of the wizard will ask you to enter the Destination Address. This is the public IP address of the Chicago VPN server, **15.15.15.15**. Type this IP address in and click **Next** to continue.



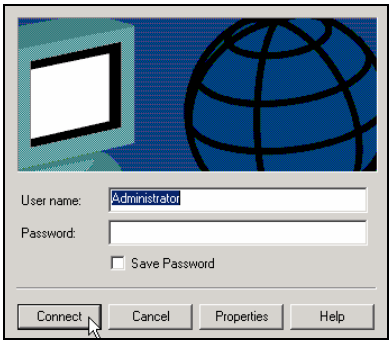
© Train Signal, Inc., 2002-2003

3. This will bring you to the Connection Availability screen. Select **For all users** and click **Next** to continue. Also click **Next** on the Internet Connection Sharing screen and **Finish** on the last screen of the wizard to complete setting up the VPN client.



4. Once you are done setting up your VPN client, you will immediately get the Connect Virtual Private Connection dialog box. Just type in ***administrator*** as the user name and your password. Click **Connect** to establish the VPN connection.

   Note: if you do not know the password for the administrator, just log on to **SRV-11** and reset its password in Active Directory Users and Computers.



5. After you have established the VPN connection, you need to make SRV-12 a member server of greenlizardbooks.com. Simply right click on the **"My Computer"** icon on the desktop and select **Properties**. From here, select the **Network identification** tab, select **Properties**, select **domain** and type in the domain name of the domain SRV-12 will join, which is **greenlizardbooks.com** or its NetBIOS name, **greenlizardbook**. Note: NetBIOS names are a single label (no periods) up to 15 characters in length. Click **OK**. It will then ask for a username and password. Use ***administrator*** as the account name and the password from the greenlizardbooks.com domain. When it has joined successfully, it will "welcome you to the domain" and then tell you that it needs to restart in order for the changes to take effect. **Restart the computer** and log back on to **SRV-12** after it has finished rebooting.

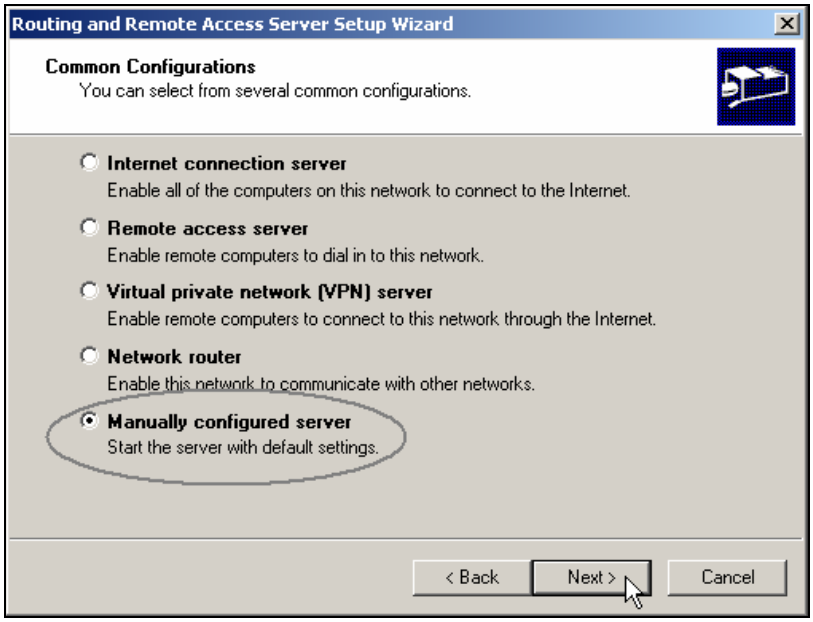
© Train Signal, Inc., 2002-2003

Manually configuring RRAS as a VPN server on SRV12

To create a site-to-site VPN connection, not only do you need to have a VPN server at the Chicago site, but you will also need a VPN server at the Cleveland site. As you see in the lab setup, SRV-12 has two NICs, one of which is the public interface, directly attached to the Internet. Therefore, SRV-12 will be the computer to configure as Cleveland's VPN server. For this lab, you will configure this VPN server manually (without the wizard).

1. Log on to **SRV-12** and open RRAS. Right click **SRV-12** and click **Configure and Enable Routing And Remote Access**. This will bring up the Routing and Remote Access Server Setup Wizard, just click **Next** to continue.

   On the Common Configurations page, select **Manually configured server** to start the server with default settings. Click **Next** and **Finish** on the last screen of the wizard to complete the installation.

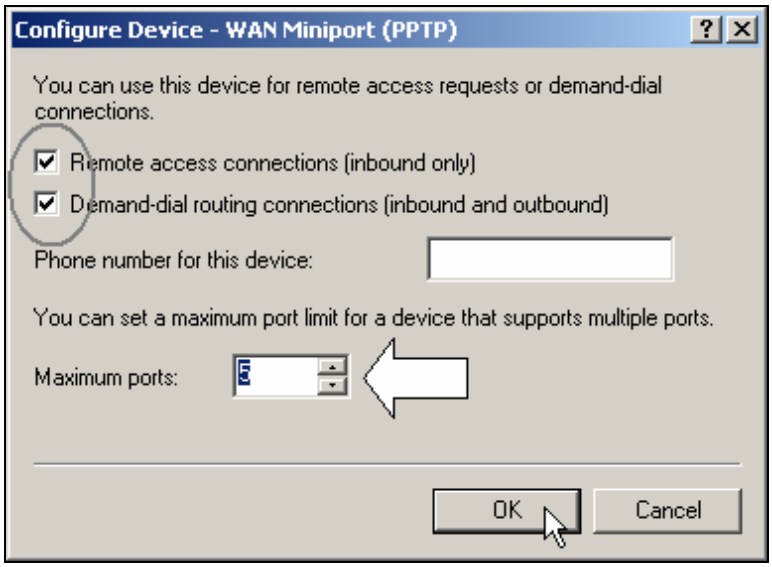


© Train Signal, Inc., 2002-2003

PPTP Ports on the Cleveland VPN Server

There should be 128 PPTP ports available on the Cleveland VPN server by default (your number may differ). Because the Cleveland office currently has very few users, for security reasons, the number of ports available should be changed to reflect the maximum number of concurrent users that will be accessing the VPN Server. Only one (1) port is needed for the site to site connection and one port would be needed for each remote user trying to access the VPN Server.

1. In Routing and Remote Access, right click **Ports** and select **Properties**. In the Ports Properties dialog box, select **WAN Miniport (PPTP)** and click **Configure**. In the Configure Device – WAN Miniport (PPTP) dialog box, make sure **Remote access connections (inbound only)** and the **Demand-dial routing connections (inbound and outbound)** are checked. Enter **5** as the number of available ports and click **OK** and then **OK** again on the Ports Properties dialog box to complete the configuration. You should now have 5 PPTP ports available on your Cleveland VPN server.

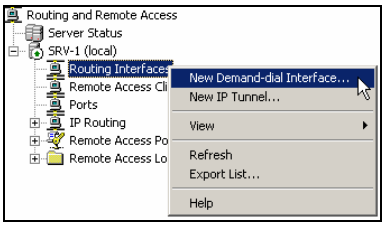


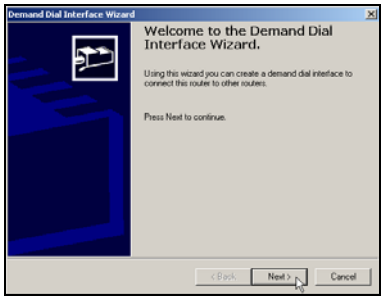
© Train Signal, Inc., 2002-2003

Configuring a Demand-Dial Interface on the Chicago VPN server

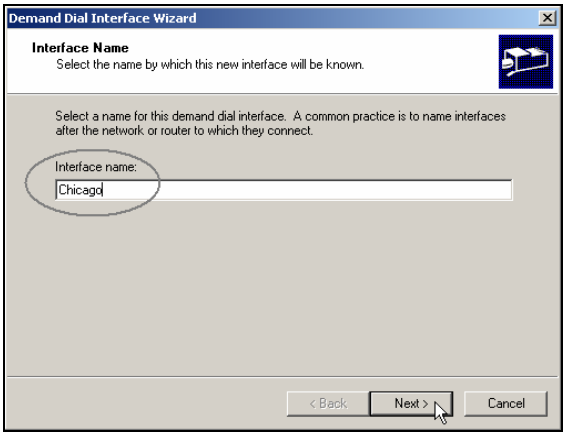
For a Site-to-Site VPN connection between SRV-1 (Chicago) and SRV12 (Cleveland), you will have to configure demand-dial interfaces on both VPN servers. This interface will allow the Chicago VPN Server to initiate a VPN session to the Cleveland VPN Server any time it receives traffic destined for the Cleveland network.

1. To add a new demand-dial interface on the Chicago VPN server, log back on to **SRV-1** and open **Routing and Remote Access** by going to **Start → Programs→ Administrative Tools→Routing and Remote Access**. In the left pane of the console, right click on **Routing Interfaces** and choose **New Demand-dial Interface**. This will bring up the Demand Dial Interface Wizard. Just click **Next** to continue.



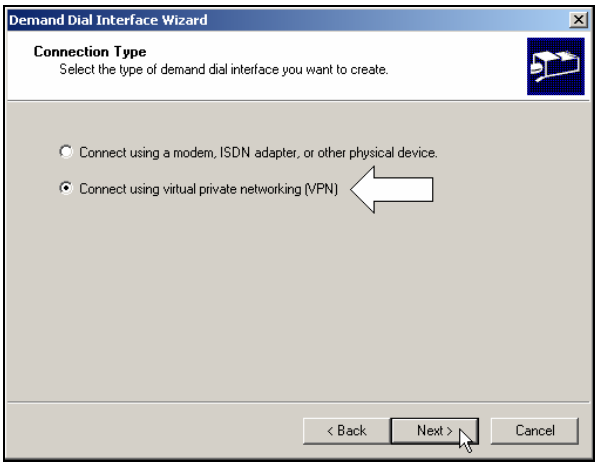


2. You should then see the Interface Name page, where you name your demand-dial interface. Type in **Chicago** as the interface name and click **Next** to continue.

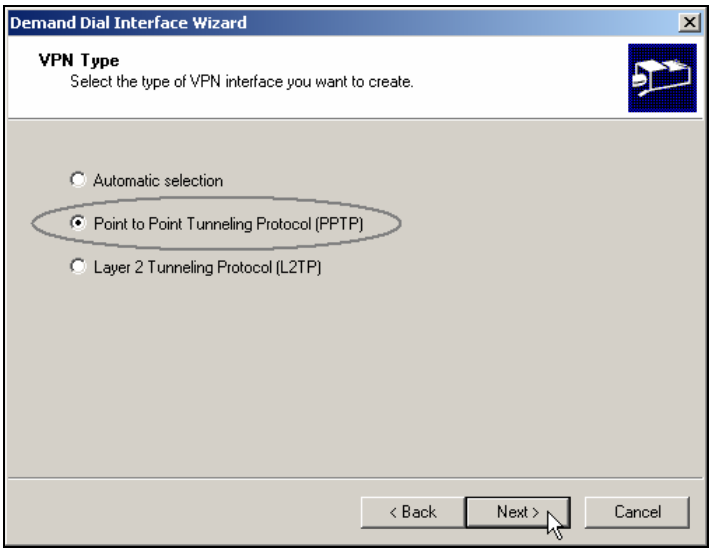


© Train Signal, Inc., 2002-2003

3. The next screen should be the Connection Type screen, where you can either choose a modem, ISDN adapter or VPN for this connection. Since this is going to be a VPN connection, select **Connect using virtual private networking (VPN)** as the Connection Type and click **Next** to continue.

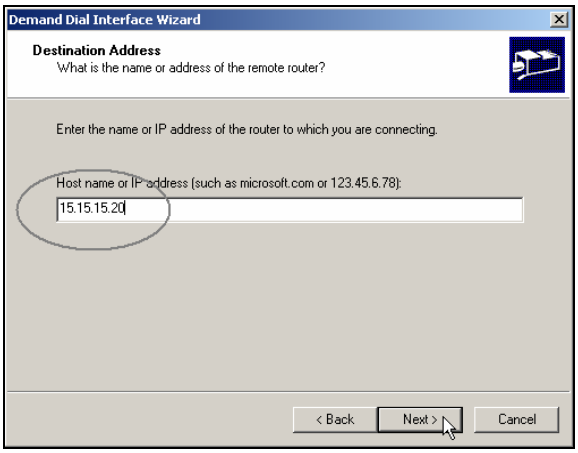


4. On the VPN type page, there are 3 VPN types for you to choose from. You can choose either to use PPTP, L2TP or Automatic selection as the tunneling protocol. Automatic selection will have your Chicago VPN server attempt a L2TP connection first. If the Cleveland VPN server does not support L2TP, it will then try to use PPTP to establish the connection. Since this is going to be a PPTP Site-to-Site VPN connection, select **Point to Point Tunneling Protocol (PPTP)** as the tunneling protocol and click **Next** to continue.

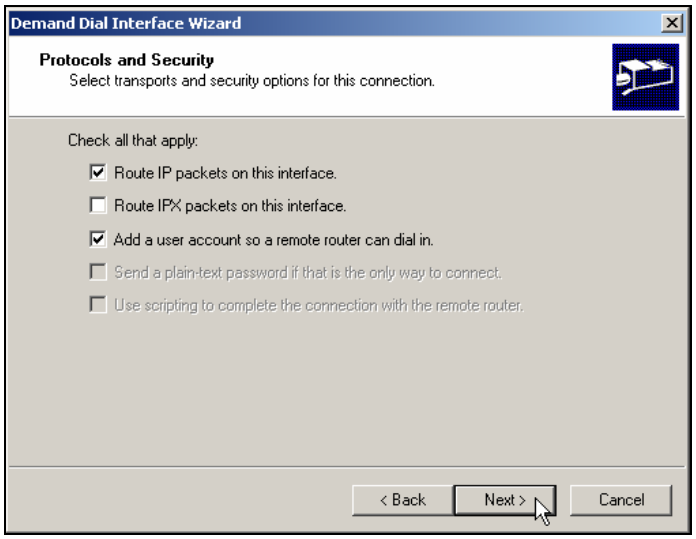


© Train Signal, Inc., 2002-2003

5. The next screen of the wizard will ask you to enter the destination IP address. Referring to the lab setup, the destination address is the public IP address of your Cleveland VPN server, which is 15.15.15.20. Type in **15.15.15.20** and click **Next** to continue.

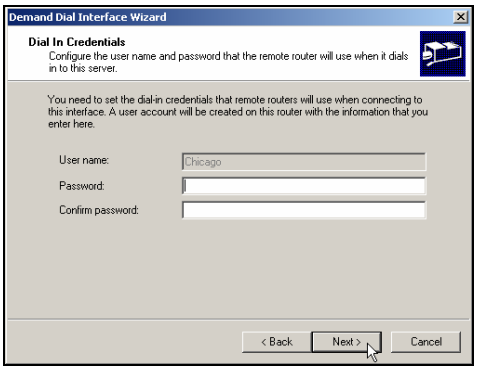


6. This will then bring you to the Protocols and Security screen. You can configure transport options and security options on this screen. Check **Route IP packets on this interface** for IP routing and also check **Add a user account so a remote router can dial in**. The second option allows the Cleveland VPN server to connect into Chicago by specifying a user account for it to use. Since this is going to be a two-way initiated connection, you will also have to add another user account at the Cleveland VPN server for the Chicago VPN server to connect into. This will be set up when you are adding a new demand-dial interface on the Cleveland VPN server later in the lab. For now, just click **Next** to continue.

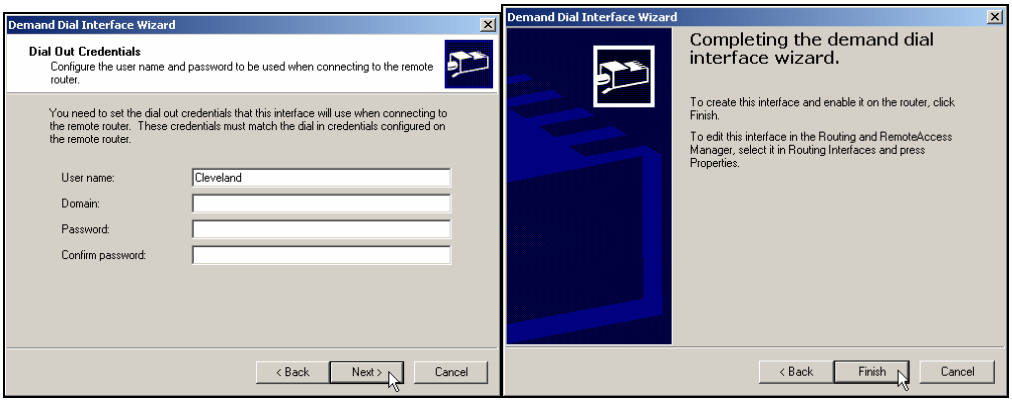


© Train Signal, Inc., 2002-2003

7. On the Dial in Credentials page, verify the user name, **Chicago**, which the Cleveland VPN server will be using as the dial-**out** user account to Chicago VPN server. Leave the password field and the confirm password field **blank** and click **Next** to continue.



8. The next page is used to enter the "Dial out Credentials," where you specify a user name and password to be used when authenticating to the Cleveland VPN server. This *dial-out* credential will be the same as the Cleveland *dial-in* credential that you will be adding at the Cleveland VPN server later in this lab. Type in **Cleveland** as the user name and leave the rest of the fields blank. Click **Next** to continue. Also, make sure that you remember this user name so that you can configure it as the dial-in credential when configuring the Cleveland VPN server. On the last screen of the wizard, click **Finish** to complete the process of adding the demand dial interface.

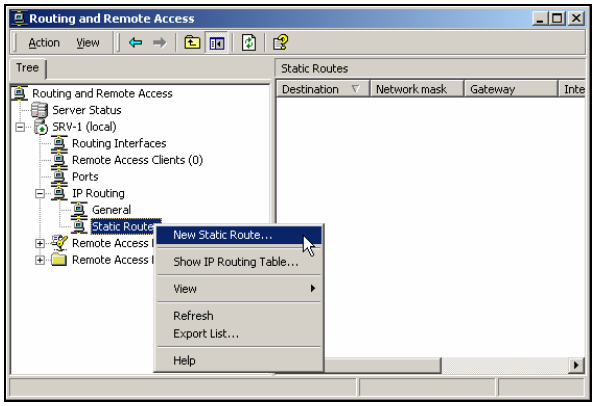


© Train Signal, Inc., 2002-2003

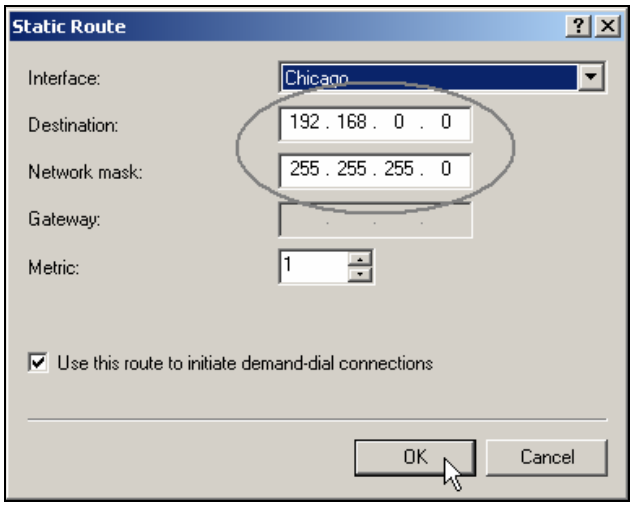
Configuring a static route on the Chicago VPN server

In order to allow network traffic to be forwarded from the Chicago network to the Cleveland network, you will need to configure static routes.

1. On **SRV-1**, in the left pane of the Routing and Remote Access console, double click **IP routing** and right click on **Static Routes.** Select **New Static Route**.



2. This will bring up the Static Route dialog box. First, make sure that **Chicago** is selected as the interface. This is the demand-dial interface that was just created in the last step. You must specify the Chicago interface and **NOT** the public interface in order for the VPN connection to Cleveland to be established. You will also need to configure the destination and the network mask. The destination will correspond to the Cleveland network's Network ID, which is 192.168.0.0. The Cleveland network's subnet mask is 255.255.255.0, and this should be configured for the static route as well. Also, make sure that you check the box for **Use this route to initiate demand-dial connections.** After your configuration matches what you see below, Click **OK** to create the route.

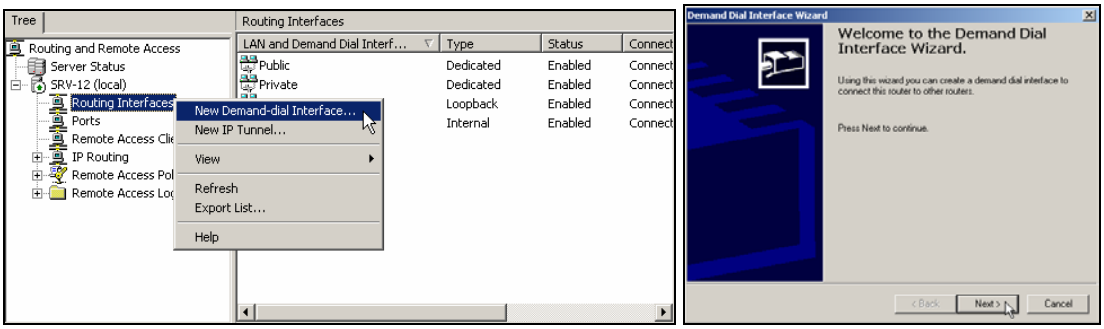


© Train Signal, Inc., 2002-2003

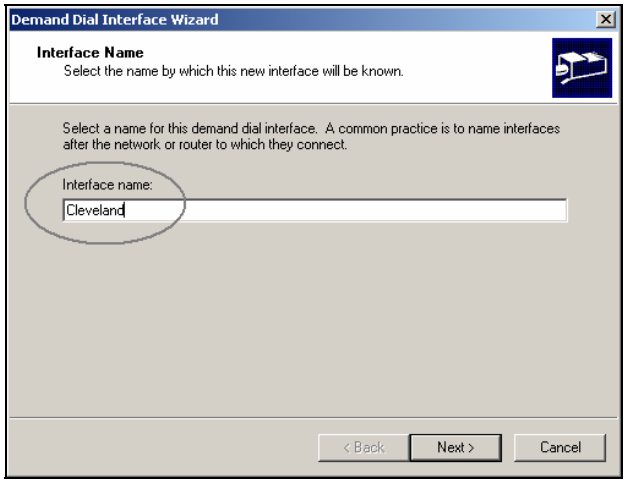
Configuring a Demand-Dial Interface on the Cleveland VPN server

To set up the site to site VPN, you will also have to add a demand-dial interface on the Cleveland VPN server.

1. Log on to **SRV-12** and open **Routing and Remote Access** by going to **Start→Programs→ Administrative Tools→Routing and Remote Access**. In the left pane of the console, right click on **Routing Interfaces** and choose **New Demand-dial Interface**. This will bring up the Demand Dial Interface Wizard. Click **Next** to continue.

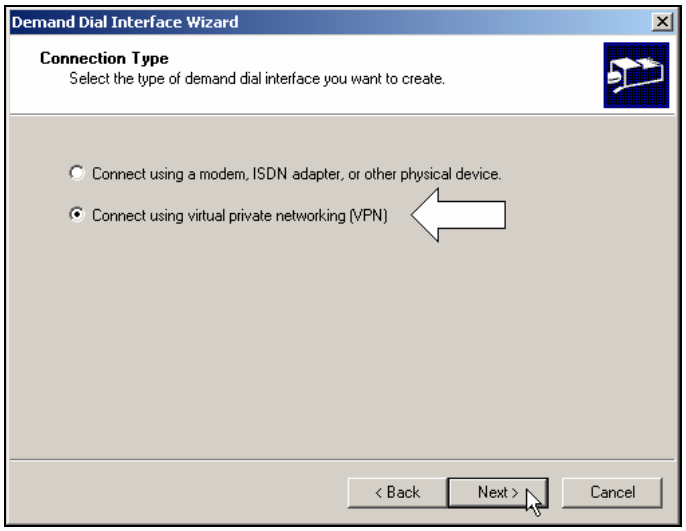


2. The Interface Name page is where you name the demand-dial interface. This interface name is also used as the user account name when the Chicago VPN Server authenticates to this server. Remember, this is the name that you set up as the dial-out credential on the Chicago VPN server. Type in **Cleveland** as the interface name and click **Next** to continue.

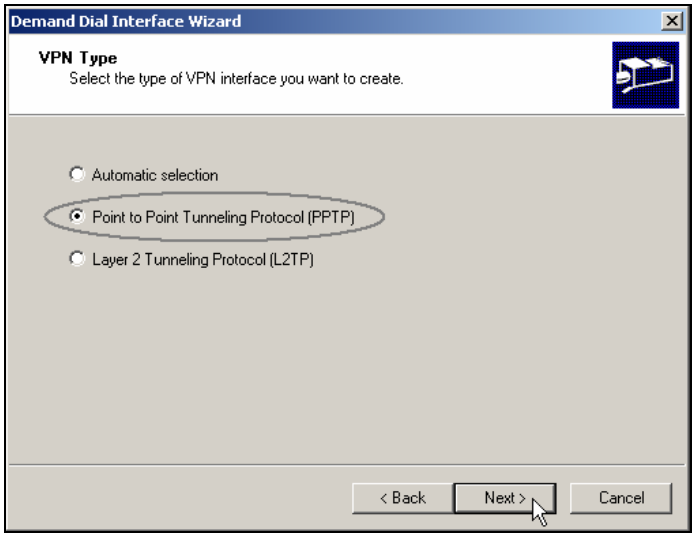


© Train Signal, Inc., 2002-2003

3. This will bring you to the Connection Type screen, select **Connect using virtual private networking (VPN)** as the Connection Type and click **Next** to continue.

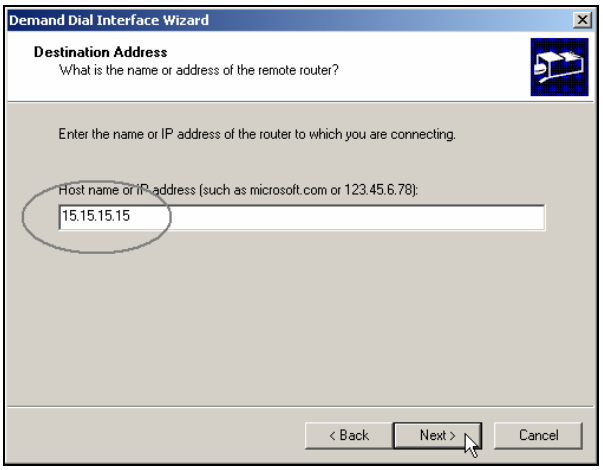


4. On the VPN type page, once again, there are 3 VPN types for you to choose from. You can choose either to use PPTP, L2TP or Automatic selection as the protocol type. Since this is going to be a PPTP Site-to-Site VPN connection, just **select Point to Point Tunneling Protocol (PPTP)** as the tunneling protocol and click **Next** to continue.

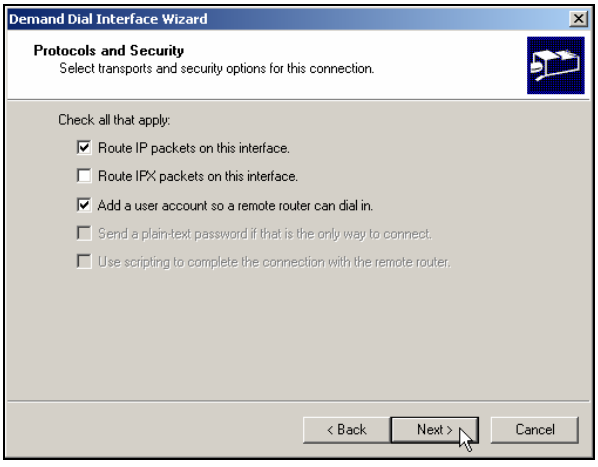


© Train Signal, Inc., 2002-2003

5. The next screen of the wizard will ask you to enter the Destination Address. Referring to the lab setup, the destination address will be the public IP address of your Chicago VPN server, which is 15.15.15.15. Type in **15.15.15.15** and click **Next** to continue.

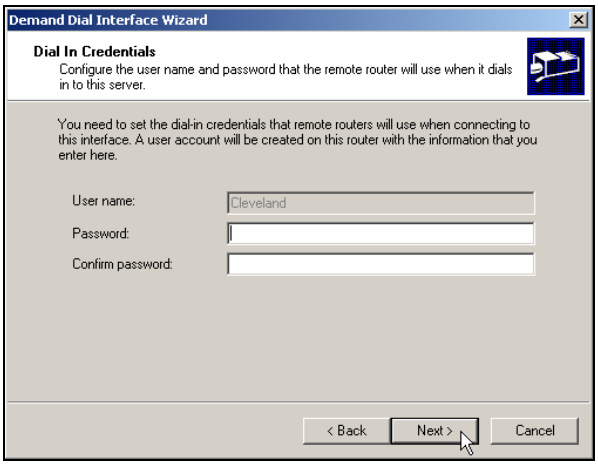


6. Next, you will see the Protocols and Security screen. You can configure transports options and security options on this screen. Check **Route IP packets on this interface** for IP routing and also check **Add a user account to remote router can dial in**. Again, adding a user account will allow the Chicago VPN server to dial in using a specific user account. You will be adding these user accounts for dial in at both VPN servers because you are setting up this Site-to-Site connection as a two-way initiated connection. Click **Next** to continue

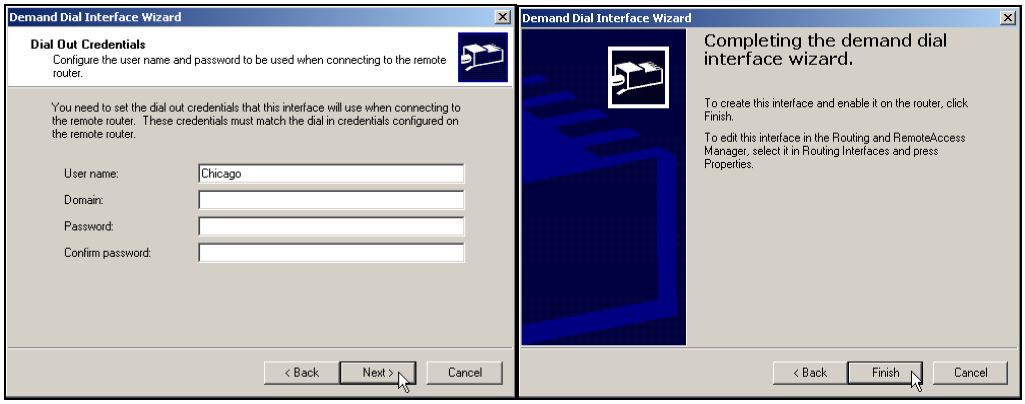


© Train Signal, Inc., 2002-2003

7. On the Dial in Credentials screen, verify the user name, **Cleveland**, which the Chicago VPN server is using as it's dial out credential. Make sure to leave the password field and confirm password field **blank** and click **Next** to continue.



8. On the Dial out Credentials page, you will specify the user name and password to be used when connecting to the Chicago VPN server. Remember, you have already setup a dial-in credential, Chicago, on the Chicago VPN server. In the User name field enter **Chicago** and leave the rest of the fields blank. Click **Next** to continue. Click **Finish** on the last screen of the wizard to complete the process of adding the demand dial interface.

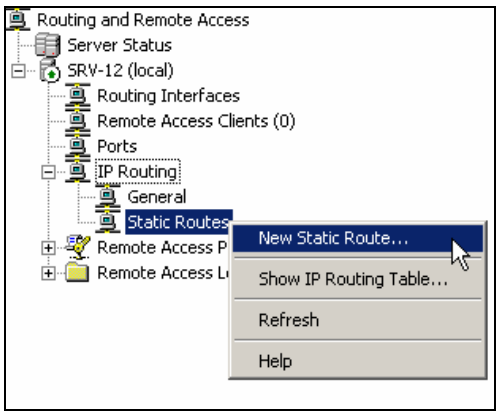


© Train Signal, Inc., 2002-2003

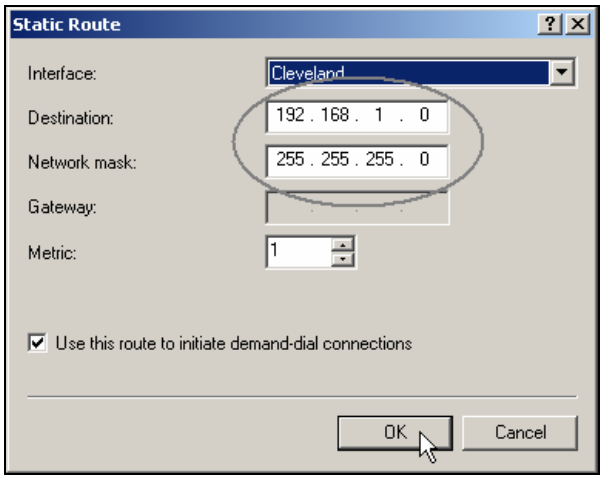
Configuring a static route on the Cleveland VPN server

In order to allow network traffic to be forwarded from the Cleveland to Chicago, just like on the Chicago VPN Server, you will need to configure a static route.

1. On **SRV-12**, in the left pane of the Routing and Remote Access console, double click on **IP routing** and right click on **Static Routes.** Select **New Static Route**.



2. This will bring up the Static Route dialog box. Make sure that **Cleveland** is selected as the interface. This demand-dial interface will be used to forward network traffic to the Chicago site. You will also need to configure the destination and the network mask. The destination will be the route corresponding to the Chicago network, which is 192.168.1.0. The subnet mask should be set at 255.255.255.0. Also, be sure that **Use this route to initiate demand-dial connections** is checked. When your configuration matches the screen shot below, click **OK** to create the Static Route.

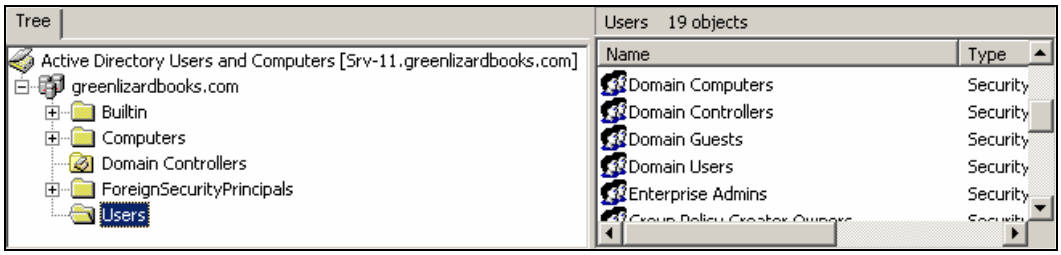


© Train Signal, Inc., 2002-2003

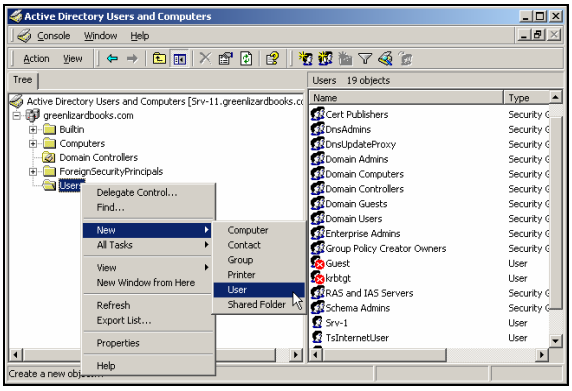
Service Accounts for the VPN servers

You now have to set up service accounts on each VPN Server. Service accounts are used when a demand-dial connection is initiated and one VPN server needs to authenticate to the other VPN server. These service accounts (one for each VPN server) are created like normal user accounts, within Active Directory or within Local Users and groups, if your VPN servers are not part of a domain.

1. To create these two user accounts, log on to **SRV-11**, your domain controller, and open the **Active Directory Users and Computers** console by going to **Start→Programs→Administrative Tools→Active Directory Users and Computers**. In the left pane of the console, open the container named **Users**.

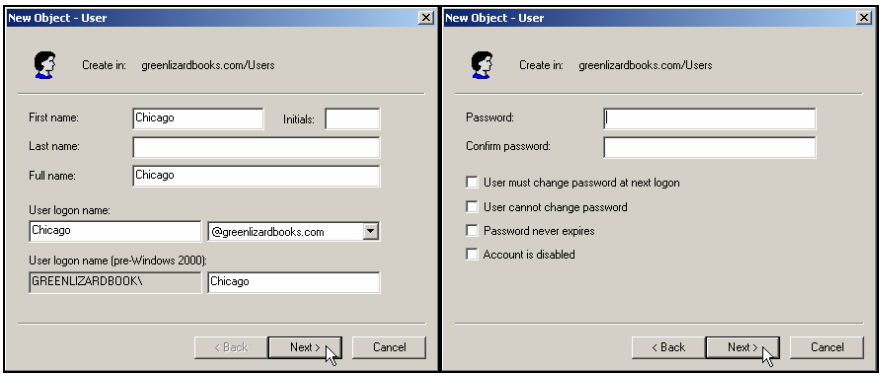


2. To create a user account, right click on the **Users** container in the left pane and select **New→User**.

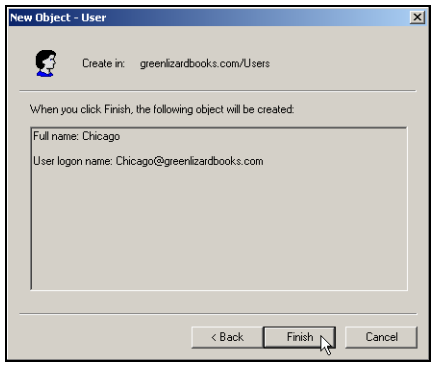


© Train Signal, Inc., 2002-2003

3. This will bring up a wizard for creating a new user. On the first screen, type in **Chicago** as the first name and **Chicago** as the user logon name, click **Next**. On the next screen, just leave the password and confirm password fields **blank** and click **Next**.



4. The final screen is just a summary of all the information that you entered in the wizard. Confirm that the information is correct and click **Finish** to complete the process of adding the Chicago VPN Service account.

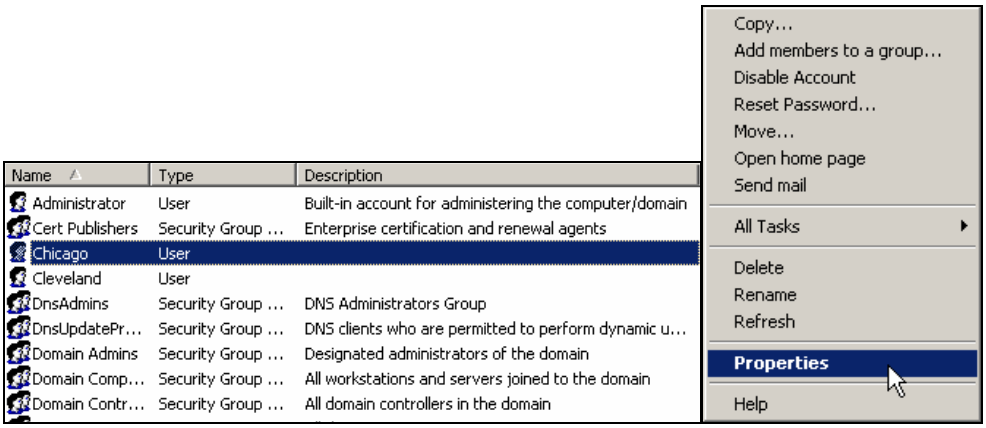


5. From Srv-11 still, repeat these same steps within Active Directory to create a VPN service account named **Cleveland**.

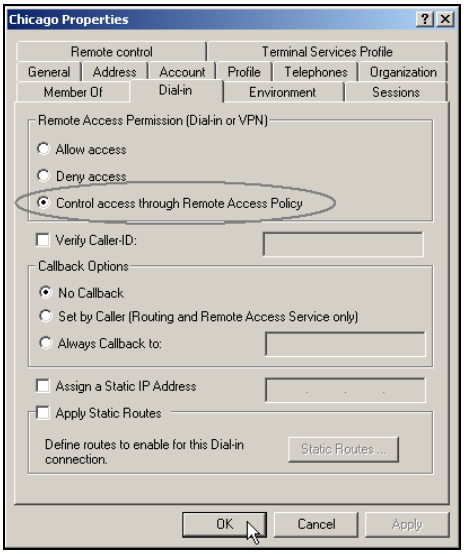
*****Please Note*****
It is very important that the account names of these VPN service accounts match the account names that were entered when you set up the demand-dial interfaces.

© Train Signal, Inc., 2002-2003

5. In order to allow remote access for both VPN service accounts, you need to configure their dial-in permissions. Right click on **Chicago** in the right pane and select **Properties**.

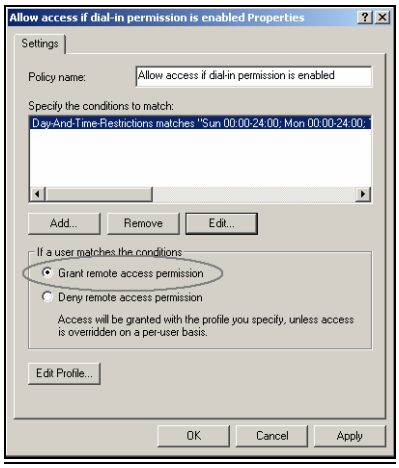


6. This will bring you to the Chicago Properties dialog box. In the Dial-in tab, select **Control access through Remote Access Policy** under Remote Access Permission (Dial-in or VPN). You will be controlling remote access through Remote Access policy on the Chicago RRAS server. Click **OK** when you are done with the configuration. **Repeat** the same steps to configure the remote access permission for the **Cleveland** service account as well.



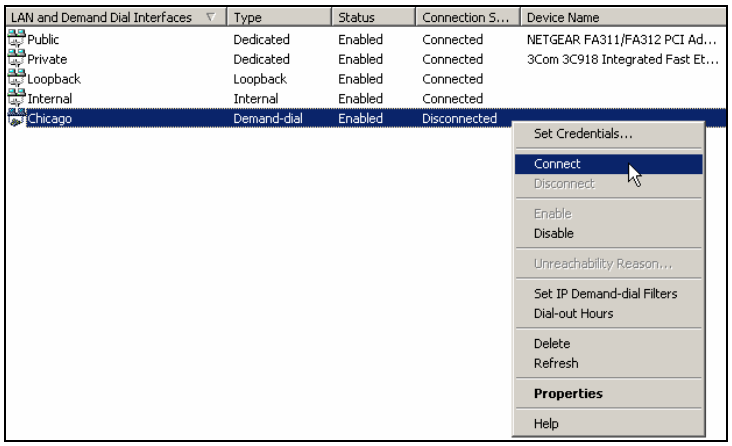
© Train Signal, Inc., 2002-2003

7. Since **control access through Remote Access Policy** was specified, you will want to make sure you grant remote access in the default remote access policy on **both** VPN servers. Log on to **SRV-1**, your Chicago VPN server, and **open Routing and Remote Access** by going to **Start→Programs→Administrative Tools→Routing and Remote Access**. Double click the **default remote access policy**, which will bring you to its properties. Verify that the **Grant remote access permission** is set and click **OK** to close the default remote access policy. Log on to **SRV-12**, your Cleveland VPN server and **repeat the same steps** to verify the permission of the default RAS policy.



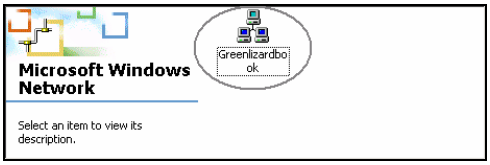
8. At this point, you have completed all of the configurations necessary for the Site-to-Site VPN connection and it should now be functional.

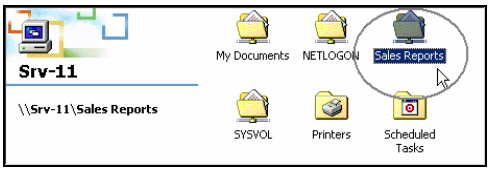
   To establish a Site-to-Site VPN connection, on either VPN server, right click on the **demand-dial interface** and select **Connect** to establish the connection.

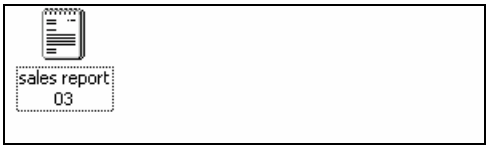


© Train Signal, Inc., 2002-2003

9. Also, since this is a demand-dial connection, a VPN session will automatically be established as you try to access files in one site from another. In Lab 1 you created a file named sales report in a shared folder on the domain controller, SRV-11. You can now test access to this sales report file that you shared in the Chicago from Client-1 in Cleveland. To accomplish this, Log on to **Client-1**, double click on **My Network Places,** click on the **Entire Network**, click on **entire contents,** click on the **Microsoft Windows Network**, double click on the **Greenlizardbooks domain**, double click on **SRV-11**, double click on the **Sales Reports** folder, double click on the **sales report 03** file and you should be able to view the contents of this file. Keep in mind that communication is taking place across the simulated Internet and that it is encrypted.







© Train Signal, Inc., 2002-2003