



TunnelBuilder® for Mac

User's Guide

Copyright © 1997-1999 by Network TeleSystems, Inc.
Printed in the United States of America. All rights reserved.

Trademarks

Shadow IPserver, Shadow IPmanager, Shadow IPclient, TunnelMaster, are trademarks and TunnelBuilder, IPcentral and TCP Pro are registered trademarks of Network TeleSystems, Inc. All other trademarks or trade names that appear in this document are the sole property of their respective companies.



Network TeleSystems, Inc.
550 Del Rey Avenue
Sunnyvale, CA 94086
Voice (408) 523-8100
Fax (408) 523-8118
www.nts.com

March, 1999

TunnelBuilder User's Guide

Contents

Chapter 1: About TunnelBuilder for Mac.	1 - 1
TunnelBuilder Overview	1 - 1
System Requirements	1 - 3
Chapter 2: Installing TunnelBuilder.	2 - 1
Configuration Information	2 - 1
Installing the TunnelBuilder Files	2 - 1
Install Log File	2 - 3
Chapter 3: Configuring and Using TunnelBuilder's LAN Capability	3 - 1
Control Strip Modules	3 - 1
Setting up the TCP/IP Control Panel	3 - 1
Setting up the AppleTalk Control Panel.	3 - 3
Setting Up the LAN TunnelBuilder Settings Control Panel	3 - 4
Connecting To a PPTP/L2TP Server.	3 - 7
Connect using the Settings panel.	3 - 7
Connect using the Control Strip.	3 - 7
Using SecurID Authentication	3 - 8
The Log Window	3 - 10
The Info Window	3 - 13
Using the Location Manager	3 - 15
Installing the Location Manager module	3 - 15
Configuring LAN TunnelBuilder settings in Location Manager	3 - 15
Additional Information	3 - 16
Encryption and Decryption.	3 - 17
Getting Disconnected	3 - 17

Chapter 4: Configuring and Using TunnelBuilder's Dial-up (Remote) Capabilities . . .	4 - 1
Setting up Your Connection	4 - 1
Setting up your MacTCP or TCP/IP control panel	4 - 1
Setting up the MacTCP control panel	4 - 1
Setting up the TCP/IP control panel	4 - 3
Setting up the Network or AppleTalk Control Panel	4 - 4
Setting up the Network control panel	4 - 5
Setting up the AppleTalk control panel.	4 - 6
Setting Up Your First Configuration.	4 - 7
Tunneling AppleTalk.	4 - 12
Using SecurID Authentication	4 - 12
Connecting To a Remote Access Server	4 - 15
Creating and Using Other Configurations	4 - 16
Selecting an existing configuration	4 - 17
Switching Connections	4 - 17
Tearing Down the Tunnel	4 - 18
Changing VPN Information	4 - 18
Thank You!	4 - 18
Further support, and product comments	4 - 18
Appendix A: Using Ping	A - 1
Saving Ping Data	A - 2

Chapter 1 About TunnelBuilder for Mac

TunnelBuilder™ for Mac, coupled with TunnelMaster™ or another PPTP/L2TP server, gives you secure connections from any Macintosh through the Internet to your company's private network.

This chapter describes TunnelBuilder and the system requirements for installing it. To install TunnelBuilder, see Chapter 2.

TunnelBuilder Overview

TunnelBuilder is communications software that lets you establish a secure connection to a private LAN (Local Area Network) over a standard, non-secure connection to the Internet.

For example, if you telecommute from a site that has a LAN (including Cable Modem or xDSL), you can access your company's LAN by securely opening a tunnel to your company's PPTP/L2TP server. If you have a dial up connection, either from home or while on the road, use TunnelBuilder to make your Internet connection and build a tunnel to your office.

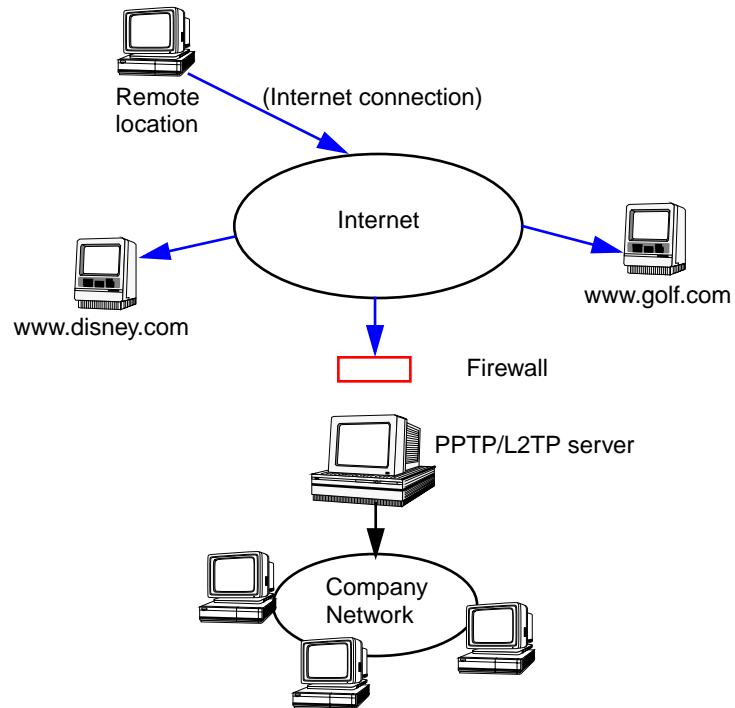
TunnelBuilder uses your Internet connection as a carrier for the private information destined for your company's LAN. All data is encrypted and encapsulated using a PPTP (Point-to-Point Tunneling Protocol) or L2TP (Layer 2 Tunneling Protocol) tunnel and carried inside standard IP packets which are sent to (and decrypted and forwarded by) the server.

You can access file servers, printers, and private Web pages just as if you were directly connected to your company LAN. Moreover, you can access your company network resources with complete confidence that your connection and your company's network are secure.

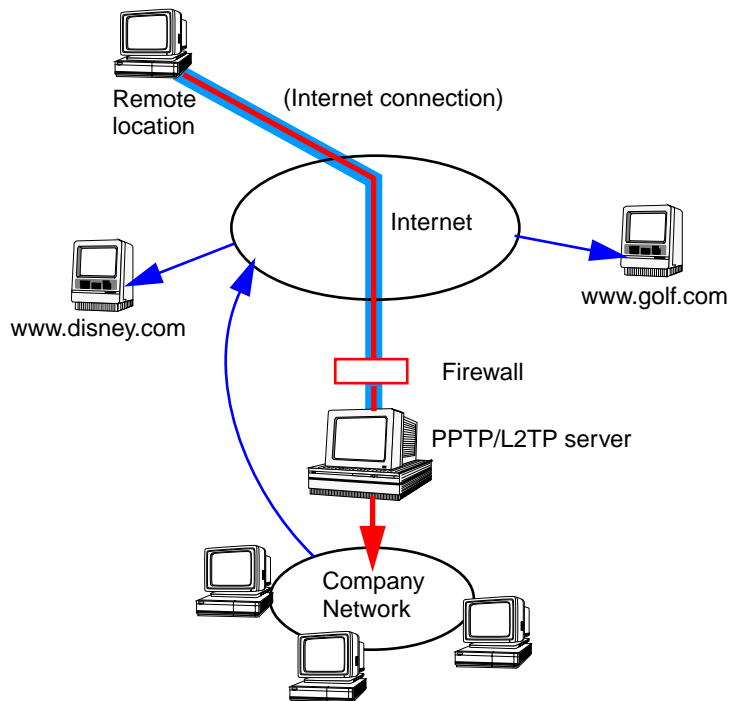
Both PPTP and L2TP as implemented in TunnelBuilder use RC-4 encryption. This kind of encryption is extremely secure, because the "key" to unlock the encrypted code changes regularly. In fact, when used with TunnelMaster™, the PPTP/L2TP server available from NTS, the key is exchanged every packet. So even if someone were able to capture the traffic, they would have to break the packets out of the tunnel and then break the "key." If they were successful at breaking a key, they would still have only a small part of the traffic. This is something like passing someone else on a sidewalk and hearing two or three words of their conversation.

The international version (can be distributed worldwide) of TunnelBuilder uses encryption keys that are 40-bits in length. The domestic version (can be distributed in the U.S. and Canada to citizens or resident aliens) uses encryption keys that are 128-bits in length.

The following illustration shows an example of a typical connection. In this example, the remote user is not working but is instead visiting websites for recreation. There is access to the Internet, but no access to the company's private LAN.



When the remote user is ready to do some work, he or she opens a tunnel to the server on the company network. This is shown in the following illustration.



In this example, the user has built a tunnel through the Internet to the PPTP/L2TP server that is attached to the company network. Note that all traffic is going through the tunnel, which helps ensure privacy. The user can still access favorite websites but now does so through the company's access to the Internet.

System Requirements

To use TunnelBuilder, you must:

- Install the TunnelBuilder software.
- Set up an appropriate user account on your company's PPTP/L2TP server.
- Have LAN connectivity.
- Know the IP address of the PPTP/L2TP server.

The parameters that TunnelBuilder uses to secure the PPTP/L2TP connection (tunnel) are learned during negotiations at the creation of the

tunnel. They do not require any installation or configuration procedures. TunnelBuilder automatically encrypts all data sent through the tunnel.

Before you install the TunnelBuilder software, be sure your system meets these requirements:

- Mac OS-compatible computer with 68030 processor or later
- Mac OS version 7.1 or later (version 7.5 or later recommended)
- Open Transport 1.0.8 or later (1.1.2 or later recommended)
- 8 megabytes (MB) of RAM (16 MB recommended)
- 6 MB of available hard disk space

Note: If you are not currently using Open Transport, it will require independent installation. If installed, Open Transport requires an additional 4MB of available hard disk space.

To install TunnelBuilder, see Chapter 2.

Chapter 2 Installing TunnelBuilder



To install TunnelBuilder, you must complete the following installation tasks:

- Install the TunnelBuilder files.
- Set up your Macintosh computer's Open Transport to use TunnelBuilder.
- Set up the TunnelBuilder Settings Control Panel.

In addition, you must have "LAN" connectivity, such as is obtained through a Cable Modem connection, xDSL, or simply being physically connected to a Local Area Network. You also need an appropriately configured user account on the PPTP/L2TP server you will use as the remote end of the tunnel.

After you complete the procedures in this chapter, see your network administrator for information about setting up your user account on the PPTP/L2TP server.

Configuration Information

After you install the software, you will need to have certain configuration information to complete the setup. This includes the IP address or the domain name of the PPTP/L2TP server you wish to connect through. After you set up your configuration and save it using the TunnelBuilder Settings panel, you then can click a single button to make a connection.

If you wish, you can set up and save a different configuration for each network or server you access.

Installing the TunnelBuilder Files

Before you begin installation be sure to save any documents you're working on, because at the end of the installation you'll need to restart your computer. Also, turn off any virus detection software because it could interfere with the installation process.

Note: You can temporarily turn off Virus detection tools (and all other extensions) during start-up by holding down the Shift key.

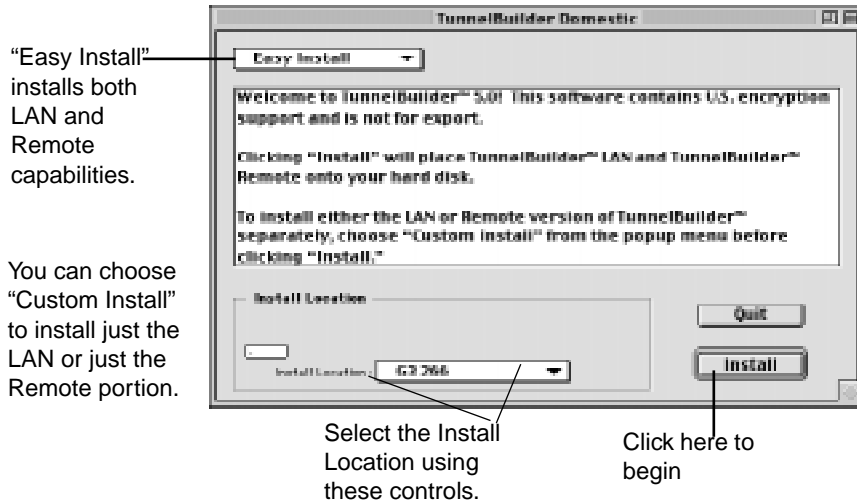
1. Double-click the TunnelBuilder Installer icon.



TunnelBuilder International

2. When you see the TunnelBuilder screen, click Continue.

The Install dialog box appears.



3. Select the Install Location by using the controls provided.

If you have multiple hard disks, a button will appear that says Switch Disk, along with a pop-up menu showing the available hard disks and the option to select a folder.

If you have a single hard disk, a button will appear that says Select Folder.

Whether you select a hard disk or a folder on a hard disk, TunnelBuilder will create its own folder within the disk or folder you select. The folder name created by TunnelBuilder is simply "TunnelBuilder." TunnelBuilder installs the applications you selected in the TunnelBuilder Folder.

4. To install both of the TunnelBuilder applications (Remote and LAN), click Install.

If you wish to install only one application or the other, select Custom Install, check the box for either LAN Only or Remote Only, then click Install. Checking both boxes is the same as Easy Install.

5. Follow the instructions that appear on the screen.

After the software is installed, a dialog box may appear asking you to restart your computer.



6. Click **Restart**.

Your computer automatically restarts. The TunnelBuilder installation is complete.

Note: Remember to turn on any virus detection software you turned off earlier. You are now ready to set up your connection.

Install Log File

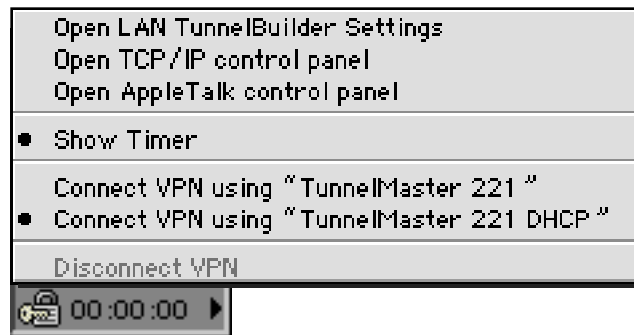
The installation will automatically create an Install Log File and place it in the LAN TunnelBuilder folder. This file can be opened with any text editor, and it will tell you exactly which components have been installed and into which locations.

Chapter 3 Configuring and Using TunnelBuilder's LAN Capability

Now that you have successfully installed the files, a few minutes of orientation and setup are all you'll need to build a tunnel.

Control Strip Modules

If you use the Control Strip, you will notice that two Control Strip Modules were installed. Using these modules will make the following steps easier and will greatly ease your ability to connect to a VPN server. Clicking the LAN TunnelBuilder control strip module reveals this menu.



Setting up the TCP/IP Control Panel

Because the LAN portion of TunnelBuilder for Mac relies on Open Transport, you will use the TCP/IP control panel to set up your network connection. Any version of Open Transport will work, but we recommend using 1.1.2 or later, and highly recommend 1.3 or later.

Beginning with 1.3, Open Transport has single-link multihoming capability. This allows more than one TCP connection "device" to be loaded at a time (multihoming), though only one can be used at a time (single-link). Also, beginning with OT 1.3, the version of Open Transport

is tied to the version of the operating system. OT 1.3 is only available with and can only be used with Mac OS 8.1.

Note: If you have MacTCP you must upgrade to Open Transport TCP/IP in order to be able to use LAN TunnelBuilder. If you install Open Transport on a Mac OS computer that already has MacTCP installed and configured, Open Transport will use the configuration settings such as the gateway Address and Domain Name Server from MacTCP. You do not need to reenter these settings.

To set up the TCP/IP control panel with information about your connection:

1. Choose Control Panels from the Apple menu.

Note: You may also open the TCP/IP Control Panel from the TunnelBuilder control strip.

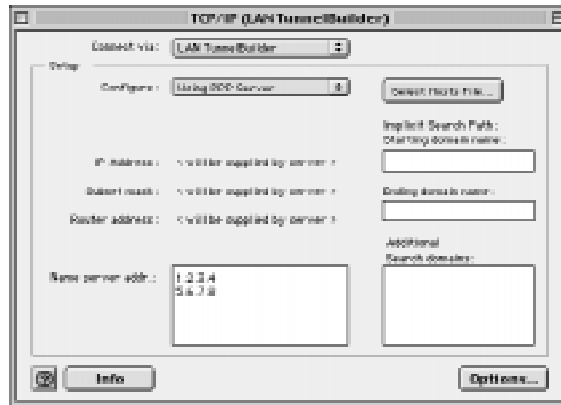
2. Open the TCP/IP control panel.
3. Select Configurations. from the File menu.
4. Make sure Default is selected, then click Duplicate. ...
5. Give the duplicated configuration a unique name such as "LAN VPN" or "Work from home," then click OK .
6. Make sure the new configuration is selected, then click Make Active. This will return you to the TCP/IP Control Panel.
7. Choose TunnelBuilder from the Connect via pop-up menu.

Choose TunnelBuilder from this pop-up menu.



8. In the Configure pop-up menu, "Using PPP Server" will be automatically selected. This is the setting you must use with LAN TunnelBuilder, even if you are using DHCP to connect to the VPN server.

9. Type one or two addresses in the Name server addr.: box. These addresses (also called DNS addresses) are only used as placeholders and are currently required because of a limitation in Open Transport. If you don't have DNS addresses, type in 1.2.3.4 and 5.6.7.8. These addresses will not be used.



Note: Once the tunnel is established, you will be assigned a new and different IP address, gateway and DNS server address(es).

10. Close the control panel (see next Note).

You will be asked if you wish to save the changes you have made. Click **Save** and your new TCP/IP settings will take effect immediately.

Note: Using this method, you can create and save multiple TCP/IP configurations. If you wish to create more configurations now, instead of closing the Control Panel select **Configurations...**. You will still be asked if you wish to save changes you have made, but when you do so you will then be returned to the Configurations screen and the TCP Control Panel will still be open. Settings will not take effect until the control panel is closed.

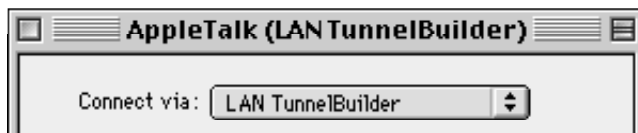
Setting up the AppleTalk Control Panel

Note: As of this writing, the only PPTP/L2TP server which supports tunneling AppleTalk over PPTP or L2TP is TunnelMaster from NTS. It is anticipated that Microsoft, and perhaps others, will support this in the future.

The set up of your AppleTalk Control Panel is very much like the setup of TCP/IP except there is only one setting to make.

1. Open the AppleTalk control panel.

2. Select **Configurations** from the **File** menu.
3. Make sure **Default** is selected, then click **Duplicate...**
4. Give the duplicated configuration a unique name such as "LAN TunnelBuilder," then click **OK**.
5. Make sure the new configuration is selected, then click **Make Active**. This will return you to the **AppleTalk Control Panel**.
6. Choose "LAN TunnelBuilder" from the popup menu.



7. Close the **AppleTalk** control panel. Remember that if you select **Configurations** instead of closing the **Control Panel**, you will still be able to save the changes you have made and then create more configurations.

If you leave the **AppleTalk Control Panel** set to use **Ethernet**, you will still be able to see local **Apple share** resources even though your **IP traffic** will be going through a tunnel. With this configuration you will not, however, be able to see remote **Apple share** resources using **AppleTalk**.

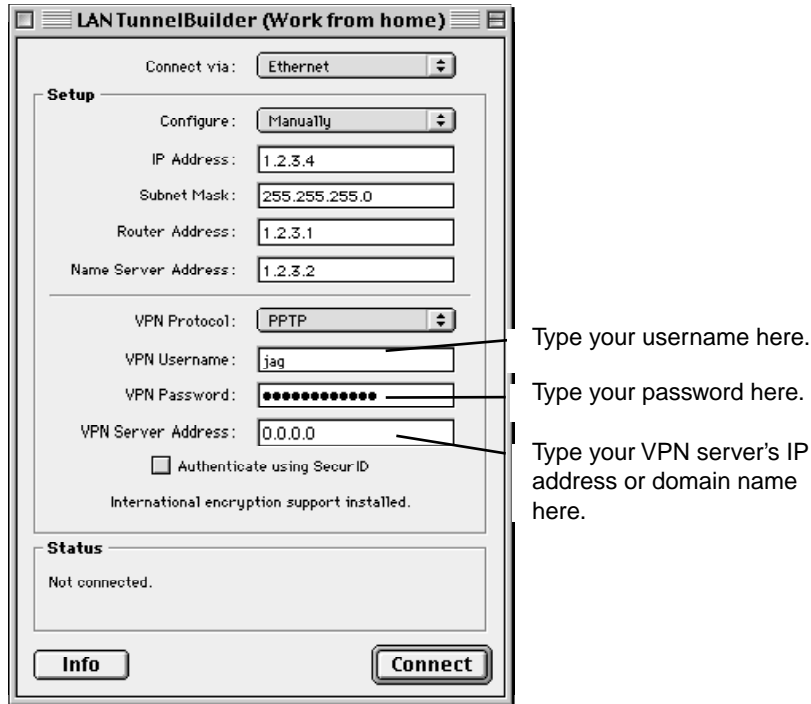
Setting Up the LAN TunnelBuilder Settings Control Panel

You configure the **TunnelBuilder Settings** in exactly the same way you configured the **TCP/IP Control Panel** and the **AppleTalk Control Panel**.



1. Open the **TunnelBuilder Settings** application. Double-click the **TunnelBuilder Settings** icon, or simply open **TunnelBuilder Settings** from the control strip.
2. Select **Configurations** from the **File** menu.
3. Make sure **Default** is selected, then click **Duplicate...**
4. Give the duplicated configuration a new name such as "Work from home," then click **OK**. (This can be the same name used in the **TCP/IP Control Panel**.)
5. Make sure the new configuration is selected, then click **Make Active**. This will return you to the **TunnelBuilder Settings** panel.
6. Enter information. The information asked for in the first half of **Setup** is for the "clear" connection.

- Information in the top half of the settings box can be configured manually (as in the example below) or by using a DHCP server. More details about using DHCP to configure local settings is located at the end of this section.



Note: There are three choices for the VPN protocol, but only PPTP and L2TP are supported in this version of TunnelBuilder. NTS-TP is planned for a future version.

- Enter your VPN server user name.

This is the user name that your system administrator entered for you on the VPN server.

Note: If your PPTP server is an NT server and it is not the Primary Domain Controller, you may need to enter the NTDomain name in front of your user-name in order to be authenticated. The NTDomain is followed by a backslash, as in this example: NTDomain\username.

- Enter your VPN server password.

This is the password that your system administrator entered for you on the VPN server.

10. Enter the IP Address of your VPN Server. You may also use a domain name in place of an IP address.

Note: If you use a domain name, the Name Server listed in the setup information must be able to resolve that domain name.

11. If you wish to create other configurations, choose `Configurations...` from the `File` menu. Otherwise close the settings window.

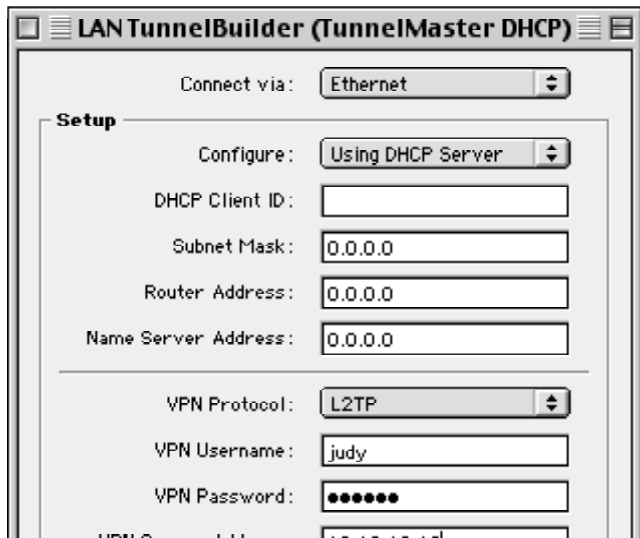
12. Click `Save` when asked if you wish to save changes.

Your configuration is now saved as the active configuration.

Configuring LAN TunnelBuilder settings using DHCP:

Many people use LAN TunnelBuilder on a network that uses DHCP (Dynamic Host Configuration Protocol) servers to assign IP address information. In some cases it is their “home” network, while in other cases they are a guest on another network. At such times it is appropriate to configure LAN TunnelBuilder to obtain its information via DHCP.

To do so, select “Using DHCP Server” in the Configure pop up menu, as in the illustration below.



Select “Using DHCP Server” in the Configure: pop up menu, then enter 0.0.0.0 in the Subnet Mask, Router, and Name Server Address fields, or leave them empty.

When you select Using DHCP Server, either leave the remaining fields blank or enter 0.0.0.0 in the address fields. DHCP Client ID only appears if you have OT 2.0 or later. Your network administrator should instruct you on how to use that special field.

Connecting To a PPTP/L2TP Server

After entering configuration information in the TunnelBuilder Settings window, you are ready to connect to a PPTP/L2TP server.

Connect using the Settings panel

Open the TunnelBuilder Settings window and make sure that the Configuration you have selected is correct. If it is not correct, select Configurations. from the File menu, then choose the correct configuration and activate it.

Click Connect, and within a few seconds the connection should be complete. Note that while the connection is being completed the Connect button is grayed out. Before, during, and after the connection, information about the connection is displayed in the Status section of the Settings window.

Once a connection is complete, the Connect button becomes the Disconnect button. To disconnect, simply click the Disconnect button.

Connect using the Control Strip

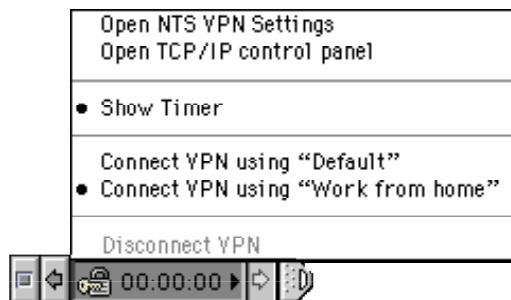
When you install TunnelBuilder on a Macintosh that uses the Control Strip, a Control Strip module will be installed automatically.



Control Strip module with timer shown.

The Control Strip module will allow you to connect using various configurations, disconnect, open the Settings panel, open the TCP/IP control panel, and either show or hide the timer.

To connect in this way, click and hold the Control Strip module to view a list of options.



Currently selected items have a bullet beside them. Simply make your selection, release the mouse button, and your selection will be invoked.

Note: When no connection is active, the Disconnect option will be grayed out. Conversely, when a connection is active all the Connect choices will be grayed out.

If you selected one of the “Connect” configurations, the Control Strip menu will close, and as soon as the connection is complete the appearance of the module will change to indicate an active connection.



Red arrows indicate an active connection. When the timer is shown (right) it increments in one second intervals when a connection is active.

Using SecurID Authentication

TunnelBuilder can be used in conjunction with TunnelMaster to use SecurID authentication in addition to the user authentication (user name and password) that is already done in the connection process. SecurID is “one time” password authentication, which means the password is dynamic in nature and will be used only one time.

In order for SecurID authentication to work, you must be tunneling to a PPTP/L2TP server that supports SecurID. As of this writing, only TunnelMaster from NTS has native support for SecurID. It is anticipated that other vendors of PPTP/L2TP servers will add this capability in the future.

No special configuration is required to enable SecurID. TunnelBuilder will know that the information is required and will prompt you automatically for your SecurID information.

If SecurID is enabled, a log in to a TunnelMaster server will be successful if the configured user name and password are allowed, but further communication through the server will not be allowed until SecurID authentication is completed.

After login, the SecurID user will see this dialog box:

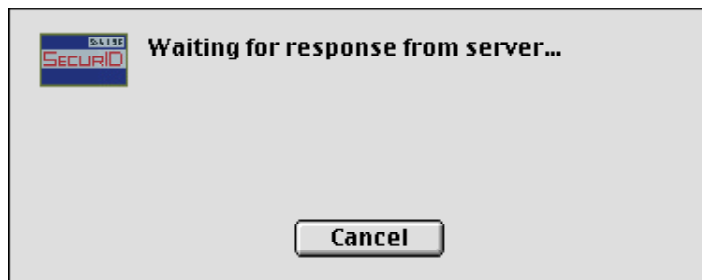


Enter your user name and one time password (Token) and click OK.

Note: Your user name and password will be visible on the screen as clear text. This is to assist in verification that all data has been entered correctly and is not a security risk because the password will immediately expire.

Clicking cancel or entering incorrect data will cause the connection to the PPTP/L2TP server to be lost.

While SecurID authentication is being completed, you will see the following screen:



Followed by:



Clicking OK completes the SecurID process.

The Log Window

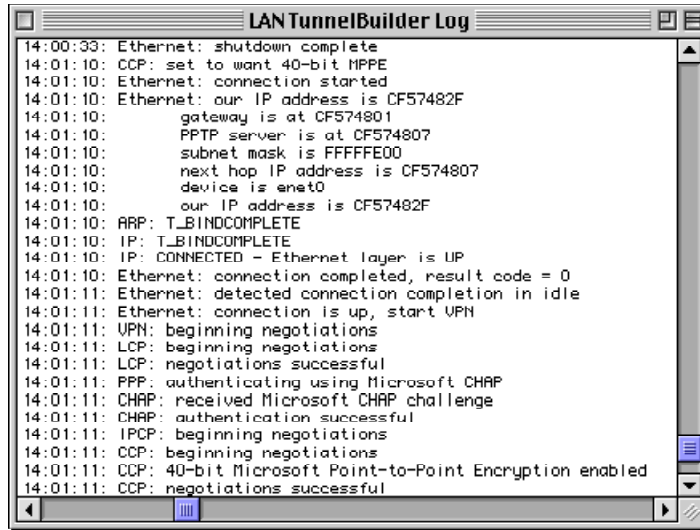
A Log window is available for informational and troubleshooting purposes. It can only be accessed when the TunnelBuilder Settings window is open. The log can be viewed, cleared or saved as a text file.

In order to view the Log window, first open the TunnelBuilder settings window. Next, select Log from the VPN menu, or use the keyboard selection of Command-3.



The Log comes up in a separate window and shows information about the current connection. Unless the Log is cleared, information about previous connections will be stored as well.

Shown below is a typical Log entry for traffic that occurred during a connection.



```

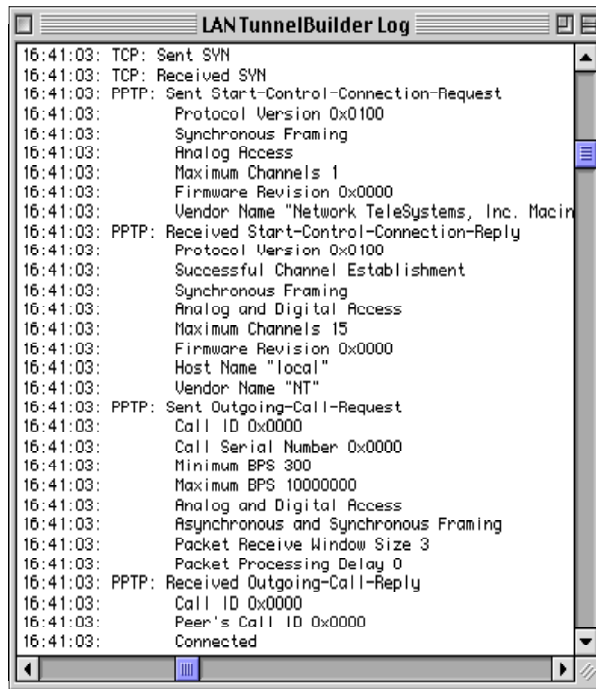
LAN TunnelBuilder Log
14:00:33: Ethernet: shutdown complete
14:01:10: CCP: set to want 40-bit MPPE
14:01:10: Ethernet: connection started
14:01:10: Ethernet: our IP address is CF57482F
14:01:10:     gateway is at CF574801
14:01:10:     PPTP server is at CF574807
14:01:10:     subnet mask is FFFFFFF0
14:01:10:     next hop IP address is CF574807
14:01:10:     device is enet0
14:01:10:     our IP address is CF57482F
14:01:10: ARP: T_BINDCOMPLETE
14:01:10: IP: T_BINDCOMPLETE
14:01:10: IP: CONNECTED - Ethernet layer is UP
14:01:10: Ethernet: connection completed, result code = 0
14:01:11: Ethernet: detected connection completion in idle
14:01:11: Ethernet: connection is up, start VPN
14:01:11: VPN: beginning negotiations
14:01:11: LCP: beginning negotiations
14:01:11: LCP: negotiations successful
14:01:11: PPP: authenticating using Microsoft CHAP
14:01:11: CHAP: received Microsoft CHAP challenge
14:01:11: CHAP: authentication successful
14:01:11: IPCP: beginning negotiations
14:01:11: CCP: beginning negotiations
14:01:11: CCP: 40-bit Microsoft Point-to-Point Encryption enabled
14:01:11: CCP: negotiations successful

```

Note that the connection was initiated at 13:45:55 (1:45 p.m. and 55 seconds) and was completed within seconds.

To get more information about the traffic that is passing back and forth between your client and server, hold down the **option** key before clicking the Connect button. This will give you “verbose” mode, essentially showing you every packet that traverses the connection.

An example of a log output from verbose mode is shown on the next page.



```

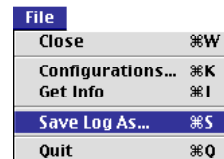
16:41:03: TCP: Sent SYN
16:41:03: TCP: Received SYN
16:41:03: PPTP: Sent Start-Control-Connection-Request
16:41:03:   Protocol Version 0x0100
16:41:03:   Synchronous Framing
16:41:03:   Analog Access
16:41:03:   Maximum Channels 1
16:41:03:   Firmware Revision 0x0000
16:41:03:   Vendor Name "Network TeleSystems, Inc. Macin
16:41:03: PPTP: Received Start-Control-Connection-Reply
16:41:03:   Protocol Version 0x0100
16:41:03:   Successful Channel Establishment
16:41:03:   Synchronous Framing
16:41:03:   Analog and Digital Access
16:41:03:   Maximum Channels 15
16:41:03:   Firmware Revision 0x0000
16:41:03:   Host Name "local"
16:41:03:   Vendor Name "NT"
16:41:03: PPTP: Sent Outgoing-Call-Request
16:41:03:   Call ID 0x0000
16:41:03:   Call Serial Number 0x0000
16:41:03:   Minimum BPS 300
16:41:03:   Maximum BPS 10000000
16:41:03:   Analog and Digital Access
16:41:03:   Asynchronous and Synchronous Framing
16:41:03:   Packet Receive Window Size 3
16:41:03:   Packet Processing Delay 0
16:41:03: PPTP: Received Outgoing-Call-Reply
16:41:03:   Call ID 0x0000
16:41:03:   Peer's Call ID 0x0000
16:41:03:   Connected

```

This example of log in verbose mode show packet details. This can be useful in troubleshooting.

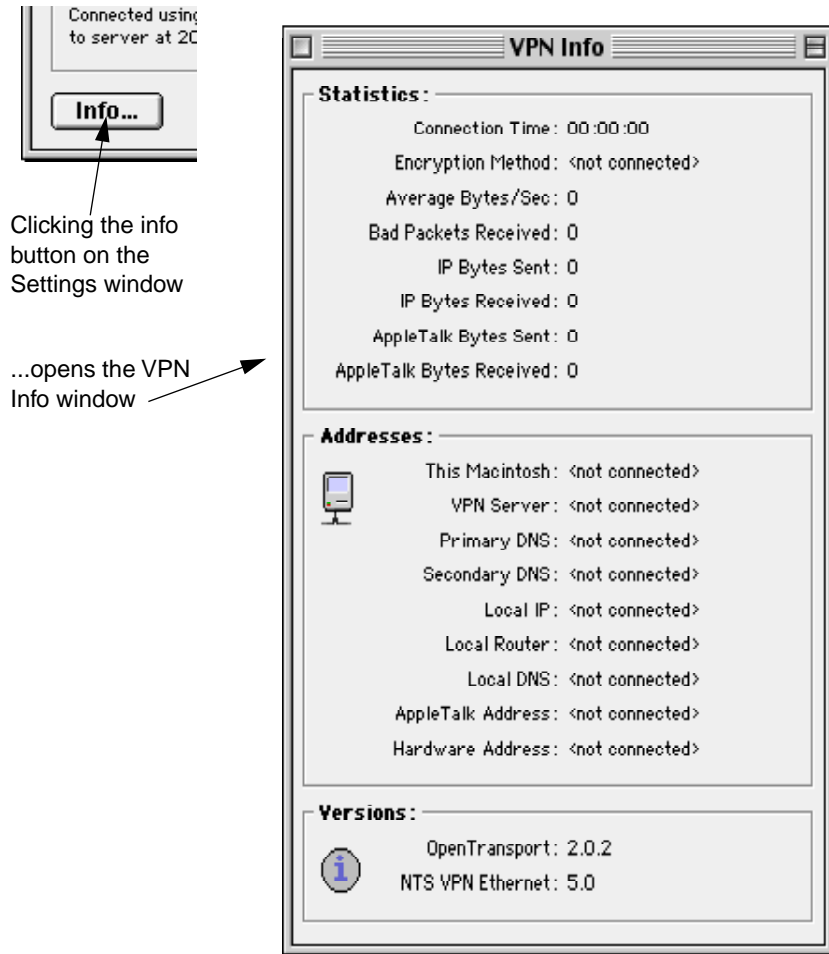
If you wish to save a log:

1. Make the Log window the active window
2. The File menu changes to include a Save Log As...option
3. After selecting Save Log As...,you will be prompted to name the file and select a location for the file
4. The log will be saved and you will be returned to TunnelBuilder.



The Info Window

On the bottom left of the LAN TunnelBuilder Settings window there is an Info... button. Clicking Info... brings up the following display:



Clicking the info button on the Settings window

...opens the VPN Info window

The information given is as follows:

Statistics:

- Connection Time is the time in hours, minutes, and seconds that VPN has been connected.
- Encryption Method is either 40-bit (International) or 128-bit, and

depends on both the capability of the client and the server.

- Average Bytes/Sec is a rough average of the number of bytes sent and received over the last three seconds.
- Bad Packets Received shows the number of bad packets received from the remote host when VPN is connected. Note that it is quite normal to receive a few bad packets at the beginning of a connection.
- IP Bytes Sent shows the total amount of IP traffic out in bytes.
- IP Bytes Received shows the total amount of IP traffic that has come in. Shown in bytes.
- AppleTalk Bytes Sent shows the total amount of AppleTalk traffic out in bytes.
- AppleTalk Bytes Received shows the total amount of AppleTalk traffic that has come in. Shown in bytes.

Addresses:

- This Macintosh is the address assigned to this Mac by DHCP or configured manually by the user. (Non-tunneled address.)
- VPN Server is the address of the VPN Server to which you are connected
- Primary DNS Address and Secondary DNS Address are those assigned by the remote host when VPN is connected.
- Local IP is the address assigned to this Mac by the remote host when VPN is connected.
- Local Router is the gateway assigned to this Mac by the remote host when VPN is connected.
- Local DNS is the name server assigned by the remote host when VPN is connected.
- AppleTalk Address is the AppleTalk address assigned by the remote host when VPN is connected.
- Hardware Address is the MAC (Media Access Control) address of this Macintosh.

Using the Location Manager

If you are using a Mac OS that supports Location Manager 2.0 or greater, you can take advantage of an additional module that is installed with TunnelBuilder.

Location Manager is a Control Panel utility supplied by Apple that simplifies switching configurations. Designed originally for PowerBooks, Location Manager now works on desktop machines as well.

Note: A number of different items are configurable within Location Manager, and it is beyond the scope of this document to describe them. For more information on Location Manager or to download the latest version of Location Manager, visit Apple's web site at www.apple.com.

Installing the Location Manager module

When you installed TunnelBuilder, a folder called LAN TunnelBuilder for Mac OS was installed on the destination drive. Inside that folder is a file called "LAN TunnelBuilder Loc Module." This module belongs in the Location Manager folder, which is in the Extensions folder (in the System folder). Simply drag and drop the module into the Location Manager folder then restart.

Configuring LAN TunnelBuilder settings in Location Manager

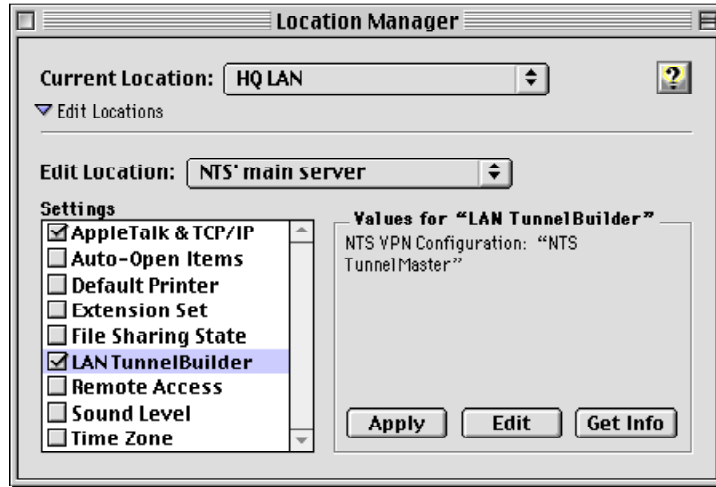
TunnelBuilder settings are not editable from within Location Manager. To ensure that you have the configuration you desire, make sure that configuration is active. To do so:

1. Open the TunnelBuilder Settings panel.
2. Open the `Configurations`.window.
3. Select the Configuration you wish to invoke in the Location Manager setting and make it active.

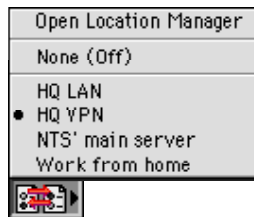
You can now open Location Manager and create a new configuration.

4. Open the Location Manager control panel.
5. Select LAN TunnelBuilder in the list of parameters.
6. Review the values for LAN TunnelBuilder, and if they are the ones you want, click Apply. (If they are not, repeat steps 1 – 3 above.)

An example is shown in the following illustration:



To activate a location, select the location from the Control Strip, or open Location Manager and change the location in the pop-up menu.



Though it may take a few minutes to set up Location Manager initially, this handy utility will make it very simple for you to switch back and forth between a LAN connection and a tunneled (VPN) LAN connection.

Additional Information

If you are new to the world of Virtual Private Networking, and even if you are not, the following information may be useful to you.

Encryption and Decryption

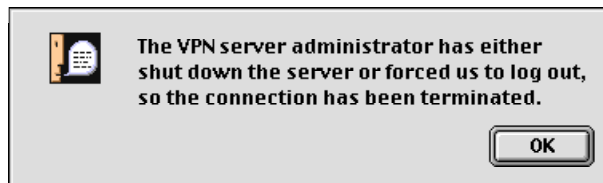
TunnelBuilder uses RC-4 encryption (as described in Chapter 1). While encryption is the feature that makes the transmission of data through the Internet secure, it is also the feature that makes the transmission of data slightly slower.

In our performance testing we have determined that:

- Because processing power is required for encryption/decryption, “faster” machines provide an advantage in doing PPTP/L2TP. However, unless you are sending and receiving very large files the speed differential is probably not significant enough to cause you to purchase the latest machine.
- Stronger encryption gives slower performance than weaker encryption. This is because a longer key length requires more processing.
- The more you write to a log, the slower the performance will be. Therefore connecting without using verbose mode is faster than with verbose mode.
- Network activity can slow down performance.
- The trade-off between security and performance is a personal (or corporate) decision.

Getting Disconnected

If you are using an NT server to terminate your PPTP traffic, you should be aware that the server has a default inactivity time out setting of 20 minutes. If you are not actively transmitting or receiving data when you reach that threshold, you will get a message like this:



Ask your network administrator to change this setting if it becomes problematic for you. If you are using TunnelMaster as your VPN server, you should be aware that the amount of time you will be allowed to stay connected may be controlled by your system administrator. The default is for unlimited connectivity.

If you have selected TunnelBuilder as your connection method, either through the TCP/IP control panel or through Location Manager, you must first connect before you will be able to use Internet applications. If you invoke an Internet application without connecting first, you will get the following message:



Chapter 4 Configuring and Using TunnelBuilder's Dial-up (Remote) Capabilities

Setting up Your Connection

To use Remote TunnelBuilder, you will need to connect to an ISP using a modem. Therefore, you need to set up your MacTCP or TCP/IP control panel with information from your service provider.

If you are using AppleTalk over PPP, you will also need to set up your Network or AppleTalk control panel.

Setting up your MacTCP or TCP/IP control panel

Your Mac OS computer uses either the MacTCP or TCP/IP control panel to set up your network connection. Look in your Control Panels folder to determine which control panel you have.

If your Macintosh uses what is sometimes referred to as “classic” networking, you’ll find the MacTCP control panel. Follow the procedure in “Setting Up the MacTCP Control Panel.”

If your Macintosh uses Open Transport networking, you’ll find the TCP/IP control panel. Follow the procedure in “Setting Up the TCP/IP Control Panel” given later in this chapter.

Should you use MacTCP or Open Transport TCP/IP? We highly recommend Open Transport for its stability. For more details, see the Read Me file on the installation disk or in the Remote TunnelBuilder Folder.

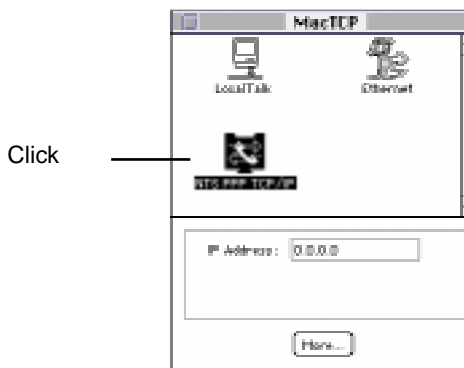
Note: If you are using Open Transport, you must use version 1.1.2 or later.

Setting up the MacTCP control panel

If you are using the MacTCP control panel, follow this procedure:

1. Choose Control Panels from the Apple menu.
2. Open the MacTCP control panel.

3. Click on NTS PPP TCP/IP so it is selected (highlighted).



NTS PPP TCP/IP is the protocol you use, although other icons may also appear.

If other PPPs are installed, they will also appear to be selected. This is a behavior of the MacTCP software and does not mean that all the PPPs are selected.

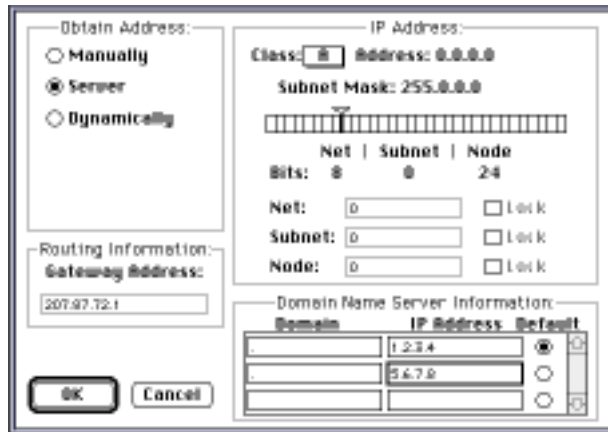
4. Click More.

Next, enter your MacTCP setup information. Refer to Table 1 on page 8 for the information to enter.

5. Select Manually and type your Gateway Address in the Gateway Address box.
6. Select Server. You must do this only after you have selected Manually and entered the Gateway Address.
7. Indicate your Subnet Mask by sliding the handle above the bar.
8. Select the address class using the Class popup dialog.
9. Type a period (.) in the Domain box for the Primary DNS server and Secondary DNS server (one period in each box).
10. Type "1.2.3.4" in the first IP Address box and "5.6.7.8" in the second IP Address box.

Note: Although you must enter IP addresses for a primary and secondary domain name server in the MacTCP control panel, these are only placeholders for the real DNS addresses you will configure in the NTS PPP Dialer. Therefore, you can use any two distinct values (such as "1.2.3.4" and "5.6.7.8"). See "Setting Up Your First Configuration" on page Chapter 4 - 7.

Your dialog box should look similar to the one shown here:



11. Click OK.
12. Close the MacTCP control panel.
A message prompts you to restart your computer.
13. Restart your computer.
Your MacTCP settings take effect after you restart.

Setting up the TCP/IP control panel

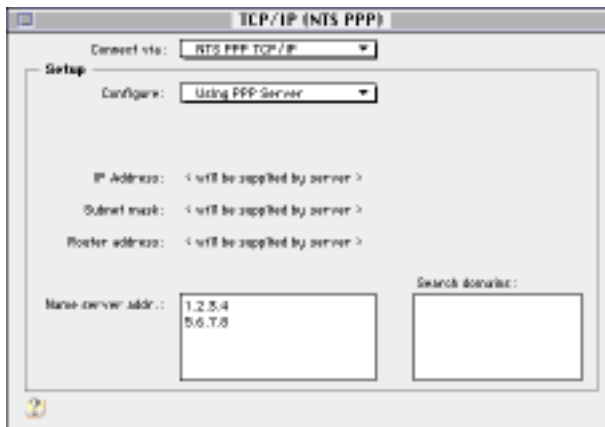
If your Macintosh uses Open Transport (see the note under Table 1 for system requirements), you must set up the TCP/IP control panel with information about your connection.

Note: If you are using Open Transport, you must use version 1.1.2 or later. Open Transport is not included in the Remote TunnelBuilder package and has its own installation procedure.

Note: If you install Open Transport on a Mac OS computer that already has MacTCP installed and configured, Open Transport will use the configuration settings such as the gateway Address and Domain Name Server from MacTCP. You do not need to reenter these settings.

1. Choose Control Panels from the Apple menu.
2. Open the TCP/IP control panel.
3. Choose NTS PPP TCP/IP from the Connect via pop-up menu.
4. Choose Using PPP Server from the Configure pop-up menu.

5. Type in any IP addresses in the IP Address boxes for the Domain Name Servers. The addresses do not need to be valid. They just need to be expressed in dotted-decimal notation (x.x.x.x).



Note: Although you must enter IP addresses for a primary and secondary domain name server in the TCP/IP control panel, these are only placeholders for the real DNS addresses you will configure in the NTS PPP Dialer. Therefore, you can use any two distinct values (such as “1.2.3.4” and “5.6.7.8”). See “Setting Up Your First Configuration” on page 7.

6. Close the control panel.

Your TCP/IP settings take effect immediately.

Note: You can create and save multiple TCP/IP configurations. To create and save a configuration, use the procedure above. To select a saved configuration, use Configurations... from the File option in the TCP/IP control panel.

Setting up the Network or AppleTalk Control Panel

As of this writing, only TunnelMaster from NTS supports tunneling AppleTalk over PPTP/L2TP. Instructions on how to enable that feature are included later in this chapter. (See “Tunneling AppleTalk” on page 12.)

Whether or not you are using TunnelBuilder to tunnel AppleTalk, you may want to use the NTS PPP Dialer to connect to a remote access server that supports AppleTalk over PPP. In either event, use the following procedure to set up AppleTalk for NTS PPP.

After you set up your MacTCP and have restarted your computer, or after you set up TCP/IP (Open Transport) control panel, you need to set up either your Network or AppleTalk control panel.

If you are using MacTCP, you need to set up the Network control panel. Use the procedure below.

If you are using TCP/IP (Open Transport), you need to set up the AppleTalk control panel. Use the procedure beginning on page 6.

Setting up the Network control panel

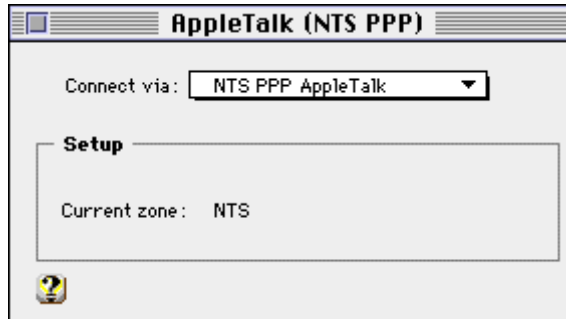
1. Choose Control Panels from the Apple menu.
2. Open the Network control panel.
3. Click on NTS PPP so it is selected (highlighted).



4. Close the Network control panel and proceed to the “Setting Up Your First Configuration” on page 7.

Setting up the AppleTalk control panel

1. Open the AppleTalk control panel.
2. Choose “NTS PPP AppleTalk” from the popup menu.



3. Close the AppleTalk control panel.

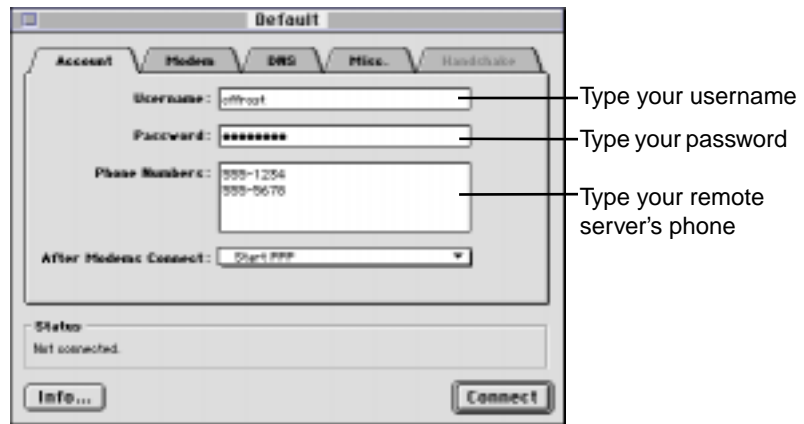
Note: You can create and save multiple AppleTalk configurations. To create and save a configuration, use the procedure above. To select a saved configuration, use Configurations... from the File option in the AppleTalk control panel.

Setting Up Your First Configuration

You configure the NTS PPP Dialer by entering information in the PPP configuration window. When the PPP configuration window first opens, it is blank and you can enter the configuration information NTS PPP should use to initiate a connection.

1. To open the NTS PPP Dialer application, double-click the NTS PPP Dialer icon.

The Default window appears.



2. Type your ISP username and password in the boxes, if necessary.
3. Type the phone number of the ISP server in the Phone Numbers box.

You can enter phone numbers longer than the width of the box. In addition, you can enter more than one phone number. Separate each phone number by pressing the Return key.

Type the phone number just as you would dial it from your current location. For example, if you dial 1 before your area code or dial 9 to access an outside line, enter these numbers accordingly.

If you'll be using a telephone calling card, enter the telephone numbers and calling card numbers exactly as you would dial them.

If dialing the numbers requires a pause to establish a connection before continuing to dial, type a comma after a number to create a three-second pause. You can enter multiple commas in a row to create longer pauses, if necessary.

Here is an example:

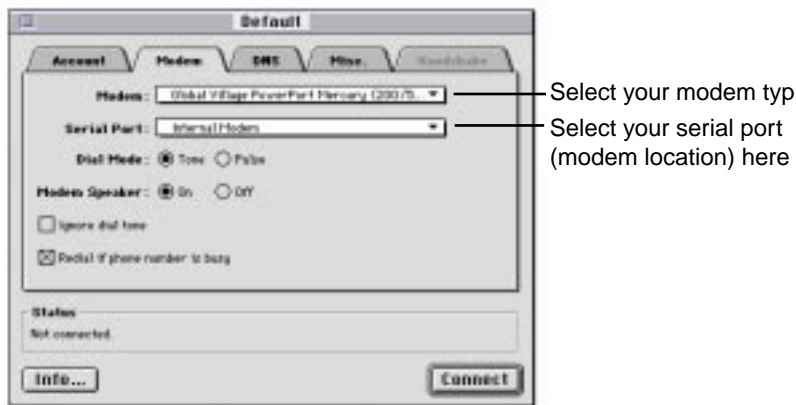
9, 1 800 225 5288, 1, 408 523 8100, 1234567890

4. Choose “Start PPP” from the After Modems Connect pop-up menu, if necessary.

In most cases, this choice is the correct one for making a connection. If you have difficulty establishing a connection, you can choose “Attempt Handshaking Before PPP” from this menu to specify additional log-in information. See your system administrator for such information.

5. Click on the Modem tab.

The Modem area appears.



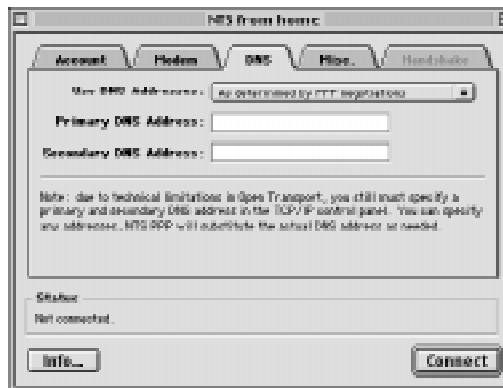
6. Choose your modem type from the Modem pop-up menu.

The menu lists many commonly used modems. If the name of your modem doesn't appear, choose a generic modem type, such as “Generic High Speed.”

Note: You can also create a modem entry or modify a modem string by selecting Modems... from the file menu and using the tools available there.

7. Choose the port to which your modem is connected from the Serial Port pop-up menu, if necessary.
8. Click Tone or Pulse to indicate the type of phone dialing your telephone uses, if necessary.
9. Change the remaining modem options, if you wish:
 - Click On or Off in the Modem Speaker option to turn the modem speaker sounds on or off.

- Click the “Ignore dial tone” checkbox to have the modem attempt dialing immediately when you click Connect without waiting for a dial tone.
 - Click the “Redial if phone number is busy” checkbox to have the Dialer automatically redial the number if it is busy. The Dialer will redial the number three times, waiting 30 seconds between redial attempts. If you have more than one phone number, the Dialer will try them all, wait 30 seconds, then try them all again.
10. Click the DNS tab to set DNS options, if you wish.



11. Choose the source you want NTS PPP to use for the DNS server address.

If your remote PPP server supports negotiating for the DNS addresses, we recommend that you select “As determined by PPP negotiations.” Try this option first. If you receive the following warning message after you connect to the remote PPP server, use the DNS tab to enter the addresses manually:

The remote host did not assign this Macintosh a DNS address. The DNS addresses configured in the TCP/IP (or MacTCP) control panel will be used instead.

12. Click the Misc. tab to change miscellaneous options. You may decide not to change some of these options, but you need to set the VPN (Virtual Private Networking) options if you plan to use Remote

TunnelBuilder to connect to a PPTP/L2TP server.



- Click the “Connect automatically when needed” checkbox to have your Internet applications automatically connect to your ISP when you open or use an application that requires Internet access.
When a mark appears in the box, NTS PPP will allow your Internet applications to dial automatically without using the Dialer user interface. If you want to always use the Dialer to establish a connection, do not check this option.
- Click the “Notify me if an illegal automatic connection is attempted” checkbox to have NTS PPP display a message if an Internet application requires TCP/IP services when PPP is not connected.
When a mark appears in the checkbox, NTS PPP is set to notify you if an illegal automatic connection is attempted. If you want to disable the notification messages, deselect this option. For example, you might want to deselect this option if you configure Open Transport TCP/IP to always load at boot time, which causes NTS PPP to attempt to dial the phone if the current TCP configuration is set to use PPP.
- Click the “Notify me if the connection drops unexpectedly” checkbox to have NTS PPP display or not display a warning when your Internet connection is broken.
When a mark appears in the checkbox, the Dialer is set to warn you when your connection is broken. If you don’t want to see this warning, deselect this option.
- Click the “Drop idle connection after” checkbox and enter a number of minutes to specify how long NTS PPP should wait before dropping your connection when it’s not being used.

- Click the “Attempt to negotiate for AppleTalk” checkbox if you want NTS PPP to attempt to negotiate to support AppleTalk over PPP when connecting to the remote host.

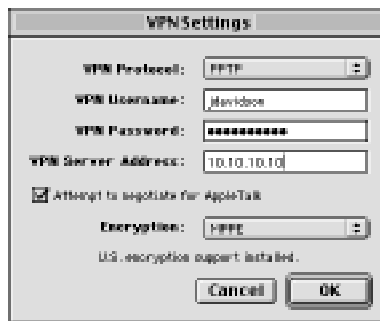
When a mark appears in the checkbox, the Dialer is set to attempt to negotiate for AppleTalk. The dialed remote access server must support AppleTalk over PPP for this feature to work.

Note: This checkbox deals only with PPP. Checking it will not enable the tunneling of AppleTalk using PPTP/L2TP.

- Click the “Start virtual private networking after connecting” checkbox if you want TunnelBuilder to automatically attempt to build a tunnel to your company’s PPTP/L2TP server as soon as the Dialer has established the connection to your ISP.

When a mark appears in the checkbox, the Dialer is set to attempt to establish the tunnel automatically.

13. Click VPN Settings... to enter your account information for the Windows NT PPTP/L2TP server.



- Select PPTP or L2TP as your VPN protocol. (There are three choices for the VPN protocol, but NTS-TP is not supported in this version of TunnelBuilder.)

Note: If you change VPN settings while the PPP connection is active, you must disconnect from the ISP and reconnect in order for the new settings to take effect.

- Enter your VPN server user name.
- Enter your VPN server password.
- Enter the IP Address or domain name of your VPN Server.
- Select special features by checking the appropriate boxes, as described below:

Tunneling AppleTalk

If you are tunneling to a TunnelMaster server and wish to have access to Apple share resources available on the target network, check the “Attempt to negotiate for AppleTalk” box. Make sure NTS PPP AppleTalk is selected in either your MacTCP network settings or in the AppleTalk Control Panel.

A few seconds after you have established a tunnel you may see a message indicating that AppleTalk services are now available. When you disconnect, you may see a message saying that AppleTalk is no longer available.

Once a connection is properly established, you will be able to access all Apple share resources through the conventional use of the Chooser.

Using SecurID Authentication

TunnelBuilder can be used in conjunction with TunnelMaster to use SecurID authentication in addition to the user authentication (user name and password) that is already done in the connection process. SecurID is “one time” password authentication, which means the password is dynamic in nature and will be used only one time.

In order for SecurID authentication to work, you must be tunneling to a PPTP/L2TP server that supports SecurID. As of this writing, only TunnelMaster from NTS has native support for SecurID. It is anticipated that other vendors of PPTP/L2TP servers will add this capability in the future.

No special configuration is required to enable SecurID. Remote TunnelBuilder will know that the information is required and will prompt you automatically for your SecurID information.

If SecurID is enabled, a log in to a TunnelMaster server will be successful if the configured user name and password are allowed, but further communication through the server will not be allowed until SecurID authentication is completed.

After login, the SecurID user will see this dialog box:

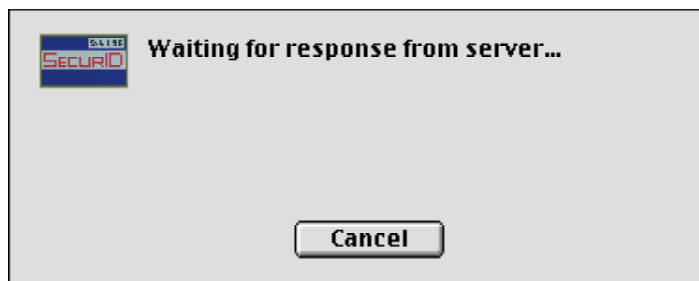


Enter your user name and one time password (Token) and click OK.

Note: Your user name and password will be visible on the screen as clear text. This is to assist in verification that all data has been entered correctly and is not a security risk because the password will immediately expire.

Clicking cancel or entering incorrect data will cause the connection to the PPTP/L2TP server to be lost.

While SecurID authentication is being completed, you will see the following screen:

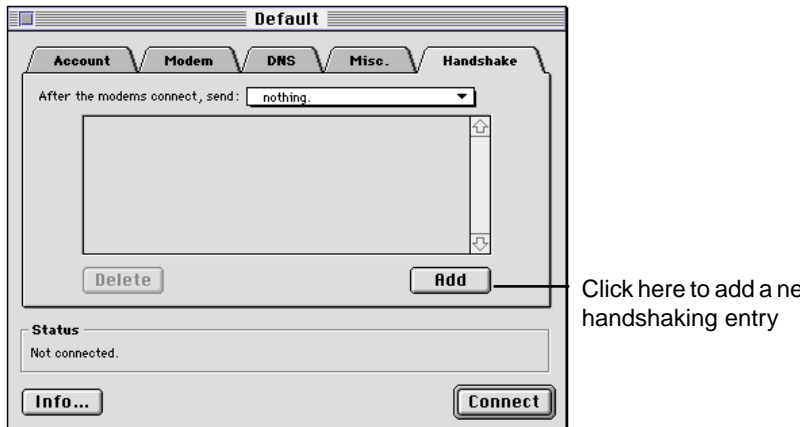


Followed by:



Clicking OK completes the SecurID process.

- Click OK.
14. Click the Handshaking tab to change handshaking options, if you wish.



Note: You can access the handshaking options only if you selected "Attempt Handshaking Before PPP" in the Account tab.

To specify the Dialer's response after your modem and the remote access server's modem connect, select a response from the "After the modems connect, send" pop-up menu.

To specify the Dialer's response to a specific prompt from the remote access server, click on Add to create a new pair of "When prompted by" and response entry fields.

Enter the remote access server's prompt in the "When prompted by" field. Then specify how you want the Dialer to respond to the prompt. You can specify a specific string, your username, or your password. If you specify your username or password, the Dialer automatically uses the values specified in the Account tab.

You can enter up to ten handshaking entries.

15. Choose Save Configuration from the File menu.

Your configuration is now saved as the default configuration and the NTS PPP Dialer will use it each time you open the application.

Connecting To a Remote Access Server

After entering configuration information in the NTS PPP Dialer configuration window, you're ready to connect to the remote access server.

If the "Connect automatically when needed" option is selected in your configuration, opening an Internet application automatically invokes the connection program a connection. You don't have to open the Dialer to establish a connection.

In addition, if you selected the "Start virtual private networking" option on the Misc. tab, Remote TunnelBuilder automatically attempts to establish a PPTP/L2TP tunnel to the remote server.

You can also use the Dialer to establish your connection, then open an Internet application.

To connect using the Dialer:

1. Open the PPP configuration window by choosing PPP Configuration from the Windows menu, if necessary.
2. Click Connect in the PPP configuration window.

The NTS PPP Dialer dials the phone number of the remote access server and logs on using the information you supplied.

When the connection process is successfully completed, you will see the word "Connected" followed by other pertinent information in the Status area of the window.

You can now use your Internet applications to access information on the remote network, whether that is the Internet or your intranet.

If the connection process fails, you can check a log to see what errors occurred. To open the log, choose **PPP Log** from the **Windows** menu. If you need help, see your system administrator.

If you did not select the “Start virtual private networking” option on the **Misc.** tab, you are not yet connected to the VPN server (PPTP/L2TP server) on your company network.

To build a tunnel to the remote access server:

1. Select **Connect to VPN Server** from the **File** menu. (Note that this menu only appears if the NTS PPP Dialer is running and is the active application.) If you are using the Control Strip you may also select **Connect to VPN** from its pop-up menu. This may prove to be more convenient because it is always available (if PPP is established).

Note: These menu items are enabled only if you have entered valid information in the VPN Settings dialog and are already connected to your ISP. The VPN Settings dialog is accessed from the **Misc.** tab in the PPP Dialer.

To tear down the tunnel to the remote access server:

2. Select **Disconnect from VPN Server** from the **File** menu, or **disconnect from VPN** using the Control Strip module.

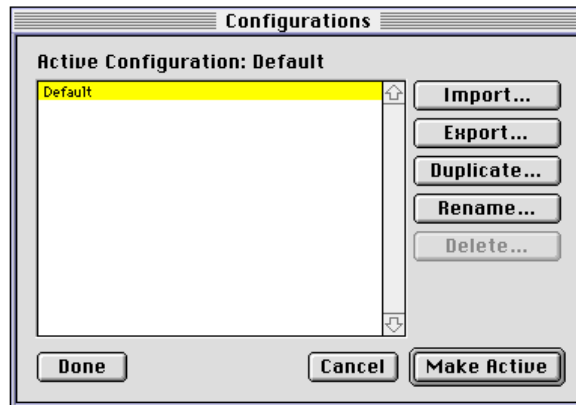
Note: These menu items are enabled only if you currently have a tunnel connection to the PPTP/L2TP server.

Creating and Using Other Configurations

After you create a default configuration, you can create additional configurations for other remote servers.

1. Choose **Configurations . . .** from the **File** menu.

The Configuration dialog box appears.



To create a new configuration, you can duplicate an existing one that already has most of your information recorded in it.

2. Select a configuration from the list and click Duplicate.

Note: You can rename the configuration by selecting it and clicking Rename.

3. With the new configuration selected, click Make Active.
4. Enter your changes in the PPP configuration window for the configuration document.

See “Setting Up Your First Configuration” on page 7 for more information about changing settings.

5. Choose Save Configuration from the File menu.

Selecting an existing configuration

You can use a specific configuration when you want to connect to a specific network or service provider.

1. Choose Configurations from the File menu.
2. Select the configuration you want to use, and click Make Active.

Switching Connections

The File menu in the PPP application contains options that let you switch between the PPP connection (unsecured) and the PPTP/L2TP connection (secure tunnel).

If you selected “Start virtual networking after connecting” in the Misc. tab of the NTS PPP Dialer when you set up Remote TunnelBuilder, the software automatically builds a tunnel to the designated PPTP or L2TP server each time you dial your ISP. If you did not select this option, you must manually build the tunnel after dialing in to your ISP.

Note: The PPTP/L2TP connection (the tunnel) is built on top of the PPP connection. You cannot close the PPP connection and still use the tunnel.

Tearing Down the Tunnel

To tear down the tunnel, select the Disconnect from VPN Server item from the File menu in the NTS PPP Dialer.

Note: This menu item is enabled only if you currently have an active tunnel connection.

Changing VPN Information

After you tear down a tunnel, whether PPP is active or not, you can change the VPN Settings. You must save the new settings before they become active, and you will be prompted to do so by the program.

Thank You!

We sincerely appreciate your purchase and use of TunnelBuilder for Mac, and hope that it is a tool that you find to be both useful and friendly. If you have product suggestions or other feedback, please send them via e-mail to tbsales@nts.com.

Further support, and product comments

For support questions that might not have been answered in this document, please check the ReadMe file that came with the product, and the FAQ section of our web site. We can be found at <http://www.nts.com>.

Appendix A Using Ping



TunnelBuilder contains an NTS developed version of a troubleshooting/utility application called Ping. You can use Ping whether or not you have established a tunnel to a PPTP/L2TP server.

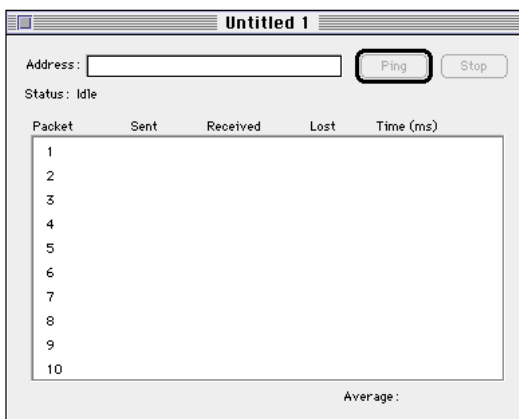
When the tunnel to the PPTP server is active, you use Ping to test for the presence of active servers and devices, such as printers, on your company network. Ping is useful when you want to find out if a particular printer is operating or if a server containing files you need is available.

You supply the Ping application with the IP address or domain name of a network server or device, and Ping sends packets over the network to determine if the server or device is active. The process of sending such network packets is called *pinging*.

Make sure you have the domain name or the IP address of the server or device you want to access. If you don't have this information, see your system administrator or contact the person whose system you want to ping.

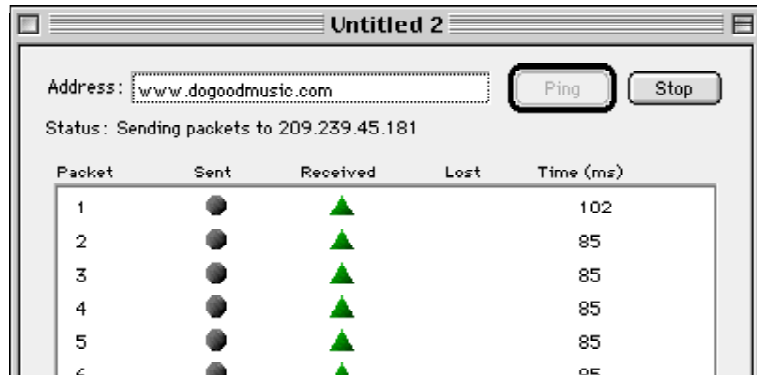
Double-click the "Ping" icon in the NTS PPP Folder.

A new Ping window appears.



3. In the area labeled **Address:**, enter the name or IP address of the server or device you want to ping.
4. Click **Ping**.

As the application pings the server or device, you see the results in the Ping window. Note that while Ping is active, it shows the address to which packets are being sent.



If the server or device is active on the network, you see green triangles in the Received column. If the device isn't found on the network, red hexagonal dots (like small stop signs) appear in the Lost column. The application pings the server or device 10 times and shows the results of each ping, including the round trip time for the ping packet if it returned successfully.

To check for the presence of other servers or devices on the network, enter another IP address and click Ping again.

Saving Ping Data

You can save the results of the ping procedure in a file. Both the address and results of the last ping are saved in the file.

1. To save the results, choose **Save** from the **File** menu.
2. Enter a name for the file and click **Save**.

Note: You can open a saved ping file and use the file to test the connection again.