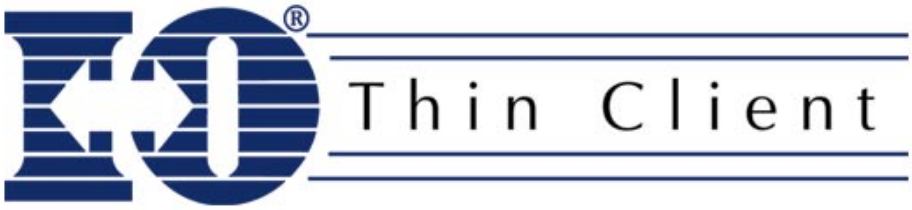


Thin Client Administrator's Guide

Copyright and Trademark notices

Document Number: 600 0101 610 67 A01 (I-O Document Number: WBT100-OMAN02-100)

Second Edition, May 2002 (with I-O Corporation modifications July 2002)

Applicable to clients with firmware version TC4111-55-XXX

I-O Corporation

1490 North 2200 West, Suite 100

Salt Lake City, UT 84116

801-973-6767

www.iocorp.com

Table of Contents

Introduction

About The I-O Thin Client

The I-O Thin Client is one of the smartest and most robust solutions available for thin client computing.

Equipped with Microsoft's Windows CE 3.0 operating system, the product provides seamless connectivity to Windows NT 4.0 TSE and Windows 2000 servers using Citrix's ICA and Microsoft's RDP protocols. The thin client also includes a terminal emulation suite for UNIX connectivity.

Microsoft's Internet Explorer V4.0 browser is built into the thin client to provide instant access to the Internet.

The user-friendly interface of the software allows the system administrator to easily configure the clients and create up to 30 different connections.

Besides ensuring login-security through a system of user-accounts, the product can also be configured to use the optional **smart AX-s** security feature. (Please visit us at www.iocorp.com to determine when this option will become available.)

The term **Client** is used in this guide to represent the I-O Thin Client.

Consistent with our policy of continuous development, the product you received may have features in addition to those described in this guide. Please visit us at www.iocorp.com for current information.

About this Guide

This guide is intended to assist the network administrator of your organization to setup and configure the software of the thin client.

The following symbols are used in the guide.

Caution: This symbol highlights procedures that, if not correctly performed or adhered to, could damage or corrupt the product or adversely affect the security and functionality of the product. Do not proceed beyond such points until the required conditions are fully understood and achieved.

Note: This symbol denotes useful additional information that is relevant to the procedure or feature being described.

Tip: This symbol denotes a hint, shortcut or alternate method to aid or supplement the procedure being described.

The guide contains screenshots of relevant dialog-boxes and windows for your reference. The sizes of screenshots are not representative of the actual sizes of the dialog-boxes and windows on your screen.

Scope of the Guide

Information in this guide is applicable to clients with the following firmware versions:

TC4111-55-XXX

TIP: THE FIRMWARE VERSION OF THE CLIENT IS DISPLAYED IN THE DIAGNOSTICS TAB OF THE **TERMINAL PROPERTIES** WINDOW (*PAGE NO. 60*).

Related Information

Besides this guide, the following other documents contain information relevant to the thin client. These documents are available in PDF format on the CD that was provided with the product.

- ***I-O 5250 Printer Emulation User's Guide***

  This document provides detailed information about I-O Corporation's 5250 printer emulation.

- ***I-O 5250 Display Emulation User's Guide***

  This document provides detailed information about I-O Corporation's 5250 display emulation.

- ***Thin Client Hardware User's Guide***

  This document describes the procedure to install and operate the hardware of the thin client.

- ***PERICOM Terminal Emulation User's Guide***

  This document provides detailed information about the generic terminal emulation suite included in the thin client.

- ***inControl for Terminals Administrator's Guide***

  This document describes *inControl for Terminals*: a client management utility to control and configure multiple thin clients from a remote server.

Initial Setup

This chapter describes the procedure to setup the software of the client. This procedure must be performed by the system administrator. It is assumed that you have installed the product as described in the *Hardware User's Guide.*

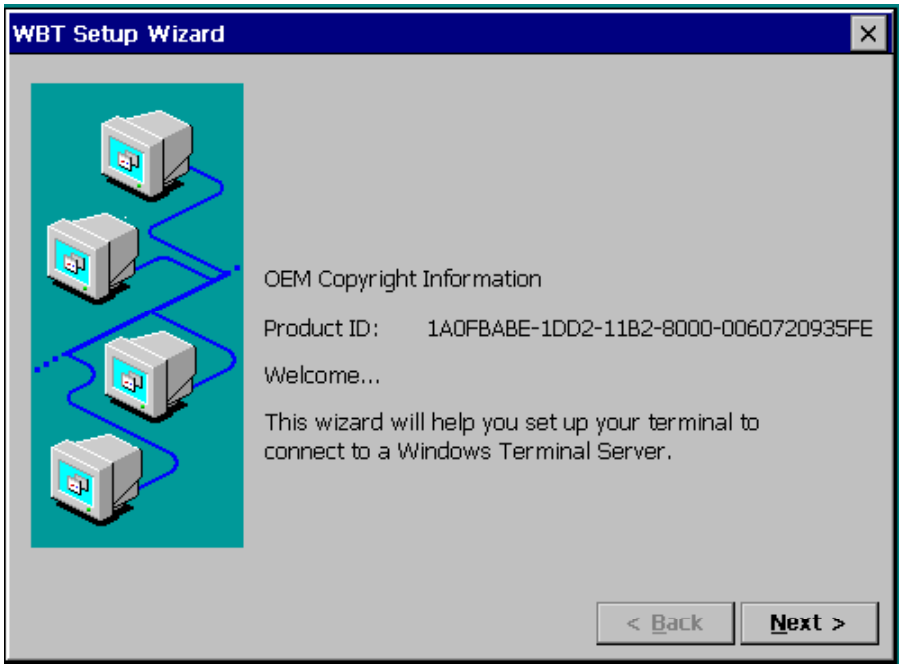
When you switch the client on for the first time, a **Setup Wizard** is automatically started. *However, if the client has been "pre-configured" by I-O, this setup wizard will not start.*

NOTE: THE SETUP WIZARD IS STARTED AUTOMATICALLY UNDER THE FOLLOWING CIRCUMSTANCES:

- WHEN YOU SWITCH THE CLIENT ON FOR THE FIRST TIME. *IF THE CLIENT HAS BEEN "PRE-CONFIGURED" BY I-O, THIS SETUP WIZARD WILL NOT START.*
- WHEN YOU RESTORE DEFAULT-SETTINGS OF THE CLIENT THROUGH THE GENERAL TAB OF THE **TERMINAL PROPERTIES** DIALOG-BOX (*PAGE NO.21*).

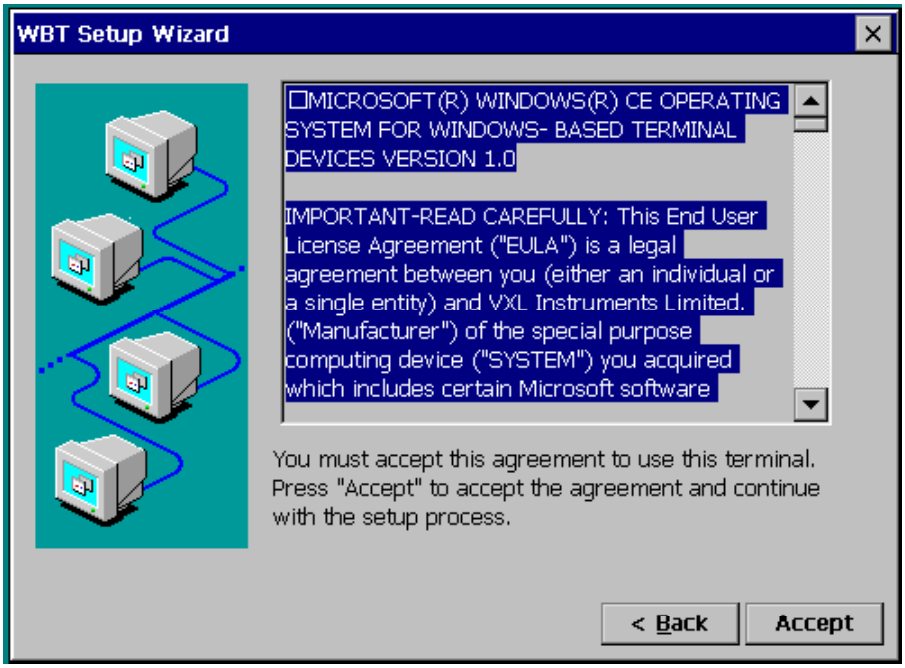
The **Setup Wizard** has several dialog-boxes that display in succession. Some dialog-boxes provide information, while others require input. Every dialog-box contains buttons to take you backward or forward through the setup process, and to confirm or cancel input and selections.

The first dialog-box of the **Setup Wizard** is shown below.



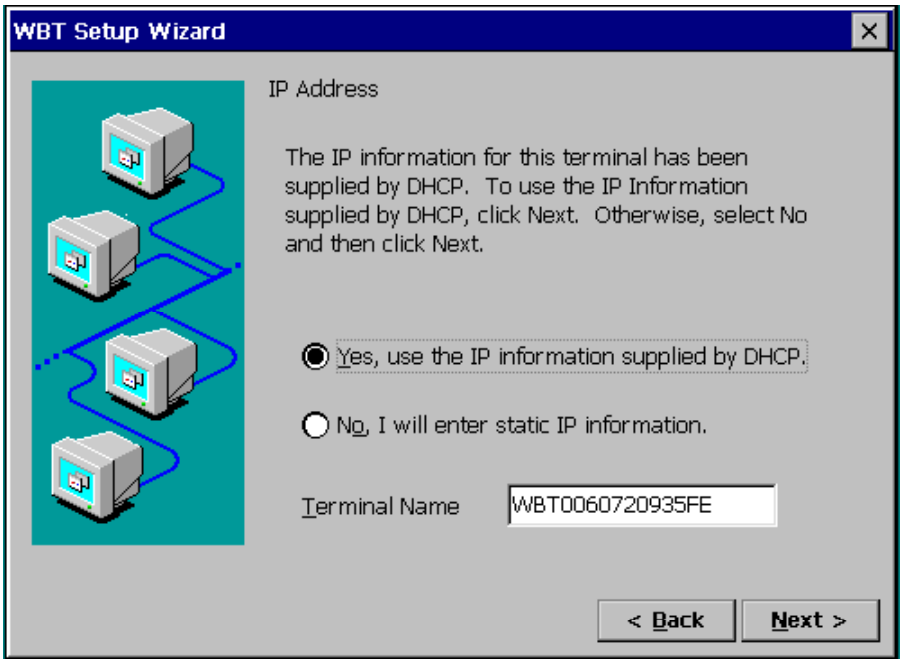
The above dialog-box contains the product ID of the firmware. Click **Next>** to continue.

End User License Agreement



The above dialog-box contains the License Agreement. Please read the agreement carefully to understand the terms and conditions governing use of the software. Click **Accept** to signify your acceptance of the terms and conditions of the agreement.

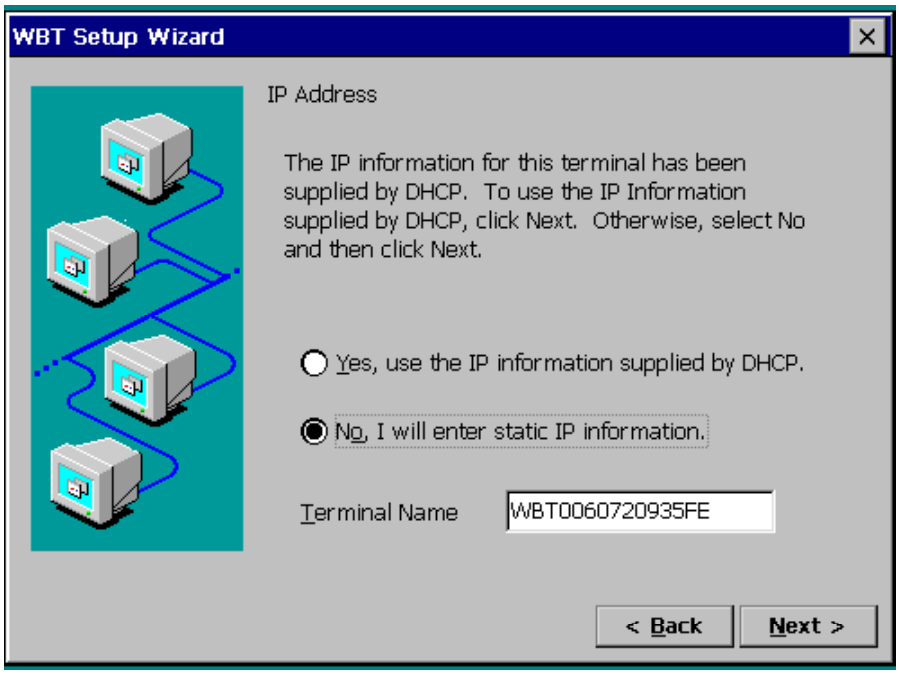
IP Address



The client requires a unique IP address to communicate with the network. If the client detects a DHCP (*Dynamic Host Configuration Protocol*) server in the network, the **Yes, use the IP information supplied by DHCP** radio-button is automatically selected. To continue, click **Next>**. The **Desktop Area and Refresh Frequency** dialog-box (*page 11*) is displayed.

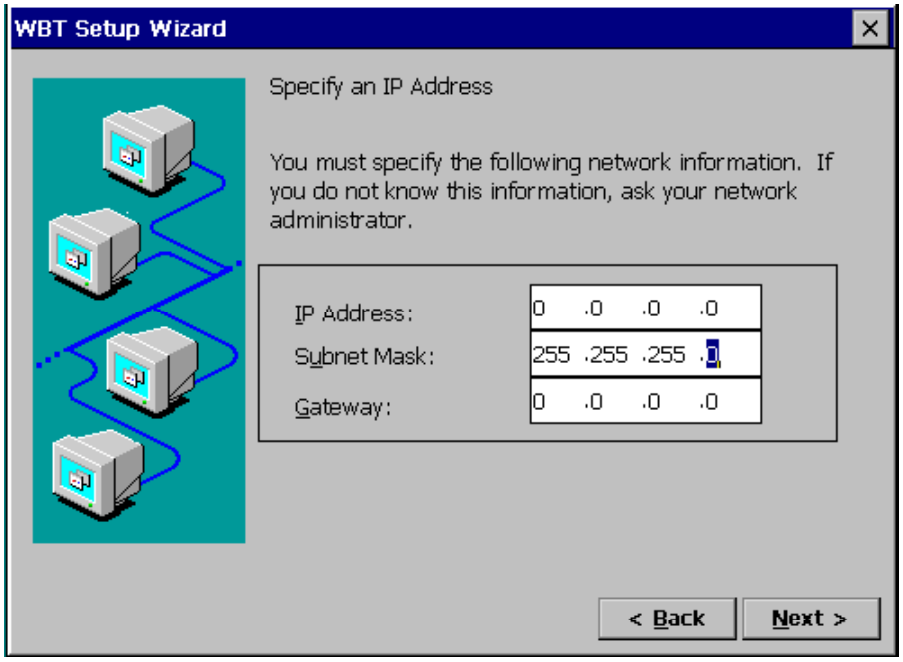
TIP: TO IMPLEMENT LPD PRINTING (*PAGE. NO. 35*), IT IS RECOMMENDED THAT YOU SPECIFY A **FIXED IP ADDRESS** FOR THE CLIENT. THIS IS NECESSARY BECAUSE, ON THE SERVER-SIDE YOU MUST SPECIFY THE IP ADDRESS OF THE CLIENT. IF YOU MUST USE **DHCP**, THEN IT IS PREFERABLE THAT YOU RESERVE AN IP ADDRESS ON THE DHCP SERVER, FOR THE CLIENT THAT YOU PLAN TO CONFIGURE AS THE LPD SERVER.

If you want to specify a fixed IP address, select the **No, I will enter static IP information** radio-button. The dialog-box will change as shown below.



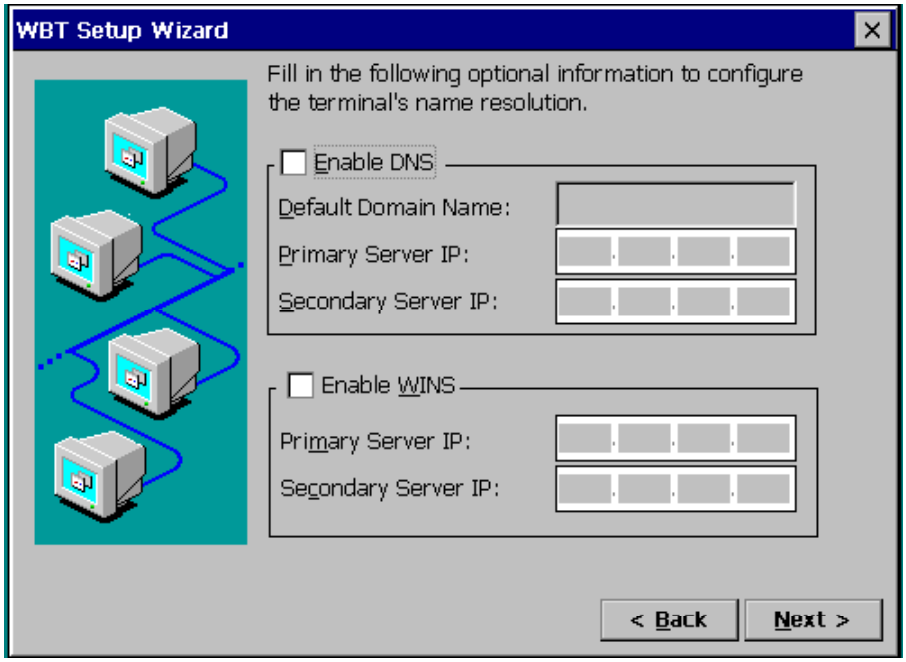
Click **Next>** to continue. The following dialog-box is displayed.

Specify an IP Address



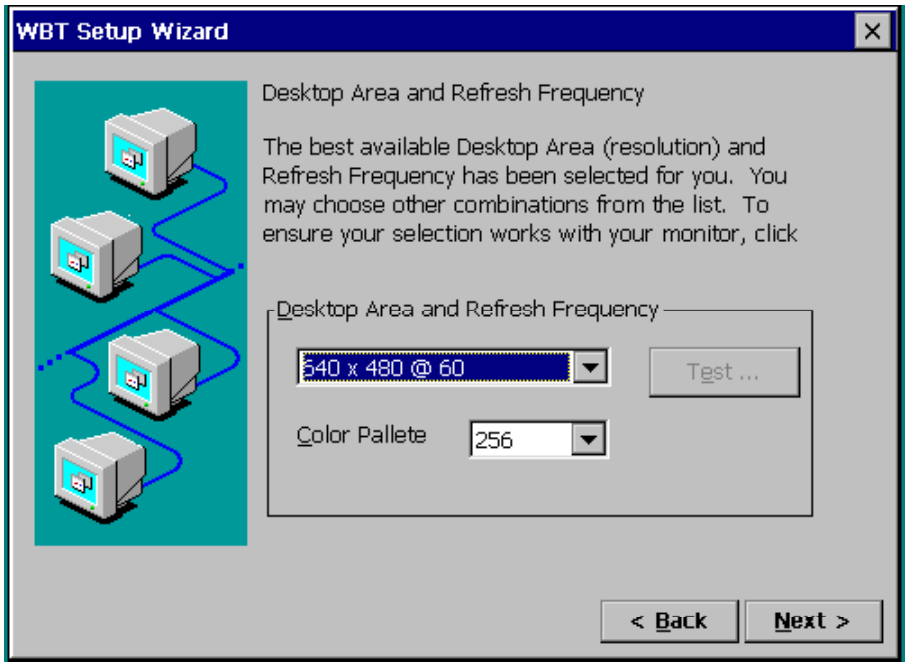
In the above dialog-box, provide a unique **IP address** for the client, the **Subnet Mask** corresponding to your network, and the **Gateway**. The gateway is essential to browse the Internet using the in-built Internet Explorer browser. Click **Next>** to continue.

Optional Information



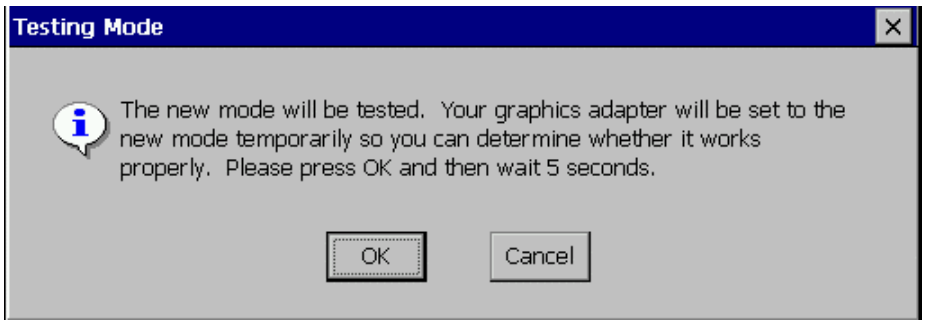
If there are active DNS or WINS servers in your network, you can enable their use by providing appropriate information in the above dialog-box. If the client uses a fixed IP address, the DNS **must** be enabled in order to browse the Internet using the in-built Internet Explorer browser.

Desktop Area and Refresh Frequency



By default, the client is configured to display at a resolution of 640x480 and a refresh frequency of 60Hz. This **Color Palette** drop-down list allows you to define the color depth for the display unit connected to the client. The options available are **256** (*8-bit*) and **65536** (*16-bit*).

If you select a resolution or refresh frequency other than the default setting, verify whether your monitor supports the selected setting by clicking the **Test** button. The following prompt is displayed.



Click **OK** to continue. The screen becomes blank. After a delay of approximately 5 to 10 seconds, one of the following test patterns is displayed depending on the setting that you selected.

NOTE: MONITORS WITH ON SCREEN DISPLAY (OSD) FEATURE MAY DISPLAY APPROPRIATE MESSAGES (*SUCH AS 'OUT OF SYNC' OR 'OUT OF RANGE'*) IF THE SELECTED RESOLUTION AND FREQUENCY ARE NOT SUPPORTED. THE EXACT TEXT OF THE OSD MESSAGE WOULD DEPEND ON THE MODEL OF THE MONITOR CONNECTED TO THE CLIENT.

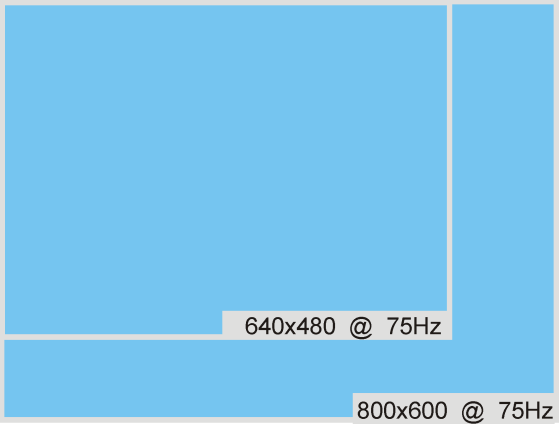
Display Test Patterns

The images shown here are not to scale. The exact color might vary depending on your monitor.

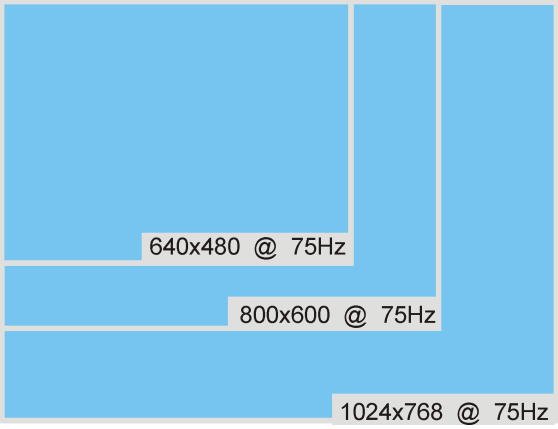
The patterns shown here are at a refresh frequency of 75Hz. At other refresh frequencies, the text '75Hz' in the images would be replaced with the appropriate refresh frequency.

Resolution: 640 x 480

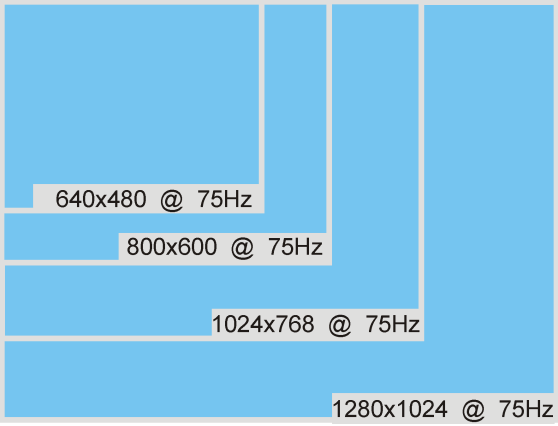
Resolution: 800 x 600



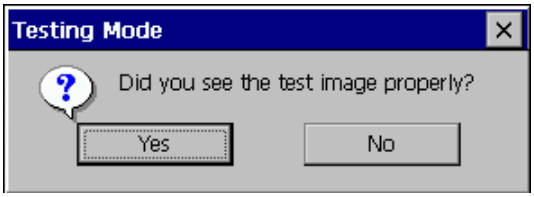
Resolution: 1024 x 768



Resolution: 1280 x 1024

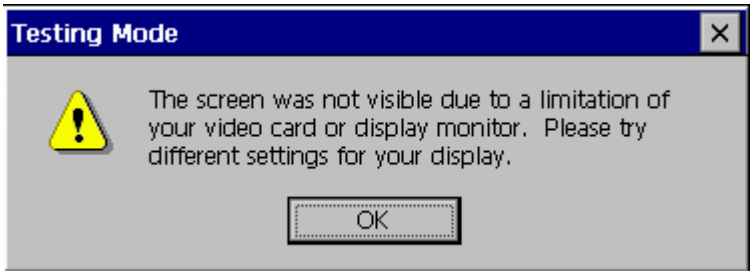


If the monitor supports the selected display setting, one of the above test patterns is displayed for approximately 5 to 10 seconds. Then, the screen becomes blank again. After another delay of approximately 5 to 10 seconds, the following prompt is displayed.



NOTE: IN MONITORS WITH OSD FEATURE, THE ABOVE PROMPT IS DISPLAYED AFTER A DELAY OF 35 TO 40 SECONDS. THE EXACT DURATION OF THE DELAY WOULD DEPEND ON THE MODEL OF THE MONITOR CONNECTED TO THE CLIENT.

- If the test pattern was not properly displayed, click **No**. The following message is displayed.

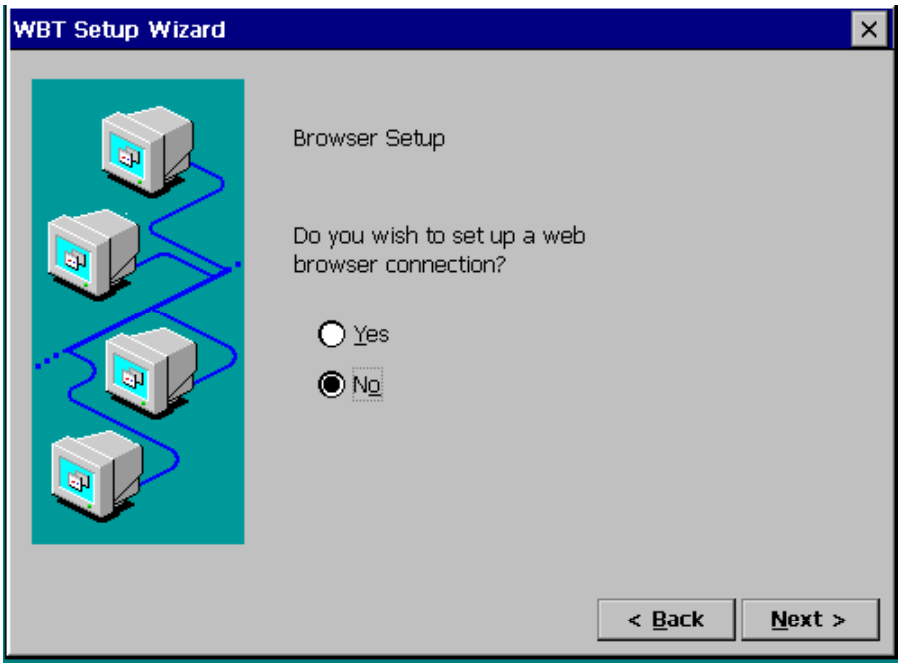


  Click **OK** to change the setting and repeat the test.

- If the appropriate test pattern was displayed, click **Yes** to return to the setup wizard.

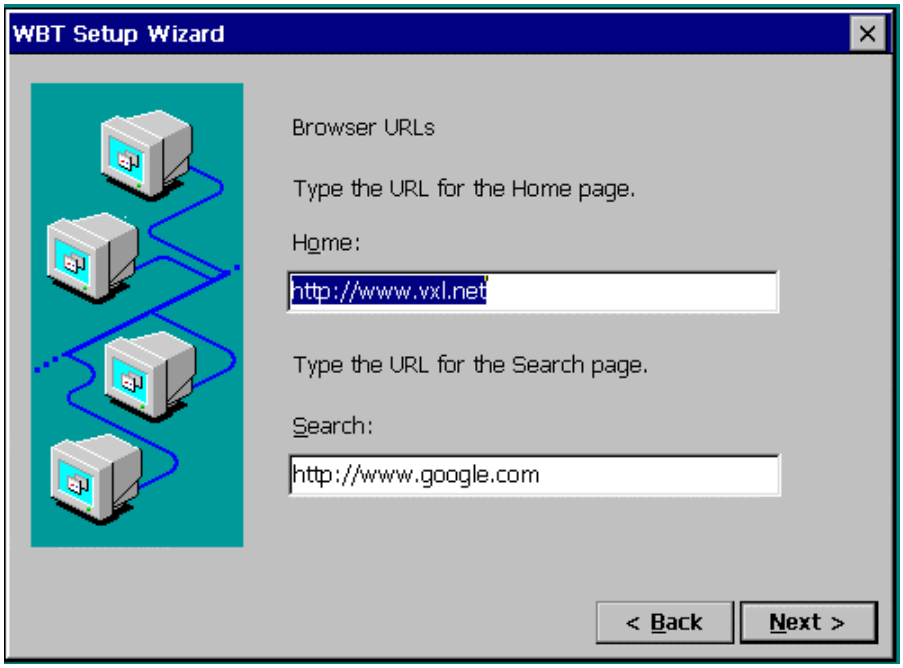
Click **Next** to proceed.

Browser Setup

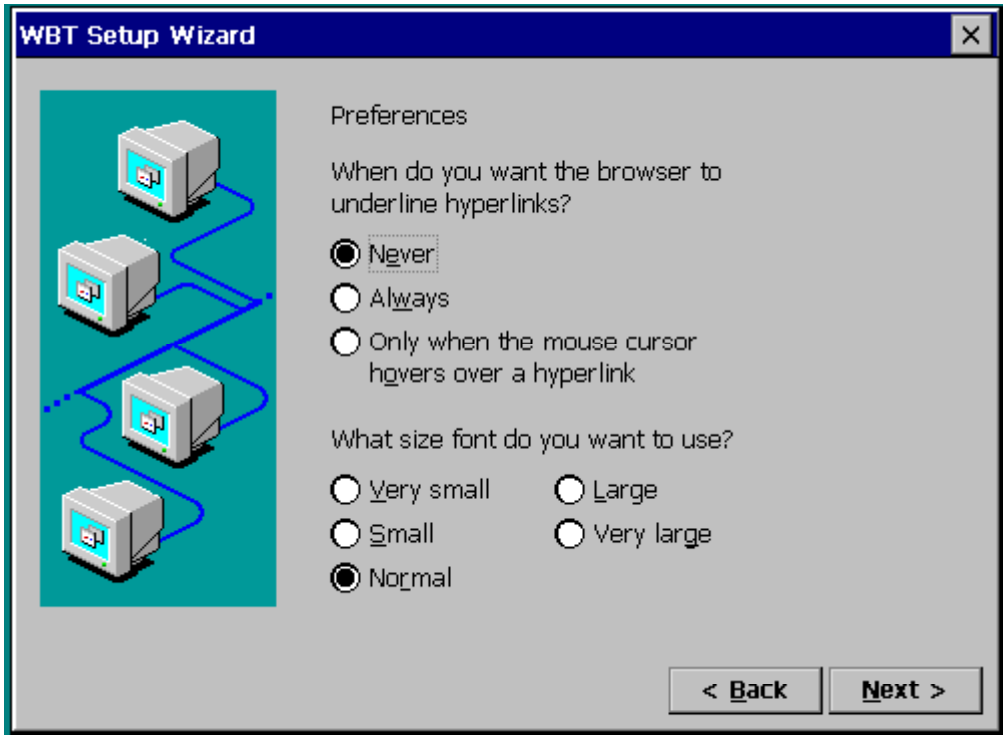


The firmware of the client includes Microsoft Internet Explorer 4.01.

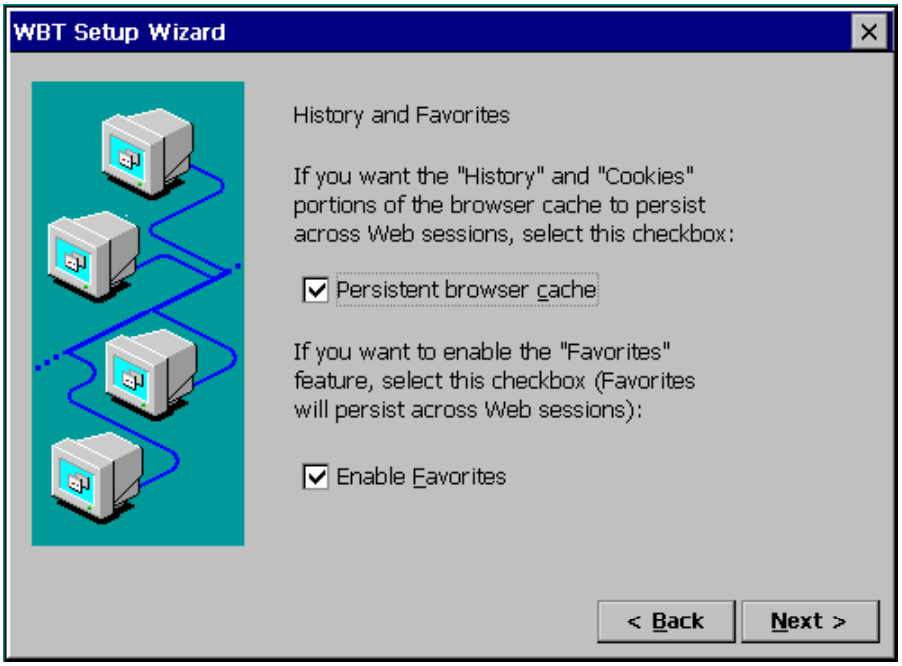
Select **Yes** to setup a web browser connection. Click **Next>**



Enter the URL for the home page and the search page to be displayed while opening the browser. Click **Next>**



Make appropriate selections in the above preferences options. Click **Next>**

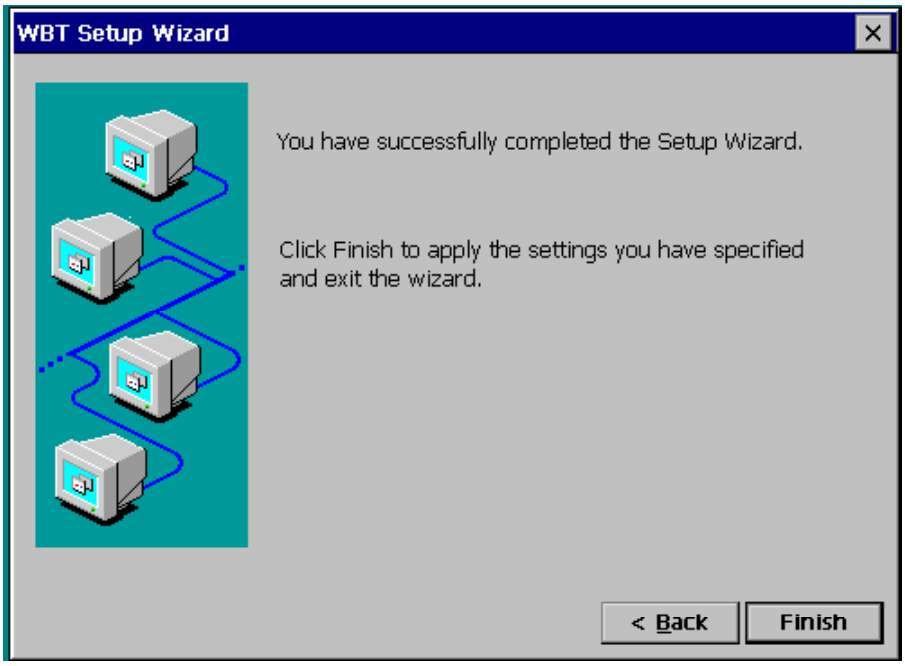


Select **Persistent browser cache** check box if you want the contents of the browser cache to be retained between the sessions.

Select **Enable Favorites** to enable the Favorite feature of the web browser. Click **Next>.**

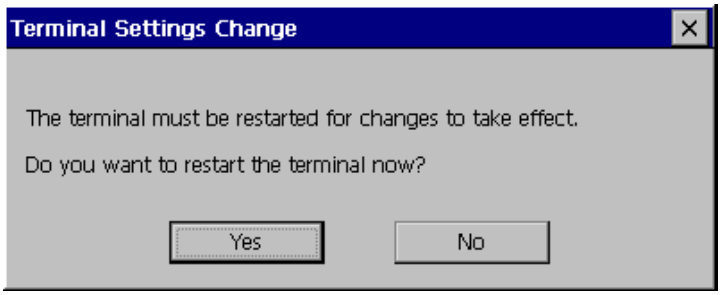
If you access the Internet through the proxy server, enable User Proxy Server check box and type the name of the computer running the proxy server and the port number. Click **Next>**

Finish



The above dialog-box marks the end of the **Setup Wizard**. Click **Finish**.

- If you made any changes during the setup process, the **Terminal Settings Change** dialog-box will be displayed.



  Click **Yes** to shutdown and restart the client.

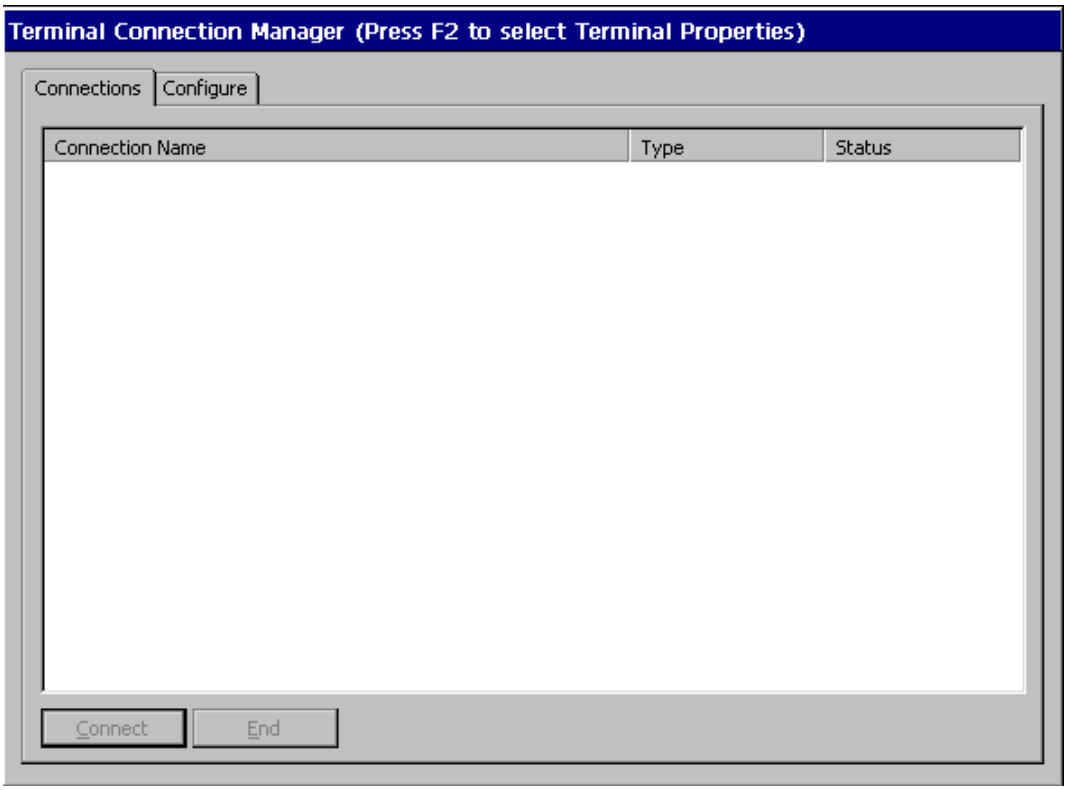
- If you did not change any parameter during the setup process, the login prompt (*described in the next chapter*) will be displayed after the client has restarted.

Overview of Terminal Connection Manager

This chapter provides an overview of the **Terminal Connection Manager** window. The **Terminal Connection Manager** window is displayed after the setup process, and each time you subsequently switch the client on. Please see the note below, for exceptions to this rule.

NOTE: IN THE FOLLOWING SITUATIONS, THE **TERMINAL CONNECTION MANAGER** WILL **NOT** BE DISPLAYED WHEN THE CLIENT IS SWITCHED ON.

- IF YOU CONFIGURE A CONNECTION TO AUTO-START MODE (*PAGE 144*), THE CLIENT AUTOMATICALLY STARTS THE PARTICULAR CONNECTION, INSTEAD OF DISPLAYING THE TERMINAL CONNECTION MANAGER.
- IF YOU RESTORE PROPERTIES OF THE CLIENT TO DEFAULT SETTINGS (*PAGE 21*), THE CLIENT AUTOMATICALLY STARTS THE SETUP WIZARD INSTEAD OF DISPLAYING THE TERMINAL CONNECTION MANAGER.

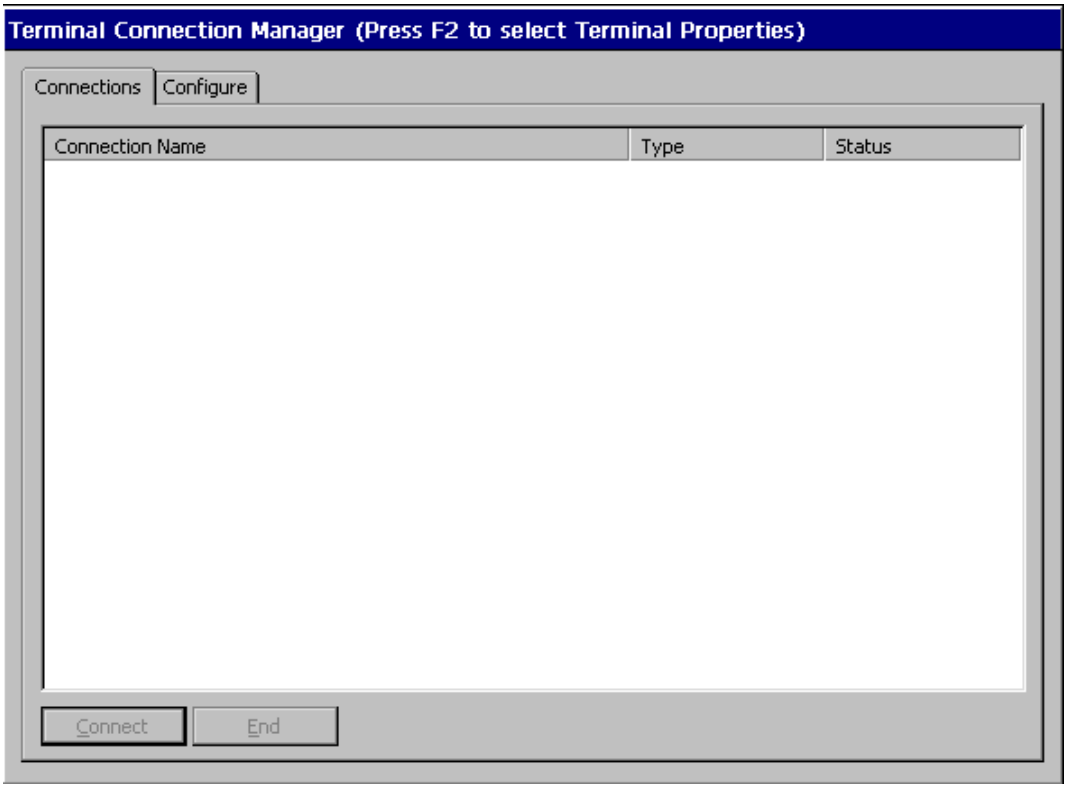


The **Terminal Connection Manager** has two tabs:

- The **Connections** tab displays a list of available connections, and allows you to start/end connections.
- The **Configure** tab allows you to add, edit and delete connections, and to specify startup properties for defined connections.

TIP: AT ANY TIME, YOU CAN INVOKE THE **TERMINAL CONNECTION MANAGER** FROM AN OPEN SESSION, BY PRESSING **Ctrl+Alt+End**. TO RETURN TO AN OPEN SESSION AND TO SWITCH BETWEEN SESSIONS, PRESS **Ctrl+Alt+[UP ARROW KEY]/[DOWN ARROW KEY]**.

Terminal Connection Manager - Connections tab



The **Connections** tab has the following buttons and a list (*initially empty*) of defined connections.

- **Connect**: to start a highlighted connection.

TIP: YOU CAN ALSO START A CONNECTION BY HIGHLIGHTING AND THEN DOUBLE CLICKING ON IT.

- **End**: to close an active connection
- **Shutdown**: to logout of or to shutdown the client

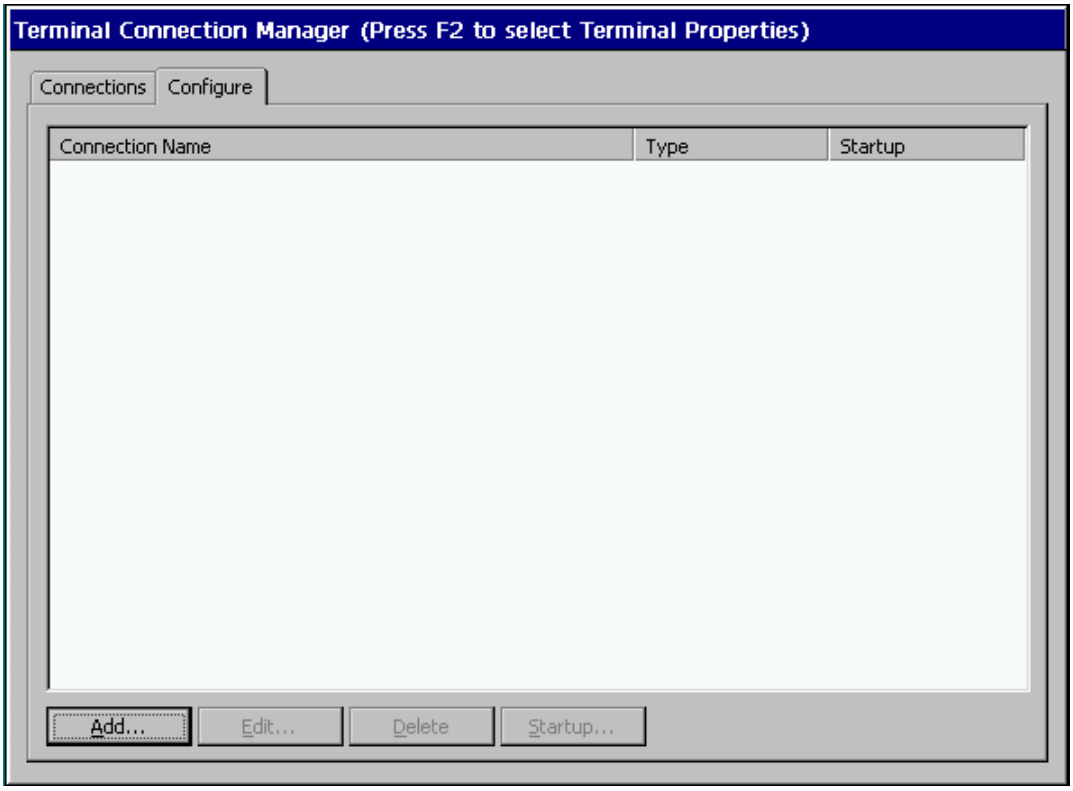
The list area has the following columns:

- **Connection Name**: names of available connections
- **Type**

Connection Type	***Description***
ICA	LAN connection to a server that supports Citrix's ICA protocol.
RDP	LAN connection to a Windows Terminal Server
Dialup	Dial-up connection to a remote server.
TEC	Terminal emulation connection
Web	Internet Explorer

- **Status**: status of the connection.

Terminal Connection Manager - Configure tab



The **Configure** tab contains four buttons and a list (*initially empty*) of defined connections.

Add…

With this button, you can create a connection entry using the **New Connection** wizard.

Edit…

With this button, you can edit defined connections.

Delete

With this button, you can delete defined connections.

Startup…

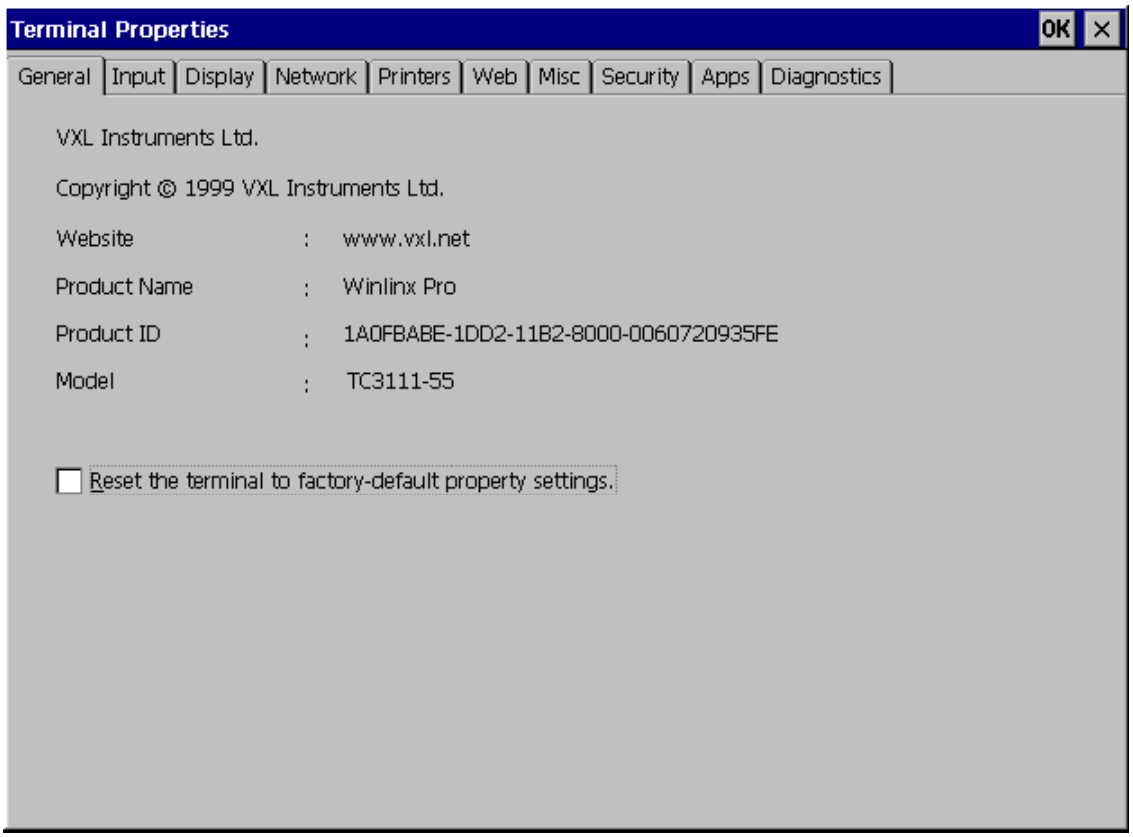
With this button, you can designate a particular connection to be the default connection, or to automatically start when the client is switched on. See Specifying AutoStart / Default Connection (*page 144)*. The startup status is displayed in the **Startup** column.

Configuring the Client

This chapter describes the procedure to modify client properties. It is recommended that these procedures be performed only by the System Administrator. All the client parameters can be configured through the **Terminal Properties** dialog-box.

To invoke the **Terminal Properties** dialog-box, press the **F2** key while the **Terminal Connection Manager** window is displayed.

TIP: TO SWITCH TO THE **TERMINAL CONNECTION MANAGER** FROM AN OPEN SESSION, PRESS **CTRL+ALT+END**.



To select a tab, click on the required tab.

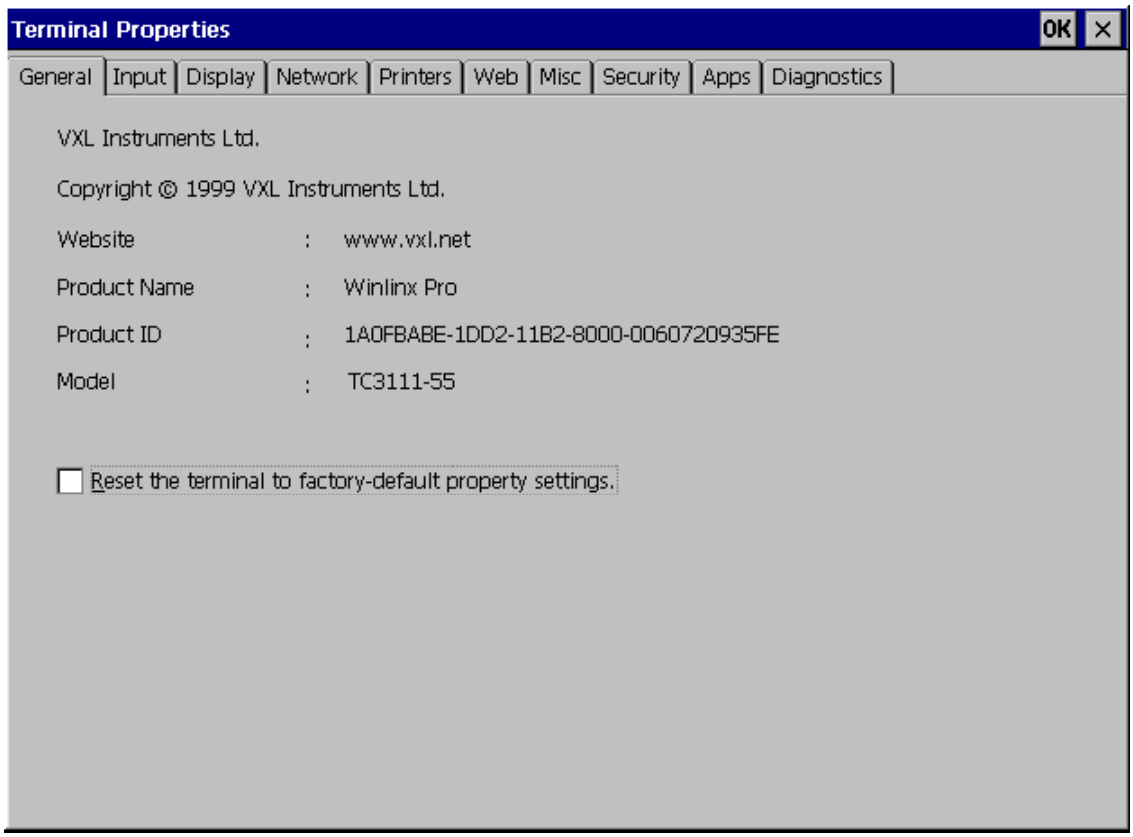
- General: contains product information, and allows you to reset the client to default settings.
- Input: to configure the keyboard and mouse.
- Display: to configure the display and screensaver parameters.
- Network: to configure network parameters.
- Printers: to add, configure, delete local printers, and implement Thin Print and LBT.
- Web: to setup the web browser
- Misc: to configure global ICA settings and configure the client for accessing applications published by a Citrix NFuse server.
- Security: to configure security parameters.
- Apps: to configure touch screen settings, to configure SNTP and Timezone, and the Ping utility.
- Diagnostics: contains system information and copyright notices.

Each of the above sheets is explained individually on the following pages

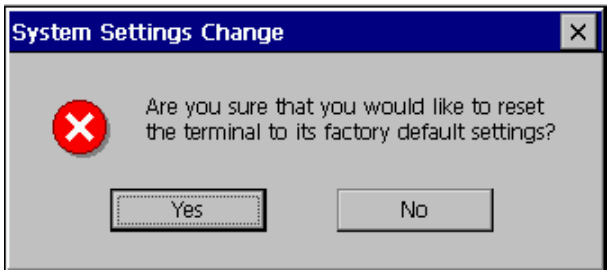
General (view product information and restore default settings)

To view product information or restore default settings, press the **F2** key on your keyboard while the **Terminal Connection Manager** window is displayed. The **General** tab is displayed by default.

TIP: TO SWITCH TO THE **TERMINAL CONNECTION MANAGER** FROM AN OPEN SESSION, PRESS **CTRL+ALT+END**.



- The **General** tab contains product information (*product name and product ID*).
- **Reset the terminal to factory-default property settings**: If you want to restore the default settings of the client, select this check-box and click **OK**. The following prompt is displayed.



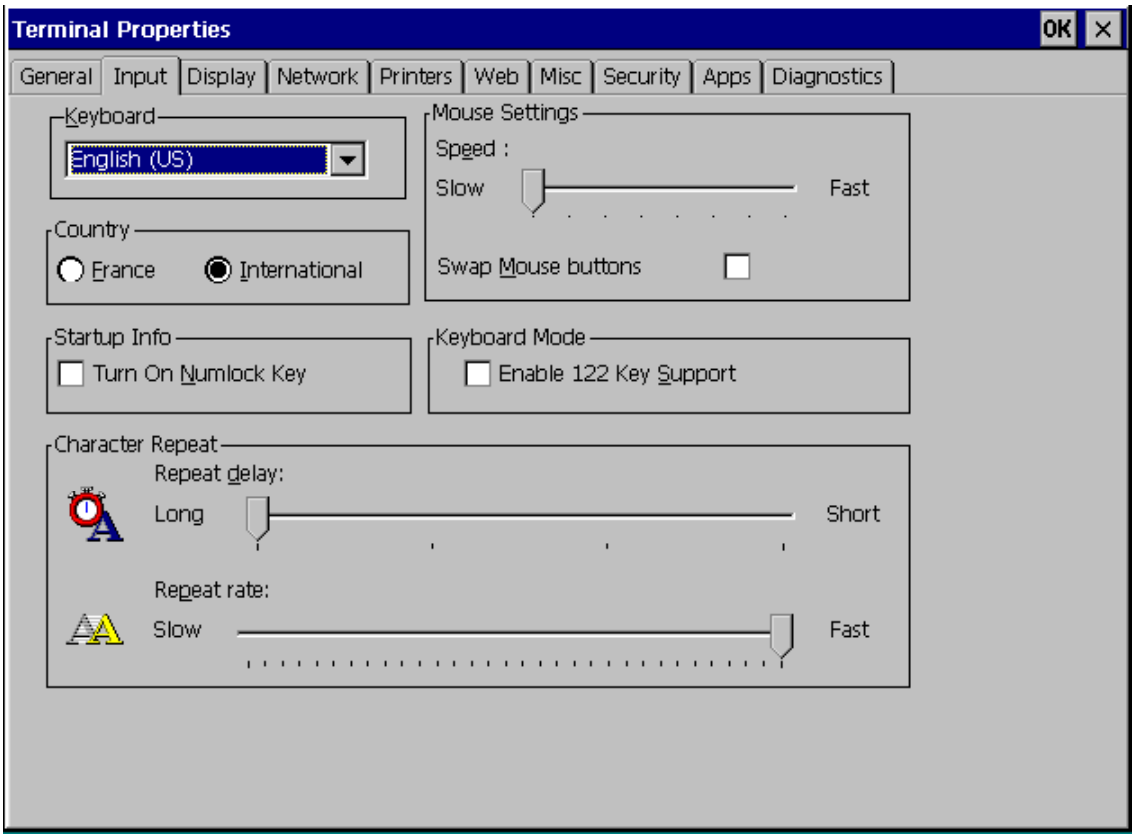
If you click **Yes**, the client will restart and invoke the Setup Wizard (*page 7*).

Input (configure the keyboard and mouse)

To configure the keyboard or mouse,

1. Press the **F2** key on your keyboard while the **Terminal Connection Manager** window is displayed.
2. Select the **Input** tab.

TIP: TO SWITCH TO THE **TERMINAL CONNECTION MANAGER** FROM AN OPEN SESSION, PRESS **CTRL+ALT+END**.



- **Keyboard**: Select a country corresponding to the keyboard language. **English (US)** is selected by default. If the drop-down list does not contain an entry for your country, contact I-O Corporation. Ensure that the servers to which the client would connect, supports the keyboard language selected for the client.
- **Country**: Select the appropriate keyboard layout. **International** is selected by default.
- **Mouse Settings**

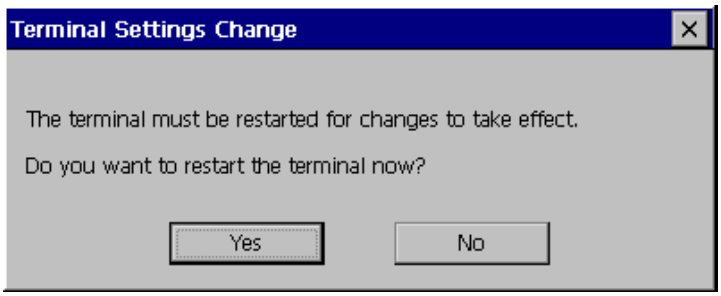
  Speed: Set the speed of the pointer's movement on the screen relative to the movement of the mouse. The default setting is **Slow**.

  Swap Mouse buttons: This check-box allows you to interchange functions of the left and right mouse-buttons.
- **Turn On Numlock** Key: If you want the Num Lock position to be ON when the client boots up, select this check-box. Otherwise, leave it unchecked.
- **Enable 122 Key Support: Enable this option to use the keyboard with 122 keys**
- **Repeat Delay**: This is a slider control to set the repeat delay of keyboard characters. This setting determines the speed (*in seconds*) at which a character appears on screen when typed repeatedly. The default setting is **Long**.

- **Repeat Rate:** This is a slider control is to set the repeat rate of a keyboard character. This value determines the speed (*in seconds*) at which a character appears on screen when the associated key is held down. The default setting is **Fast**.

3. Click **OK** to save changes or **X** to cancel changes.

If you click **OK**, the following prompt is displayed.



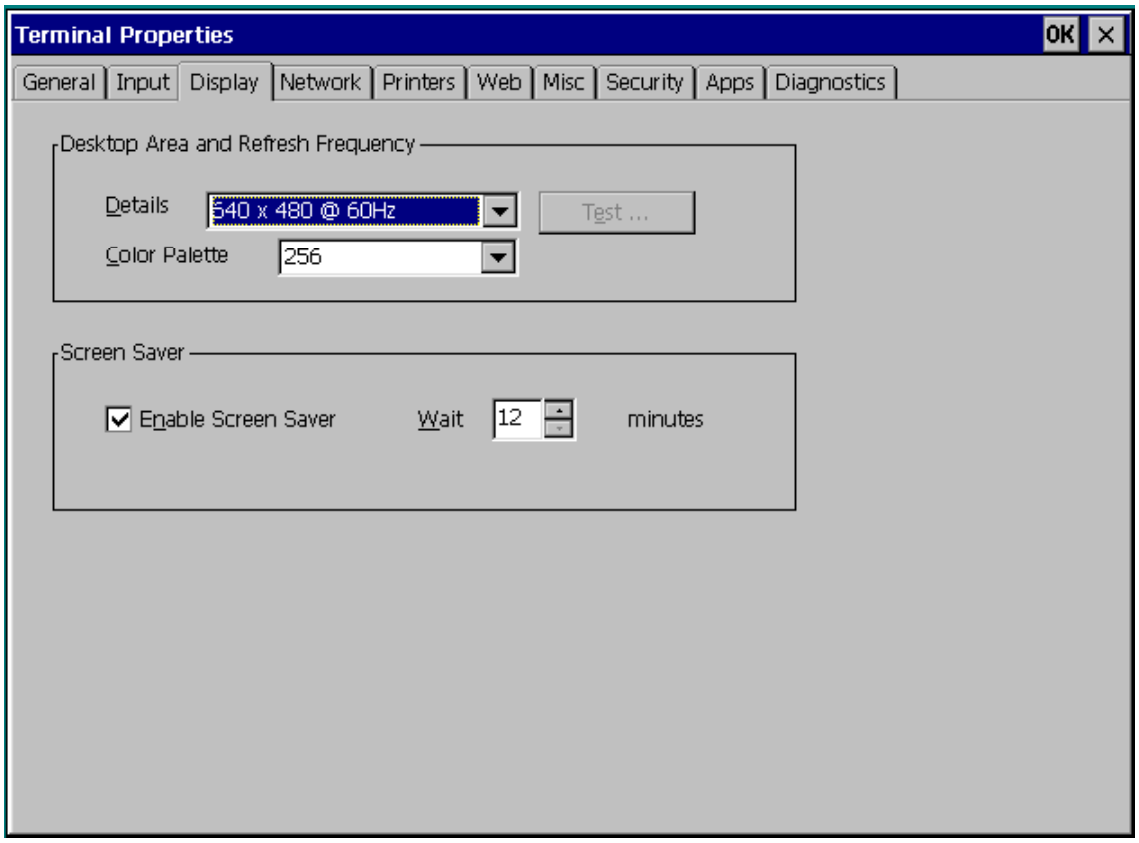
Click **Yes** to shutdown and restart the client. Click **No**, if you do not want to restart the client.

Display (resolution, frequency and screensaver)

To configure display resolution, refresh frequency and the screensaver delay,

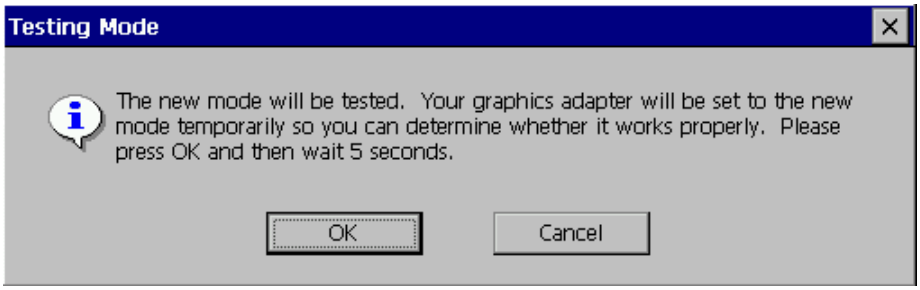
1. Press the **F2** key on your keyboard while the **Terminal Connection Manager** window is displayed.
2. Select the **Display** tab.

TIP: TO SWITCH TO THE **TERMINAL CONNECTION MANAGER** FROM AN OPEN SESSION, PRESS **CTRL+ALT+END**.



- **Desktop Area and Refresh Frequency - Details**: The default setting is **640 x 480@ 60 Hz**. From the drop-down list, select a display resolution and refresh frequency that your display unit supports.

  If you select any setting other than the default, the **Test …** button is enabled. Click on it to test whether the selected setting is compatible with your display unit. The following prompt is displayed.



  Click **OK** to proceed. The screen becomes blank. After a delay of approximately 5 to 10 seconds, one of the following test patterns is displayed depending on the resolution selected.

NOTE: MONITORS WITH ON SCREEN DISPLAY (OSD) FEATURE MAY DISPLAY APPROPRIATE MESSAGES (*SUCH AS 'OUT OF SYNC' OR 'OUT OF RANGE'*), IF THE SELECTED RESOLUTION AND FREQUENCY ARE NOT SUPPORTED. THE EXACT TEXT OF THE OSD MESSAGE WOULD DEPEND ON THE MODEL OF THE MONITOR CONNECTED TO THE CLIENT.

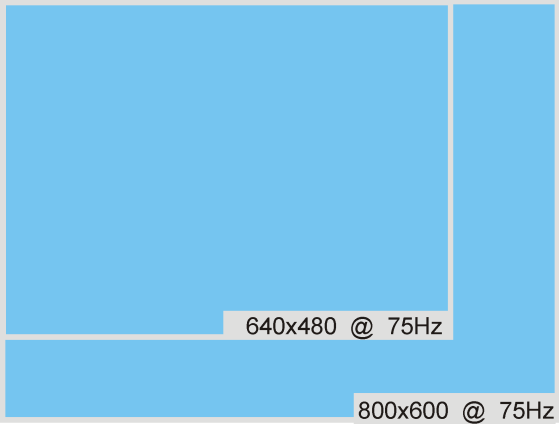
Display Test Patterns

The images shown here are not to scale. The exact color might vary depending on your monitor.

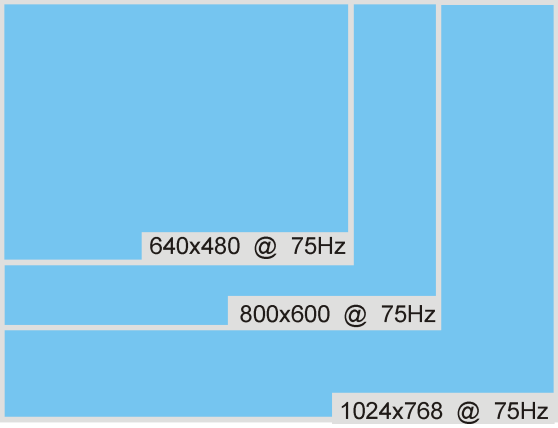
The patterns shown here are for various resolutions at a refresh frequency of 75Hz. At other refresh frequencies, the text '75Hz' in the images would be replaced with the appropriate refresh frequency.

Resolution: 640 x 480

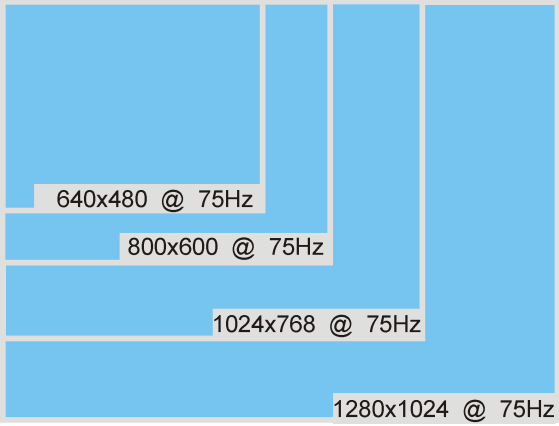
Resolution: 800 x 600



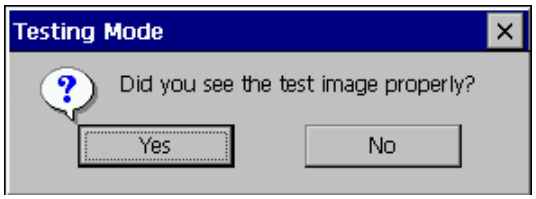
Resolution: 1024 x 768



Resolution: 1280 x 1024

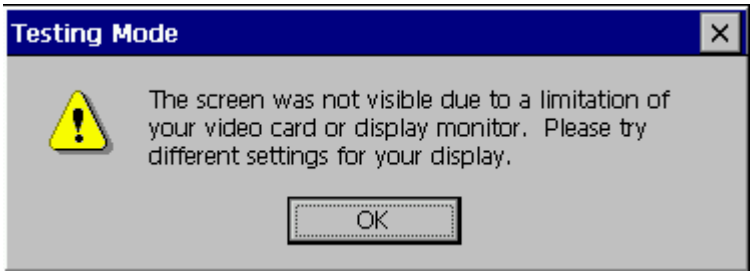


If your monitor supports the selected setting, one of the above test patterns is displayed for approximately 5 to 10 seconds. Then the screen becomes blank again. After another delay of approximately 5 to 10 seconds, the following prompt is displayed.



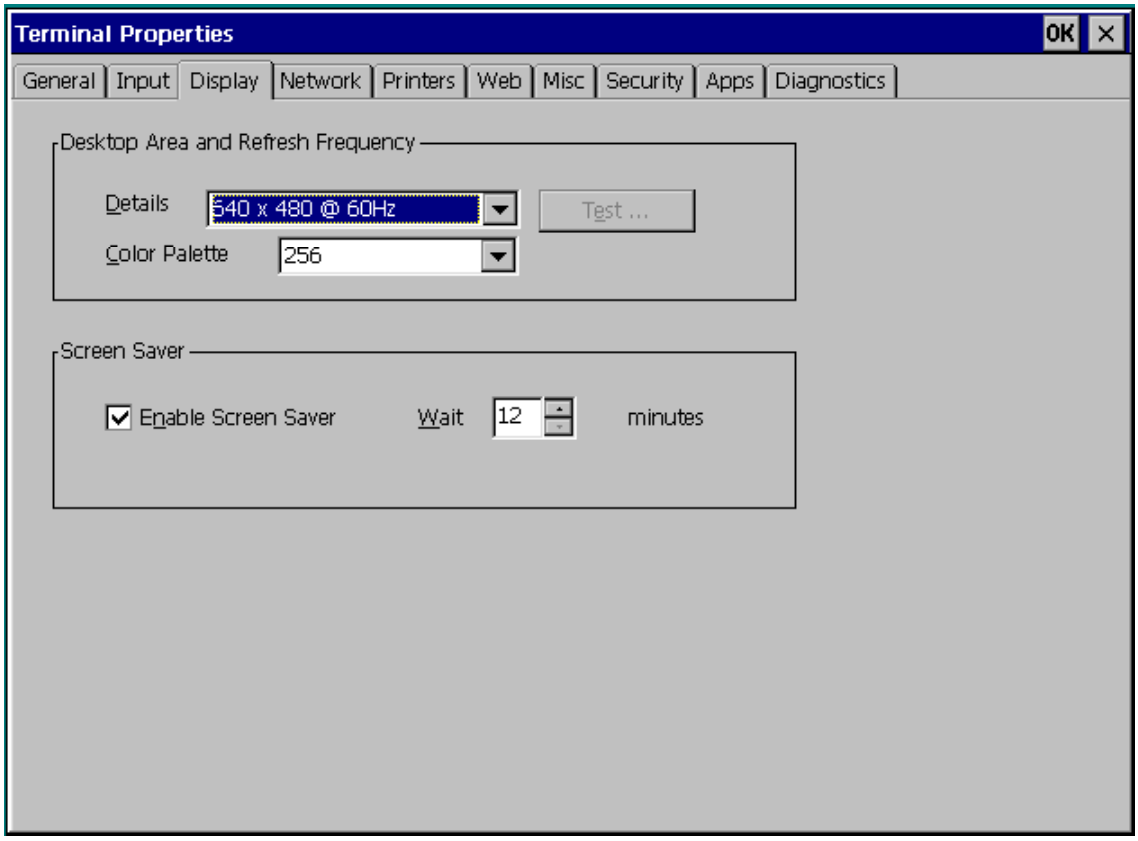
NOTE: IN MONITORS WITH OSD FEATURE, THE ABOVE PROMPT IS DISPLAYED AFTER A DELAY OF 35 TO 40 SECONDS. THE EXACT DURATION OF THE DELAY WOULD DEPEND ON THE MODEL OF THE MONITOR CONNECTED TO THE CLIENT.

- If the appropriate test pattern was not displayed, click **No**. The following message is displayed.



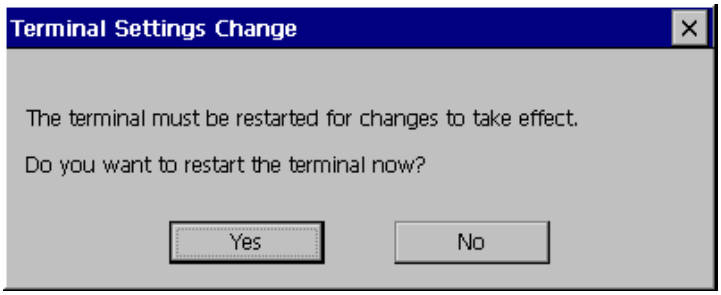
Click **OK** to return to the **Terminal Properties** dialog-box. Select a different setting and repeat the test until you hit the right setting.

- If the appropriate test pattern was displayed, click **Yes** to return to the **Terminal Properties** dialog-box.



- **Color Palette**: This drop-down list allows you to define the color depth for the display unit connected to the client. The options available are **256** (*8-bit*) and **65536** (*16-bit*).
- **Enable Screen Saver:** By default, this check-box is selected. It is recommended that the screen saver be enabled to protect your display unit.
- **Wait:** This field is enabled only when the **Enable Screen Saver** check-box is selected. Specify the duration (*in minutes*) of inactivity after which the screensaver should be launched. The default duration is **12** minutes.

3. Click **OK** to save changes or **X** to cancel changes. If you click **OK**, the following prompt is displayed.



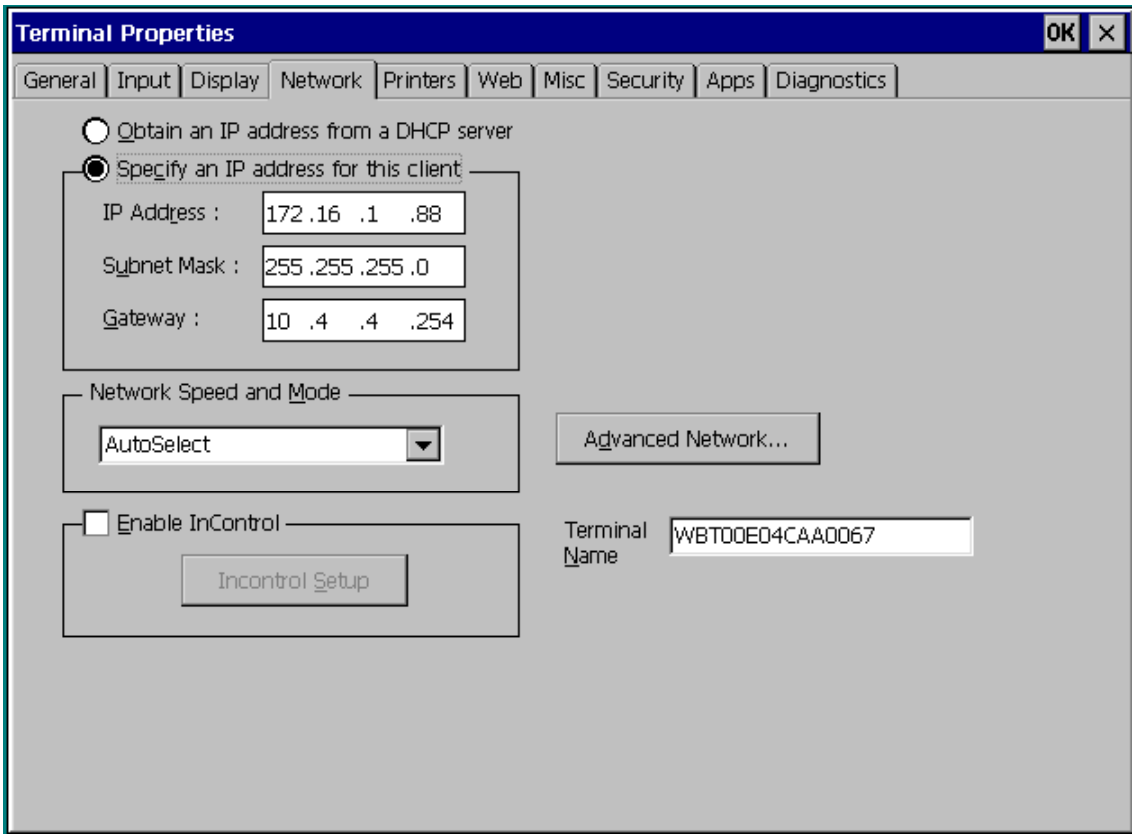
Click **Yes** to shutdown and restart the client. Click **No** if you do not want to restart the client.

Network (IP address, network speed, inControl, DNS, WINS)

To configure the IP address, network speed, inControl settings and other network parameters,

1. Press the **F2** key on your keyboard while the **Terminal Connection Manager** window is displayed.
2. Select the **Network** tab.

TIP: TO SWITCH TO THE **TERMINAL CONNECTION MANAGER** FROM AN OPEN SESSION, PRESS **CTRL+ALT+END**.



- **Obtain an IP Address from a DHCP Server**: If this radio-button is selected, the client tries to obtain an IP address from a DHCP server on the network. You can select this option if your network has a DHCP server.

TIP: TO IMPLEMENT LPD PRINTING (*PAGE 35*), IT IS RECOMMENDED THAT YOU SPECIFY A **FIXED IP ADDRESS** FOR THE CLIENT. THIS IS BECAUSE AT THE SERVER-SIDE YOU MUST SPECIFY THE IP ADDRESS OF THE CLIENT THAT IS CONFIGURED AS A PRINT-SERVER. IF YOU MUST USE **DHCP**, THEN IT IS PREFERABLE THAT YOU RESERVE AN IP ADDRESS ON THE DHCP SERVER, FOR THE CLIENT THAT YOU PLAN TO CONFIGURE AS LPD-SERVER.

- **Specify an IP Address**: If you want to assign a fixed IP address to the client, select this radio-button. The **IP Address** and **Subnet Mask** fields will be enabled.

  IP Address: Provide a fixed IP address for the client in this field.

  Subnet Mask: Provide the subnet mask.

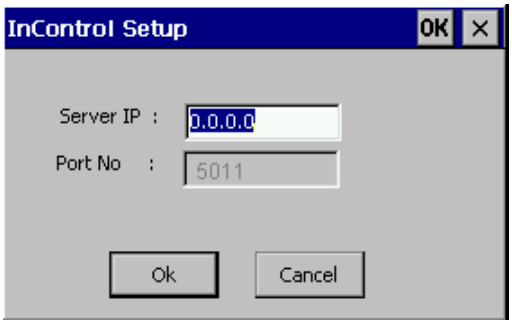
  Gateway: Provide the IP address of the gateway in this field. The gateway is essential to browse the Internet using the in-built Internet Explorer browser, and to enumerate applications published on NFuse servers.

- **Network Speed and Mode**: From this drop-down list, select an appropriate network speed and transmission mode. By default, the **AutoSelect** option is selected.

- **Enable InControl**: *inControl* is a utility using which the system administrator can control and configure the clients from a remote server. Detailed information about this utility is provided in the *inControl for Terminals Administrator's Guide*, which is in the CD supplied with the product.

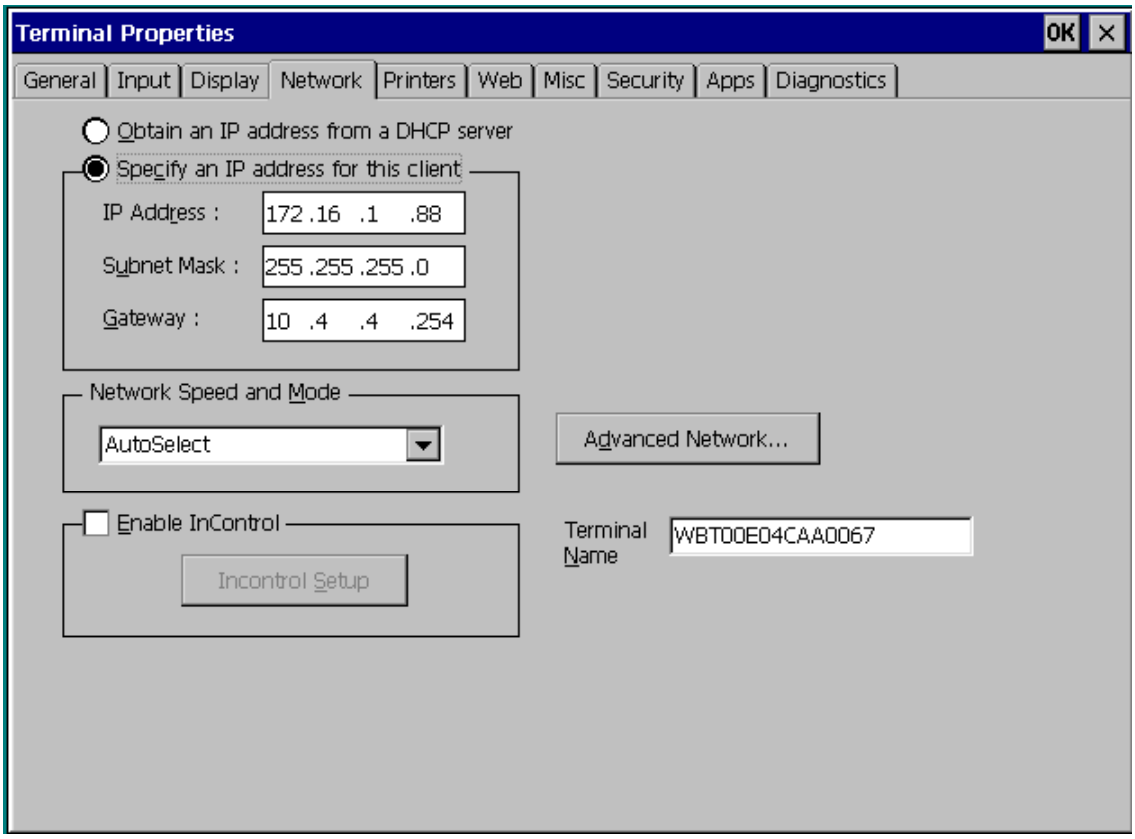
  If the server, on which the inControl software is installed, is not in the same network or subnet as the client, select the **Enable InControl** check-box. The **InControl Setup** button is enabled. Click this button. The following dialog-box is displayed.

NOTE: YOU NEED NOT PERFORM THIS PROCEDURE ON CLIENTS IN THE SAME NETWORK OR SUBNET AS THE INCONTROL SERVER, BECAUSE SUCH CLIENTS AUTOMATICALLY RECOGNIZE THE IP ADDRESS AND PORT NUMBER OF THE INCONTROL SERVER.

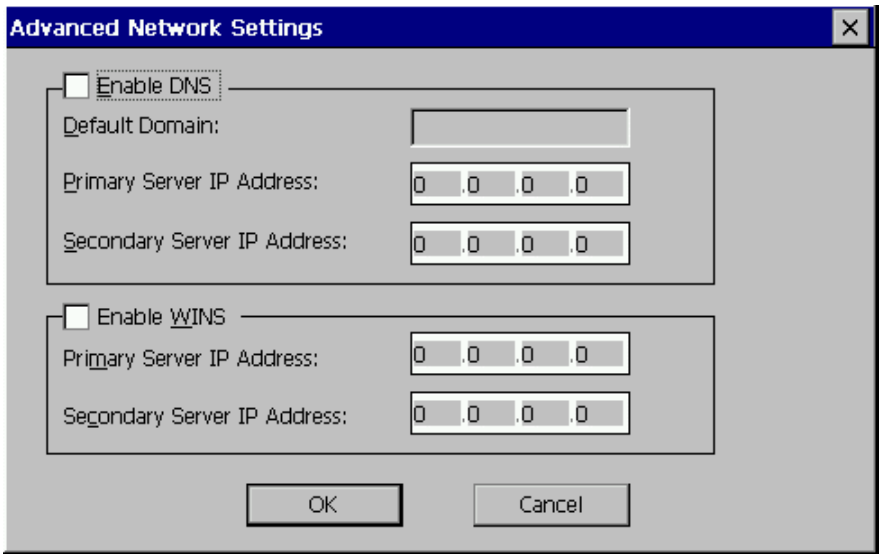


Enter the IP address of the server on which inControl for Terminals is installed in the **Server IP** field. The **Port No** field cannot be edited.

Click **OK** to return to the **Terminal Properties** dialog-box.



- **Advanced Network:** Click this button to invoke the **Advanced Network Settings** dialog-box.



- **Enable DNS**: If your network has a DNS server and you want to use it, enable this option. When this check-box is enabled, the following text fields will also be enabled:

NOTE: DNS MUST BE ENABLED TO BROWSE THE INTERNET USING THE IN-BUILT INTERNET EXPLORER BROWSER.

Default domain: Specify the default domain name of your network

Primary Server IP Address: Provide the IP address of the primary Domain Name Server in your network.

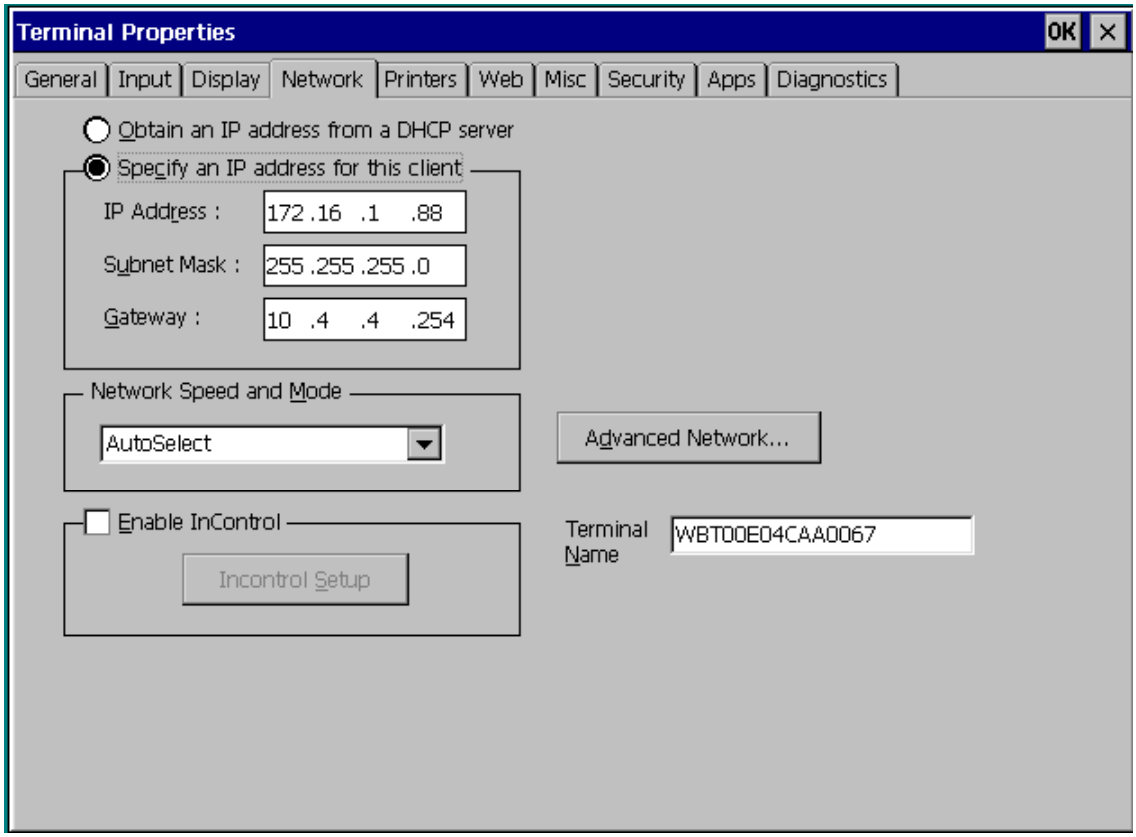
Secondary Server IP Address: Provide the IP address of the secondary Domain Name Server in your network.

- **Enable WINS**: As with the DNS server, your network may make use of the WINS services provided by Windows based networking. Enable this check-box to set parameters for the WINS Server.

  Primary Server IP Address: Provide the IP address of the primary WINS Server.

  Secondary Server IP Address: Provide the IP address of the secondary WINS Server.

Click OK to return to the **Terminal Properties** dialog-box.



- **Terminal Name**: This field automatically displays a unique client-name for the client. The default name consists of the letter 'R' followed by the last six characters of the MAC address (*page* 60) of the client.

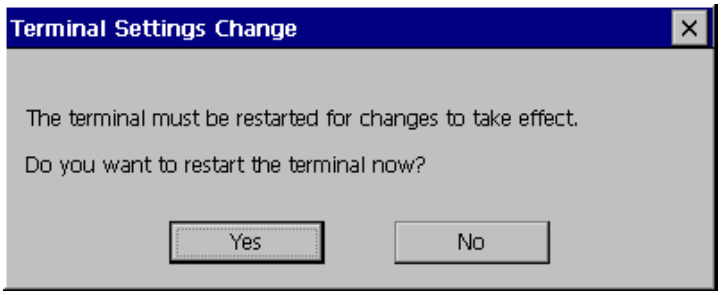
  When the client is connected to servers using RDP connections, this name is used to identify resources such as printer and COM ports of the client. If you do not provide a unique name, you may have problems accessing resources or published applications. Besides, since the name specified here is used by the Windows 2000 license-manager, duplicate names could cause licensing problems.

  You can change the RDP client name by editing this field. Ensure that the name you provide is unique. The following rules are applicable to the RDP client-name parameter.

  - The name can have a maximum of seven characters.
  - Blank spaces and the following special characters are not allowed: < > * + = \\ | ? : ; ~ $ % ^ { } @ / \ # and ,(comma).

3. Click **OK** to save changes or **X** to cancel changes.

If you click **OK**, the following prompt is displayed.



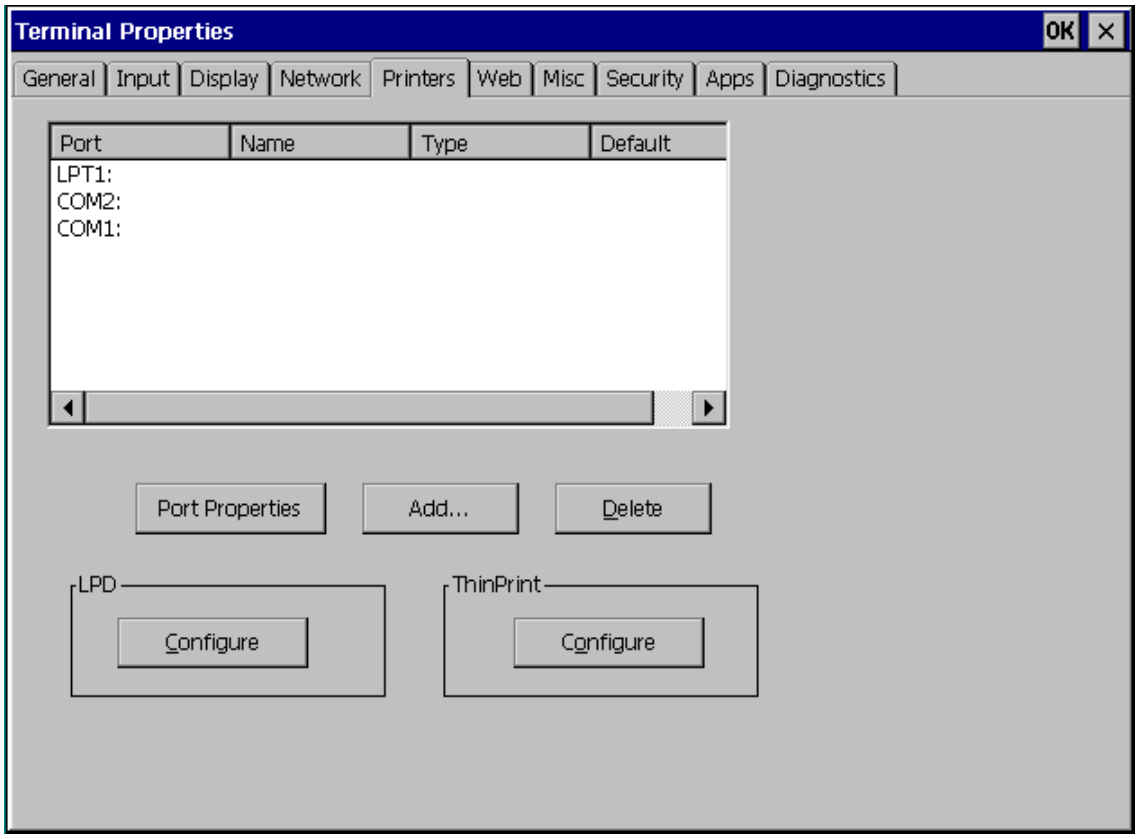
The client **must** be restarted for changes to take effect. Click **Yes** to shutdown and restart the client.

Printers

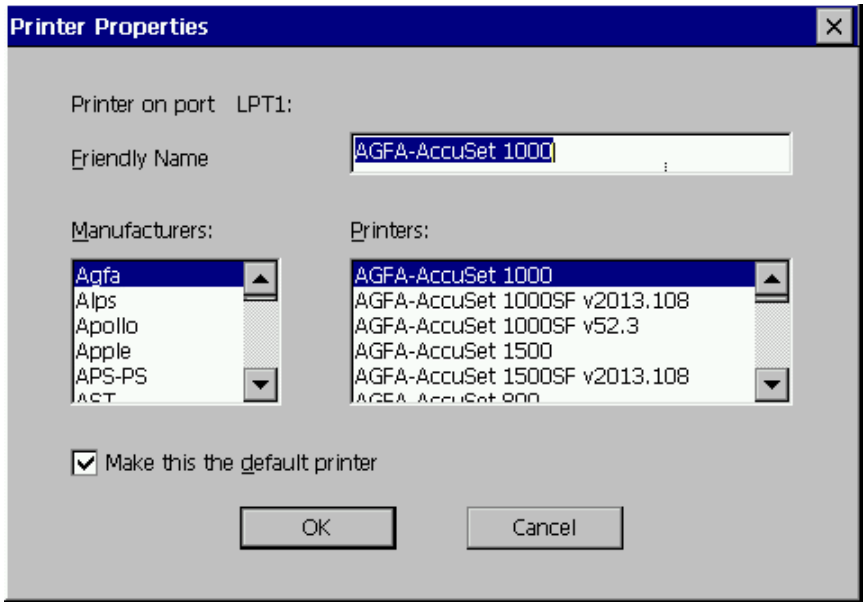
When the client is connected to a Windows 2000 server through an RDP connection, other RDP users connected to the server can access printer-ports of the client. To configure the client for this function,

1. Press the **F2** key on your keyboard while the **Terminal Connection Manager** window is displayed.
2. Select the **Printers** tab. There is a brief delay, before the tab is displayed.

TIP: TO SWITCH TO THE **TERMINAL CONNECTION MANAGER** FROM AN OPEN SESSION, PRESS **CTRL+ALT+END**.



- To add a printer, select a **Port** and click **Add**. After a brief delay, the following dialog-box is displayed.



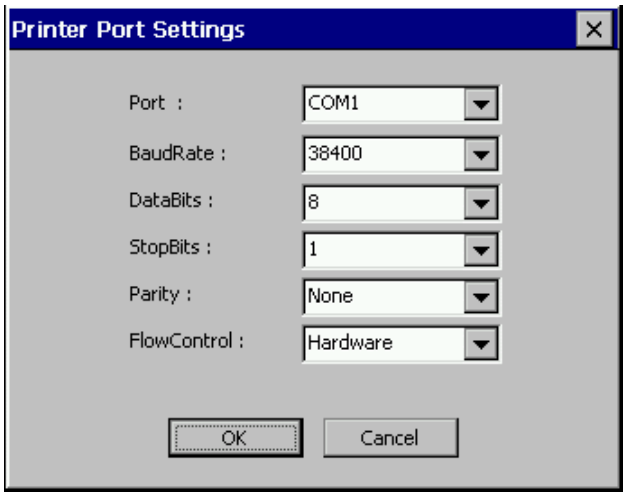
The **Printers** scroll-list in the above dialog-box contains the printer models corresponding to the printer-make selected in the **Manufacturers** scroll-list. Select the required printer-model.

By default, the model-name becomes the name of the printer. You may provide a different name in the **Friendly Name** field.

To designate the printer as the default printer, select the **Make this the default printer** check-box. After selecting the printer, click **OK** to return to the **Terminal Properties** dialog-box.

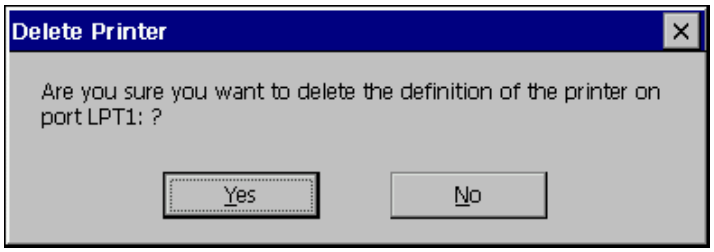
The name of the printer that you added is displayed next to the appropriate port. If the printer has been designated as the default printer, the **Default** column contains the word **Yes**.

- To configure port-parameters for a printer, highlight the appropriate entry. The **Add** button changes to **Properties**. Click this button. The following dialog-box is displayed.

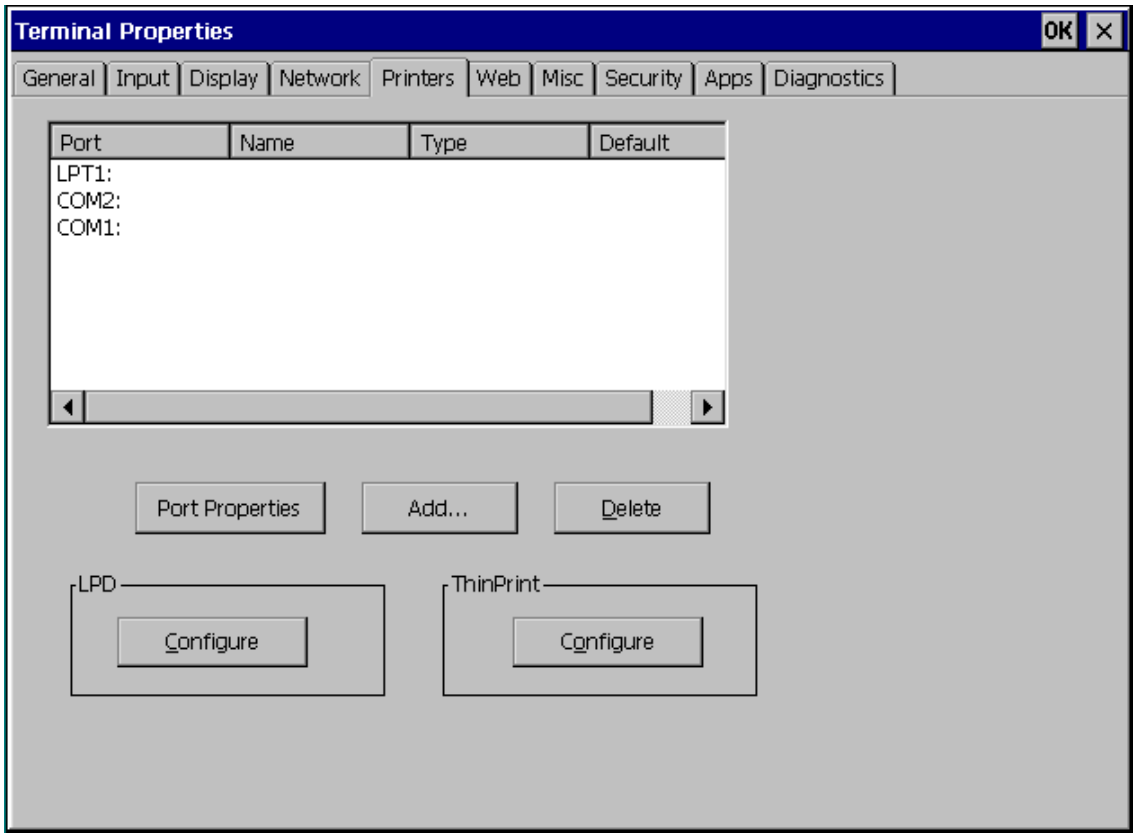


Select appropriate settings and click **OK** to return to the **Terminal Properties** dialog-box.

- To delete a printer, highlight the appropriate entry and click the **Delete** button. The following prompt is displayed.



Select **Yes** to delete the printer or **No** to cancel deletion and return to the **Terminal Properties** dialog-box.



3. Click **OK** to save changes or **X** to cancel changes. The **Terminal Connection Manager** is displayed.

LPD (Line Printer Daemon)

This is a feature with which network users can access printers connected to the client. To implement the feature you must configure appropriate client/s as print-servers (*as described in this section*) and then configure the Windows NT 4.0 TSE/2000 and UNIX/Linux servers (*as described on page 145*).

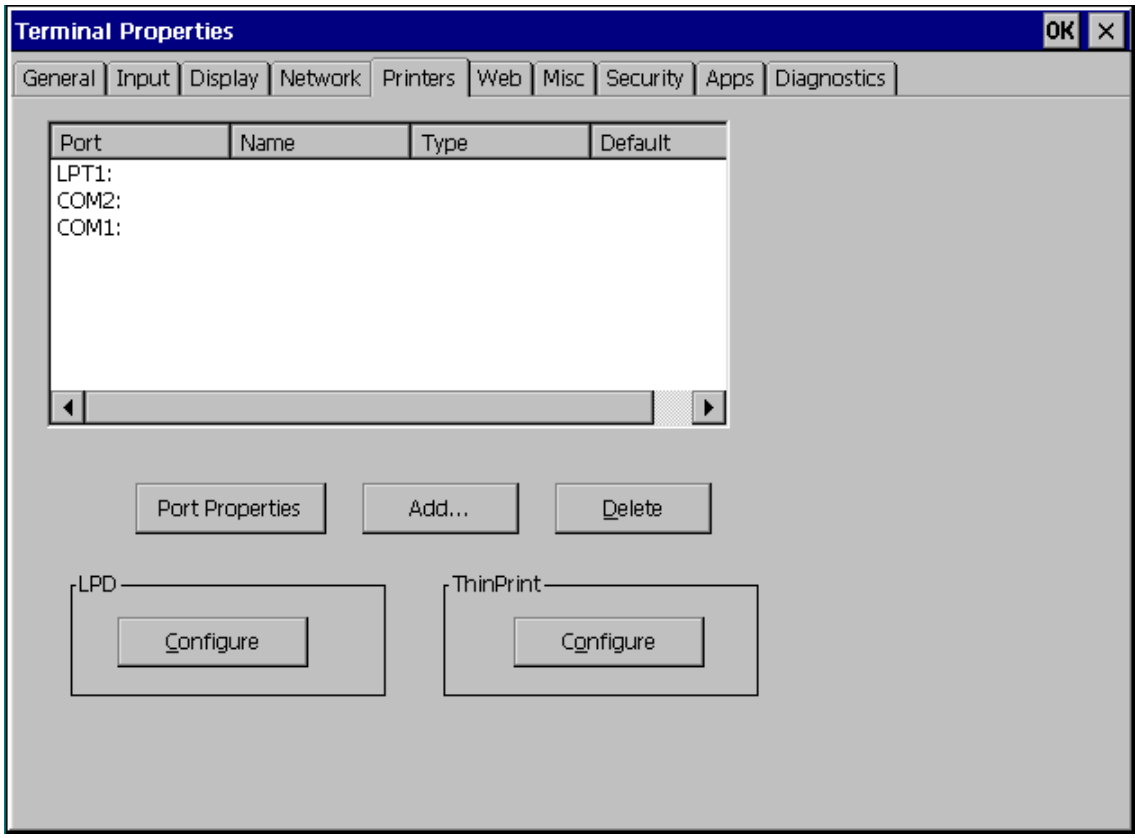
LPD printing provides the following advantages when compared to other local printing options (*see note below for the other local printing options*).

- In other local printing options, the client must be connected to the server to act as a print-server. Clients configured using the Line Printer Daemon start functioning as print-servers as soon as they are switched on.
- During an ICA session, if a client receives a print-job from another ICA user, the receiving client may become slow and even temporarily unusable until the print-job is completed. This is because in ICA-printing, the print-job and other client-server traffic use the same communication channel. On the other hand, if the client is configured as a print-server using LPD, the performance of the client is not affected while it is executing print-jobs as the Line Printer Daemon uses a separate communication channel for printing.

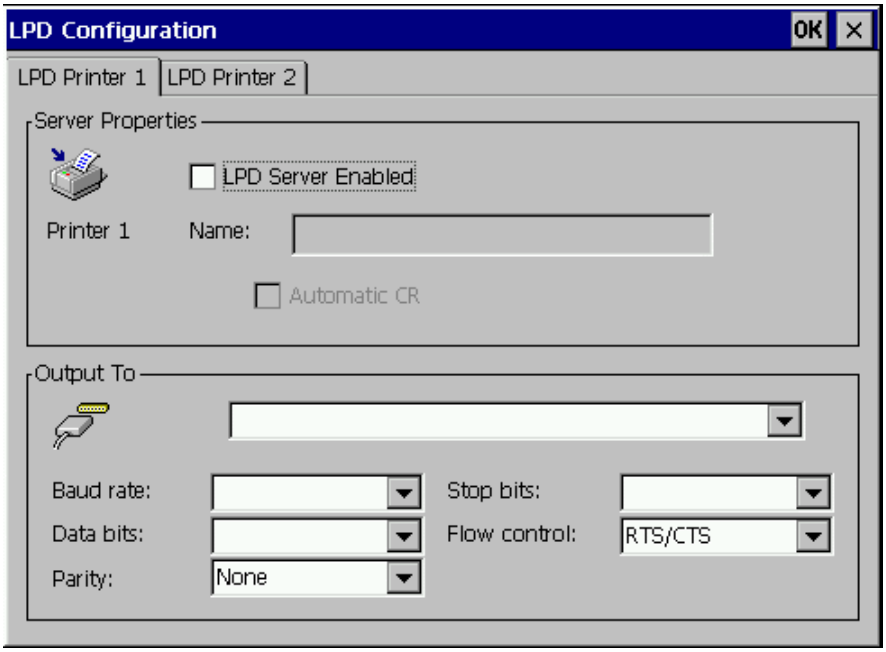
NOTE: THE FOLLOWING ARE OTHER LOCAL PRINTING OPTIONS BESIDES THE LINE PRINTER DAEMON.

- WHEN A CLIENT IS CONNECTED TO A WINDOWS 2000 SERVER USING AN RDP CONNECTION, RDP USERS IN THE NETWORK CAN ACCESS THE PRINTER PORT OF THE CLIENT. THE PROCEDURE TO IMPLEMENT THIS FEATURE IS DESCRIBED ON PAGE 32.
- DURING ICA SESSIONS, THE PRINTER PORTS OF CLIENTS CAN BE ACCESSED BY ICA USERS IN THE NETWORK IF THE USE PRINTER CONFIGURATION UTILITY OPTION (*PAGE 76*) IS APPROPRIATELY CONFIGURED WHILE CREATING THE ICA CONNECTION.

To configure a client as a print server using LPD, press **F2** while the **Terminal Connection Manager** window is displayed. Select the **Printers** Tab.



Click the **Configure** button under **LPD**. The following dialog-box is displayed.

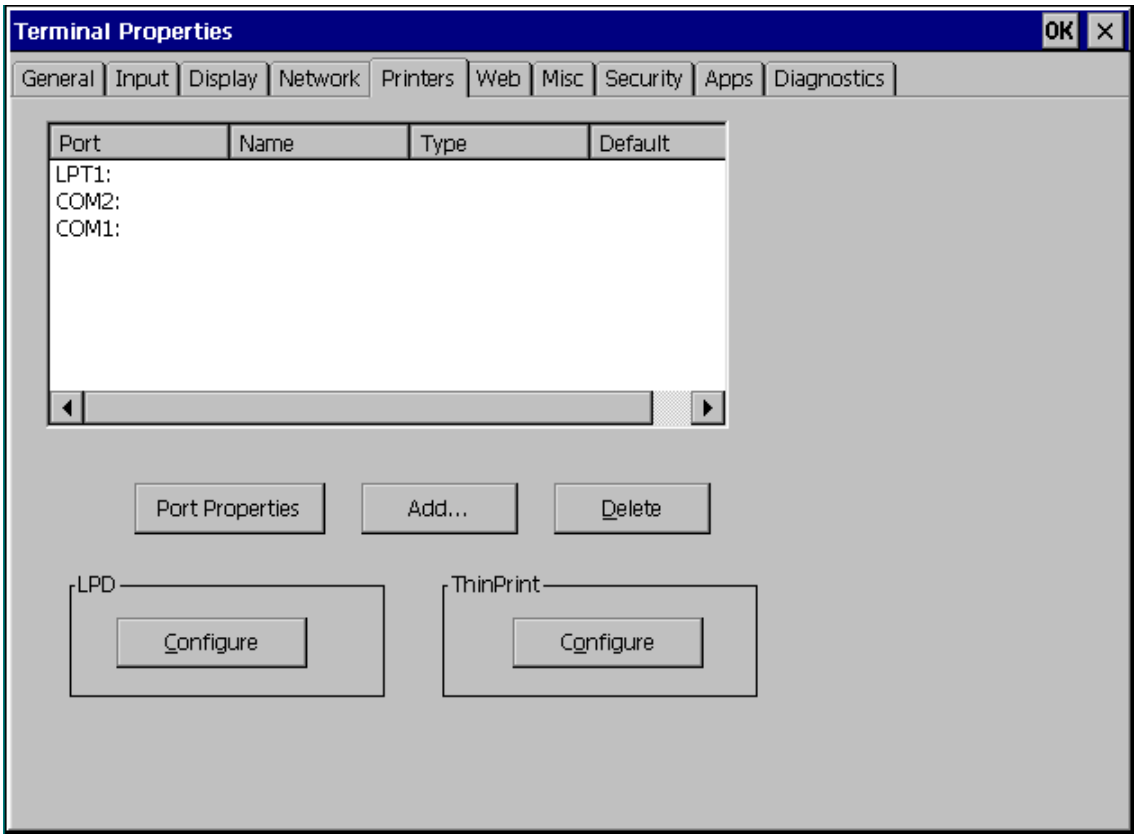


TIP: TO IMPLEMENT LPD PRINTING, IT IS RECOMMENDED THAT YOU SPECIFY A **FIXED IP ADDRESS** FOR THE CLIENT. THIS IS BECAUSE AT THE SERVER-SIDE YOU MUST SPECIFY THE IP ADDRESS OF THE CLIENT THAT IS CONFIGURED AS A PRINT SERVER. IF YOU MUST USE **DHCP**, THEN IT IS PREFERABLE THAT YOU RESERVE AN IP ADDRESS ON THE DHCP SERVER, FOR THE CLIENT THAT YOU WANT TO CONFIGURE AS LPD-SERVER.

The above dialog-box has two tabs. You can configure one printer in each tab. The fields in both tabs are identical.

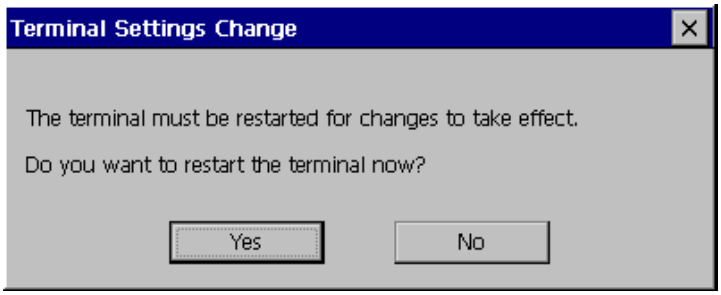
- **LPD Server Enabled**: Select this check-box to enable the Line Printer Daemon server. The **Name** field is enabled.
- **Name**: Provide a name for the printer in this field.
- **Automatic CR**: Most print spoolers automatically perform carriage returns. However, certain print spoolers (*for instance printing from a SCO UNIX server*) require carriage returns to be explicitly specified. In such cases, select this check-box. On the other hand, if you have custom printing applications with in-built carriage returns, you must ensure that this check-box is not selected.
- **Output To**: From this drop-down list, select the port to which the printer is connected. If you select a COM port, the **Baud rate**, **Data bits**, **Parity**, **Stop bits** and **Flow control** fields are enabled.

Select appropriate settings for the above parameters and click **OK** to return to the **Terminal Properties** dialog-box.



Click **OK** to save changes or **X** to cancel changes.

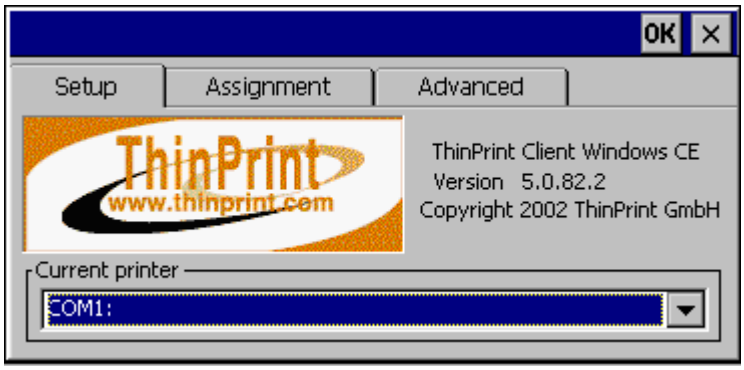
If you click **OK**, the following prompt is displayed.



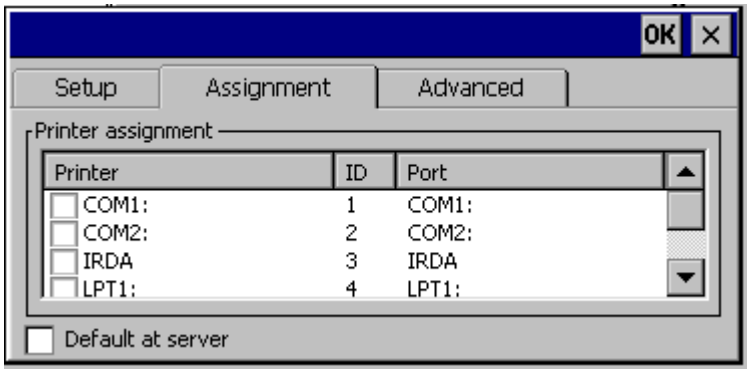
Click **Yes** to shutdown and restart the client.

Thin Print

You can also print to the client's local printer using the Thin Print. Click Configure under Thin Print in the Terminal Properties box. The following dialog box is displayed.

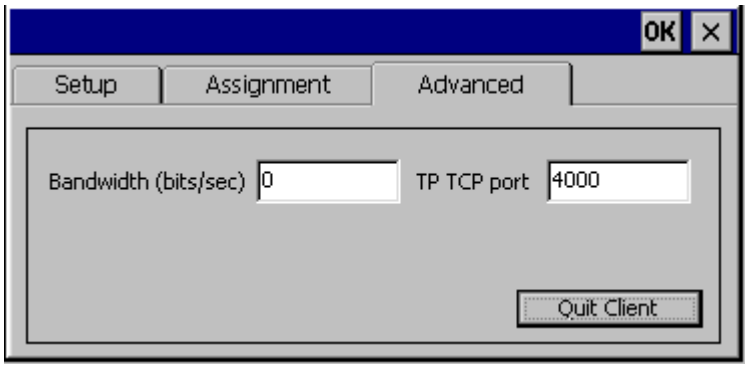


Current Printer list box displays the default printer port. Select the Assignment tab.



The Assignment tab displays information about available printers. You can assign a printer name to the printer connected to the corresponding printer port by double clicking on it and assigning a name to it.

Select the Advanced tab.



Enter a bandwidth value which is the same or smaller than that set in the server. The port number should be the same on both the server and the client.

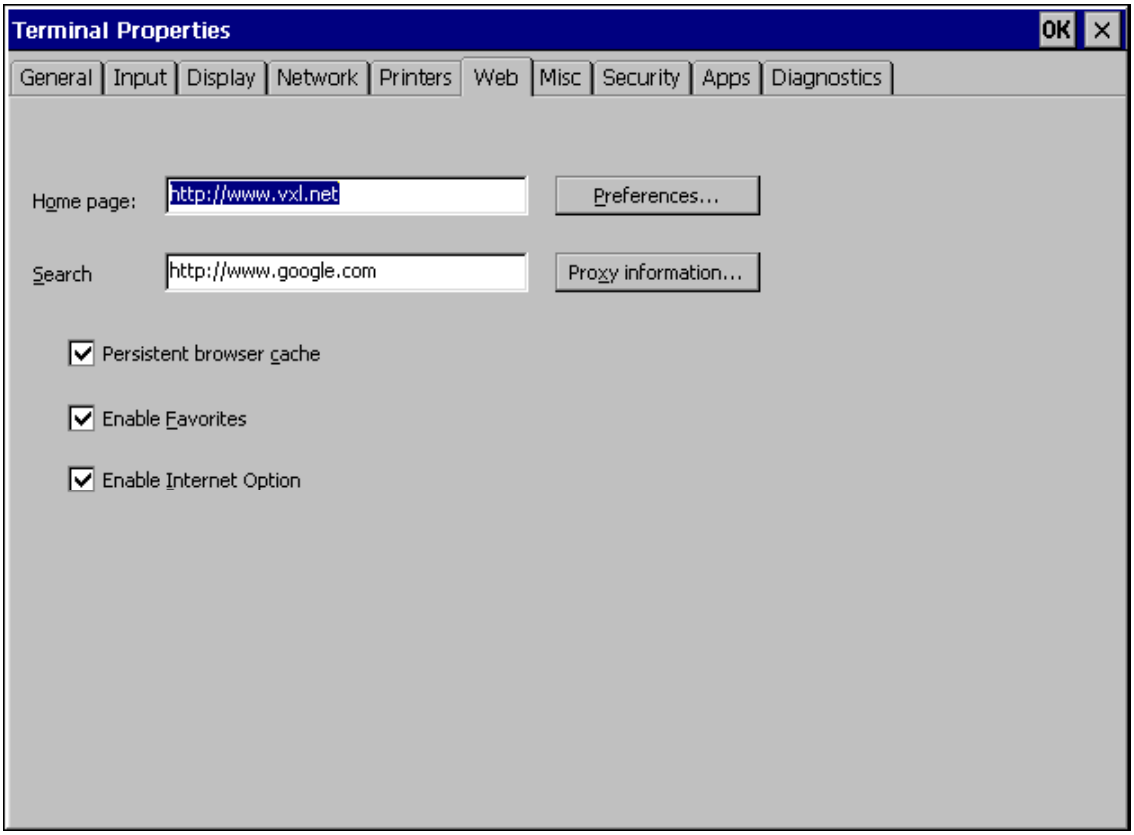
For details about Thin Print and server settings for Thin Print, refer to the Thin Print User Manual.

Web

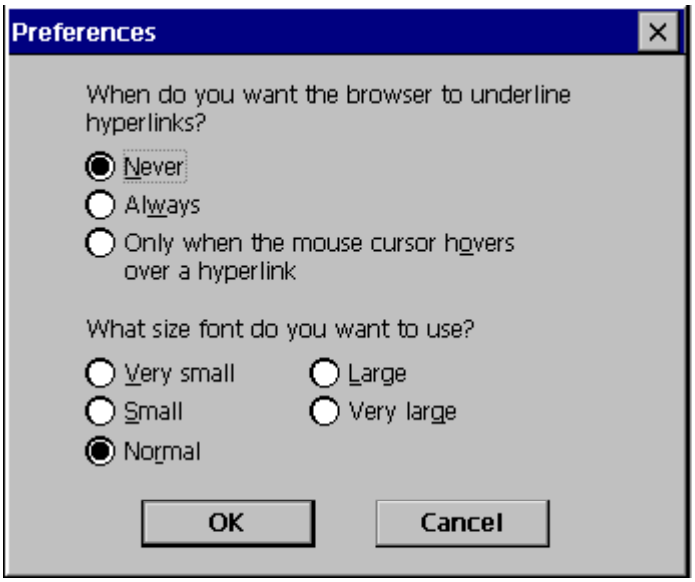
The firmware of the client includes Microsoft Internet Explorer 4.01. You can set the appearance and enable the features of the browser window.

1. Press the **F2** key on your keyboard while the **Terminal Connection Manager** window is displayed.
2. Select the **Web** tab.

TIP: TO SWITCH TO THE **TERMINAL CONNECTION MANAGER** FROM AN OPEN SESSION, PRESS **CTRL+ALT+END**.

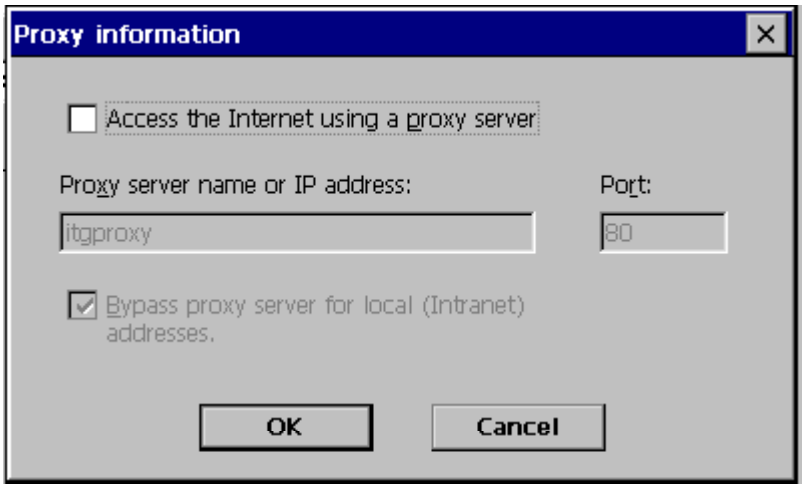


- **Home page:** Enter the URL of the home page to be displayed when opening the browser window.
- **Search:** Enter the URL of the search page to be displayed when you click the search option.
- **Persistent browser cache:** Enable this option if you want the contents of the browser cache to be retained between the sessions
- **Enable Favorites:** Enable this option to enable the Favorite feature of the browser:
- **Enable Internet option:** The Internet option feature allows you modify the settings of the browser including the Preferences and Proxy information.
- **Preferences:** This feature enables you to customize the appearance of the hyperlinks and the font size. Click **Preferences** button. The following dialog box appears:



Make appropriate selections/entries in the above dialog box. Click **OK** to return to the **Terminal Properties** box.

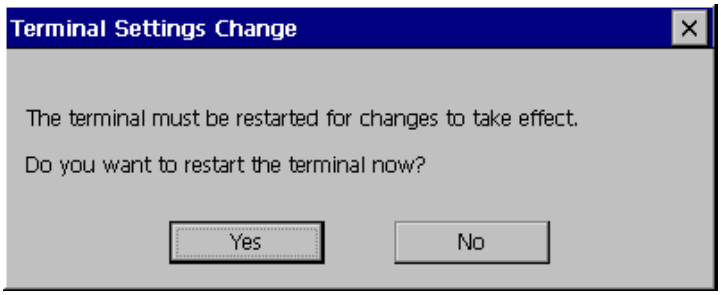
- **Proxy information:** To access the Internet using the Proxy server, click Proxy Server button.



Check **Access the Internet using a proxy server** box. Enter the Proxy server name or the IP Address and the Port number. Click **OK.**

3. Make appropriate selection/entries in the above options.
4. Click **OK** to save changes or **X** to cancel changes in the Terminal Properties box.

If you click **OK**, the following prompt is displayed.



Click **Yes** to shutdown and restart the client.

Misc (global ICA settings and audio volume)

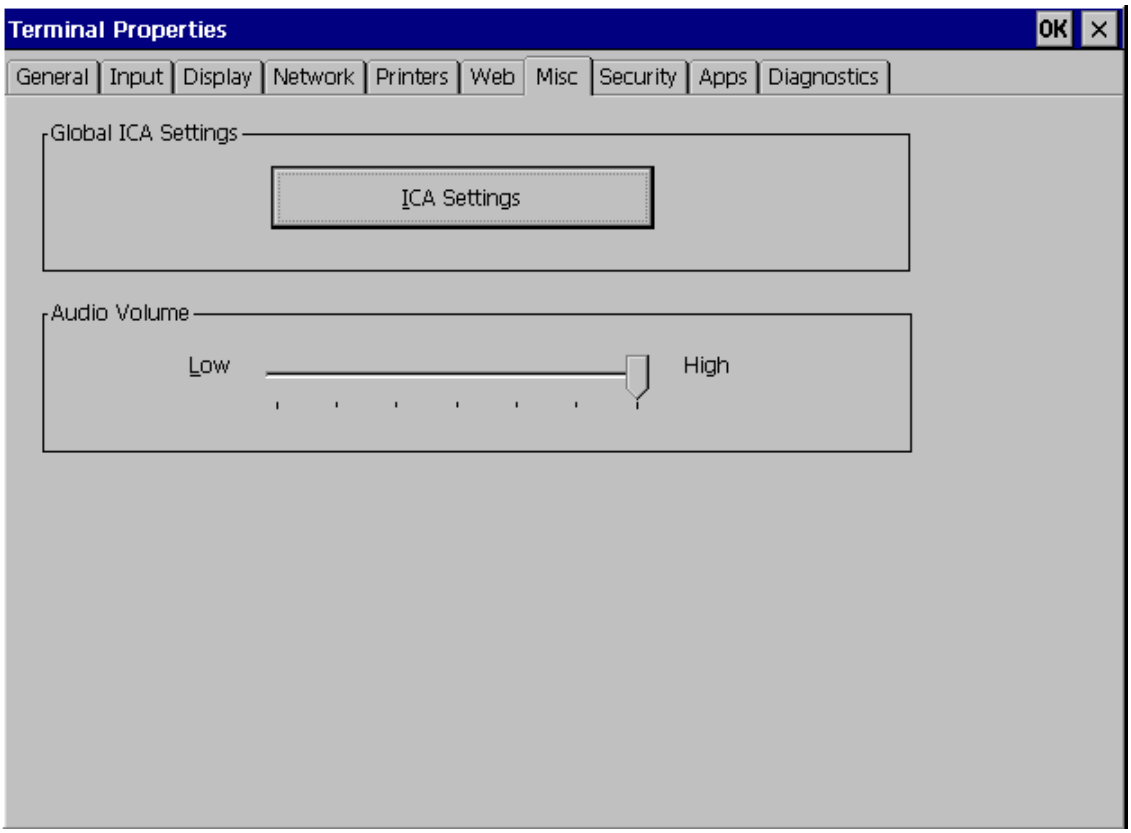
This section describes the procedure to configure the following parameters:

- Audio volume
- Global ICA settings – Hotkeys
- Global ICA settings – Window Color and Client Name
- Global ICA settings – Server Location
- Global ICA settings – Firewall Settings
- Global ICA settings – PNLite (NFuse server parameters)

To configure the above parameters,

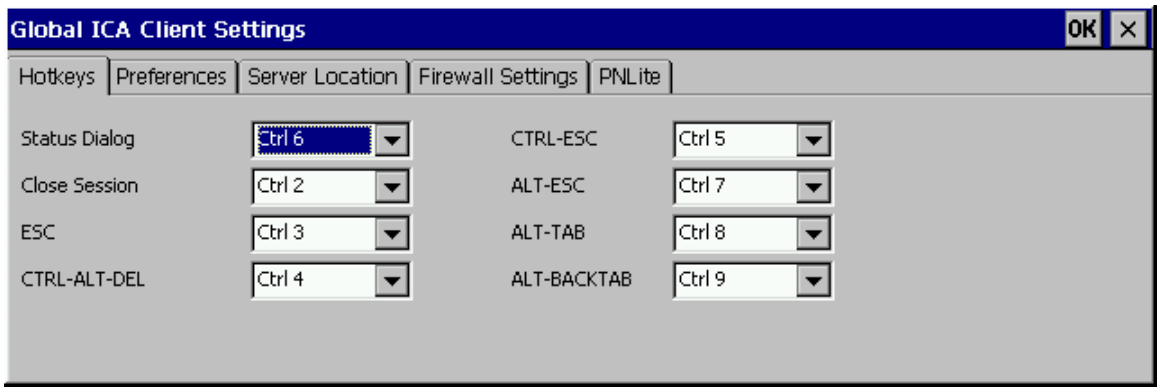
1. Press the **F2** key on your keyboard while the **Terminal Connection Manager** window is displayed.
2. Select the **Misc** tab.

TIP: TO SWITCH TO THE **TERMINAL CONNECTION MANAGER** FROM AN OPEN SESSION, PRESS **CTRL+ALT+END**.



- **Audio Volume**: Set the audio volume level using this slider-control. The default setting is **High**.
- **Global ICA Settings**: This option allows you to define hotkeys, color-depth, server-location and firewall settings globally for all defined ICA connections. It also allows you to configure the client to access applications published by a Citrix NFuse server. Click the **ICA settings** button. The **Global ICA Client Settings** dialog-box is displayed. This dialog-box has four tabs.

Global ICA Settings - Hotkeys

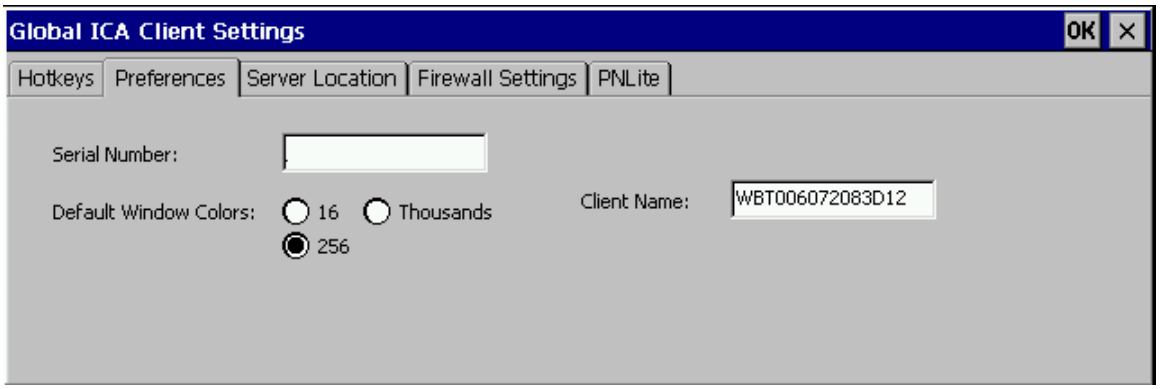


The above tab allows you to specify hotkeys that can be used during ICA sessions to invoke various functions. Some hotkeys control the behavior of ICA windows, while others emulate standard Windows hotkeys. The following table describes the various hotkeys.

Hotkey	*Function*
Status Dialog	Displays the ICA connection status.
Close Session	You can use this hotkey to disconnect an ICA session and return to the desktop. The session will however continue to run on the server until you log out.
ESC	This is a hotkey for the **Escape** function.
CTRL-ALT-DEL	Displays the Windows NT 4.0 TSE Security dialog-box.
CTRL-ESC	On WinFrame servers, pressing this key-sequence displays the Remote Task List. On MetaFrame servers, this key-sequence displays the Windows NT 4.0 TSE Start menu.
ALT-ESC	This hotkey cycles the focus through all the minimized icons and opens the associated applications.
ALT-TAB	This hotkey cycles through applications that have been opened. A popup appears, displaying the programs as you cycle through them.
ALT-BACKTAB	This hotkey cycles through open applications in the opposite direction from the **ALT+TAB** hotkey.

After configuring hotkeys, click **OK** to return to the **Terminal Properties** dialog-box.

Global ICA Settings - Window Colors and Client Name



- **Serial Number**: This is the serial number of the ICA client software. This field is necessary only when you are using the client with WinFrame Host/Terminal, which requires each client to have a Citrix PC Client Pack serial number to connect to the server. Provide the serial number exactly as it appears on the serial number card.

NOTE: THE SERIAL NUMBER IS NOT REQUIRED FOR THIN CLIENT.

- **Default Window Colors**: Specify the number of colors that will be used to display the ICA session by selecting the appropriate radio-button. While using a PPP connection, 16-color mode may provide better performance.

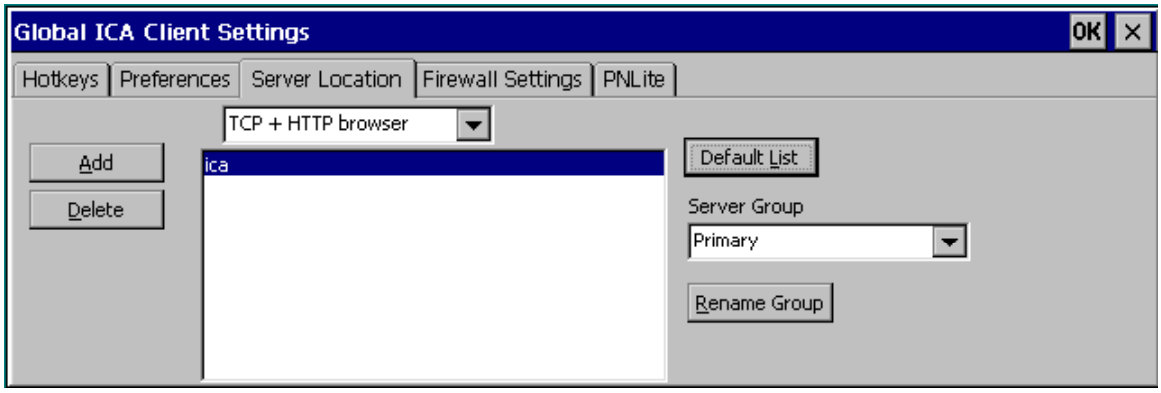
  If the window options specified exceed the capabilities of the client-hardware, the maximum size and color-depth supported by the Windows CE operating system are used. The **Thousands** option indicates 16-bit color.

NOTE: 16-BIT COLOR IS SUPPORTED ONLY BY METAFRAME 1.8 FEATURE RELEASE-1, METAFRAME XP AND ABOVE. CDS DOES NOT SUPPORT THE 16-BIT COLOR OPTION. IF YOU SELECT THE 16-BIT COLOR OPTION FOR SERVERS THAT DO NOT SUPPORT IT, THE CLIENT DISPLAYS AT 256 COLORS.

- **Client Name**: By default, the characters 'WBT' followed by the MAC address of the client are displayed in this field. You can edit the field and provide any other unique name for the client. This name is used by Citrix servers to identify resources such as printer and COM ports of the client. If you do not provide a unique name, you may have problems accessing resources or published applications.

After configuring the window color and client name, click **OK** to return to the **Terminal Properties** dialog-box.

Global ICA Settings – Server Location



If the client is part of a WAN or operates across different subnets, you must provide the IP addresses of master browsers to search for MetaFrame servers and published applications on the network.

In the above dialog-box, you can select the method to find Citrix servers and published applications on the network. If the **(Auto-Locate)** entry is highlighted in the **Address** list, the client broadcasts a 'Get Nearest Citrix Server' packet. The first MetaFrame server to respond is then requested for information about servers and published applications in the network.

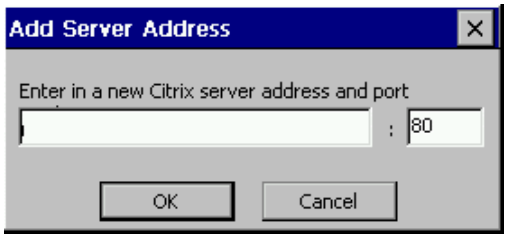
However, to eliminate broadcasts on your network, you may want to designate a particular Citrix sever as the master-browser. The network protocol setting allows you to control the way the ICA client searches. The protocols are:

- **TCP browser:** The ICA Client uses the UDP protocol to search for Citrix servers. The ICA Client communicates with the Citrix server using ICA protocol over TCP/IP.
- **TCP + HTTP browser:** The ICA Client uses the HTTP protocol to locate Citrix servers. The ICA Client communicates with the Citrix server using ICA protocol over TCP/IP. Select this option when using the ICA Client over the Internet or via a firewall or proxy server. This is the default protocol.
- **SSL + HTTPS browser:** The ICA Client uses the HTTPS protocol to locate Citrix servers. The ICA Client communicates with the Citrix server using ICA with SSL. SSL provides strong encryption of ICA traffic and Citrix server authentication. Select this option when using the ICA Client over the Internet or via a firewall or proxy server.

NOTE: THE TCP + HTTP AND SSL+HTTP PROTOCOLS CAN ONLU BE USED WITH COMPATIBLE CITRIX SERVERS. CHECK THE APPROPRIATE CTRIX SERVER ADMINISTRATOR'S GUIDE FOR FUTURE INFORMATION.

NOTE: THE TCP + HTTP AND SSL +HTTP PROTOCOLS DOES NOT SUPPORT THE **AUTO-LOCATE** FUNCTION.

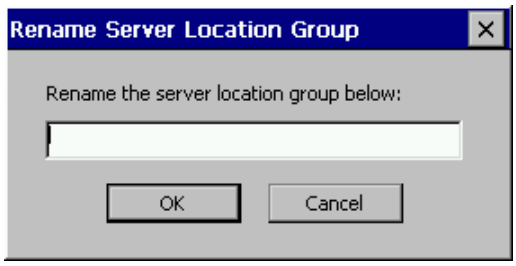
- **Server Group**: From this drop-down list you can select one of three groups of servers: **Primary**, **Backup1** and **Backup2**. The default group is **Primary**.
- To add the address of a master-browser, click **Add**. This following dialog-box is displayed.



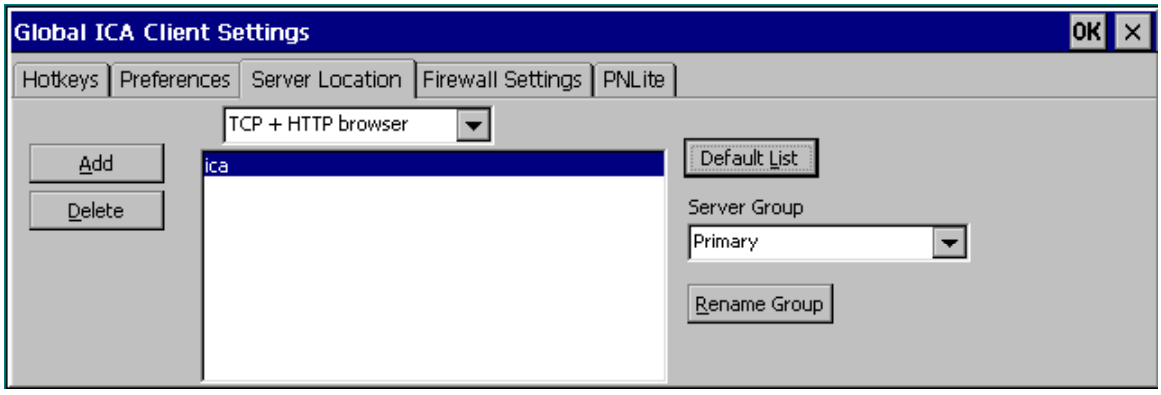
Enter the IP address of a Citrix server and a recognized port number (*the default is port 80*) and click **OK** to return to the **Server Location** dialog-box. The port number field is not displayed if you had selected TCP browser protocol in the **Server Location** dialog-box.

If you select the **TCP + HTTP or SSL + HTTP protocol** and do not add any master-browser, you must have a Citrix server on your network mapped to the default name: **ICA**. The specified server responds with a list of servers and published applications in its server farm.

- To delete an entry from the list, select it and click **Delete**.
- To recall the previous saved list of servers, click **Default List**.
- **Server Group**: With this drop-down list, you can classify listed servers into three groups - **Primary**, **Backup1** and **Backup2**. The default selection is **Primary**.
- **Rename Group**: To rename a server group, select the group and click this button. The following dialog-box is displayed.

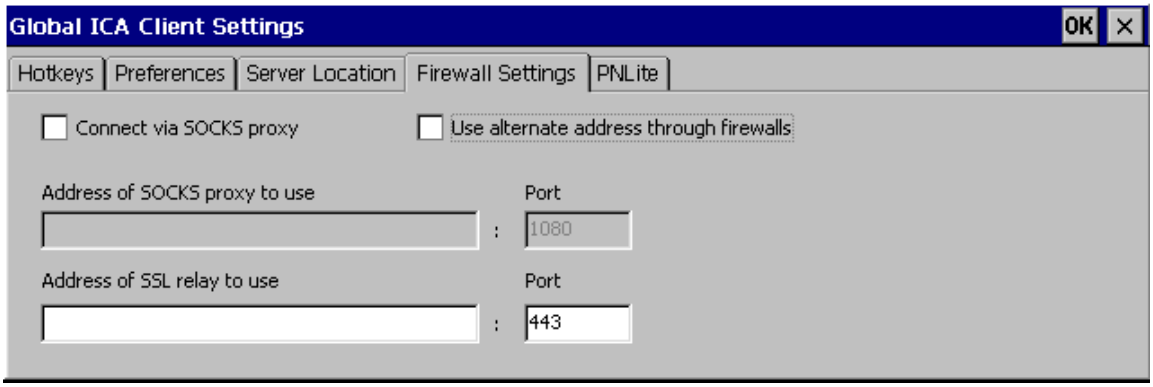


Provide a new name for the server-location group and click **OK** to return to the **Server Location** tab.



Click **OK** to return to the **Terminal Properties** dialog-box.

Global ICA Settings – Firewall Parameters



- **Use alternate address through firewalls**: Select this check-box to browse for Citrix servers or published applications that are inside a firewall from a client outside the firewall. The firewall and Citrix servers must be configured to map the internal network addresses of Citrix servers to external Internet addresses.
- **Connect via SOCKS proxy**: Select this check-box to enable a SOCKS proxy connection and to enable the input fields for the SOCKS parameters.

  SOCKS (*Socket Secure*) is a protocol that sets up a proxy server between a client and a server. The proxy server acts as a channel for communication between the client and the server.
- **Address of proxy to use**: Provide the address of the proxy server.
- **Port**: Provide the port number for the proxy server.
- **SSL:** ICA with SSL provides strong encryption to increase the privacy of your ICA connections and certificate-based server authentication to ensure the server you are connecting to is a genuine server.

  To enable SSL you must perform the following tasks:

  1. Ensure that your Citrix servers support SSL or have the SSL Relay service installed. See your Citrix server documentation for more information about configuring SSL on the server.
  2. Change the Server Location protocol to SSL+HTTPS.
  3. If the SSL Relay is not installed on the same machine as a Citrix server, or is configured to use a port other than 443, you must specify the SSL Relay address and port.
     - **Address of SSL Relay to use**: Enter the SSL Relay's domain name
     - **Port:** Enter the SSL Relay's port number

After configuring firewall settings, click **OK** to return to the **Terminal Properties** dialog-box.

Global ICA Settings – PNLite (NFuse Server Parameters)

You can configure the client to use the PNLite (Program Neighborhood Lite) feature to access applications published from a Citrix NFuse server. With this feature, clients can access applications published on the internet, without a browser.

Once configured, all applications published on the specified NFuse server are displayed as ICA connections in the **Terminal Connection Manager** window. The list of applications is refreshed every time the client is restarted.

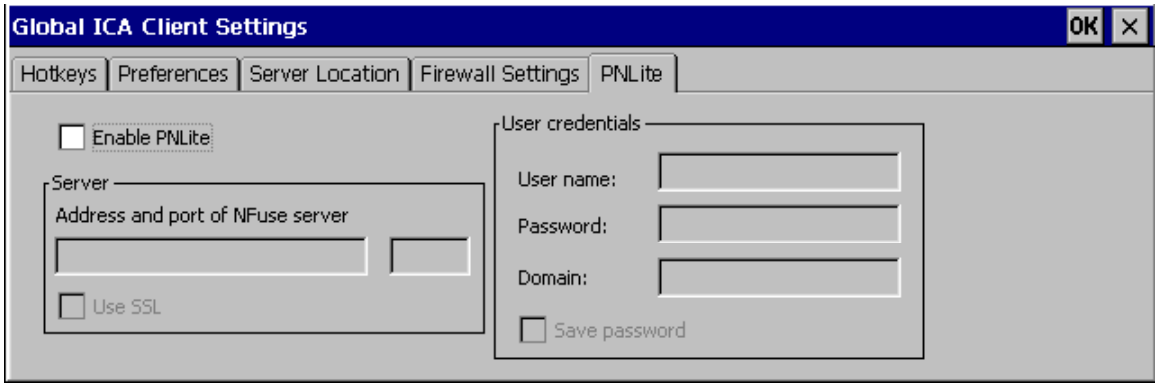
To implement this feature, you must install Citrix's NFuse on the appropriate application server.

NOTE: CDS (*CITRIX DEVICE SERVICES*) DOES NOT SUPPORT NFUSE. YOU MUST INSTALL METAFRAME TO IMPLEMENT THE NFUSE CAPABILITY.

NOTE: IF THE CLIENT/S AND THE NFUSE SERVER ARE IN DIFFERENT NETWORKS, YOU MUST SPECIFY THE GATEWAY IN THE **NETWORK** TAB OF THE **TERMINAL PROPERTIES** DIALOG-BOX.

TIP: WHILE CONFIGURING THE SERVER, NOTE THE TCP/IP PORT NUMBER THAT YOU ASSIGN TO THE NFUSE SERVICE.

After installing NFuse on the application server, configure the client through the **PNLite** tab of the **Global ICA Client Settings** dialog-box.



- **Enable PNLite**: Select this check-box to allow the client to access applications published from Citrix servers through the NFuse capability.
- **Server**: Specify the IP address of the application server and the port number assigned to the NFuse service.
- **Use SSL**: ICA with SSL provides strong encryption to increase the privacy of your ICA connections and certificate-based server authentication to ensure the server you are connecting to is a genuine server Enable this option to use SSL.
- **User credentials**: This information is used to automatically logon to the application server when you start the connection. Provide appropriate information in the **User name**, **Password** and **Domain** fields. If you want the password to be saved, select the **Save password** check-box. If you do not select the **Save password** check-box, a password prompt will be displayed every time you start a connection.

Click **OK** to save the settings. You will be prompted to restart the client. After restarting, the client automatically finds applications published on the specified NFuse server and displays them in the **Terminal Connection Manager** window. The list of applications is refreshed every time the client is restarted.

Security

This section describes the procedure to configure the following features of the client.

- Security for Client-Configuration functions: With this feature, you can introduce password-control over access to the **Terminal Properties** (F2) dialog-box.
- smart AX-s security: With this feature, you can implement the optional smart AX-s security feature of the client.

NOTE: **SMART AX-S** AND **CLIENT-CONFIGURATION SECURITY** CANNOT BE IMPLEMENTED SIMULTANEOUSLY. ENABLING ONE OF THE FEATURES AUTOMATICALLY CAUSES THE OTHER TO BE DISABLED.

- Connection fail-over: With this feature, you can configure the client to automatically attempt alternative connections in a predefined order, when a selected connection cannot be started.
- Persistent Reconnect: With this feature enabled, the client on the background continuously tries to invoke the connection.

To configure security parameters for the client, Press **F2** while the **Terminal Connection Manager** window is displayed. The **Terminal Properties** dialog-box is displayed.

Select the **Security** tab.

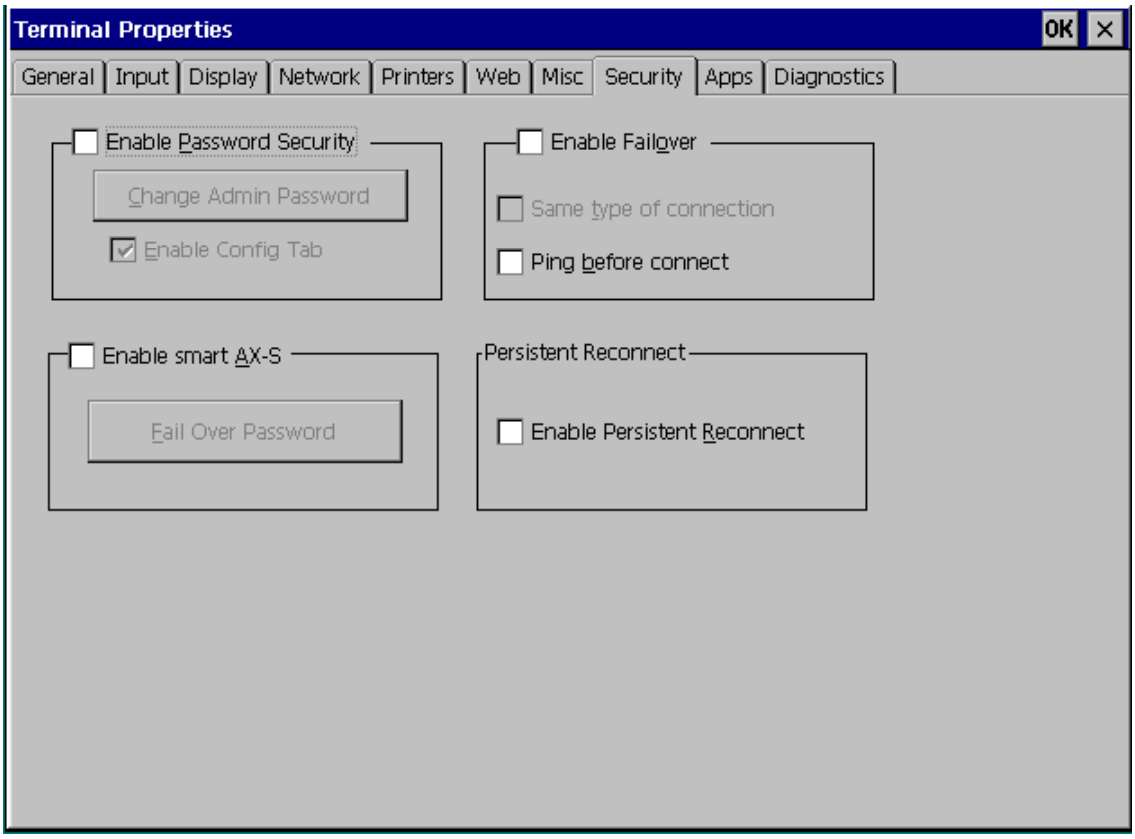
TIP: TO SWITCH TO THE **TERMINAL CONNECTION MANAGER** FROM AN OPEN SESSION, PRESS **Ctrl+Alt+End**.

Security for Client-Configuration

You can set a password to control access to the **Terminal Properties** (F2) dialog-box. When users press **F2**, a password prompt is displayed. The **Terminal Properties** dialog-box will be displayed only if the correct administrator-password is entered.

NOTE: EVEN AFTER ENABLING PASSWORD SECURITY, YOU CAN CONFIGURE THE CLIENT USING THE **inControl for Terminals** UTILITY. HOWEVER, IF YOU WANT TO CHANGE THE ADMIN-PASSWORD, YOU MUST NECESSARILY KNOW THE OLD PASSWORD. DOCUMENTATION FOR **inControl for Terminals** IS AVAILABLE IN THE CD SUPPLIED WITH THE PRODUCT.

CAUTION: DO NOT FORGET THE ADMIN-PASSWORD. IN CASE YOU DON'T REMEMBER THE PASSWORD, PLEASE CONTACT I-O CORPORATION FOR HELP.



- To implement this security feature, select the **Enable Password Security** check-box. The **Change Admin Password** button is enabled. Click this button. The following dialog-box is displayed.

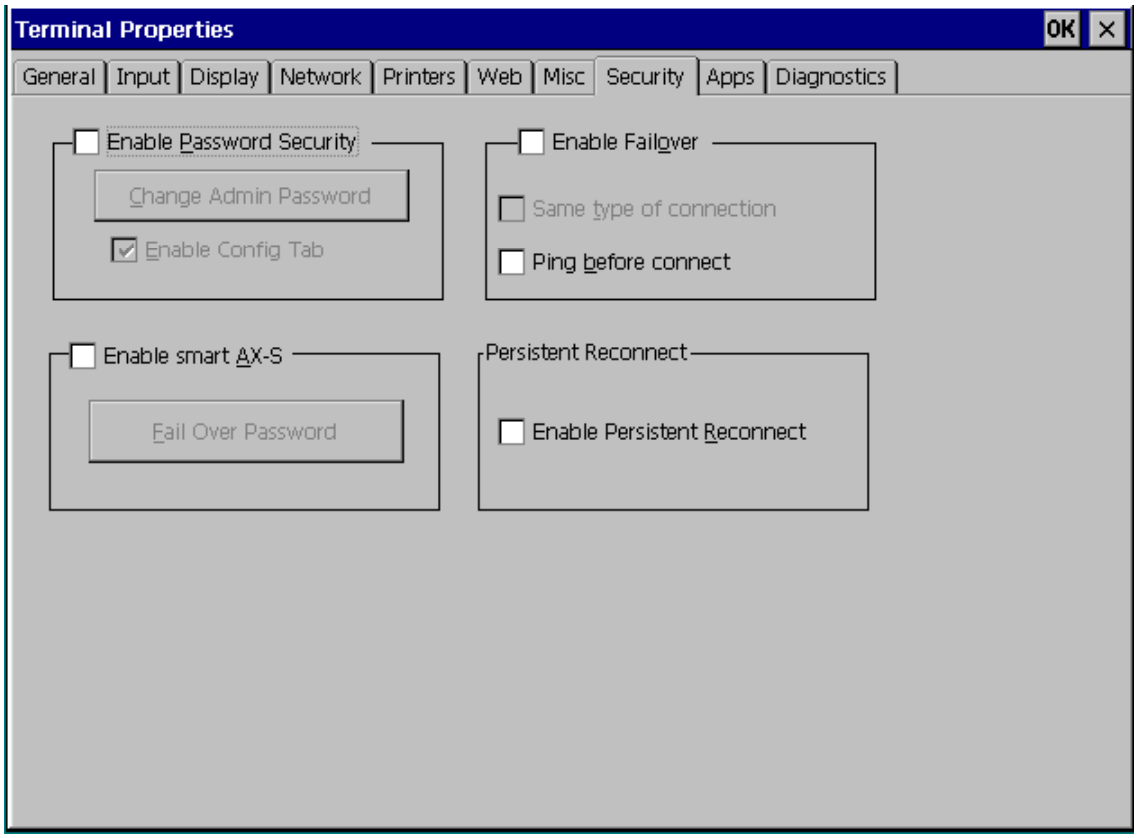
Enter a password in the **New Password** field and re-enter the same password in the **Confirm Password** field.

NOTE: THE PASSWORD IS CASE SENSITIVE. THERE IS CURRENTLY NO LIMIT ON THE LENGTH OF THE PASSWORD OR THE TYPE OF CHARACTERS ALLOWED.

Click **OK** to return to the **Terminal Properties** dialog-box.

- **Enable Config Tab**: By default, when password security is enabled, the **Configure** tab of the **Terminal Connection Manager** window is hidden. The **Configure** tab allows you to create, modify and delete connection entries. To make the **Configure** tab accessible, select the **Enable Config Tab** check-box. If you do not select this check-box, the **Terminal Connection Manager** window will display only the **Connections** tab.

smart AX-s Security



This option allows you to enable the **smart AX-s** security feature of the client.

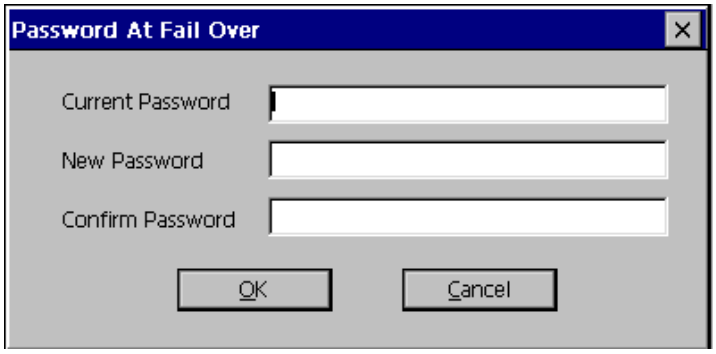
If **smart AX-s** is enabled, users have to insert valid pre-programmed smart cards to access the client. The **smart AX-s** software allows the system administrator to define the access privilege for each smart card. Smart cards with **User** privilege can only use pre-defined connections. Smart cards with **Administrator** privilege can access connection configuration and terminal configuration functions of the client as well.

More information about implementing the **smart AX-s** security option is provided in the *smart AX-s Administrator's Guide*, which is available in the CD supplied with the product.

NOTE: **SMART AX-S** AND **CLIENT-CONFIGURATION SECURITY** CANNOT BE IMPLEMENTED SIMULTANEOUSLY. ENABLING ONE OF THE FEATURES AUTOMATICALLY CAUSES THE OTHER TO BE DISABLED.

To enable **smart AX-s** security for the client, select the **Enable Smart AX-S** check-box.

- **Fail Over Password**: This button is enabled when you select the **Enable Smart AX-S** check-box. The fail-over password is a backup mechanism to access the client if the smart card reader fails. In such cases, the client displays a prompt to enter a password. To set the fail-over password, click the **Fail Over Password** button. The following dialog-box is displayed.



When you install the client for the first time, or restore factory-default settings, the default **Current Password** is **0000000** (*eight zeroes*).

Enter the current password in the **Current Password** field.

Enter the new fail-over password in the **New Password** field. The password must consist of at least four digits and must not exceed eight digits.

Enter the new password again in the **Confirm Password** field.

CAUTION: WHEN THE FAIL-OVER PASSWORD IS USED TO ACCESS A CLIENT, THE USER CAN ACCESS ALL FUNCTIONS OF THE CLIENT INCLUDING CONFIGURING CLIENT PROPERTIES AND CREATING/EDITING CONNECTIONS. THE SYSTEM ADMINISTRATOR MUST ENSURE THAT THE FAIL-OVER PASSWORD IS KEPT SECRET.

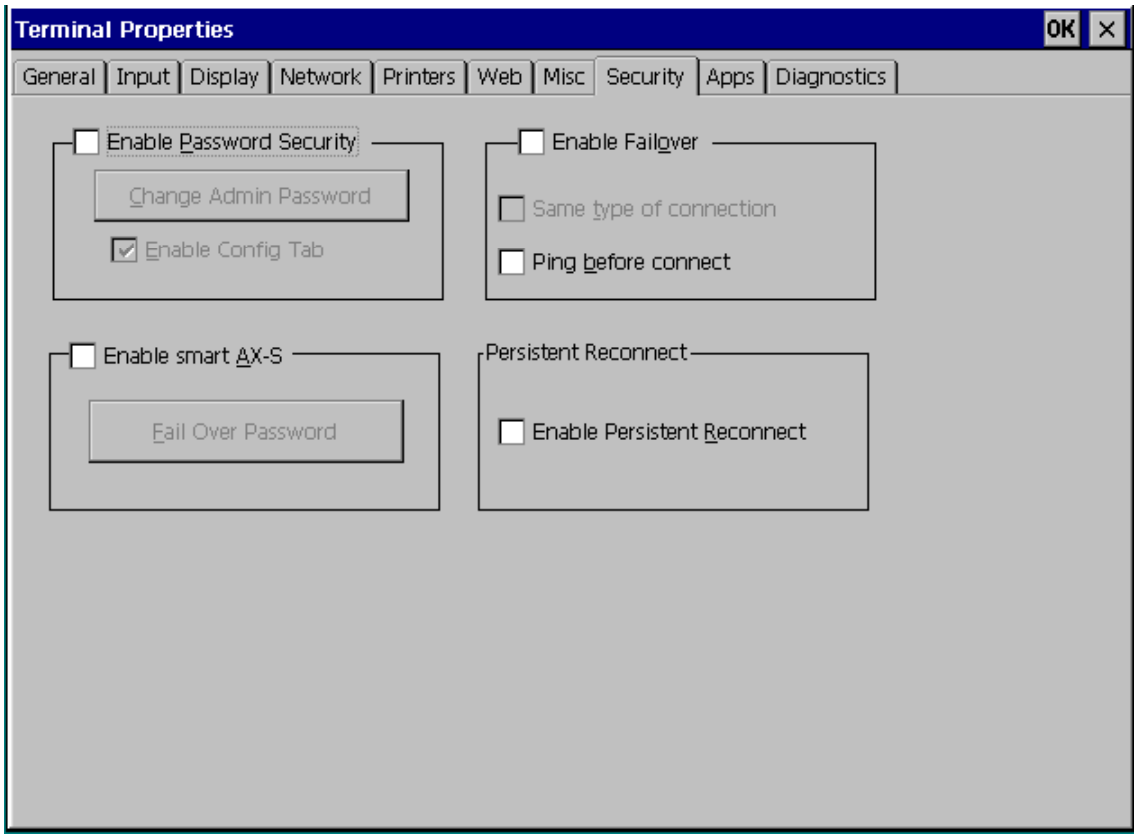
Click **OK** to return to the **Security** tab of the **Terminal Properties** dialog-box.

NOTE: IF BOTH LOGIN-SECURITY AND SMART AX-S SECURITY ARE ENABLED, SMART AX-S SECURITY TAKES PRECEDENCE.

IN SUCH CLIENTS, IF THE SMART CARD READER IS AVAILABLE, A PROMPT TO INSERT THE SMART CARD WILL BE DISPLAYED AFTER THE CLIENT BOOTS UP. USERS WHO INSERT VALID SMART CARDS AND PROVIDE CORRECT PIN NUMBERS CAN ACCESS CONNECTIONS DEFINED FOR THE CARD.

IF THE SMART CARD READER IS NOT INSTALLED OR IS DEFECTIVE, A PROMPT TO ENTER THE FAIL-OVER PASSWORD IS DISPLAYED. WHEN THE FAIL-OVER PASSWORD IS ENTERED, THE LOGIN-SECURITY PROCESS TAKES OVER.

Connection Failover



With this feature, if the client is unable to start a selected connection, it automatically tries to start another connection. If the second attempt is also unsuccessful, the client tries the next connection and so on until all available connection entries are exhausted.

To enable this feature, select the **Enable Failover** check-box. The **Same type of connection** check-box is enabled.

- **Same type of connection**: This check-box allows you to define the order in which the client selects fail-over connections.

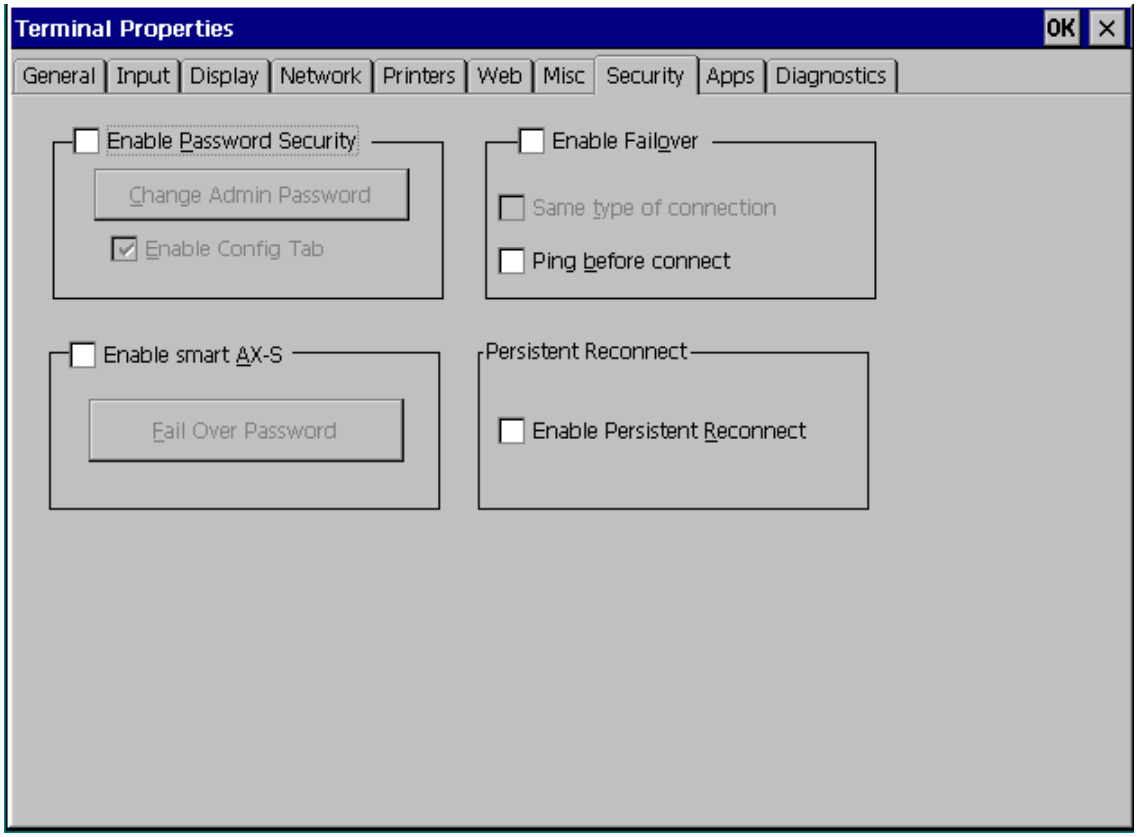
  If you select the **Same type of connection** check-box, the next available connection of the **same type** is selected as the fail-over connection. *For instance*, if the first attempt for an ICA connection fails, the client tries the next available ICA connection. After exhausting all available ICA connection entries, a message stating that the client was unable to connect to the server is displayed.

  If you do not select the **Same type of connection** check-box, the next available connection entry (*regardless of connection-type*) is selected as the fail-over connection.

- **Ping before connect**: If you select this check-box, the client pings the host to verify whether it is up, before trying to connect to the host. This feature saves time for users, who would otherwise have to wait until the 'Connection Failed' message is displayed. This option is not available if the Connection-Failover feature is enabled.

Persistent reconnect

Persistent Reconnect feature is effective only if the Auto Start feature for the connection is enabled.



Generally, the client automatically invokes the Auto-Start connection when you switch on the client. If the server to which you need to connect is not available in the network when you switch-on the client, then Persistent Reconnect feature tries to activate the connection continuously in the background.

NOTE: ENABLE FAILOVER FEATURE DOESN'T WORK IF PERSISTENT RECONNECT OPTION IS ENABLED

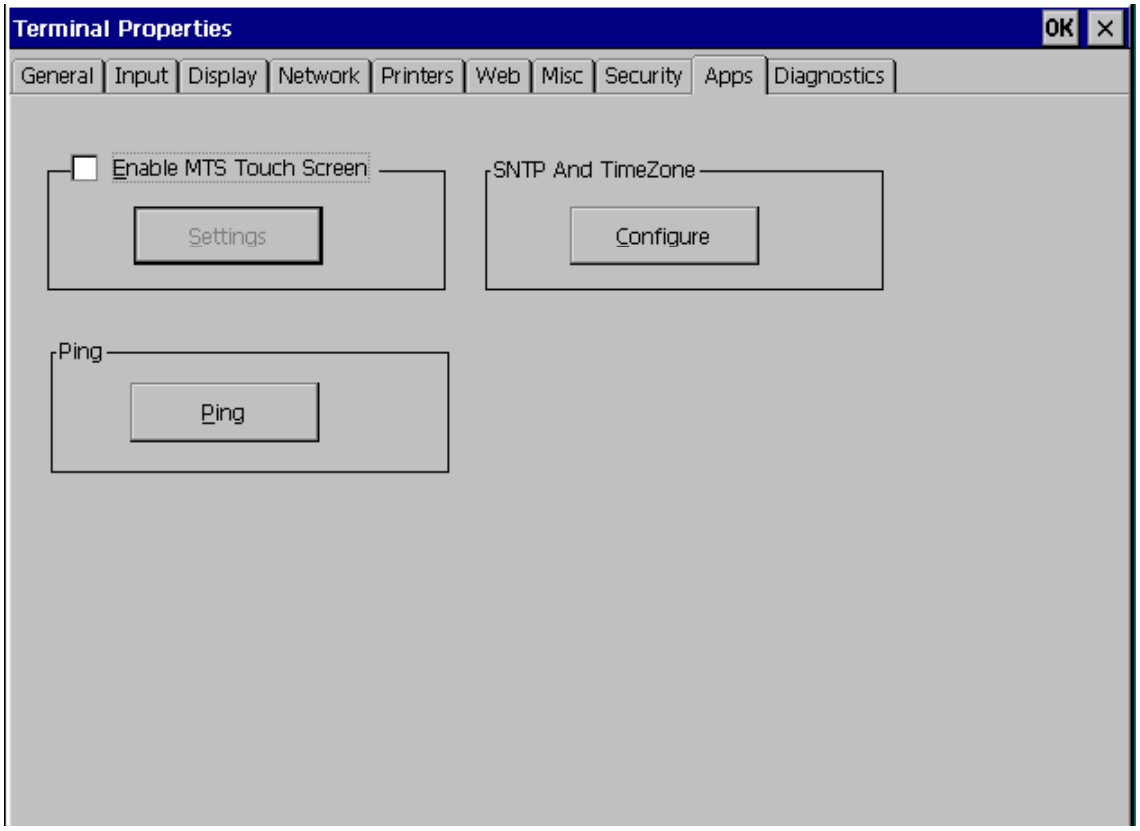
Apps (Touch screen, SNTP & TimeZone and Ping)

Touch Screen

To configure the touch screen connected to the client,

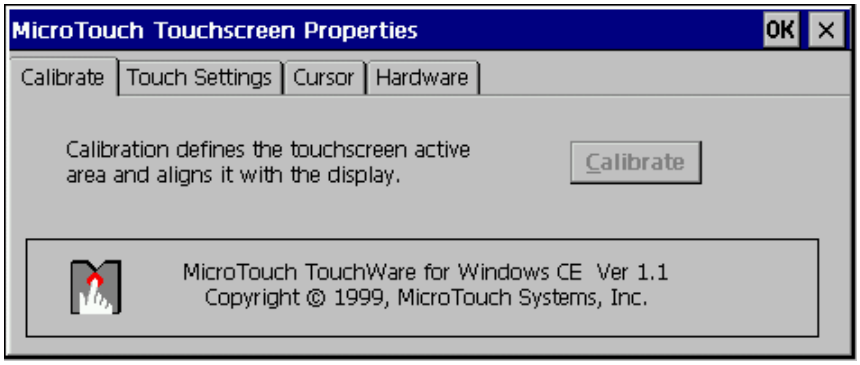
1. Press the **F2** key on your keyboard while the **Terminal Connection Manager** window is displayed.
2. Click on the **Apps** tab.

TIP: TO SWITCH TO THE **TERMINAL CONNECTION MANAGER** FROM AN OPEN SESSION, PRESS **CTRL+ALT+END**.

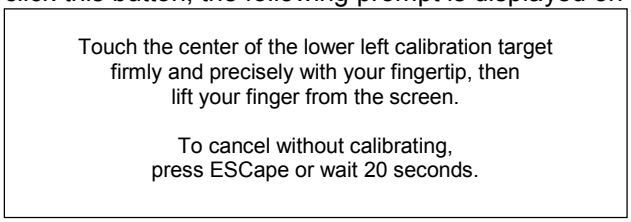


To configure the touch screen select the **Enable MTS Touch Screen** check-box and click the **Settings** button. The **MicroTouch Touchscreen Properties** dialog-box is displayed. This dialog-box contains four tabs.

Calibrate tab



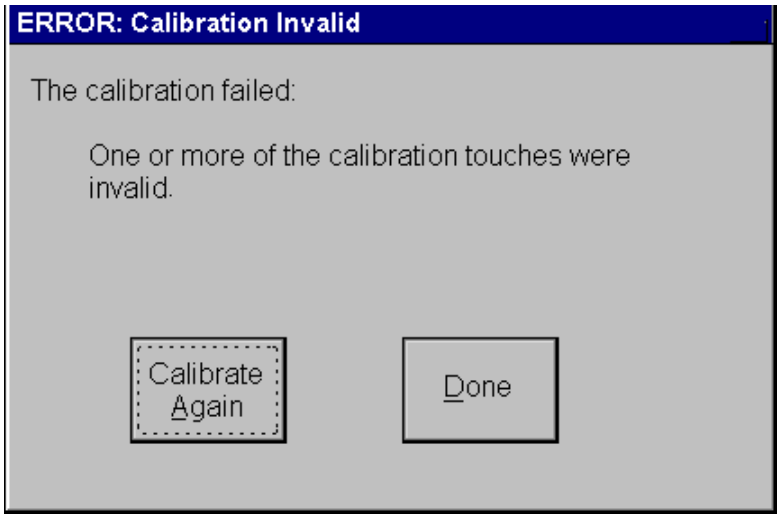
The **Calibrate** button is enabled only when a touch screen is connected to the client. When you click this button, the following prompt is displayed on a blank white screen.



A cross hair (*as shown below*) is displayed in the lower left-hand corner of the touch screen.

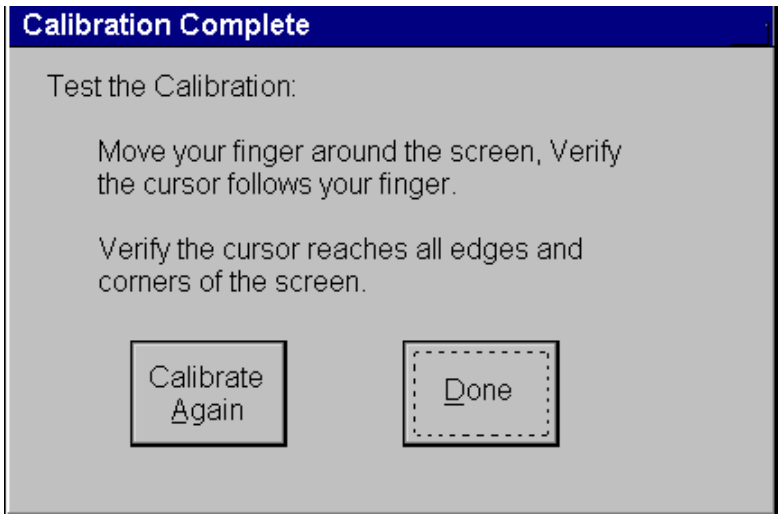
Touch the center of the cross hair. The cross hair will move to the upper right-hand corner.

Touch the center of the cross hair again. If the calibration was not successful, the following error message will be displayed.



Select **Calibrate Again** to repeat the above process.

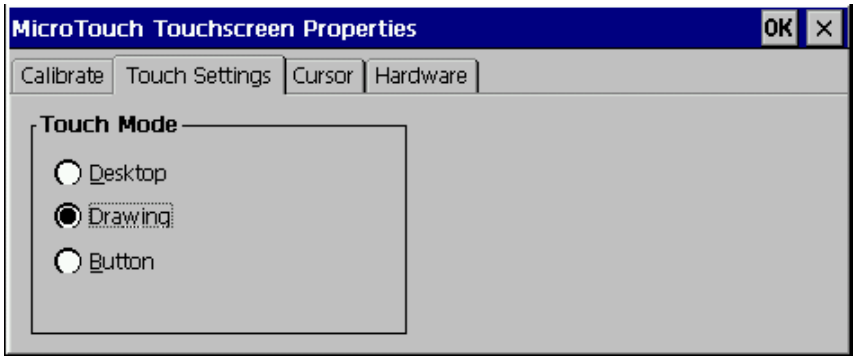
If the calibration was successful, the following message will be displayed.



To test whether the calibration was successful, move a finger over the screen and check whether the mouse-pointer follows the finger. Check whether the pointer reaches the edges and corners of the screen.

If you want to repeat calibration, select **Calibrate Again**. Otherwise, select **Done**.

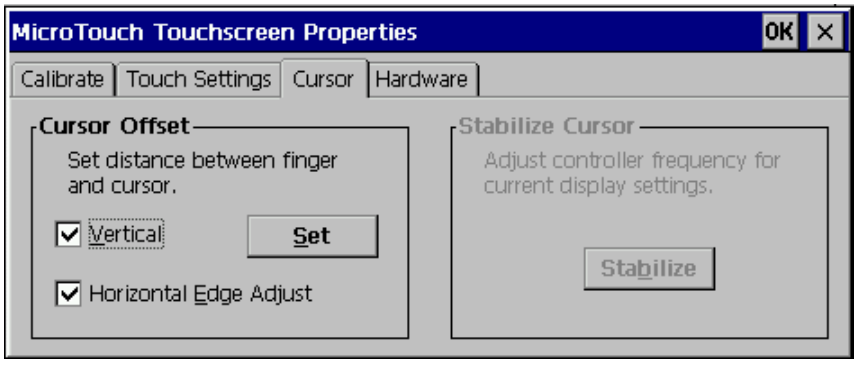
Touch Settings tab



In this sheet, you can specify the touch-mode.

- **Desktop**: Select this radio-button if the touch screen is for general desktop applications.
- **Drawing**: Select this radio-button if the touch screen is for graphics applications.
- **Button**: Select this radio-button for applications that use button-type user interfaces.

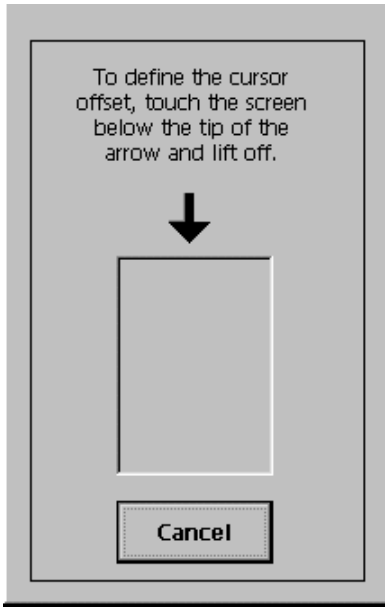
Cursor tab



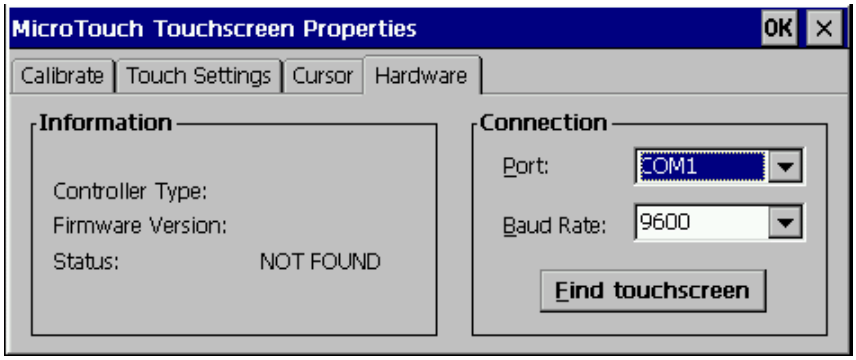
Cursor Offset: This group of fields can be used to set the distance between the cursor and the point on the touch-screen that you touch with your finger.

- **Vertical**: Select this check-box to set the vertical distance.

- **Horizontal Edge Adjust**: Select this check-box to adjust the horizontal distance.
- **Set**: Click on this button to interactively define the cursor offset.



Hardware tab



This sheet provides information about the touch screen hardware and allows you to configure the connection between the client and the touch screen.

- **Information**: This box displays information about the touch screen connected to the client. To update the information, click on the **Find touchscreen** button.

  Controller Type: displays the type of controller.

  Firmware Version: displays the version number of the firmware.

  Status: displays 'OK' if a touch screen is connected. Otherwise, displays 'NOT FOUND'.

- **Connection**: This box allows you to configure the connection between the client and the touch screen.

  Port: Select the COM port to which the touch screen is connected.

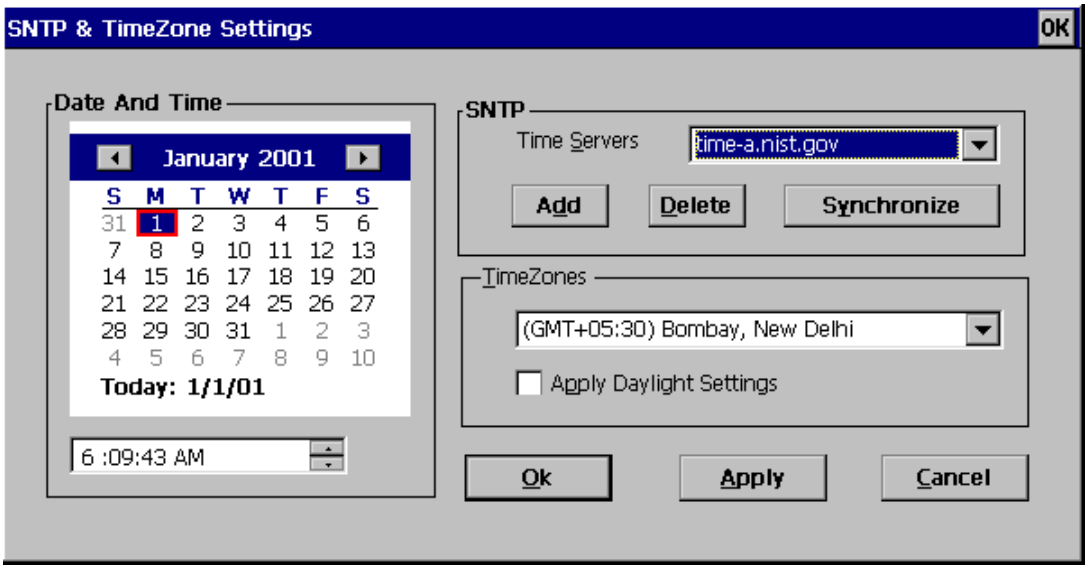
  Baud Rate: Select the appropriate baud rate for communication between the touch screen unit and the client.

- **Find touchscreen**: Click on this button to search for a touch screen connection.

After configuring the above parameters, click **OK** to return to **Terminal Properties** dialog-box.

SNTP and Timezone

You can set the date and time in the client. You can also synchronize the client clock to the SNTP server.



Use the calendar to set the date and the year. Select the Timezone from the drop-down list box.

Check the daylight setting box if the time is currently in effect. To manually set the time, enter a time slightly ahead of the actual time in the text box, and then just as the actual time reaches the set time, click on the Apply button.

NOTE: IF THE TIME SERVER IS AVAILABLE YOU CAN SYNCHRONISE THE TERMINAL TIME TO THE SERVER TIME

To set the time using the SNTP

1. The Time Servers drop-down list box lists the SNTP (Simple Network Time Protocol) servers added using the Add button. Select the Timeserver from the list. If the Timeserver you need is not listed, click Add button.

   - **Add: This command button opens the SNTP dialog box.**

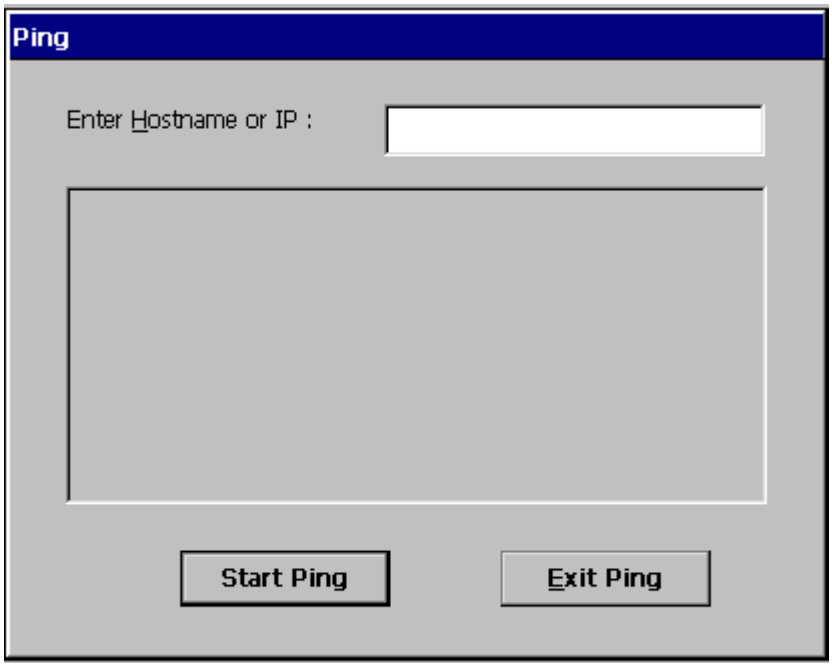
   

   Enter the IP address or the DNS name of the Timeserver. Click OK to return to the SNTP and Timezone Settings box.

2. Click **Synchronize** to set the client time to synchronize to the selected time server.
3. Make appropriate selection/entries in the SNTP and Timezone Settings box. Click OK to return to the Terminal Properties box.

Ping

You can use this option to check if a particular host is available in the network. The following Ping box is displayed.

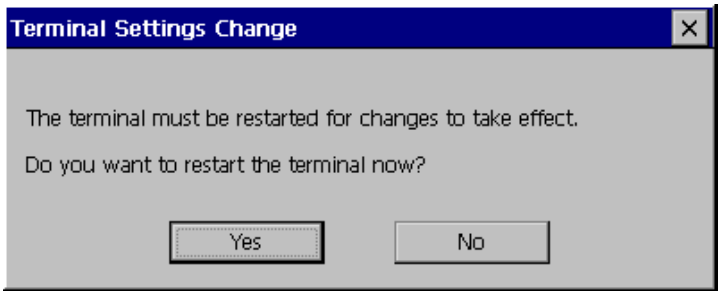


Enter the host name or the IP address of the server you need to ping. Click Start Ping.

To return to the Terminal Properties box click Exit Ping

Click **OK** to save changes, or **X** to cancel changes.

If you click **OK**, the following prompt is displayed.



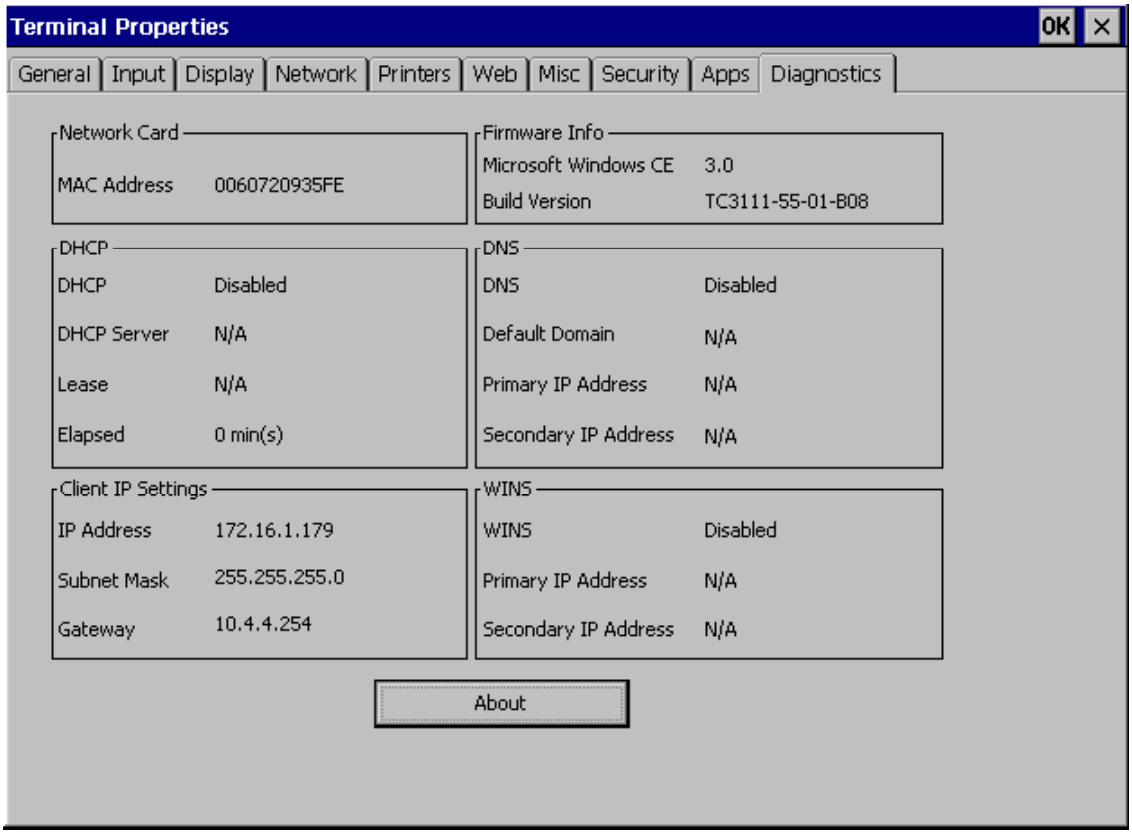
Click **Yes** to shutdown and restart the client.

Diagnostics

To view system information and copyright notices,

1. Press the **F2** key on your keyboard while the **Terminal Connection Manager** window is displayed.
2. Select the **Diagnostics** tab.

TIP: TO SWITCH TO THE **TERMINAL CONNECTION MANAGER** FROM AN OPEN SESSION, PRESS **CTRL+ALT+END**.



The above dialog-box contains information that would be required when you contact I-O CORPORATION for support.

Click **About** to view copyright notices.

Click **OK** to return to the Terminal Properties box.

RDP

Remote Desktop Protocol (RDP) allows a "thin client" to communicate with a terminal server across a Local Area Network (LAN) or Wide Area Network (WAN) by means of a dial-up, Integrated Services Digital Network (ISDN), Digital Subscriber, Line (DSL), or Virtual Private Network (VPN) connection. RDP is designed to provide remote display and input capabilities over network connections for Windows-based applications running on a server.

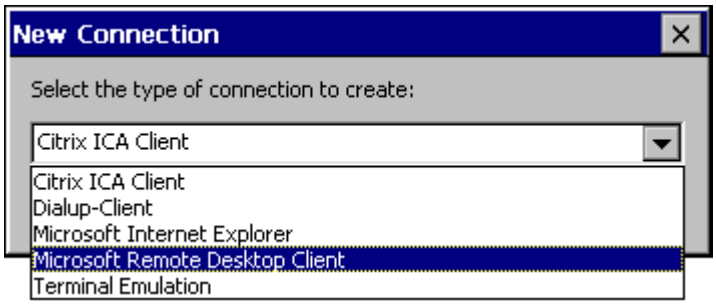
Creating TCP/IP RDP Connection

This section describes the procedure to create a connection to a Windows Terminal Server using Microsoft's Remote Desktop Protocol.

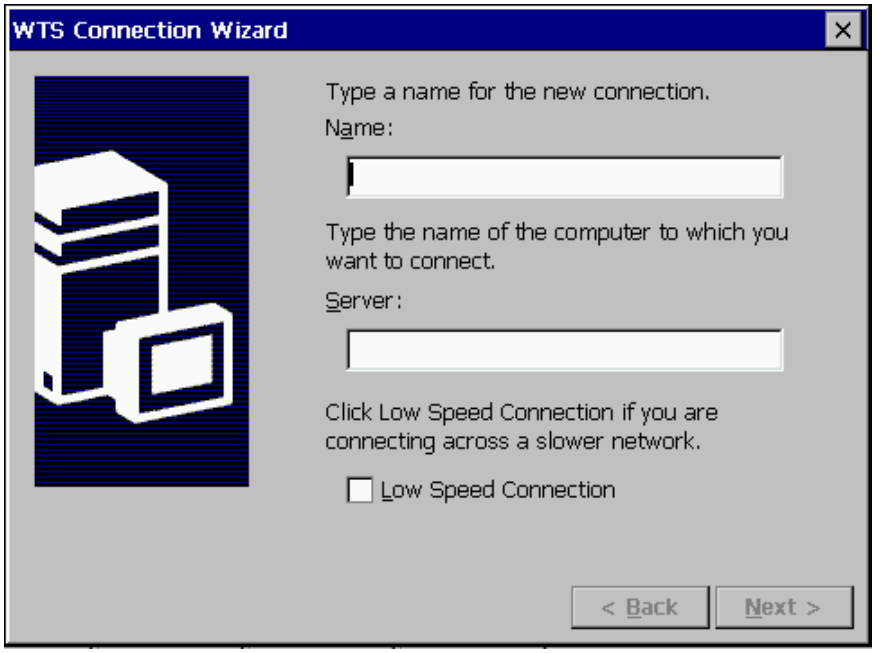
1. Select the **Configure** sheet of the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Click **Add….** The **New Connection** dialog-box is displayed.



3. Select **Microsoft Remote Desktop Client** from the drop-down list and click **OK**. The first dialog-box of the **WTS Connection Wizard** is displayed.



4. Provide a unique name for the new connection, and the IP address of the server in the **Name** and **Server** fields respectively. The connection-name that you provide here will be displayed in the **Terminal Connection Manager** window.

TIP: IF THE NETWORK HAS A WINS SERVER, YOU CAN PROVIDE THE NAME (*INSTEAD OF IP ADDRESS*) OF THE SERVER IN THE **SERVER** FIELD.

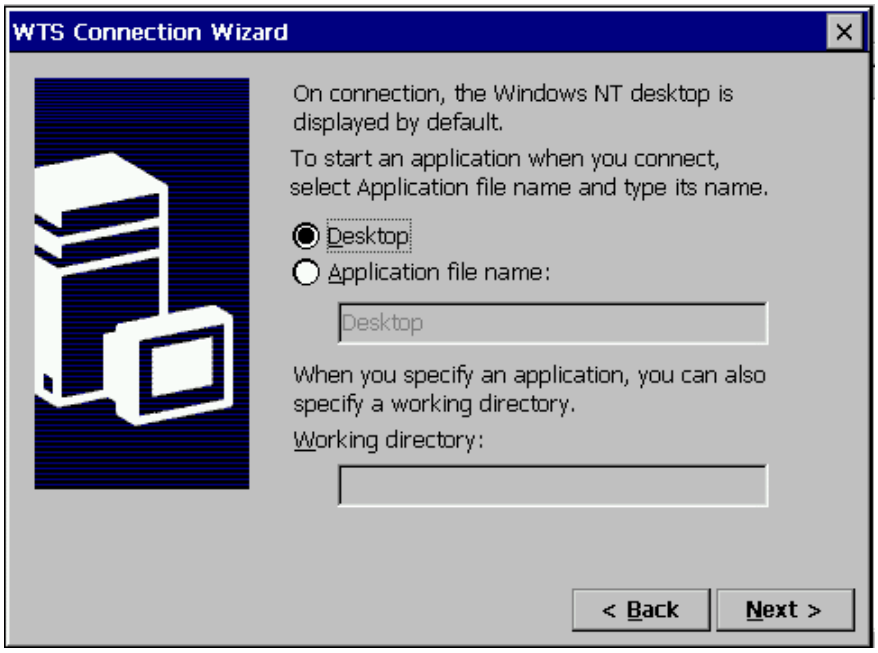
If you are connecting across a slow network (*for instance, a WAN*), enable the **Low Speed Connection** check-box. This setting causes data to be compressed before transmission, thus optimizing the bandwidth usage. Note that while data compression reduces the transmission time, it consumes more processor resources.

Click **Next>** to continue. The following dialog-box is displayed.

5. Information that you provide in the above dialog-box will be used to automatically logon to the server after the connection is started. Select the **Automatic Logon** check-box to enable the **Username**, **Password** and **Domain** fields and provide appropriate input.

If you do not enable the **Automatic Logon** option, a login prompt will be displayed each time you start the connection.

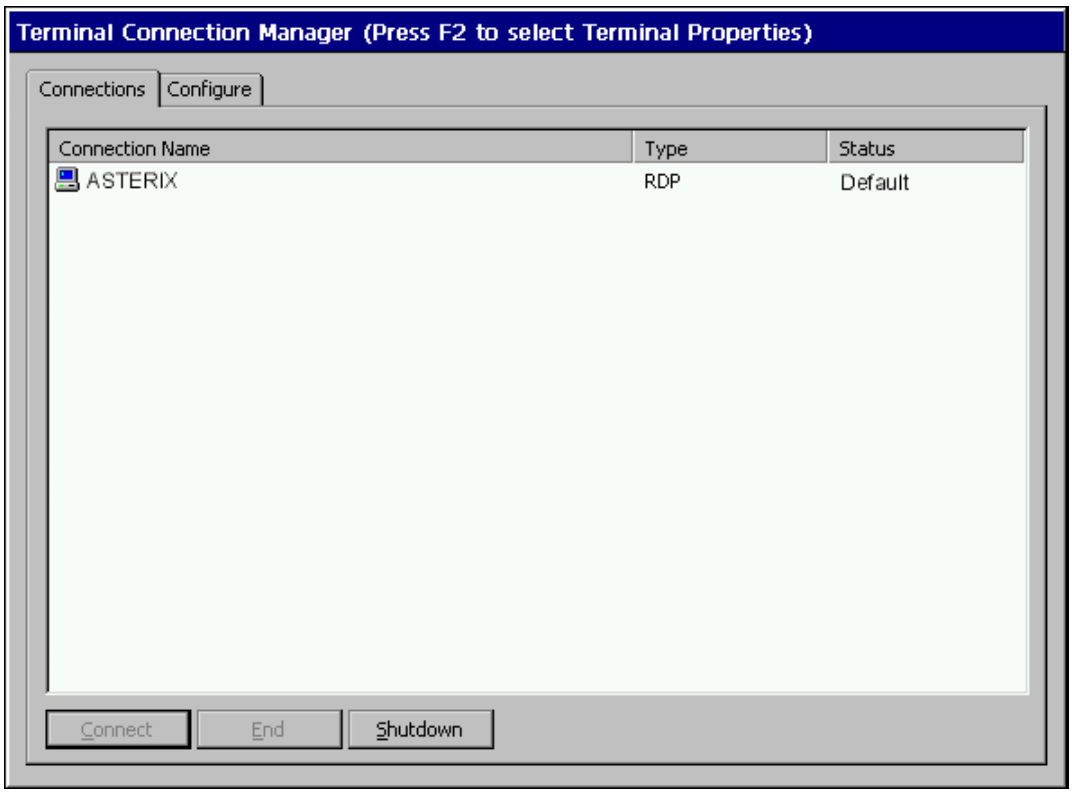
Click **Next>** to proceed. The following dialog-box is displayed.



6. After connecting to the server, the client displays the Windows NT 4.0 TSE or Windows 2000 desktop by default. Instead, if you want a particular application to be automatically started, select the **Application file name** radio-button and provide the name and path of the application file in the text field beneath the **Application file name** radio-button. You can specify a working directory in the **Working directory** field.

   Click **Next>** to continue. The following dialog-box is displayed.

7. The above dialog-box marks the end of the **WTS Connection Wizard**. Click **Finish** to complete the process. The name of the connection you created will be added to the list of connections displayed in the **Connections** tab of the **Terminal Connection Manager** window.


Terminal Connection Manager (Press F2 to select Terminal Properties)
Connections
Configure
Connection Name
Type
Status
ASTERIX
RDP
Default
Connect
End
Shutdown

Creating PPP RDP Connection

You can connect the client to a remote RDP server through a Point-to-Point protocol.

1. Create an RDP Connection. Refer to the topic Creating TCP/IP RDP Connection, Page No.62
2. Create a PPP Connection. Refer to the topic Creating PPP Connection, Page No. 133

NOTE: CREATING RDP CONNECTION IS SIMILAR TO CREATING TCP/IP RDP CONNECTION.

Editing RDP Connections

To edit an RDP connection,

1. Select the **Configure** sheet from the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

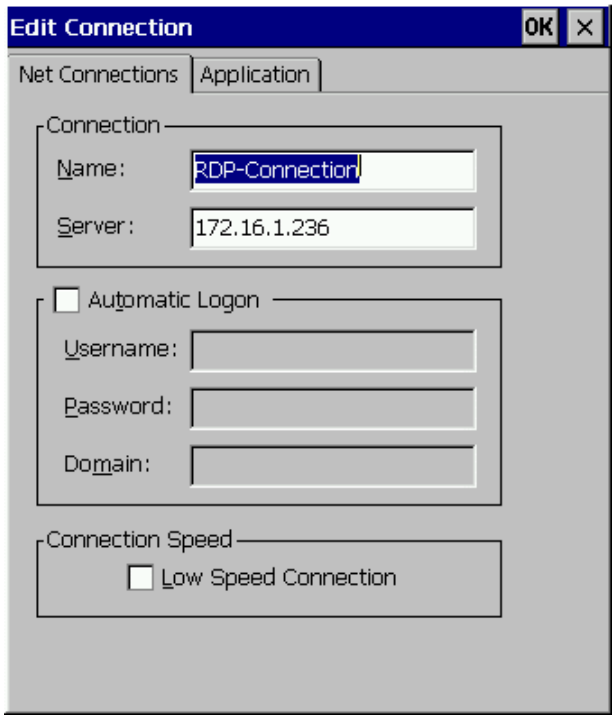
2. Highlight the RDP connection to be edited.

TIP: THE 'TYPE' OF CONNECTION IS DISPLAYED IN THE **TYPE** COLUMN OF THE **TERMINAL CONNECTION MANAGER** WINDOW.

NOTE: CONNECTIONS CANNOT BE EDITED WHILE THEY ARE ACTIVE.

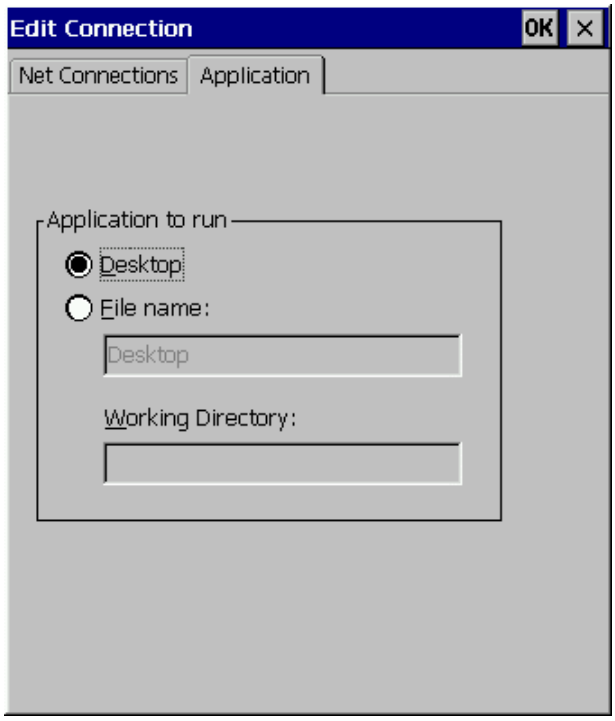
3. Click the **Edit…** button. The following dialog-box is displayed. This dialog-box has two tabs. After editing required parameters, clicks OK to save changes and return to the **Terminal Connection Manager**.

Net Connections tab



- **Connection**: In this group of text fields, you can edit the name of the connection and the server to which it connects.
- **Automatic Logon**: Select this check-box to enable the **Username**, **Password** and **Domain** text fields. If you do not enable the **Automatic Logon** option, a logon prompt will be displayed each time you start the connection.
- If you are connecting across a slow network (*for instance, a WAN*), enable the **Low Speed Connection** check-box. This setting causes data to be compressed before transmission, thus optimizing the bandwidth usage. Note that while data compression reduces the transmission time, it consumes more processor resources.

Application tab



After connecting to the server, the client displays the Windows NT 4.0 TSE or Windows 2000 desktop by default. Instead, if you want a particular application to be automatically started, select the **File name** radio-button and provide the name of the application file in the text field under the **File name** field. You can provide the path of the working directory in the **Working Directory** field.

After editing required parameters, click OK to save changes and return to the **Terminal Connection Manager**.

NOTE: YOU CAN DELETE THE RDP CONNECTION BY HIGHLIGHTING THE CONNECTION IN THE CONFIGURE SHEET OF THE TERMINAL CONNECTION WINDOW AND CLICKING ON THE DELETE BUTTON.

Initiating RDP Connection

1. Select the **Connections** sheet from the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Highlight the RDP connection to be started. Click **Connect.**

NOTE: YOU CAN ALSO DOUBLE-CLICK ON THE CONNECTION TO START/INITIATE THE CONNECTION.

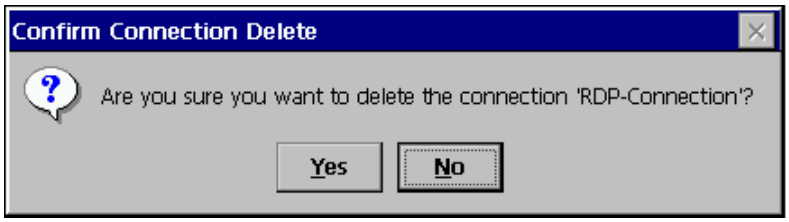
Deleting RDP Connection

To delete a defined connection,

1. Select the **Configure** sheet from the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Highlight the connection to be deleted, and click the **Delete** button. A **Confirm Connection Delete** prompt is displayed.



3. Click **Yes** to confirm deletion and **No** to cancel the delete command.

ICA

The Citrix **Independent Computing Architecture (ICA)** is a general-purpose distributed presentation services architecture. The ICA technology shifts the application processing from client to server. It is a core technology of Citrix MetaFrame™ server-based computing software. ICA helps organizations reduce total cost of ownership by delivering business-critical applications over heterogeneous computing environments. It also safeguards application performance, data security, and administrative control. The ICA protocol sends only keystrokes, mouse clicks, and screen update signals across the network. Applications consume just a fraction of the network bandwidth usually required.

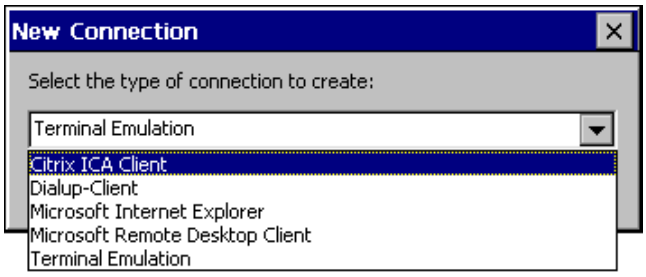
Creating TCP/IP ICA Connections

This section describes the procedure to create a connection through the network port of the client, to a server that supports the ICA protocol or an application published on a MetaFrame server.

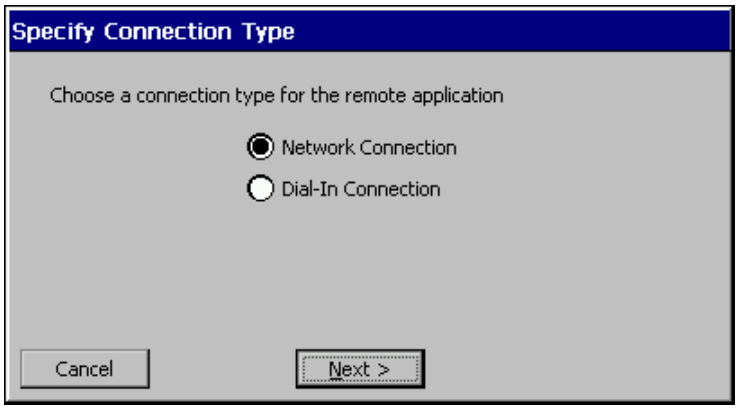
1. Select the **Configure** sheet of the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Click the **Add…** button. The **New Connection** dialog-box is displayed.



3. Select **Citrix ICA Client** from the drop-down list. The **Specify Connection Type** dialog-box is displayed.



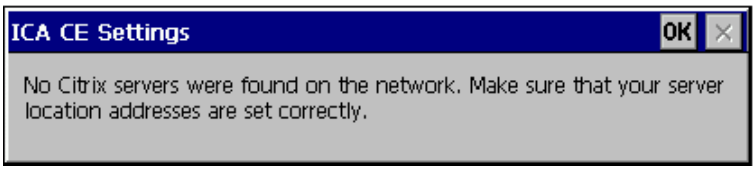
4. Select the **Network Connection** radio-button, and click **Next>**. The following box is displayed.

5. If you want to create a connection to a *server* that supports the ICA protocol, select the **Citrix Server** radio-button. If you want to create a connection to a *published-application*, select the **Published Application** radio-button.

NOTE: PUBLISHED APPLICATIONS CAN BE CREATED ONLY ON METAFRAME SERVERS.

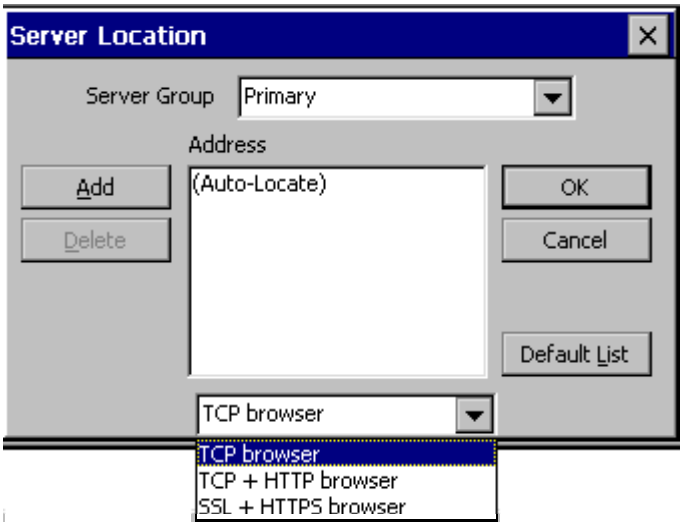
Click **Refresh**. The client automatically searches the network for servers or published applications and displays the following message briefly:

At this point, the client searches the network for Citrix servers and displays them in the **Select a Citrix Server or Published Application** dialog-box. If there are no MetaFrame servers in the network, the following message is displayed.



NOTE: ONLY METAFRAME SERVERS ARE DISPLAYED IN THE ABOVE DIALOG-BOX. TO CREATE A CONNECTION TO A SERVER THAT HAS CDS (*CITRIX DEVICE SERVICES*), YOU MUST SPECIFY THE IP ADDRESS OF THE SERVER IN THE TEXT FIELD BENEATH THE RADIO-BUTTONS. YOU MAY PROVIDE THE NAME OF THE SERVER (*INSTEAD OF IP ADDRESS*) IF THE NETWORK HAS A WINS (*WINDOWS INTERNET NAMING SERVICE*) SERVER.

6. This step is required only if the MetaFrame server or published application to which you want to create a connection is not displayed in the above dialog-box. Click **Server Location**. The following dialog-box is displayed.



In the above dialog-box, you can select the method to find Citrix servers and published applications on the network. If the **(Auto-Locate)** entry is highlighted in the **Address** list, the client broadcasts a 'Get Nearest Citrix Server' packet. The first MetaFrame server to respond is then requested for information about servers and published applications in the network.

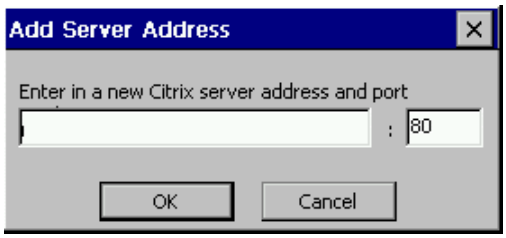
However, to eliminate broadcasts on your network, you may want to designate a particular Citrix sever as the master-browser. The network protocol setting allows you to control the way the ICA client searches. The protocols are:

- **TCP browser:** The ICA Client uses the UDP protocol to search for Citrix servers. The ICA Client communicates with the Citrix server using ICA protocol over TCP/IP.
- **TCP + HTTP browser:** The ICA Client uses the HTTP protocol to locate Citrix servers. The ICA Client communicates with the Citrix server using ICA protocol over TCP/IP. Select this option when using the ICA Client over the Internet or via a firewall or proxy server. This is the default protocol.
- **SSL + HTTPS browser:** The ICA Client uses the HTTPS protocol to locate Citrix servers. The ICA Client communicates with the Citrix server using ICA with SSL. SSL provides strong encryption of ICA traffic and Citrix server authentication. Select this option when using the ICA Client over the Internet or via a firewall or proxy server.

NOTE: THE TCP + HTTP AND SSL+HTTP PROTOCOLS CAN ONLU BE USED WITH COMPATIBLE CITRIX SERVERS. CHECK THE APPROPRIATE CTRIX SERVER ADMINISTRATOR'S GUIDE FOR FUTURE INFORMATION.

NOTE: THE TCP + HTTP AND SSL +HTTP PROTOCOLS DOES NOT SUPPORT THE **AUTO-LOCATE** FUNCTION.

- **Server Group**: From this drop-down list, you can select one of three groups of servers: **Primary**, **Backup1** and **Backup2**. The default group is **Primary**.
- To add the address of a master-browser, click **Add**. This following dialog-box is displayed.

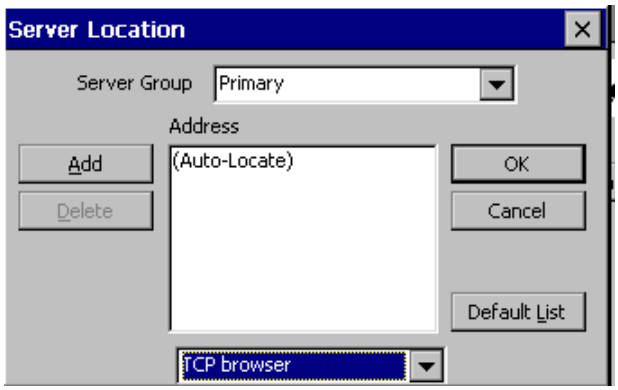


NOTE: THE PORT NUMBER FIELD IS NOT DISPLAYED IF YOU HAD SELECTED THE **TCP** PROTOCOL.

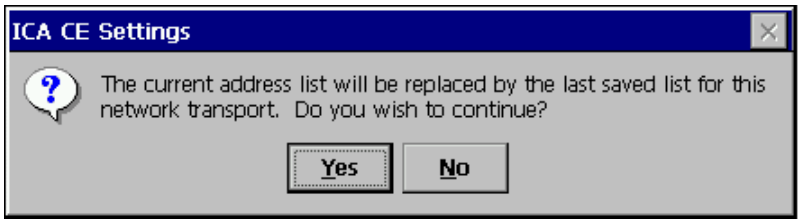
Enter the IP address or name of the Citrix server and a recognized port number (*default: 80*) and click **OK** to return to the **Server Location** dialog-box.

If you had selected the **TCP +HTTP or SSL+ HTTP** protocol in the **Server Location** dialog-box and you do not enter an IP address, you must have a Citrix server on your network mapped to the default name **ICA**.

The specified server responds with a list of all servers and published applications in its server farm.



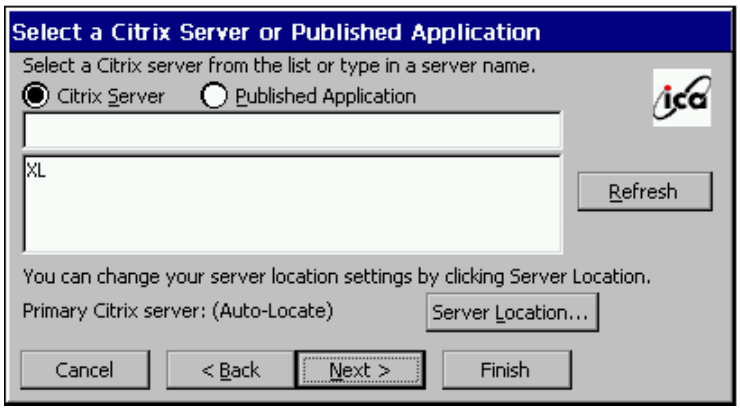
- **Default List**: Click this button to cancel any modification and to recall the saved list of servers. The following prompt is displayed.



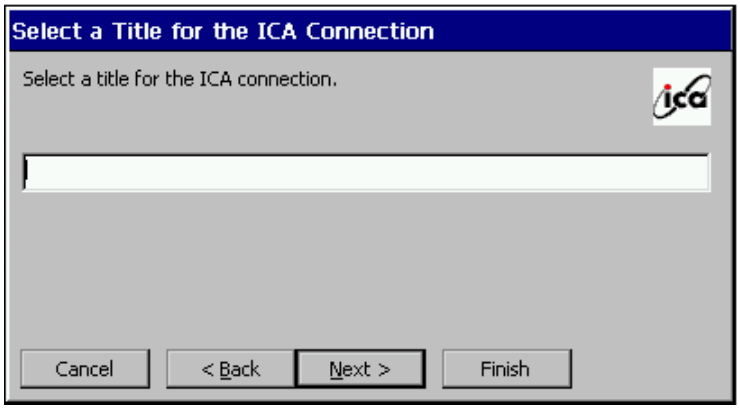
Click **Yes** to recall the saved list, and **No** to retain the current list.

- **Delete**: To delete an address from the list, select it and click this button. If you delete all the addresses in the **Primary Server Group**, the **(Auto-Locate)** entry will be highlighted in the **Address** list.

Click **OK** to return to the **Select a Citrix Server or Published Application** dialog-box.

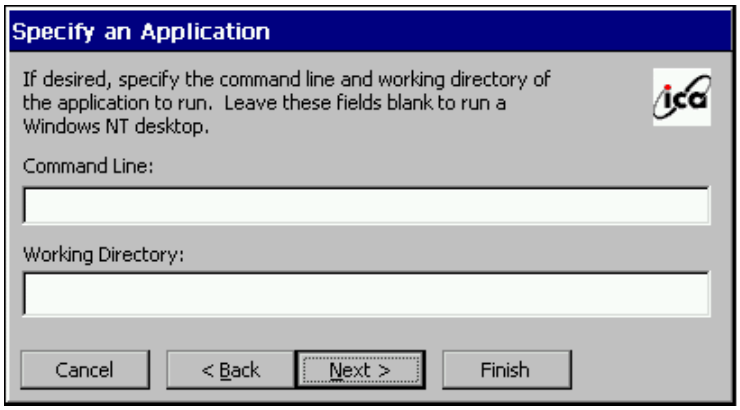


7. Click the **Refresh** button to update the list of available servers or applications.
8. Select a server from the list, or enter a server-name in the text field immediately beneath the radio-buttons and click **Next>**. The following dialog-box is displayed.



9. Enter a unique name for the new ICA connection and click **Next>**. The following dialog-box is displayed.

NOTE: IF YOU DO NOT SPECIFY A NAME FOR THE CONNECTION IN THE ABOVE DIALOG-BOX, THE NAME OF THE SERVER IS TAKEN AS THE CONNECTION NAME.

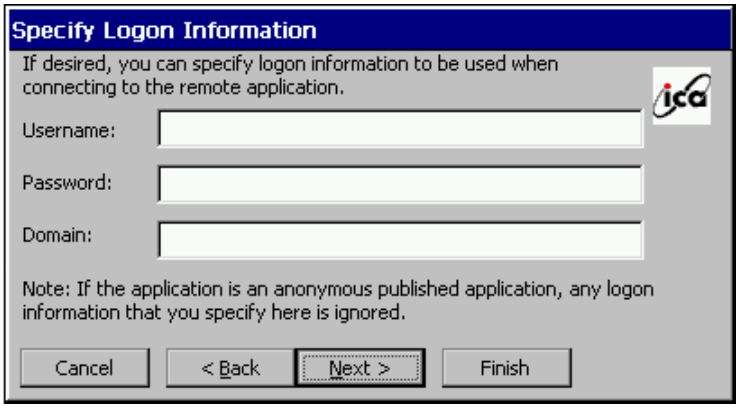


10. If you want an application to be automatically started after connecting to the server, provide appropriate information in the above dialog-box.
    - **Command Line**: Enter the directory path and file-name of the application program that you want to invoke.
    - **Working Directory**: Enter the path of the working directory to be used by the application.

If you do not provide any input in the above dialog-box blank, the Windows NT 4.0 TSE or Windows 2000 desktop will be displayed after connecting to the server.

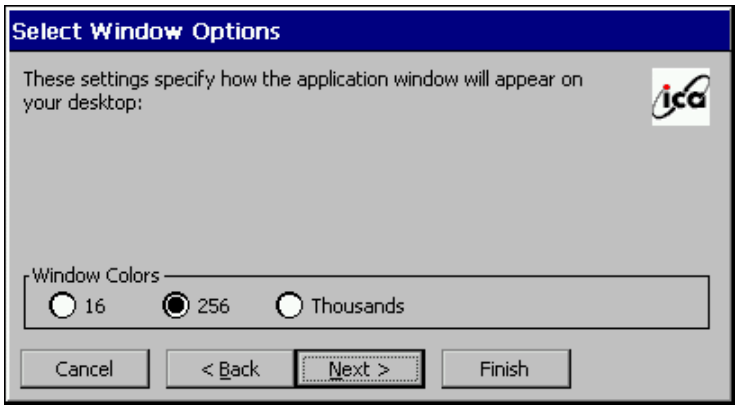
If you specify an application in this dialog-box, the user cannot access any other program or application. The client will automatically start the application when the user logs in, and will display the **Terminal Connection Manager** when the application is closed.

Click **Next>** to proceed. The following dialog-box is displayed.



11. Information in the above dialog-box is used to automatically logon to the server. To implement this feature, provide the **Username**, **Password** and **Domain**. If you leave the fields in this dialog-box blank or provide invalid input, a login prompt will be displayed when the connection is started.

    Click **Next>** to proceed. The following dialog-box is displayed.



In the above dialog-box, you can set the color depth for the monitor connected to the client. By default, **256** is selected. The **Thousands** option indicates 16-bit color.

NOTE: 16-BIT COLOR IS SUPPORTED ONLY BY METAFRAME 1.8 FEATURE RELEASE-1, METAFRAME XP AND ABOVE. CDS DOES NOT SUPPORT THE 16-BIT COLOR OPTION. IF YOU SELECT THE 16-BIT COLOR OPTION FOR SERVERS THAT DO NOT SUPPORT IT, THE CLIENT DISPLAYS AT 256 COLORS.

Select the appropriate radio-button and click **Next>** to continue. The following dialog-box is displayed.

- **Use Printer Configuration Utility**: This option is selected by default. It allows the printer port of the client to be accessed by ICA users in the network.

  If the connection you are creating is to a server with MetaFrame versions 1.8 and above, ensure that this option is selected. Otherwise, the printer port of the client cannot be accessed.

  If the connection you are creating is to a server with MetaFrame 1.0 or CDS, you **must** disable this option. Otherwise, the printer port of the client cannot be accessed.

- **Compress Data Stream**: This option is enabled by default. This setting causes data to be compressed before transmission, thus optimizing the bandwidth usage. Note that while data compression reduces the transmission time, it consumes more processor resources.

- **Enable Sound**: The client supports audio when it is connected to MetaFrame servers. Select this check-box to enable sound. You can set the audio quality from the **Sound Quality** drop-down list. The options available are **High**, **Medium** and **Low**.

NOTE: THIS SETTING HAS NO EFFECT IF THE CONNECTION YOU ARE CREATING IS TO A SERVER THAT HAS CDS (*CITRIX DEVICE SERVICES*).

- **SpeedScreen**: MetaFrame versions 1.8 Feature Release-1, MetaFrame XP and above include a feature to reduce keystroke and mouse-click latency. Latency is the delay between a keystroke/mouse-click and the corresponding change on the screen. This drop-down list allows you to specify whether you want to use the SpeedScreen feature of the MetaFrame server.

  Off: This is the default setting. The client will not benefit from the SpeedScreen feature of the server.

  On: The server manages keystroke and mouse-click latency at the client to provide improved and consistent performance.

  Auto: The server manages keystroke and mouse-click latency, if the latency is between the upper and lower threshold-limits specified at the server.

- **Encryption Level**: Data Encryption is not supported by servers that have CDS (*Citrix Device Services*). To use data encryption, **Citrix MetaFrame** (including the **Secure ICA** service) must be installed on the server.

  If you specify encryption for a connection to a server that does not have MetaFrame, the following error message is displayed when you try to start the connection:

  'Your Citrix server does not support the encryption you required'.

NOTE: THE SECURE ICA SERVICE **MUST BE INSTALLED SEPARATELY** ON SERVERS WITH THE FOLLOWING METAFRAME VERSIONS.

- METAFRAME 1.X ON WINDOWS NT 4.0 TSE SERVER
- METAFRAME 1.8 ON WINDOWS 2000 SERVER

THE SECURE ICA SERVICE **IS INSTALLED BY DEFAULT** ON SERVERS WITH THE FOLLOWING METAFRAME VERSIONS.

- METAFRAME 1.8 WITH FEATURE RELEASE 1
- METAFRAME XP

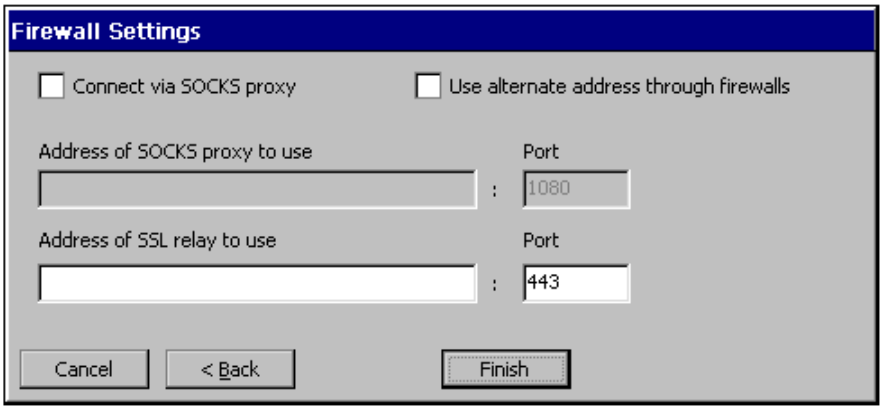
The default encryption level is **Basic**. The other options are **RC5 (128 bit – Login Only**), **RC5 (40 bit**), **RC5 (56 bit)** and **RC5 (128 bit**). The following table shows the valid client-encryption levels corresponding to the encryption level defined for the server. Select the appropriate level from the drop-down list.

CAUTION: IF YOU SELECT AN INVALID ENCRYPTION LEVEL, THE CLIENT WILL NOT BE ABLE TO CONNECT TO THE SERVER.

Valid Client-Server encryption levels

Encryption level defined for the server	*Client Encryption level*			
	Basic	***40-bit***	***56-bit***	***128-bit***
Basic	Valid	Valid	Valid	Valid
40-bit	Not valid	Valid	Valid	Valid
56-bit	Not valid	Not valid	Valid	Valid
128-bit	Not valid	Not valid	Not valid	Valid

12. Configure the above parameters as required and click **Next>** to proceed. The following dialog-box is displayed.



13. In the above dialog-box, you can define settings for the firewall in your network.

    - **Use alternate address through firewalls**: Select this check-box to browse for Citrix servers or published applications that are inside a firewall, from a client outside the firewall. The firewall and the Citrix servers must be configured to map the internal network addresses of Citrix servers to external Internet addresses.
    - **SOCKS** (*Socket Secure*) is a protocol that controls access between networks. A SOCKS enabled server authenticates requests before allowing hosts on one side of the server to access hosts on the other side. Data is relayed through a proxy or intermediate connection.

      Connect via SOCKS proxy: Select this check-box to enable the **Address of proxy to use** and **Port** fields.

      - **Address of proxy to use**: Provide the IP address of the SOCKS proxy server.
      - **Port**: Provide the port number for the proxy connection.
    - **SSL:** ICA with SSL provides strong encryption to increase the privacy of your ICA connections and certificate-based server authentication to ensure the server you are connecting to is a genuine server.

      To enable SSL you must perform the following tasks:

      1. Ensure that your Citrix servers support SSL or have the SSL Relay service installed. See your Citrix server documentation for more information about configuring SSL on the server.
      2. Change the Server Location protocol to SSL+HTTPS.
      3. If the SSL Relay is not installed on the same machine as a Citrix server, or is configured to use a port other than 443, you must specify the SSL Relay address and port.

      - **Address of SSL Relay to use**: Enter the SSL Relay's domain name
      - **Port:** Enter the SSL Relay's port number

14. Click **Finish** to complete creation of the ICA connection. The name of the connection you created will be added to the list of connections displayed in the **Terminal Connection Manager**.

Creating Dial-up ICA Connections

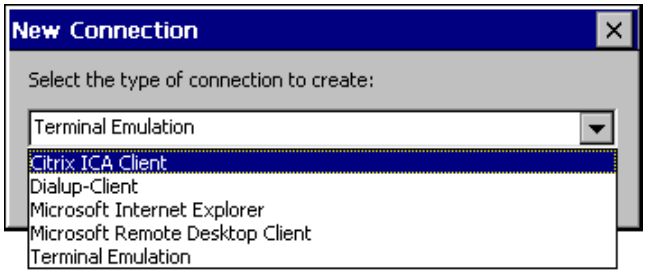
NOTE: DIAL-UP ICA CONNECTIONS CAN BE CREATED ONLY TO METAFRAME SERVERS. YOU CANNOT CREATE DIAL-UP CONNECTIONS TO SERVERS WITH CDS (*CITRIX DEVICE SERVICES*).

This section describes the procedure to create a connection to a MetaFrame server, through a modem connected to one of the COM ports of the client.

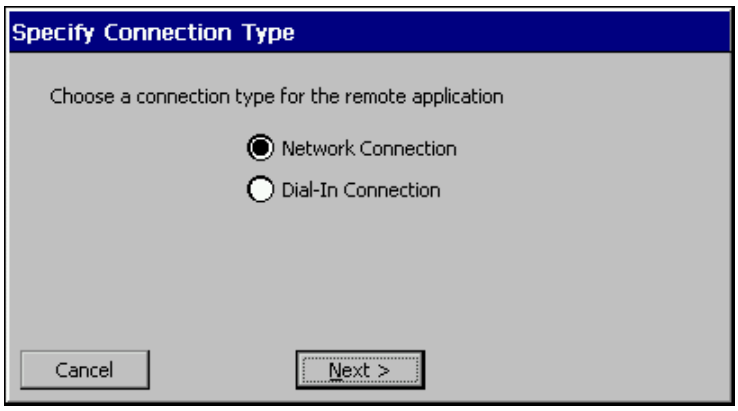
1. Select the **Configure** sheet of the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

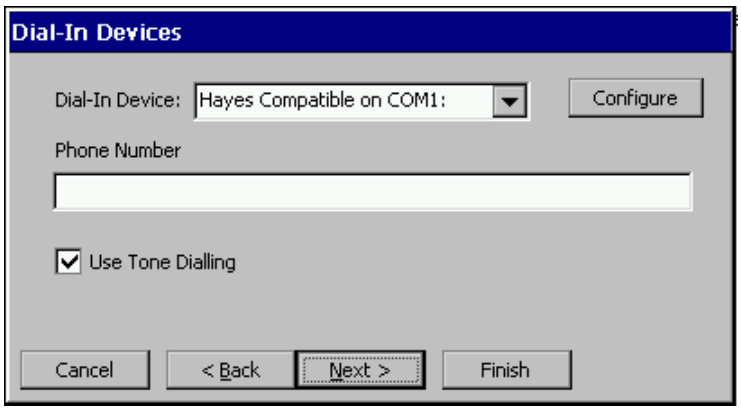
2. Click **Add…**. The **New Connection** dialog-box is displayed.



3. Select **Citrix ICA Client** from the drop-down list. The **Specify Connection Type** dialog-box is displayed.

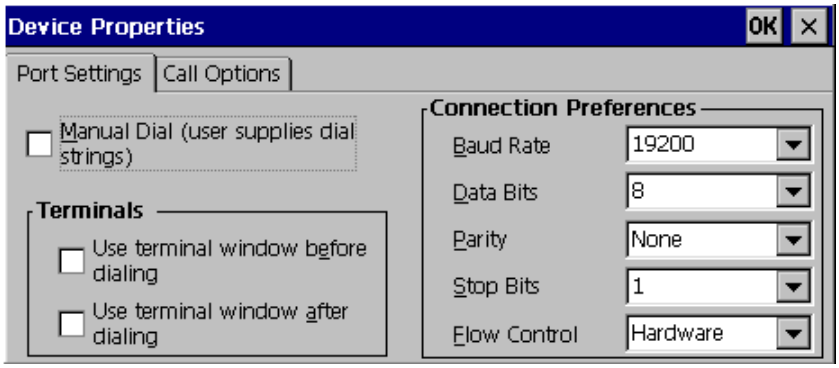


4. Select the **Dial-In Connection** radio-button, and click **Next>**. The following dialog-box is displayed.



5. From the **Dial-In Device** drop-down list, select the COM port to which the modem is connected.

6. Click the **Configure** button. The following dialog-box is displayed. This dialog-box has two tabs. The **Port Settings** tab is selected by default.

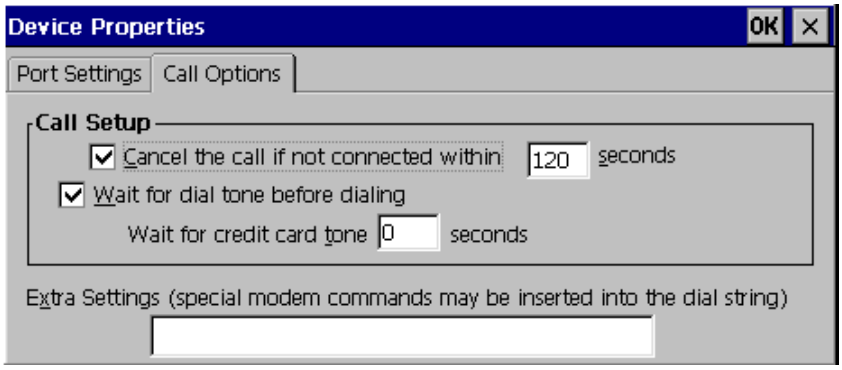


- **Manual Dial**: Select this check-box if you want to provide dial strings while attempting a dial-up connection.

NOTE: MANUAL DIALING IS NOT CURRENTLY SUPPORTED.

- **Use terminal window before dialing**: If you select this check-box, the terminal window is displayed *before* the connection is established.
- **Use terminal window after dialing**: If you select this check-box, the terminal window is displayed *after* the connection is established, prompting you for logon information.
- **Connection Preferences**: In this group of drop-down lists, select the settings for Baud Rate, Data Bits, Parity, Stop Bits and Flow Control.

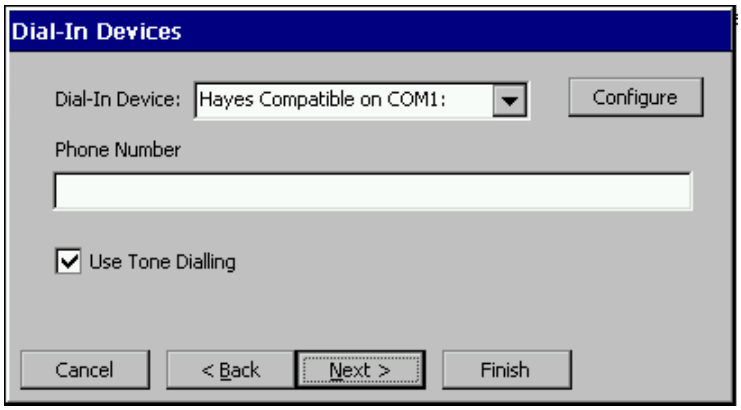
7. After configuring the port settings, select the **Call Options** tab.



- **Cancel the call if not connected within … seconds**: If you want the call to be cancelled if it does not connect within a specified duration, select this check-box and specify the duration in seconds.
- **Wait for dial tone before dialing**: Select this check-box if the dial-in device has to wait for a dial tone before dialing.
- **Wait for credit card tone**… **seconds**: In this field, specify the duration for which the client has to wait for a credit card tone.
- **Extra Settings**: In this text field, you can provide special modem commands.

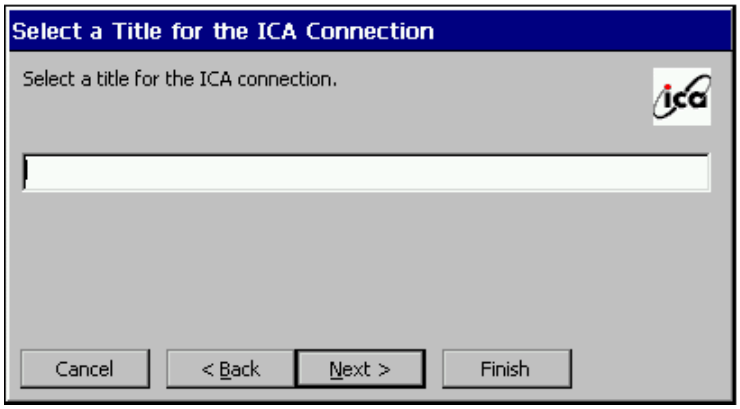
NOTE: IF YOU PROVIDE INPUT IN THIS FIELD, YOU **MUST** ALSO SELECT THE **MANUAL DIAL** CHECK-BOX IN THE **PORT SETTINGS** TAB.

8. After configuring the dial-in device, click **OK** to return to the **Dial-In Devices** dialog-box.

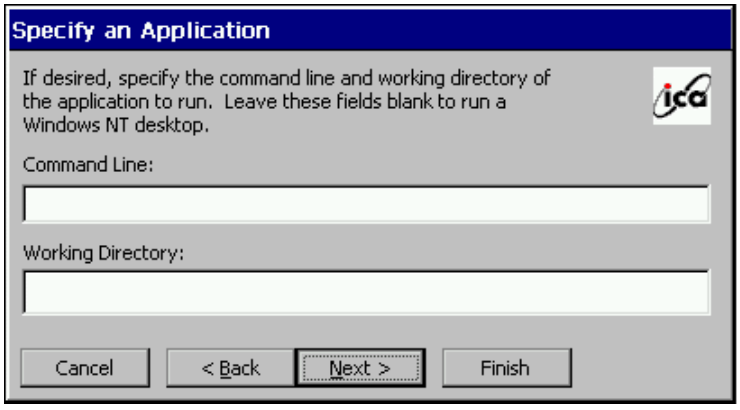


- Specify the telephone number of the server in the **Phone Number** field.
- By default, the client uses tone dialing. To use pulse dialing, deselect the **Use Tone Dialing** check-box.

9. Click **Next>** to proceed. The following dialog-box is displayed.



10. Provide a unique name for the new ICA connection and click **Next>**. The following dialog-box is displayed.



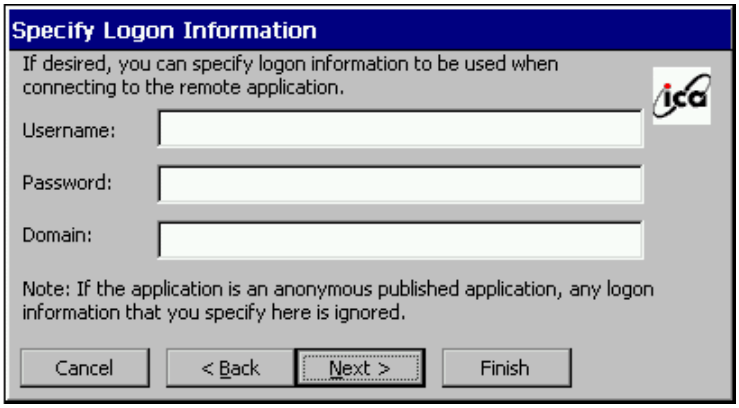
11. If you want an application to be automatically started after connection to the server has been established, provide appropriate information in the above dialog-box.

- **Command Line**: In this text field, provide the name of the application program that you want to invoke.
- **Working Directory**: In this text field, provide the path of the directory where the application program resides.

If you do not provide any input in the above dialog-box, the Windows NT 4.0 TSE or Windows 2000 desktop will be displayed after connecting to the server.

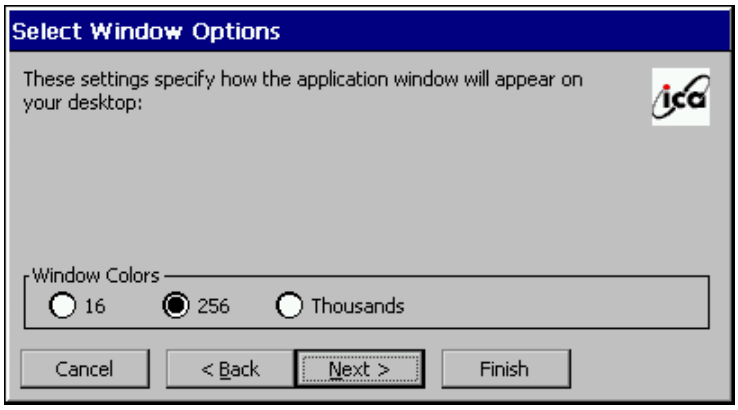
If you specify an application in this dialog-box, the user cannot access any other program or application. The client will automatically start the application when the user logs in, and will display the **Terminal Connection Manager** when the application is closed.

Click **Next>** to proceed. The following dialog-box is displayed.



12. Information in the above dialog-box is used to automatically logon to the server. To implement this feature, provide the **Username**, **Password** and **Domain**. If you leave the fields in this dialog-box blank or provide invalid input, a login prompt will be displayed when you try to connect to the server.

    Click **Next>** to proceed. The following dialog-box is displayed.



13. In the above dialog-box, you can set the color depth for the monitor connected to the client. By default, **256** colors is selected. The **Thousands** option indicates 16-bit color.

NOTE: 16-BIT COLOR IS SUPPORTED ONLY BY METAFRAME 1.8 FEATURE RELEASE-1, METAFRAME XP AND ABOVE. CDS DOES NOT SUPPORT THE 16-BIT COLOR OPTION. IF YOU SELECT THE 16-BIT COLOR OPTION FOR SERVERS THAT DO NOT SUPPORT IT, THE CLIENT DISPLAYS AT 256 COLORS.

Select the appropriate radio-button and click **Next>** to continue. The following dialog-box is displayed.

- **Use Printer Configuration Utility**: This option is selected by default. It allows the printer port of the client to be accessed by ICA users in the network.

  If the connection you are creating is to a server with MetaFrame versions 1.8 and above, ensure that this option is selected. Otherwise, the printer port of the client cannot be accessed.

  If the connection you are creating is to a server with MetaFrame 1.0 or CDS, you **must** disable this option. Otherwise, the printer port of the client cannot be accessed.

- **Compress Data Stream**: This option is enabled by default. This setting causes data to be compressed before transmission, thus optimizing the bandwidth usage. Note that while data compression reduces the transmission time, it consumes more processor resources.

- **Enable Sound**: The client supports audio when it is connected to MetaFrame servers. Select this check-box to enable sound and set the audio quality from the **Sound Quality** drop-down list. The options available are **High**, **Medium** and **Low**.

NOTE: THIS SETTING HAS NO EFFECT IF THE CONNECTION YOU ARE CREATING IS TO A SERVER THAT HAS CDS (*CITRIX DEVICE SERVICES*).

- **SpeedScreen**: MetaFrame 1.8 FR-1, MetaFrame-XP and above include a feature to reduce keystroke and mouse-click latency. Latency is the delay between a keystroke/mouse-click and the corresponding change on the screen. This drop-down list allows you to specify whether you want to use the SpeedScreen feature of the MetaFrame server.
  - **Off**: This setting indicates that the client will not benefit from the SpeedScreen feature.
  - **On**: The server manages keystroke and mouse-click latency at the client to provide improved and consistent performance.
  - **Auto**: The server manages keystroke and mouse-click latency, if the latency is between the upper and lower threshold-limits specified at the server.
- **Encryption Level**: Data Encryption is not supported by servers that have CDS (*Citrix Device Services*). To use data encryption, **Citrix MetaFrame** (including the **Secure ICA** service) must be installed on the server. If you specify encryption for a connection to a server that does not have MetaFrame, the following error message is displayed when you try to start the connection:

  'Your Citrix server does not support the encryption you required'.

NOTE: THE SECURE ICA SERVICE **MUST BE INSTALLED SEPARATELY** ON SERVERS WITH THE FOLLOWING METAFRAME VERSIONS.
- METAFRAME 1.X ON WINDOWS NT 4.0 TSE SERVER
- METAFRAME 1.8 ON WINDOWS 2000 SERVER

SECURE ICA SERVICE **IS INSTALLED BY DEFAULT** ON SERVERS WITH THE FOLLOWING METAFRAME VERSIONS.
- METAFRAME 1.8 WITH FEATURE RELEASE 1
- METAFRAME XP

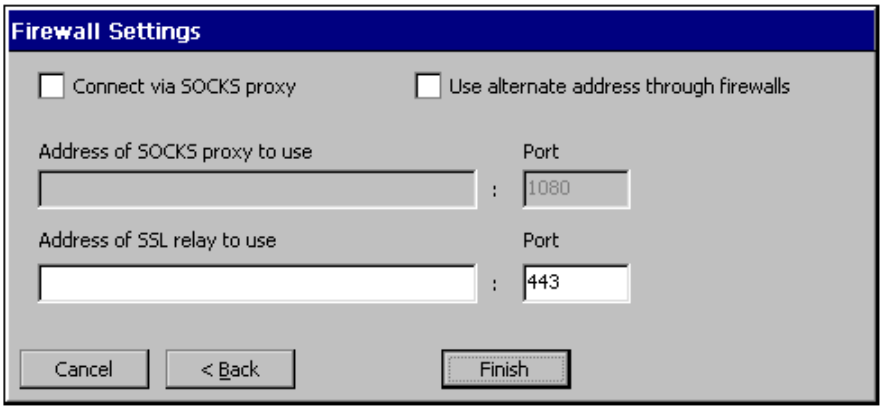
The default encryption level is **Basic**. The other options are **RC5 (128 bit – Login Only**), **RC5 (40 bit**), **RC5 (56 bit)** and **RC5 (128 bit**). The following table shows the valid client-encryption levels corresponding to the encryption level defined for the server. Select the appropriate level from the drop-down list.

CAUTION: IF YOU SELECT AN INVALID ENCRYPTION LEVEL, THE CLIENT WILL NOT BE ABLE TO CONNECT TO THE SERVER.

Valid Client-Server encryption levels

Encryption level defined for the server	*Client Encryption level*			
	Basic	***40-bit***	***56-bit***	***128-bit***
Basic	Valid	Valid	Valid	Valid
40-bit	Not valid	Valid	Valid	Valid
56-bit	Not valid	Not valid	Valid	Valid
128-bit	Not valid	Not valid	Not valid	Valid

14. Configure the above parameters and click **Next>** to proceed. The following dialog-box is displayed.



15. In the above dialog-box, you can define settings for the firewall in your network.

- **Use alternate address through firewalls**: Select this check-box to browse for Citrix servers or published applications that are inside a firewall, from a client outside the firewall. The firewall and the Citrix servers must be configured to map the internal network addresses of Citrix servers to external Internet addresses.
- **SOCKS** (*Socket Secure*) is a protocol that controls access between networks. A SOCKS enabled server authenticates requests, before allowing hosts on one side of the server to access hosts on the other side. Data is relayed through a 'proxy' or intermediate connection.

  Connect via SOCKS proxy: Select this check-box to enable the **Address of proxy to use** and **Port** fields.

  - **Address of proxy to use**: Provide the IP address of the SOCKS proxy server.
  - **Port**: Provide the port number for the proxy connection.
- **SSL:** ICA with SSL provides strong encryption to increase the privacy of your ICA connections and certificate-based server authentication to ensure the server you are connecting to is a genuine server.

  To enable SSL you must perform the following tasks:

  1. Ensure that your Citrix servers support SSL or have the SSL Relay service installed. See your Citrix server documentation for more information about configuring SSL on the server.
  2. Change the Server Location protocol to SSL+HTTPS.

3. If the SSL Relay is not installed on the same machine as a Citrix server, or is configured to use a port other than 443, you must specify the SSL Relay address and port.
   - **Address of SSL Relay to use**: Enter the SSL Relay's domain name
   - **Port:** Enter the SSL Relay's port number

16. Click **Finish** to complete creation of the ICA connection. The name of the connection you created will be added to the list of connections displayed in the **Terminal Connection Manager**.

To start the connection, double-click on it, or highlight it and click the **Connect** button in the **Terminal Connection Manager**.

Editing TCP/IP ICA Connections

This section describes the procedure to edit an ICA connection created through the network port of the client.

1. Select the **Configure** sheet from the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

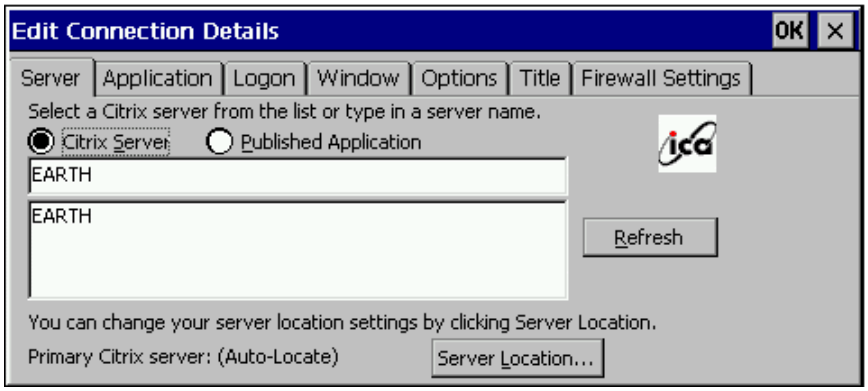
2. Highlight the ICA connection to be edited.

TIP: THE 'TYPE' OF CONNECTION IS DISPLAYED IN THE **TYPE** COLUMN OF THE **TERMINAL CONNECTION MANAGER** WINDOW.

NOTE: CONNECTIONS CANNOT BE EDITED WHILE THEY ARE ACTIVE.

3. Click the **Edit…** button. The following dialog-box is displayed. This dialog-box has seven tabs. The contents of each tab are explained in the following pages. After editing the required options, click **OK** to return to the **Terminal Connection Manager**.

Server tab



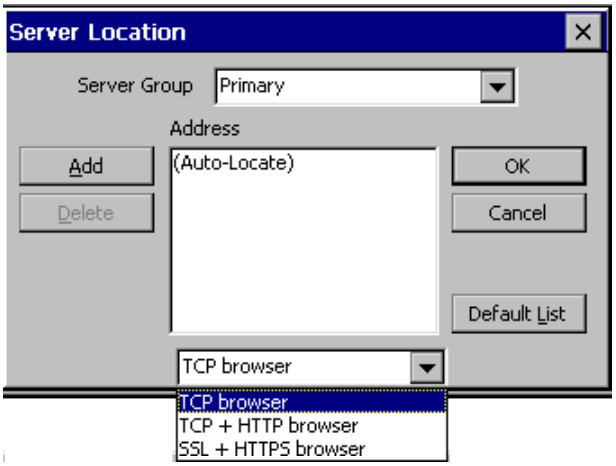
- **Citrix Server**: Select this radio-button if the connection is to a server that supports the ICA protocol.
- **Published Application**: Select this radio-button if the connection is to a published-application.

NOTE: PUBLISHED APPLICATIONS CAN BE CREATED ONLY ON METAFRAME SERVERS.

- **Refresh**: Click this button to refresh the list of servers or published applications displayed. The client searches the network for servers or published applications and displays them in the dialog-box.

NOTE: ONLY METAFRAME SERVERS ARE DISPLAYED IN THE ABOVE DIALOG-BOX. TO CREATE A CONNECTION TO A SERVER THAT HAS CDS (*CITRIX DEVICE SERVICES*), YOU MUST SPECIFY THE IP ADDRESS OF THE SERVER IN THE TEXT FIELD BENEATH THE RADIO-BUTTONS. YOU MAY PROVIDE THE NAME OF THE SERVER (*INSTEAD OF IP ADDRESS*) IF THE NETWORK HAS A WINS (*WINDOWS INTERNET NAMING SERVICE*) SERVER.

- **Server Location**: Click this button to specify a method to search the network for Citrix servers and published applications. The following dialog-box is displayed.



If the **(Auto-Locate)** entry is highlighted in the **Address** list, the client broadcasts a 'Get Nearest Citrix Server' packet. The first Citrix server to respond is then requested for lists of servers and published applications on the network.

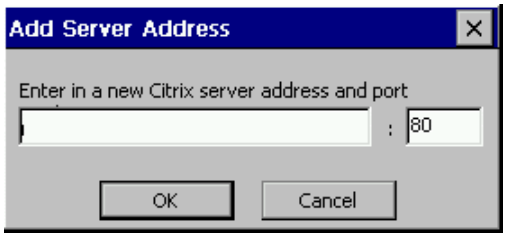
However, to eliminate broadcasts on your network, you may want to designate a particular Citrix sever as the master-browser. The network protocol setting allows you to control the way the ICA client searches. The protocols are:

- **TCP browser:** The ICA Client uses the UDP protocol to search for Citrix servers. The ICA Client communicates with the Citrix server using ICA protocol over TCP/IP.
- **TCP + HTTP browser:** The ICA Client uses the HTTP protocol to locate Citrix servers. The ICA Client communicates with the Citrix server using ICA protocol over TCP/IP. Select this option when using the ICA Client over the Internet or via a firewall or proxy server. This is the default protocol.
- **SSL + HTTPS browser:** The ICA Client uses the HTTPS protocol to locate Citrix servers. The ICA Client communicates with the Citrix server using ICA with SSL. SSL provides strong encryption of ICA traffic and Citrix server authentication. Select this option when using the ICA Client over the Internet or via a firewall or proxy server.

NOTE: THE TCP + HTTP AND SSL+HTTP PROTOCOLS CAN ONLU BE USED WITH COMPATIBLE CITRIX SERVERS. CHECK THE APPROPRIATE CTRIX SERVER ADMINISTRATOR'S GUIDE FOR FUTURE INFORMATION.

NOTE: THE TCP + HTTP AND SSL +HTTP PROTOCOLS DOES NOT SUPPORT THE **AUTO-LOCATE** FUNCTION.

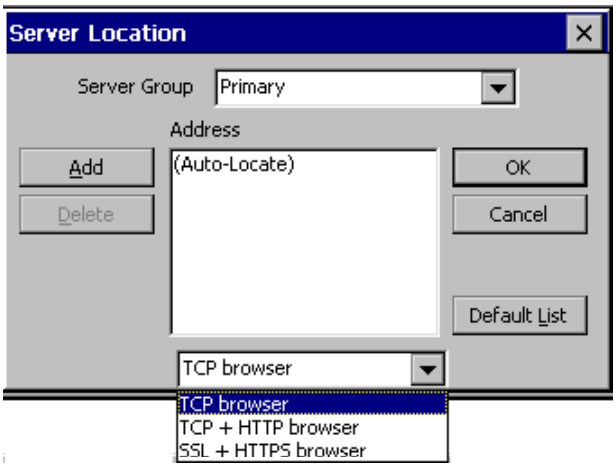
- **Server Group**: From this drop-down list you can select one of three groups of servers: **Primary**, **Backup1** and **Backup2**. The default group is **Primary**.
- To add the address of a master-browser, click **Add**. This following dialog-box is displayed.



NOTE: THE PORT NUMBER FIELD IS DISPLAYED ONLY IF YOU SELECTED THE **TCP + HTTP OR SSL + HTTPS PROTOCOL** IN THE **SERVER LOCATION** DIALOG-BOX.

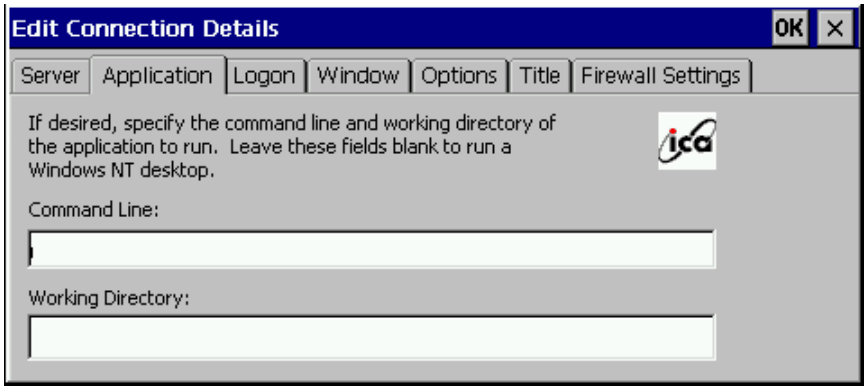
Enter the IP address of a Citrix server and a recognized port number (*default: 80*) and click **OK** to return to the **Server Location** dialog-box. The specified server responds with a list of all servers and published applications in its server farm.

NOTE: IF YOU SELECT THE **TCP + HTTP OR SSL + HTTPS** PROTOCOL IN THE **SERVER LOCATION** DIALOG-BOX AND YOU DO NOT ADD ANY MASTER BROWSER, YOU MUST HAVE A CITRIX SERVER ON YOUR NETWORK MAPPED TO THE DEFAULT NAME: **ICA**.



- **Default List**: Click this button to cancel any modification and to recall the saved list of servers. At the prompt, click **Yes** to recall the saved list, and **No** to retain the current list.
- **Delete**: Click this button to delete an address from the list. If you delete all the addresses in the **Primary Server Group**, the **(Auto-Locate)** entry will be highlighted in the **Address** list.

Application tab



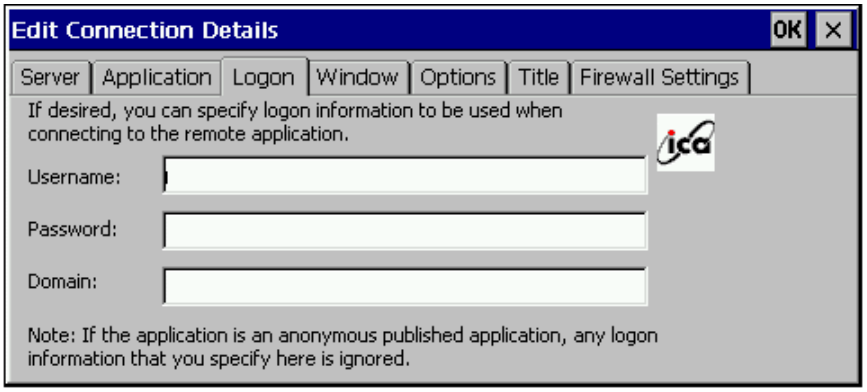
In the above dialog-box, you can provide information about the application to be automatically started after connection to the server has been established.

If you do not provide any input in the above dialog-box, the Windows NT 4.0 TSE or Windows 2000 desktop will be displayed after connecting to the server.

If you specify an application to be automatically started, the user cannot access any other program or application. The client will automatically start the application when the user logs in, and will display the **Terminal Connection Manager** when the application is closed.

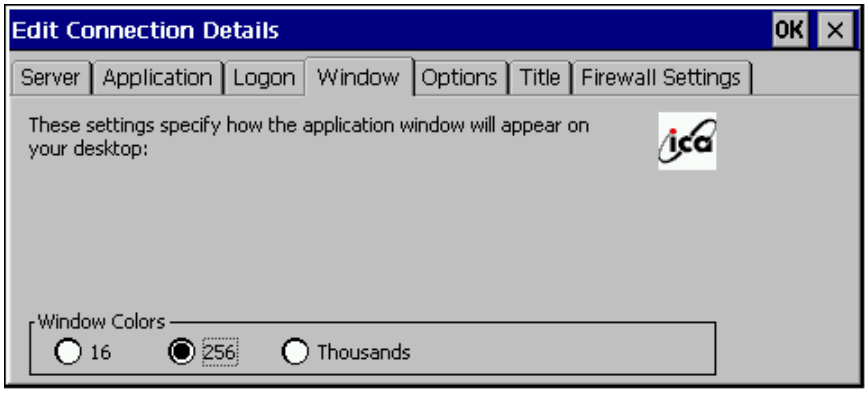
- **Command Line**: In this field, provide the directory path and name of the application program that you want to invoke.
- **Working Directory**: In this field, provide the name of the working directory to be used by the application.

Logon tab



Information in the above dialog-box will be used to automatically logon to the server. To implement this feature, provide the **Username**, **Password** and **Domain**. If you leave the fields in this dialog-box blank or provide invalid input, a login prompt will be displayed when the connection is started.

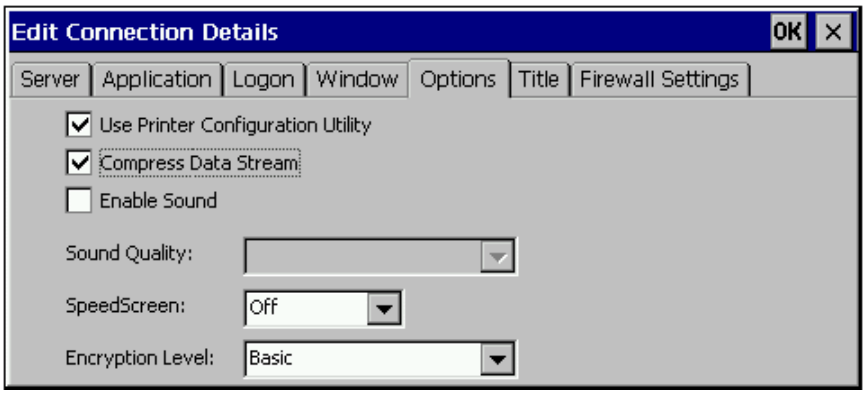
Window tab



In the above dialog-box, you can set the color depth for the monitor connected to the client. By default, **256** colors is selected. The **Thousands** option indicates 16-bit color.

NOTE: 16-BIT COLOR IS SUPPORTED ONLY BY METAFRAME 1.8 FEATURE RELEASE-1, METAFRAME XP AND ABOVE. CDS DOES NOT SUPPORT THE 16-BIT COLOR OPTION. IF YOU SELECT THE 16-BIT COLOR OPTION FOR SERVERS THAT DO NOT SUPPORT IT, THE CLIENT DISPLAYS AT 256 COLORS.

Options tab



- **Use Printer Configuration Utility**: This option is selected by default. It allows the printer port of the client to be accessed by ICA users in the network.

If the connection you are editing is to a server with MetaFrame versions 1.8 and above, ensure that this option is selected. Otherwise, the printer port of the client cannot be accessed.

If the connection you are editing is to a server with MetaFrame 1.0 or CDS, you **must** disable this option. Otherwise, the printer port of the client cannot be accessed.

- **Compress Data Stream**: This setting causes data to be compressed before transmission, thus optimizing the bandwidth usage. Note that while data compression reduces the transmission time, it consumes more processor resources.
- **Enable Sound**: The client supports audio when it is connected to MetaFrame servers. Select this check-box to enable sound. You can set the audio quality from the **Sound Quality** drop-down list. The options available are **High**, **Medium** and **Low**.

NOTE: THIS SETTING HAS NO EFFECT IF THE CONNECTION YOU ARE EDITING IS TO A SERVER THAT HAS CDS (*CITRIX DEVICE SERVICES*).

- **SpeedScreen**: MetaFrame-1.8 FR-1, MetaFrame-XP and above include a feature to reduce keystroke and mouse-click latency. Latency is the delay between a keystroke/mouse-click and the corresponding change on the screen. This drop-down list allows you to specify whether you want to use the SpeedScreen feature of the MetaFrame server.

  Off: This is the default setting. The client will not benefit from the SpeedScreen feature of the server.

  On: The server manages keystroke and mouse-click latency at the client to provide improved and consistent performance.

  Auto: The server manages keystroke and mouse-click latency, if the latency is between the upper and lower threshold-limits specified at the server.

- **Encryption Level**: Data Encryption is not supported by servers that have CDS (*Citrix Device Services*). To use data encryption, **Citrix MetaFrame** (including the **Secure ICA** service) must be installed on the server.

  If you specify encryption for a connection to a server that does not have MetaFrame, the following error message is displayed when you try to start the connection:

  'Your Citrix server does not support the encryption you required'.

NOTE: THE SECURE ICA SERVICE **MUST BE INSTALLED SEPARATELY** ON SERVERS WITH THE FOLLOWING METAFRAME VERSIONS.

- METAFRAME 1.X ON WINDOWS NT 4.0 TSE SERVER
- METAFRAME 1.8 ON WINDOWS 2000 SERVER

THE SECURE ICA SERVICE **IS INSTALLED BY DEFAULT** ON SERVERS WITH THE FOLLOWING METAFRAME VERSIONS.

- METAFRAME 1.8 WITH FEATURE RELEASE 1
- METAFRAME XP

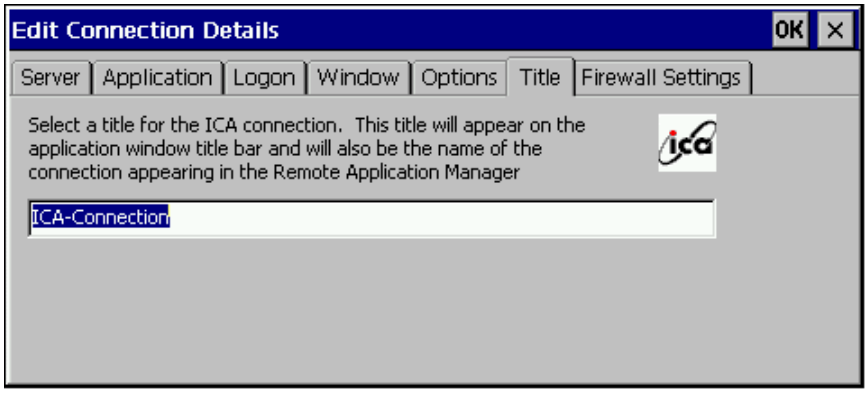
The default encryption level is **Basic**. The other options are **RC5 (128 bit – Login Only**), **RC5 (40 bit**), **RC5 (56 bit)** and **RC5 (128 bit**). The following table shows the valid client encryption levels corresponding to the encryption level defined for the server. Select the appropriate level from the drop-down list.

CAUTION: IF YOU SELECT AN INVALID ENCRYPTION LEVEL, THE CLIENT WILL NOT BE ABLE TO CONNECT TO THE SERVER.

Valid Client-Server encryption levels

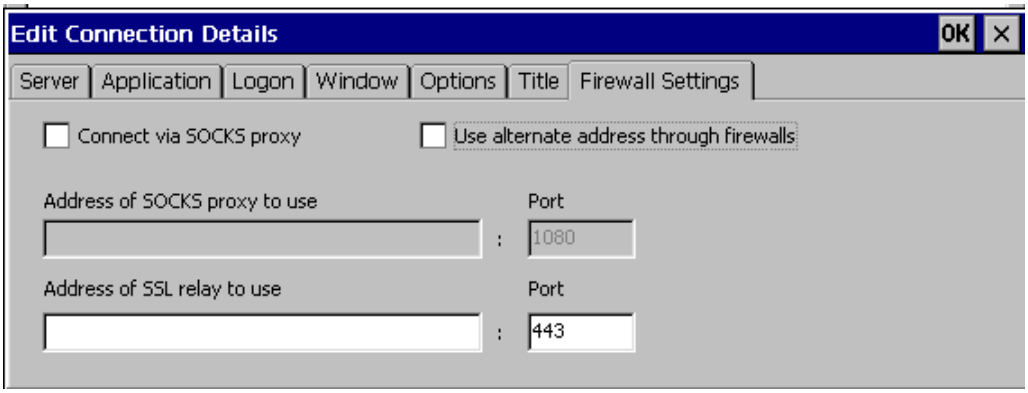
Encryption level defined for the server	*Client Encryption level*			
	Basic	***40-bit***	***56-bit***	***128-bit***
Basic	Valid	Valid	Valid	Valid
40-bit	Not valid	Valid	Valid	Valid
56-bit	Not valid	Not valid	Valid	Valid
128-bit	Not valid	Not valid	Not valid	Valid

Title tab



In the above dialog-box, you can edit the name of the ICA connection.

Firewall Settings tab



In the above dialog-box, you can define settings for the firewall in your network.

- **Use alternate address through firewalls**: Select this check-box to browse for Citrix servers or published applications that are inside a firewall, from a client outside the firewall. The firewall and the Citrix servers must be configured to map the internal network addresses of Citrix servers to external Internet addresses.
- **SOCKS** (*Socket Secure*) is a protocol that controls access between networks. A SOCKS enabled server authenticates requests, before allowing hosts on one side of the server to access hosts on the other side. Data is relayed through a 'proxy' or intermediate connection.
  - **Connect via SOCKS proxy**: Select this check-box to enable the **Address of proxy to use** and **Port** fields.
  - **Address of proxy to use**: Provide the IP address of the SOCKS proxy server.
  - **Port**: Provide the port number for the proxy connection.
  - **Address of SSL relay to use**: Enter the SSL Relay's domain name. For details about SSL, refer to the SSL option under Creating TCP/IP ICA Connection. Page. No84

- **Port:** Enter the SSL Relay's port number.

After editing the connection, click **OK** to save changes and return to the **Terminal Connection Manager**

Editing Dial-up ICA Connections

This section describes the procedure to edit an ICA connection created through a modem connected to one of the COM ports of the client.

1. Select the **Configure** sheet from the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

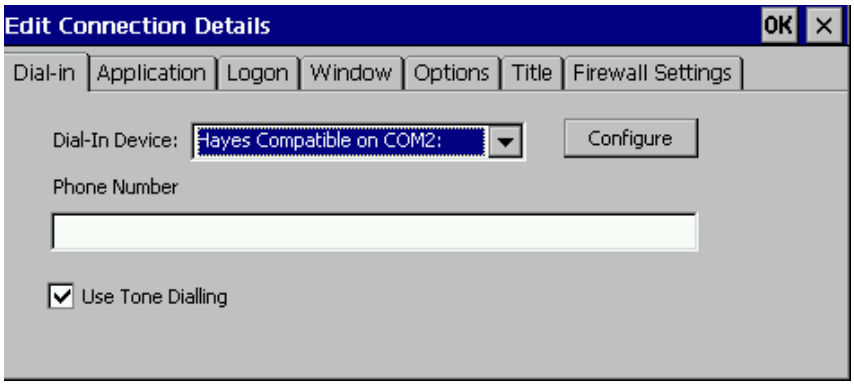
2. Highlight the ICA connection to be edited.

TIP: THE 'TYPE' OF CONNECTION IS DISPLAYED IN THE **TYPE** COLUMN OF THE **TERMINAL CONNECTION MANAGER** WINDOW.

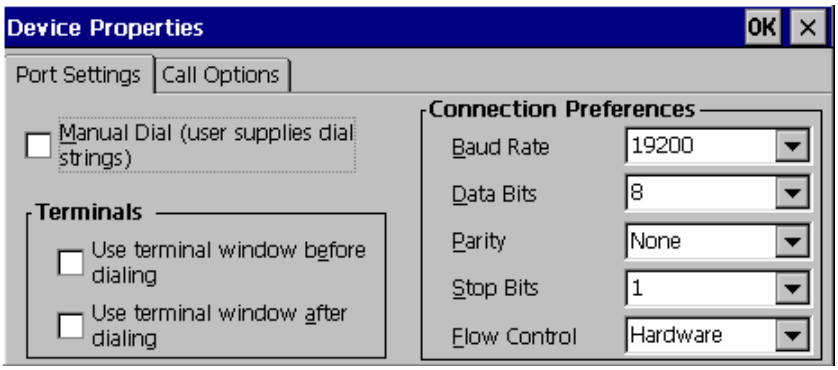
NOTE: CONNECTIONS CANNOT BE EDITED WHILE THEY ARE ACTIVE.

3. Click the **Edit…** button. The following dialog-box is displayed. This dialog-box has seven tabs. The contents of each tab are explained in the following pages. After editing the required options, click **OK** to return to the **Terminal Connection Manager**.

Dial-in tab



- **Dial-In Device**: From this drop-down list, select the COM port to which the modem is connected.
- **Configure**: Click this button to configure port settings and call options. The following dialog-box is displayed. This dialog-box has two tabs. The **Port Settings** tab is selected by default.

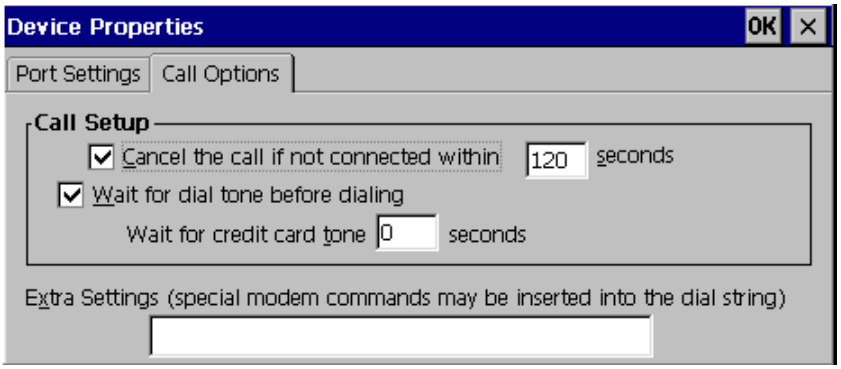


- **Manual Dial**: Select this check-box, if you want to provide dial strings while attempting a dial-up connection.

NOTE: MANUAL DIALING IS NOT CURRENTLY SUPPORTED.

- **Use terminal window before dialing**: If you select this check-box, the terminal window is displayed before the connection is established.
- **Use terminal window after dialing**: If you select this check-box, the terminal window is displayed after the connection is established, prompting you for logon information.
- **Connection Preferences**: In this group of drop-down lists select the settings for Baud Rate, Data Bits, Parity, Stop Bits and Flow Control.

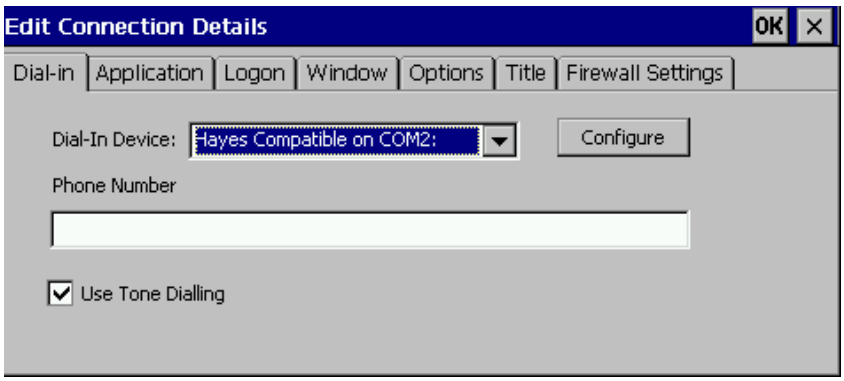
After configuring the port settings, select the **Call Options** tab.



- **Cancel the call if not connected within … seconds**: If you want the call to be cancelled if it does not connect within a specified time limit, select this check-box and specify the duration.
- **Wait for dial tone before dialing**: Select this check-box if the dial-in device has to wait for a dial tone before dialing.
- **Wait for credit card tone**… **seconds**: In this field, specify the duration for which the terminal has to wait for a credit card tone.
- **Extra Settings**: In this text field, you can provide special modem commands.

NOTE: IF YOU PROVIDE INPUT IN THIS FIELD, YOU **MUST** ALSO SELECT THE **MANUAL DIAL** CHECK-BOX IN THE **PORT SETTINGS** TAB.

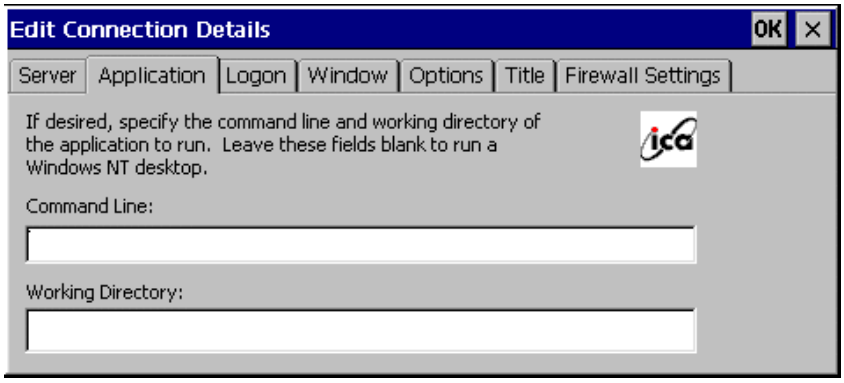
After configuring the above parameters, click **OK** to return to the **Dial-in** tab.



- Specify the telephone number of the server that you want to dial-up in the **Phone Number** field.
- By default, the client uses tone dialing. If you want to use pulse-dialing, disable the **Use Tone Dialing** check-box.

NOTE: DIAL-UP ICA CONNECTIONS CAN BE CREATED ONLY TO METAFRAME SERVERS. YOU CANNOT CREATE DIAL-UP CONNECTIONS TO SERVERS WITH CDS (*CITRIX DEVICE SERVICES*).

Application tab



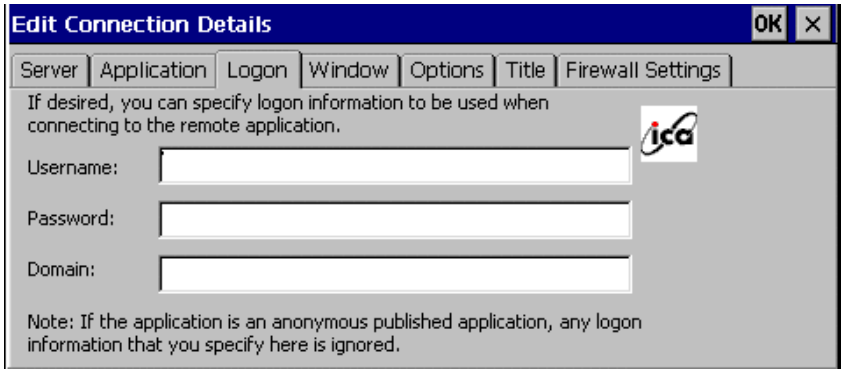
In the above dialog-box, you can provide information about the application to be automatically started after connection to the server has been established.

If you do not provide any input in the above dialog-box, the Windows NT 4.0 TSE or Windows 2000 desktop will be displayed after connecting to the server.

If you specify an application in the above dialog-box, the user cannot access any other program or application. The client will automatically start the application when the user logs in, and will display the **Terminal Connection Manager** when the application is closed.

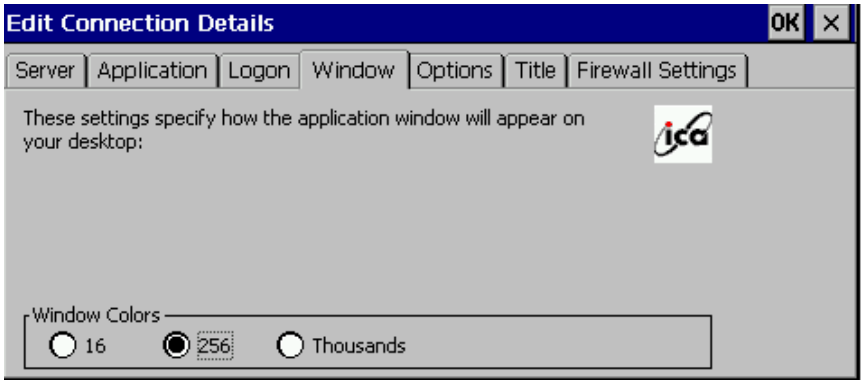
- **Command Line**: In this field, provide the directory-path and name of the application program that has to be automatically started after connecting to the server.
- **Working Directory**: In this text field, provide the name of the working directory to be used by the application.

Logon tab



Information in the above dialog-box is used to automatically logon to the server. To implement this feature, provide the **Username**, **Password** and **Domain**. If you leave the fields in this dialog-box blank or provide invalid input, a login prompt will be displayed when the connection is started.

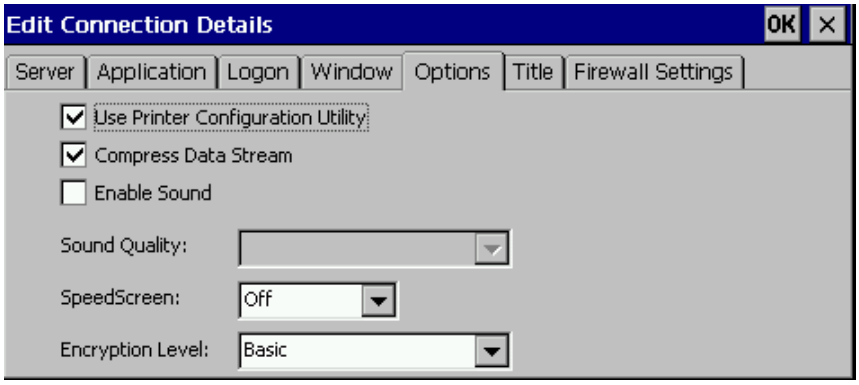
Window tab



In the above dialog-box, you can set the color depth for the monitor connected to the client. By default, **256** colors is selected. The **Thousands** option indicates 16-bit color.

NOTE: 16-BIT COLOR IS SUPPORTED ONLY BY METAFRAME 1.8 FEATURE RELEASE-1, METAFRAME XP AND ABOVE. CDS DOES NOT SUPPORT THE 16-BIT COLOR OPTION. IF YOU SELECT THE 16-BIT COLOR OPTION FOR SERVERS THAT DO NOT SUPPORT IT, THE CLIENT DISPLAYS AT 256 COLORS.

Options tab



- **Use Printer Configuration Utility**: This option is selected by default. It allows the printer port of the client to be accessed by ICA users in the network.

  If the connection you are editing is to a server with MetaFrame versions 1.8 and above, ensure that this option is selected. Otherwise, the printer port of the client cannot be accessed.

  If the connection you are editing is to a server with MetaFrame 1.0 or CDS, you **must** disable this option. Otherwise, the printer port of the client cannot be accessed.

- **Compress Data Stream**: This setting causes data to be compressed before transmission, thus optimizing the bandwidth usage. Note that while data compression reduces the transmission time, it consumes more processor resources.

- **Enable Sound**: The client supports audio when it is connected to MetaFrame servers. Select this check-box to enable sound. You can set the audio quality from the **Sound Quality** drop-down list. The options available are **High**, **Medium** and **Low**.

NOTE: THIS SETTING HAS NO EFFECT IF THE CONNECTION YOU ARE EDITING IS TO A SERVER THAT HAS CDS (*CITRIX DEVICE SERVICES*).

- **SpeedScreen**: MetaFrame-1.8 FR-1, MetaFrame-XP and above include a feature to reduce keystroke and mouse-click latency. Latency is the delay between a keystroke/mouse-click and the corresponding change on the screen. This drop-down list allows you to specify whether you want to use the SpeedScreen feature of the MetaFrame server.

  Off: This is the default setting. The client will not benefit from the SpeedScreen feature of the server.

  On: The server manages keystroke and mouse-click latency at the client to provide improved and consistent performance.

  Auto: The server manages keystroke and mouse-click latency, if the latency is between the upper and lower threshold-limits specified at the server.

- **Encryption Level**: Data Encryption is not supported by servers that have CDS (*Citrix Device Services*). To use data encryption, **Citrix MetaFrame** (including the **Secure ICA** service) must be installed on the server.

  If you specify encryption for a connection to a server that does not have MetaFrame, the following error message is displayed when you try to start the connection:

  'Your Citrix server does not support the encryption you required'.

NOTE: THE SECURE ICA SERVICE **MUST BE INSTALLED SEPARATELY** ON SERVERS WITH THE FOLLOWING METAFRAME VERSIONS.

- METAFRAME 1.X ON WINDOWS NT 4.0 TSE SERVER
- METAFRAME 1.8 ON WINDOWS 2000 SERVER

THE SECURE ICA SERVICE **IS INSTALLED BY DEFAULT** ON SERVERS WITH THE FOLLOWING METAFRAME VERSIONS.

- METAFRAME 1.8 WITH FEATURE RELEASE 1
- METAFRAME XP

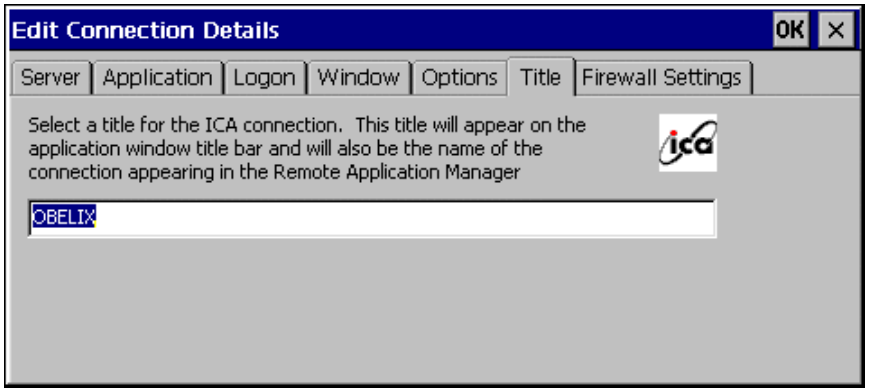
The default encryption level is **Basic**. The other options are **RC5 (128 bit – Login Only**), **RC5 (40 bit**), **RC5 (56 bit)** and **RC5 (128 bit**). The following table shows the valid client encryption levels corresponding to the encryption level defined for the server. Select the appropriate level from the drop-down list.

CAUTION: IF YOU SELECT AN INVALID ENCRYPTION LEVEL, THE CLIENT WILL NOT BE ABLE TO CONNECT TO THE SERVER.

Valid Client-Server encryption levels

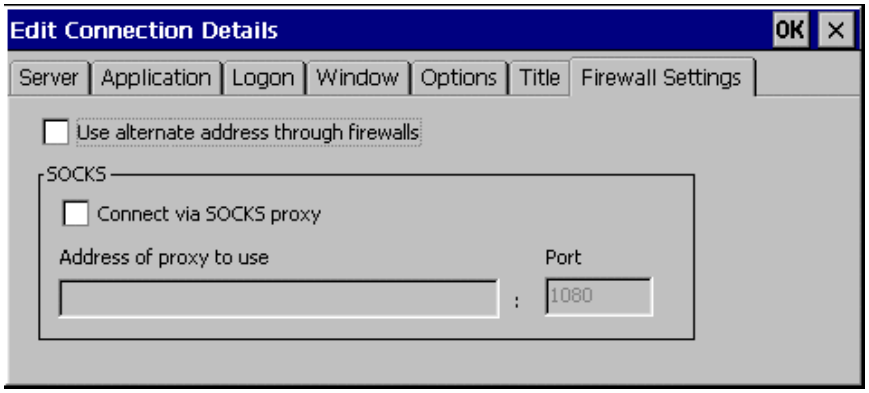
Encryption level defined for the server	*Client Encryption level*			
	Basic	***40-bit***	***56-bit***	***128-bit***
Basic	Valid	Valid	Valid	Valid
40-bit	Not valid	Valid	Valid	Valid
56-bit	Not valid	Not valid	Valid	Valid
128-bit	Not valid	Not valid	Not valid	Valid

Title tab



In the above dialog-box, you can edit the name of the ICA connection.

Firewall Settings tab



In the above dialog-box, you can define settings for the firewall in your network.

- **Use alternate address through firewalls**: Select this check-box to browse for Citrix servers or published applications that are inside a firewall, from a client outside the firewall. The firewall and the Citrix servers must be configured to map the internal network addresses of Citrix servers to external Internet addresses.
- **SOCKS** (*Socket Secure*) is a protocol that controls access between networks. A SOCKS enabled server authenticates requests, before allowing hosts on one side of the server to access hosts on the other side. Data is relayed through a 'proxy' or intermediate connection.
    - **Connect via SOCKS proxy**: Select this check-box to enable the **Address of proxy to use** and **Port** fields.
    - **Address of proxy to use**: Provide the IP address of the SOCKS proxy server.
    - **Port**: Provide the port number for the proxy connection.
    - **Address of SSL relay to use**: Enter the SSL Relays' domain name. For details about SSL, refer to SSL option under Creating TCP/IP ICA Connection. Page No.84
    - **Port**: Enter the SSL Relay's port number.

After editing the connection, click **OK** to save changes and return to the **Terminal Connection Manager**.

Initiating ICA Connection

1. Select the **Connections** sheet from the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Highlight the ICA connection to start. Click **Connect.**

NOTE: YOU CAN ALSO DOUBLE-CLICK ON THE CONNECTION TO START/INITIATE THE CONNECTION.

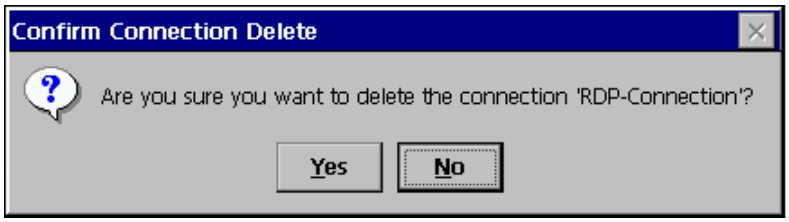
Deleting ICA Connection

To delete a defined connection,

1. Select the Configure sheet from the Terminal Connection Manager window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Highlight the connection to be deleted, and click the **Delete** button. A **Confirm Connection Delete** prompt is displayed.



3. Click **Yes** to confirm deletion and **No** to cancel the delete command.

Terminal Emulation Connection

Creating TCP/IP Terminal Emulation Connections

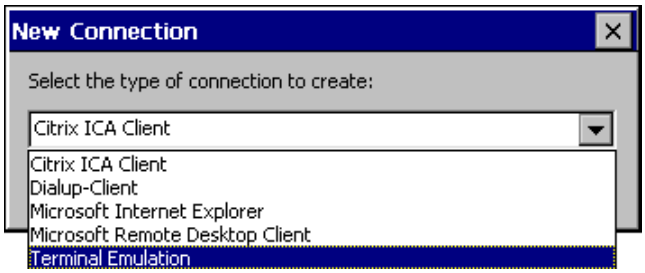
TIP: DETAILED INFORMATION ABOUT TERMINAL EMULATION SETTINGS IS PROVIDED IN THE ***PERICOM Windows CE Emulation User's Guide***, WHICH IS AVAILABLE IN THE CD SUPPLIED WITH THE PRODUCT.

This section describes the procedure to create a Terminal Emulation connection through the network port of the client.

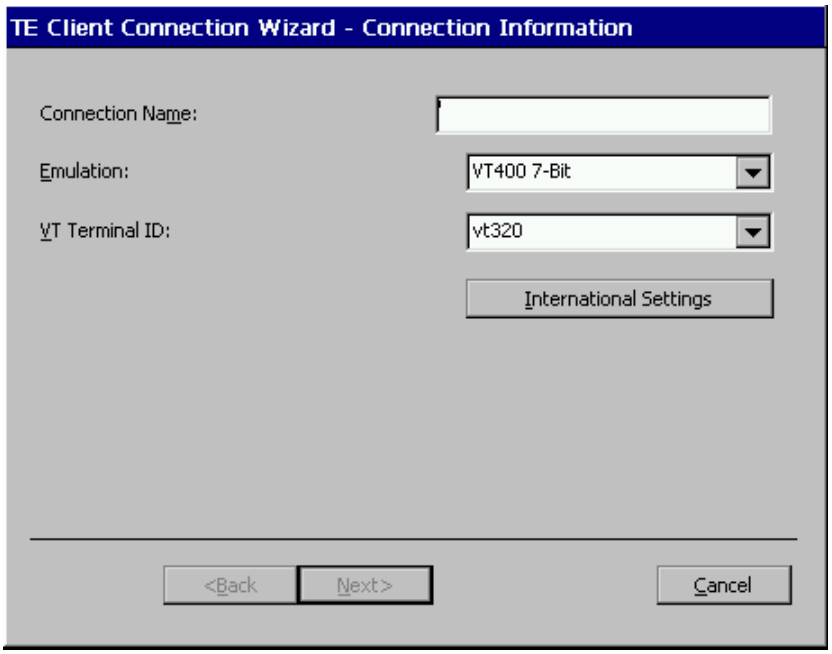
1. Select the **Configure** sheet of the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Click **Add…**. The **New Connection** dialog-box is displayed.



3. Select **Terminal Emulation** from the drop-down list and click **OK**. The first dialog-box of the **TE Client Connection Wizard** is displayed.



- **Connection Name**: In this text field, provide a name for the new connection. The connection-name can consist of a maximum of 42 characters (*including special characters*).
- **Emulation**: From this drop-down list, select the type of emulation. If you select **IBM3270** or **IBM5250** emulation-types, a few other options (*as mentioned in column-3 of the table on the following page*) will be displayed.

- **International Settings**: If you click this button, the **National Replacement Character** dialog-box is displayed. With this dialog-box you can configure the keyboard language, character set mode and other settings for the Terminal Emulation connection.

  The contents of this dialog-box vary depending on the **Emulation**-type selected.

  Additional information is available in the *PERICOM Windows CE Emulation User's Guide*, which is in the CD supplied with the thin client. *Keyboard language settings are described in the **Emulation Settings** chapter on page 68 of the Emulation User's Guide. Character-set tables are available in pages 159-189 of the Emulation User's Guide*.

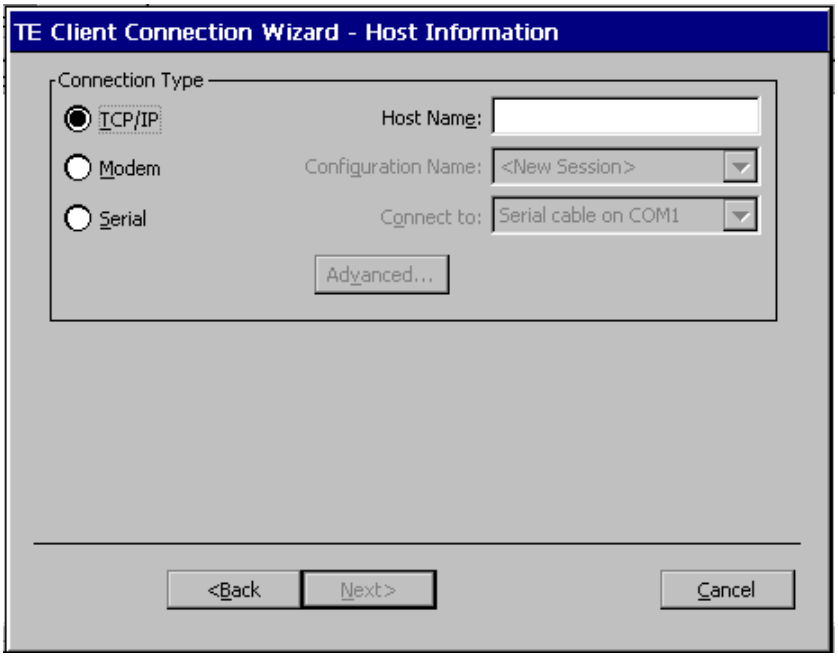
- **VT Terminal ID**: The name of this field depends on the **Emulation-**type selected. Since the default emulation-type is **VT300 7-Bit**, the default name for this field is **VT Terminal ID**. From this drop-down list, select the type of terminal.

The following table contains the emulation and terminal types supported by the client.

Select one of the following from the **Emulation** *drop-down list.*	*Then…*		*And define other options (if any)*
Column-1	***Column-2***		***Column-3***
VT52, VT100, VT300 7-Bit (*default*) or VT300 8-Bit	Select one of the following from the **VT Terminal ID** drop-down list.	Vt100, vt101, vt102, vt125, vt220, vt240, vt320 (*default*), vt340, vt420, vt131 or vt132	
ANSI BBS, SCO Console, WY50, WY50+, WY60, TV1910, TV1920, TV1925, ADDS A2, or HZ1500			
IBM3151	Select one of the following from the **IBM 3151 Model** drop-down list.	11 (*default*) or 31	
IBM3270	Select one of the following from the **IBM 3270 Model** drop-down list.	3278-2, 3278-3, 3278-4, 3278-5, 3278-2-E (*default*), 3278-3-E, 3278-4-E, 3278-5-E, 3279-2, 3279-3, 3279-4, 3279-5 or 3287-1	Select the **Right Ctrl Acts as Enter Key** or the **Left Ctrl Acts as Reset Key** check-boxes if you want to enable these functions for 3270 emulation.
IBM5250	Select one of the following from the **IBM 5250 Model** drop-down list.	5291-1, 5292-2, 5251-11, 3179-2, 3196-A1, 3180-2, 3477-FC, 3477-FG, 3486-BA, 3487-HA or 3487-HC	Select the **Right Ctrl Acts as Enter Key**, **Left Ctrl Acts as Reset Key**, or **IBM5250 Monochrome** check-boxes if you want to enable these functions for

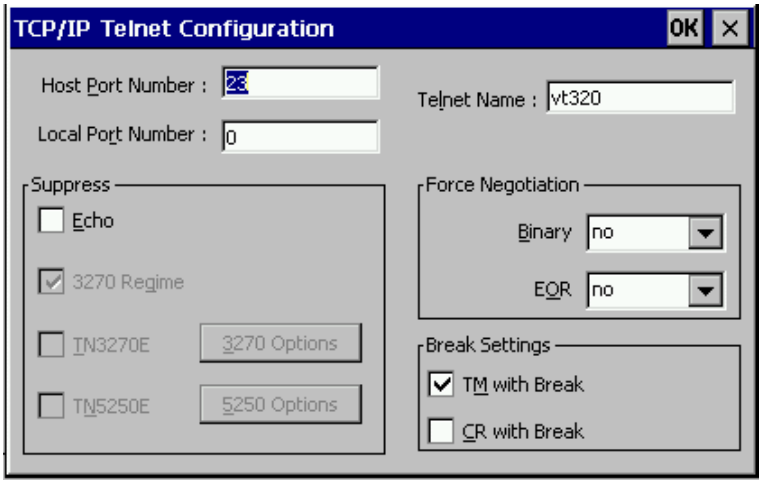
		5250 emulation.

4. After providing a name and selecting the emulation/terminal type for the connection, click **Next>** to proceed. The following dialog-box is displayed.



5. Select the **TCP/IP** radio-button from the above dialog-box and provide the name or IP address of the host in the **Host Name** field. The **Advanced** button becomes enabled. Click this button. The **TCP/IP Telnet Configuration** dialog-box is displayed.

NOTE: THE OPTIONS AND DEFAULT SETTINGS DISPLAYED IN THIS DIALOG-BOX DEPEND ON THE **EMULATION** TYPE DEFINED IN THE PREVIOUS DIALOG-BOX.



- **Host Port Number**: Provide the Telnet port number. The default value is **23**. You can specify any valid 16-bit port number. If you specify an invalid port number, this field will be set to **one**.
- **Local Port Number**: In this field, you can specify the local Telnet port number. If you want the port number to be allocated automatically, set this field to **zero**.
- **Telnet Name**: By default, the terminal type (*Example vt320*) will be displayed in this field. You can override this name.
- **Suppress**

  Echo: Select this check-box to prevent the emulation from echoing (*repeating*) keystrokes.

  3270 Regime: This field is enabled only if you select an IBM3270 type of emulation in the **Connection Information** dialog-box. Select this check-box to suppress support for the Telnet '3270 regime' option.

TN3270E: This field is enabled only if you have selected an IBM3270 type of emulation in the **Connection Information** dialog-box. Select this check-box to suppress support for the TN3270E option. If you do not suppress this option, the **3270 Options** button is enabled. With this button, you can configure 3270 options.

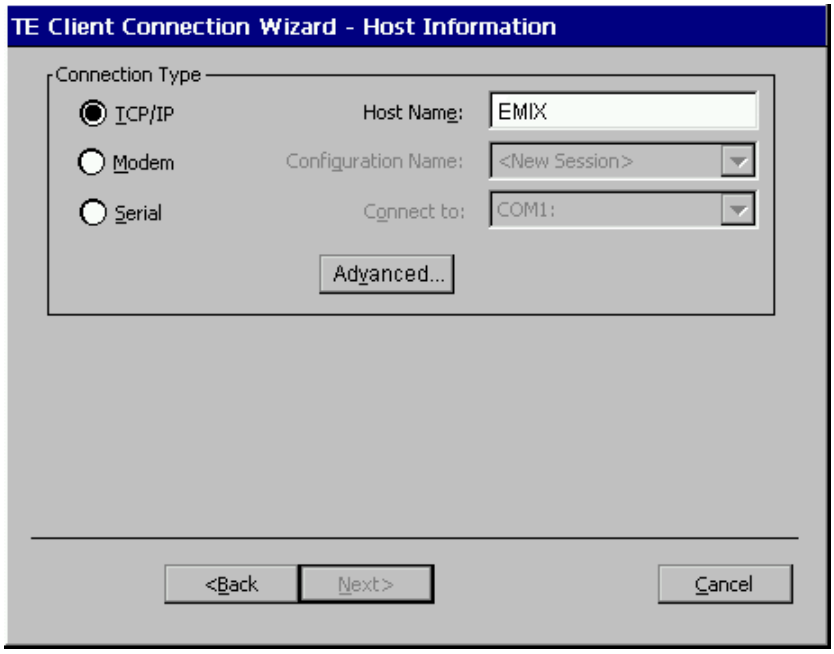
- **TN5250E**: This field is enabled only if you have selected an IBM5250 type of emulation in the **Connection Information** dialog-box. Select this check-box to suppress support for the TN5250E option. If you do not suppress this option, the **5250 Options** button is enabled. With this button, you can configure 5250 options.
- **Force Negotiation**: With these settings, you can enable or disable Telnet support for **Binary** and **EOR** (End of Record) options. The default setting for both options is **No**.

  No: This setting will not force negotiations. The host has to decide whether to support the option.

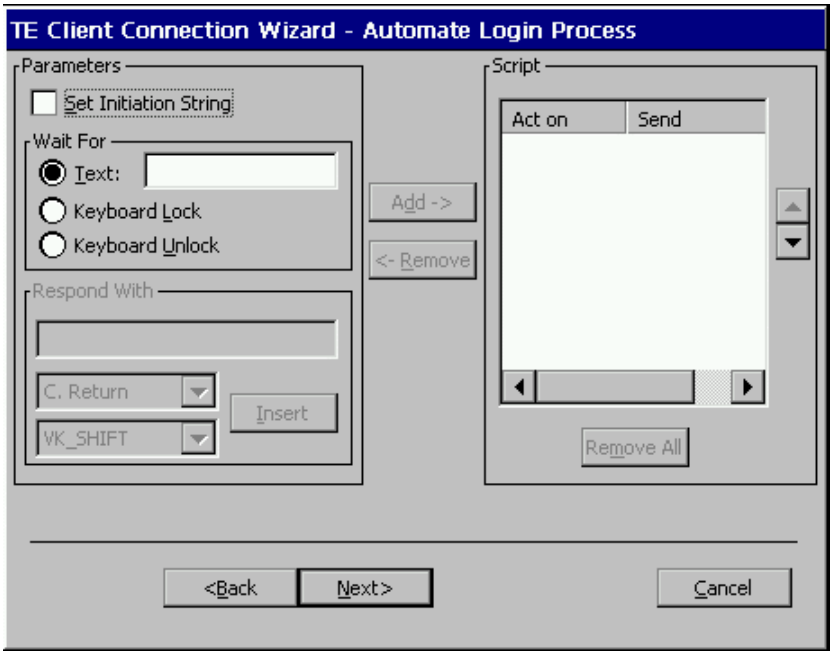
  Do: This setting will force negotiation; the host will be informed that the option is supported.

  Dont: This option will force negotiation. A negotiation packet will be sent informing the host that the option is not supported.
- **Break Settings**: With these settings you can enable or disable inclusion of a timing mark (***TM***) or carriage return (***CR***) with the Telnet break packet.

6. After configuring advanced TCP/IP settings, click **OK** to return to the **Host Information** dialog-box.



7. Click **Next>** to proceed. The following dialog-box is displayed.



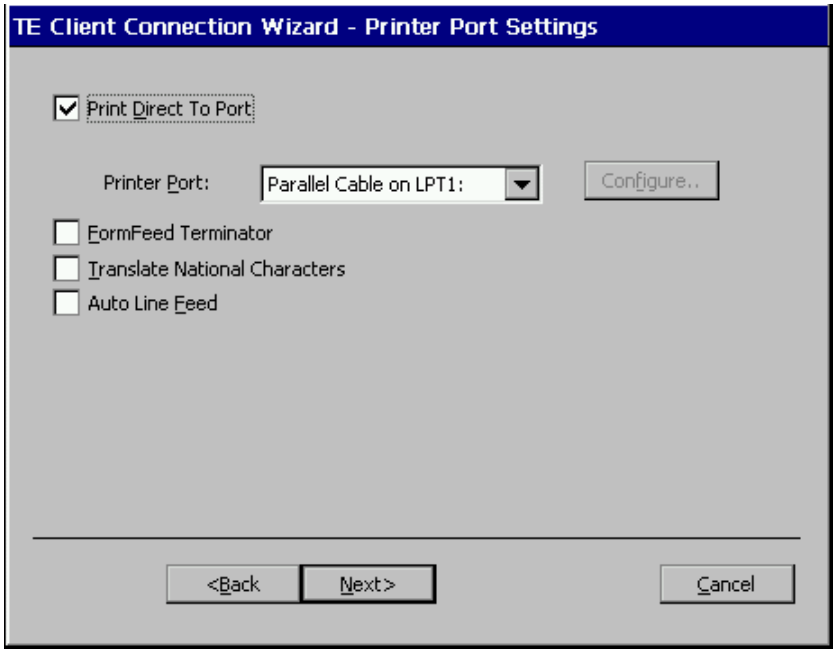
The above dialog-box allows you to automate the login process.

- **Set Initiation String**: If the host requires an initialization string when you first connect to it, select this check-box. This will enable the **Initiate With** box in place of the **Respond With** box. Provide the required characters in this field and click the **Add** button. The initialization string will be added to the **Script** window.
- **Wait For**: With the **Text** or **Keyboard Lock** or **Keyboard Unlock** radio-button, you can specify the prompt or keyboard-status command that the automatic login process has to wait for. Some systems are case sensitive; so ensure that the **Text** entry follows the correct conventions for your system.

NOTE: WHILE RUNNING IBM3270 OR IBM5250 EMULATIONS, **TEXT** ENTRIES ARE ONLY APPLICABLE IN NVT (NETWORK VIRTUAL TERMINAL) MODE.

- **Respond With**: This group of fields is enabled only when one of the **Wait For** options is specified. With these fields, you can define responses for each **Wait For** option. You can either provide the text of the response in the text field or **Insert** a pre-defined response from the two drop-down lists below the text field. After providing or inserting a response, click **Add** to include the response in the **Script** window.
- **Script**: This window lists the defined initialization and response strings. The actions will be performed in the order in which they appear in this window. You can use the **up** and **down** arrow buttons adjacent to this window to change the order of actions.
- **Remove** / **Remove All**: With these buttons, you can remove selected or all entries from the **Script** window.

8. After configuring the above parameters, click **Next>** to proceed. The following dialog-box is displayed.

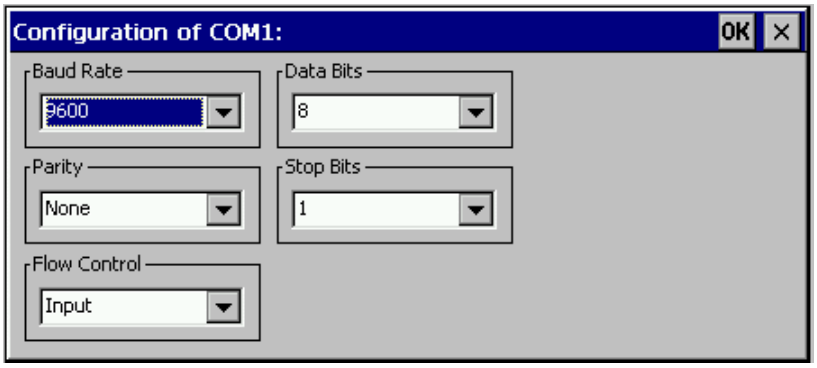


9. In the above dialog-box, you can configure your printer port.

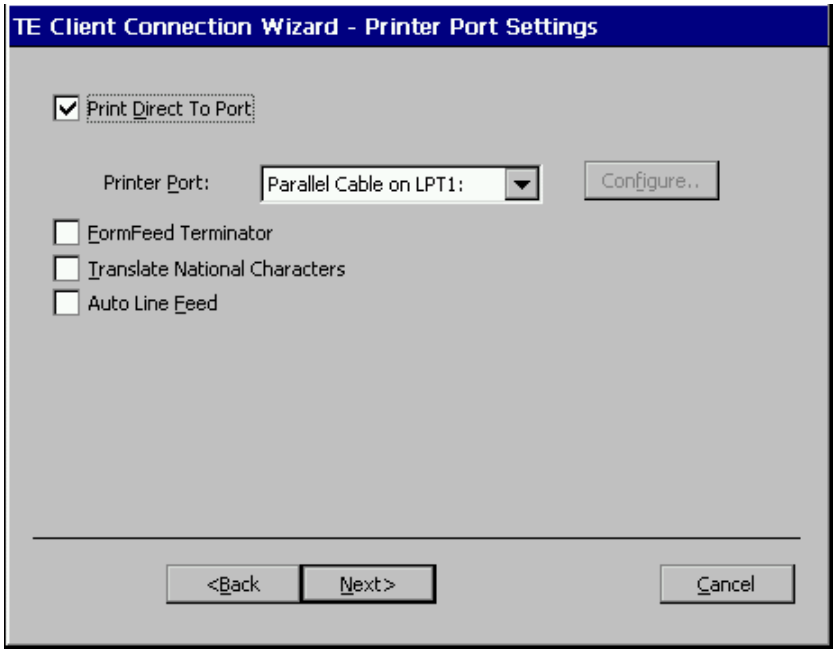
   Print Direct to Port: This check-box is selected by default indicating that a print-job fired from the emulation session will be sent directly to the printer-port of the client, bypassing the print manager (*overriding jobs in the print-queue*). This option is necessary when the host application sends control information (*for instance, 'escape' sequences sent in Print Controller and Autoprint modes in VT emulation*), which would be lost if the print-job is routed through the print manager. This option can be used when the printer-port of the client is dedicated to terminal emulation sessions.

   If on the other hand, the printer-port of the client is to be used for printing from RDP and ICA sessions as well, it is recommended that the **Print Direct to Port** check-box be deselected. In such cases, the only way to print from the emulation session is to configure the client as a print-server using LPD (*page 35*) and configure the UNIX server for LPD printing (*page 166*).

10. Select the appropriate printer port from the **Printer Port** drop-down list. If you select one of the serial (COM) ports as the printer port, the **Configure..** button is enabled. Click this button. The following dialog-box is displayed.

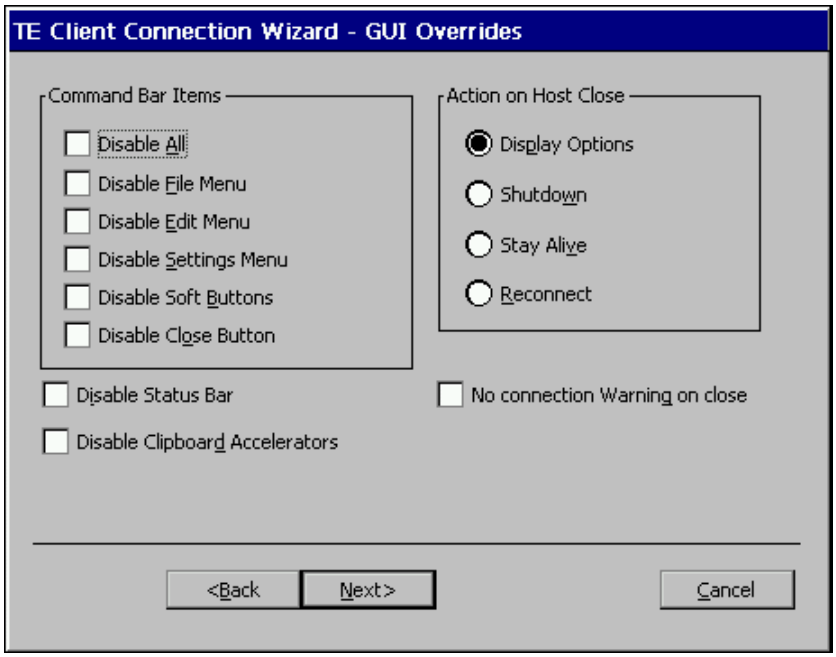


11. Configure settings (*Baud Rate, Parity, Flow Control, Data Bits and Stop Bits*) for the COM port and click **OK** to return to the **Printer Port Settings** dialog-box.



- **orm Feed Terminator**: Select this check-box if you want the printer to advance paper to the top of the next form when it has finished printing.
- **Translate National Characters**: This option determines whether ISO Latin characters used by Microsoft Windows, and Roman 8 characters used in HP mode are to be translated to IBM characters.
- **Auto Line Feed**: Select this check-box if you want the printer to start at the beginning of the next line when a carriage return command is received.

12. After configuring the above parameters, click **Next>**. The following dialog-box is displayed.



The options in the above dialog-box allow you to disable user access to settings that must not be changed. It also allows you to specify an emulator response when the connection is closed.

- **Command Bar Items**: Select appropriate options from this group of check-boxes to disable menus on the command-bar of the terminal emulation window.
- **Disable Status Bar**: Select this check-box to disable the status bar.

- **Disable Clipboard Accelerators**: Select this check-box to disable use of **Ctrl+C** and **Ctrl+V** shortcuts to 'copy to' and 'paste from' the clipboard while in the terminal emulation session.

  This feature is useful in certain emulations where Ctrl+C and Ctrl+V are used to send specific commands to the terminal. Besides, you *must* select this option if you plan to create keyboard macros for Ctrl+C and Ctrl+V using the **Settings->Keyboard Macros…** option of the terminal emulation screen. Even when the Ctrl+C and Ctrl+V shortcuts are disabled, you can use the **Edit->Copy** and **Edit->Paste** options of the terminal emulation screen for copying and pasting.

- **Action on Host Close**: Select one of these radio-buttons to specify a response when the connection is closed.

  Display Options: Select this radio-button if you want a dialog-box to be displayed with Shutdown, Stay Alive and Reconnect options.

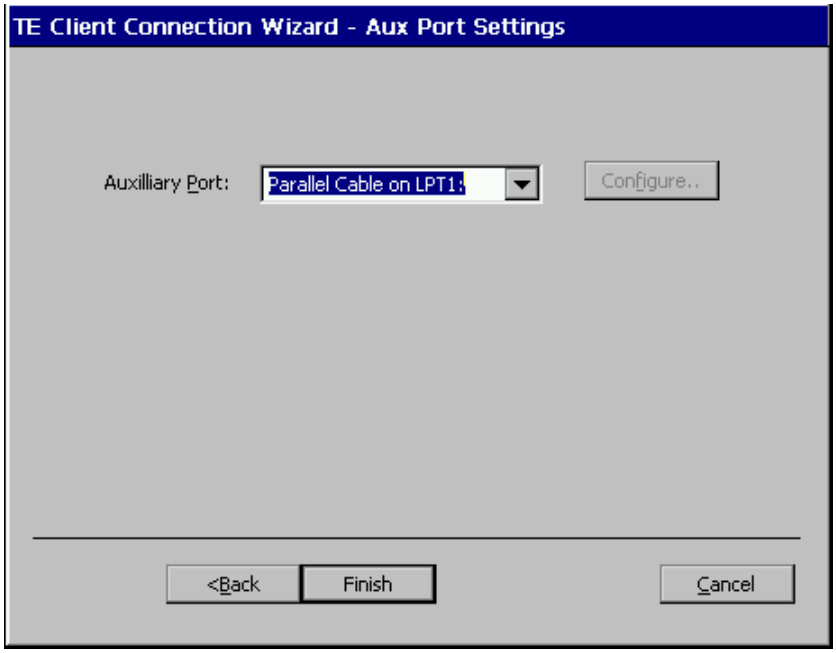
  Shutdown: Select this radio-button if you want the emulation to close down.

  Stay Alive: Select this radio-button if you want to keep the emulation running.

  Reconnect: Select this radio-button if you want the emulation to attempt to reconnect to the host.

- **No Connection warning on close**: By default, the client will display a warning message if you attempt to exit the emulation while a host connection is active. You can disable the warning message by selecting this check-box.

13. Select the appropriate GUI overrides and click **Next>**. The following dialog-box is displayed.

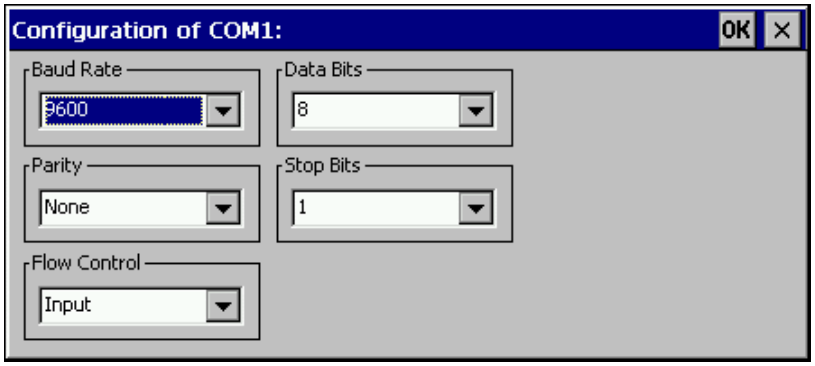


14. In the above dialog-box, you can specify a port through which external devices that require bi-directional flow of data can send data for further processing.

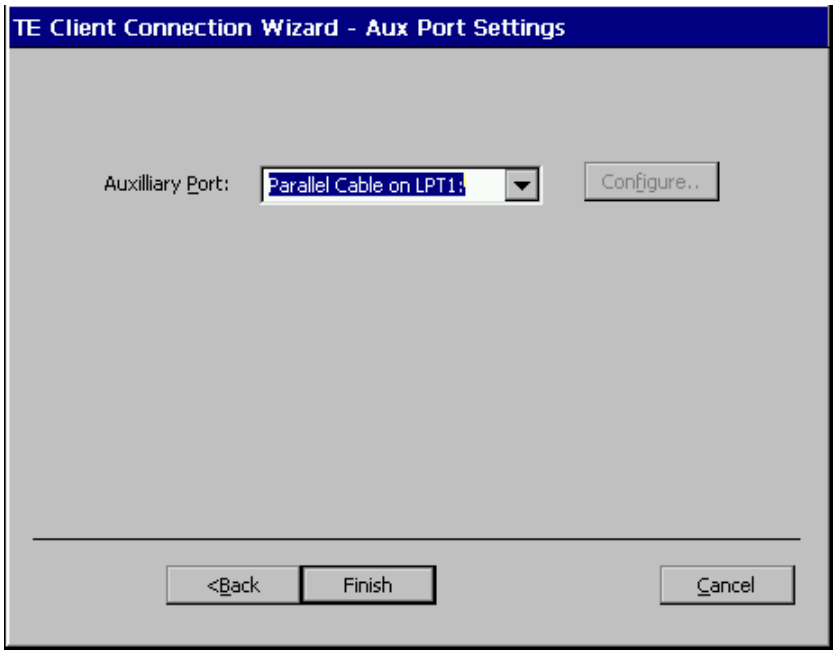
    For instance, the server pertaining to the Terminal Emulation connection may have an application that requires input from a serial device (say, a bar-code reader). In such a case, you can connect the bar-code reader to a COM port and specify that port as the auxiliary port.

NOTE: YOU MUST NOT SPECIFY THE SAME PORT AS BOTH PRINTER-PORT AS WELL AS AUXILIARY-PORT.

If you select a COM port, the **Configure..** button is enabled. Click this button. The following dialog-box is displayed.



15. Configure settings (*Baud Rate, Parity, Flow Control, Data Bits and Stop Bits*) for the COM port and click **OK** to return to the **Aux Port Settings** dialog-box.



16. Click **Finish**. The name of the connection you created will be added to the list of connections displayed in the **Terminal Connection Manager** window.

To start the connection, double-click on it, or highlight it and click the **Connect** button in the **Terminal Connection Manager**

Creating Dial-up Terminal Emulation Connections

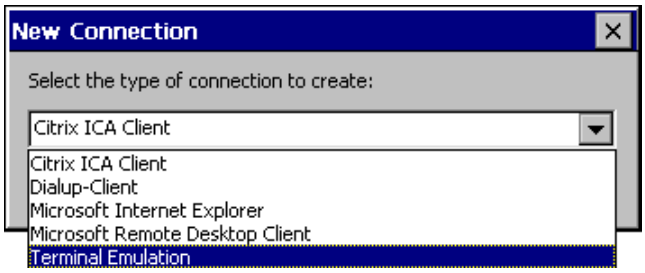
TIP: DETAILED INFORMATION ABOUT TERMINAL EMULATION SETTINGS IS PROVIDED IN THE ***PERICOM Windows CE Emulation User's Guide***, WHICH IS AVAILABLE IN THE CD SUPPLIED WITH THE PRODUCT.

This section describes the procedure to create a Terminal Emulation connection through a modem connected to one of the COM ports of the client.

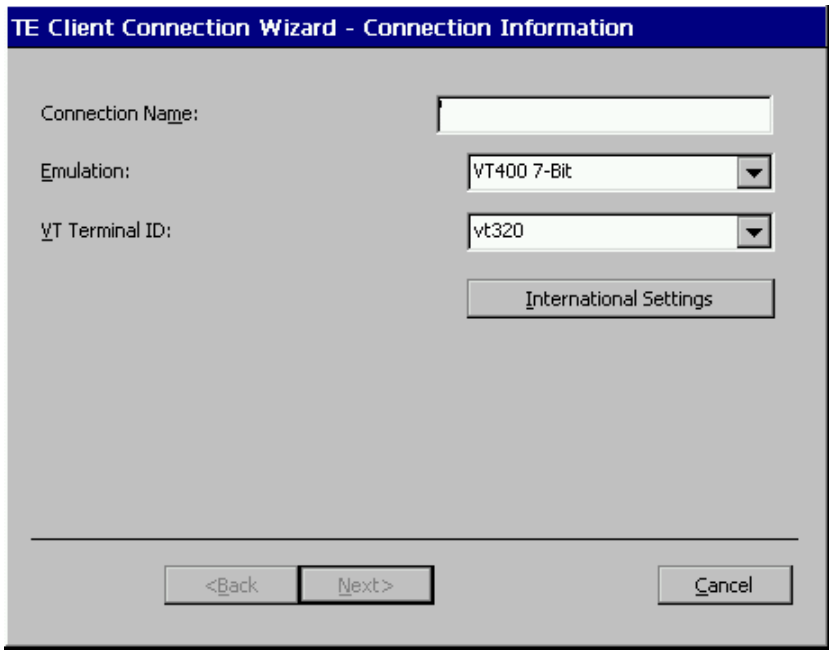
1. Select the **Configure** sheet of the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Click **Add…**. The **New Connection** dialog-box is displayed.



3. Select **Terminal Emulation** from the drop-down list and click **OK**. The first dialog-box of the **TE Client Connection Wizard** is displayed.



- **Connection Name**: Provide a name for the new connection. The connection-name can consist of a maximum of 42 characters (*including special characters*).
- **Emulation**: From this drop-down list, select the type of emulation. If you select **IBM3270** or **IBM5250** emulation-types, a few other options (*as mentioned in column-3 of the table on the following page*) will be displayed.
- **International Settings**: If you click this button, the **National Replacement Character** dialog-box is displayed. With this dialog-box you can configure the keyboard language, character set mode and other settings for the Terminal Emulation connection.

The contents of this dialog-box vary depending on the **Emulation**-type selected.

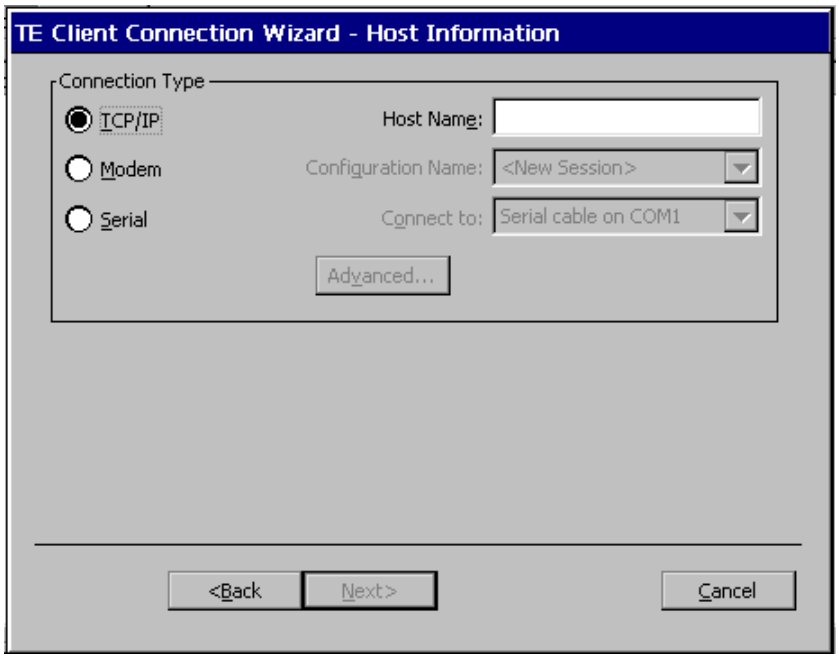
Additional information is available in the *PERICOM Windows CE Emulation User's Guide*, which is in the CD supplied with the thin client. *Keyboard language settings are described in the **Emulation Settings** chapter on page 68 of the Emulation User's Guide. Character-set tables are available in pages 159-189 of the Emulation User's Guide*.

- **VT Terminal ID**: The name of this field will depend on the **Emulation-**type that is selected. Since the default emulation-type is **VT300 7-Bit**, the default name for this field will be **VT Terminal ID**. From this drop-down list, select the type of the terminal.

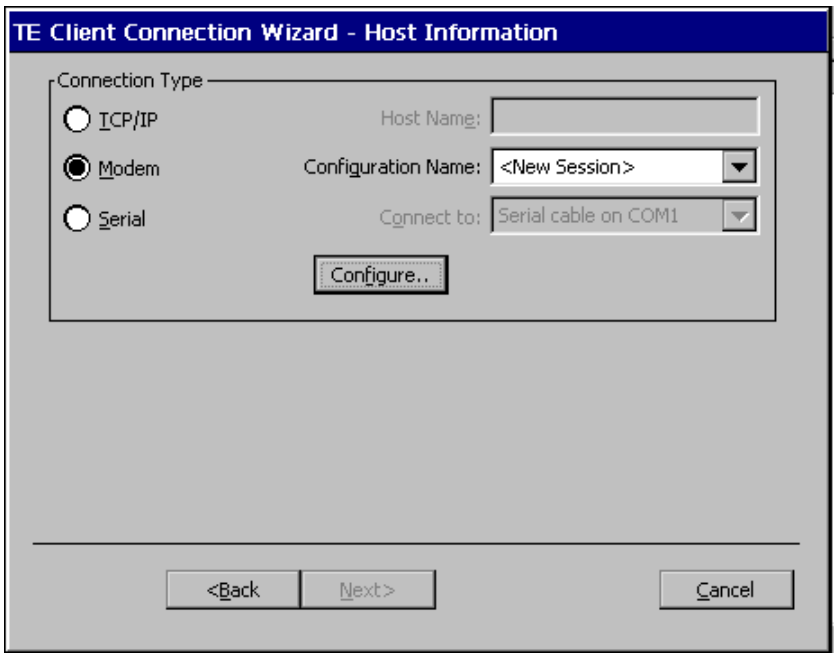
The following table contains the emulation and terminal types supported by the client.

Select one of the following from the **Emulation** *drop-down list.*	*Then…*		*And define other options (if any)*
Column-1	***Column-2***		***Column-3***
VT52, VT100, VT300 7-Bit (*default*) or VT300 8-Bit	Select one of the following from the **VT Terminal ID** drop-down list.	Vt100, vt101, vt102, vt125, vt220, vt240, vt320 (*default*), vt340, vt420, vt131 or vt132	
ANSI BBS, SCO Console, WY50, WY50+, WY60, TV1910, TV1920, TV1925, ADDS A2, or HZ1500			
IBM3151	Select one of the following from the **IBM 3151 Model** drop-down list.	11 (*default*) or 31	
IBM3270	Select one of the following from the **IBM 3270 Model** drop-down list.	3278-2, 3278-3, 3278-4, 3278-5, 3278-2-E (*default*), 3278-3-E, 3278-4-E, 3278-5-E, 3279-2, 3279-3, 3279-4, 3279-5 or 3287-1	Select the **Right Ctrl Acts as Enter Key** or the **Left Ctrl Acts as Reset Key** check-boxes if you want to enable these functions for 3270 emulation.
IBM5250	Select one of the following from the **IBM 5250 Model** drop-down list.	5291-1, 5292-2, 5251-11, 3179-2, 3196-A1, 3180-2, 3477-FC, 3477-FG, 3486-BA, 3487-HA or 3487-HC	Select the **Right Ctrl Acts as Enter Key**, **Left Ctrl Acts as Reset Key**, or **IBM5250 Monochrome** check-boxes if you want to enable these functions for 5250 emulation.

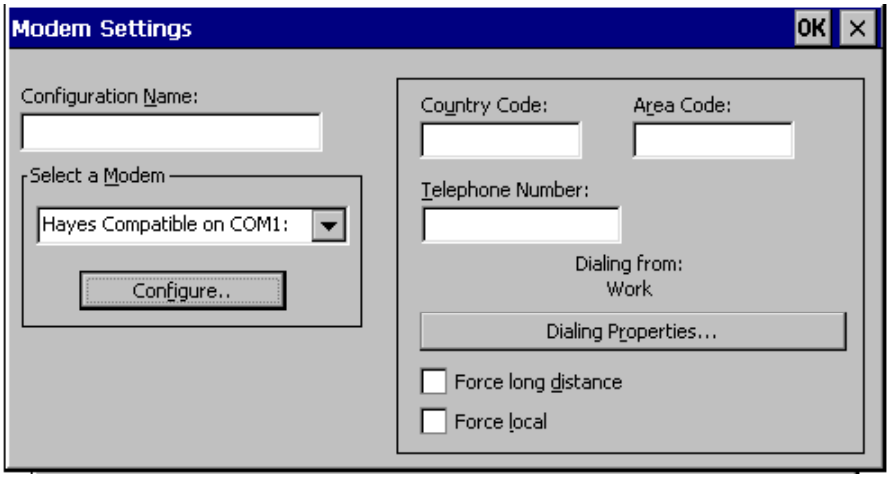
4. After providing a name and selecting the emulation/terminal type for the connection, click **Next>** to proceed. The following dialog-box is displayed.



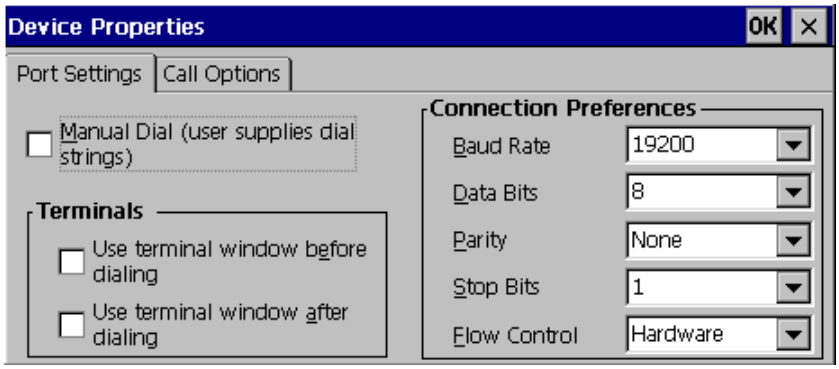
5. Select the **Modem** radio-button. The dialog-box changes as shown below.



6. Click **Configure…**. The following dialog-box is displayed.



7. Specify a name for the connection, in the **Configuration Name** text field, select a modem from the **Select a Modem** drop-down list and click **Configure**. The following dialog-box is displayed.



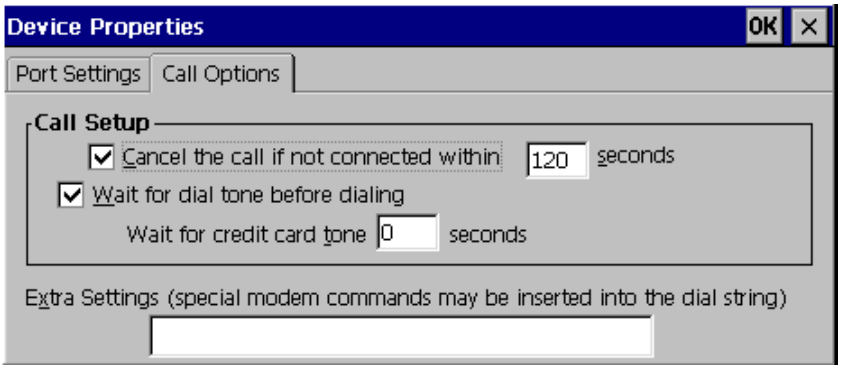
The above dialog-box has two tabs. The **Port Settings** tab is selected by default.

- **Manual Dial**: Select this check-box if you want to provide dial strings while attempting a dial-up connection.

NOTE: MANUAL DIALING IS NOT CURRENTLY SUPPORTED.

- **Use terminal window before dialing**: If you select this check-box, the terminal window is displayed *before* the connection is established.
- **Use terminal window after dialing**: If you select this check-box, the terminal window is displayed *after* the connection is established, prompting you for logon information.
- **Connection Preferences**: In this group of drop-down lists, select the settings for Baud Rate, Data Bits, Parity, Stop Bits and Flow Control.

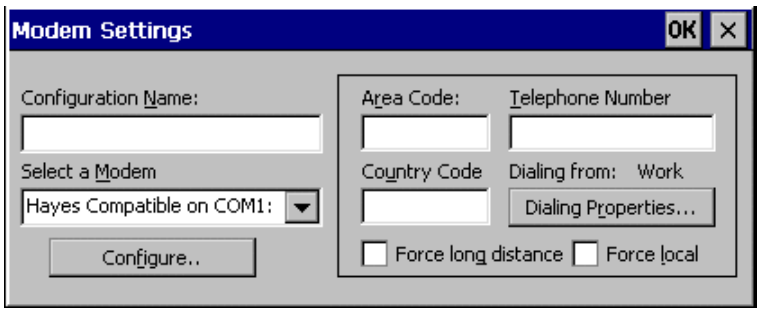
8. After configuring port settings, select the **Call Options** tab.



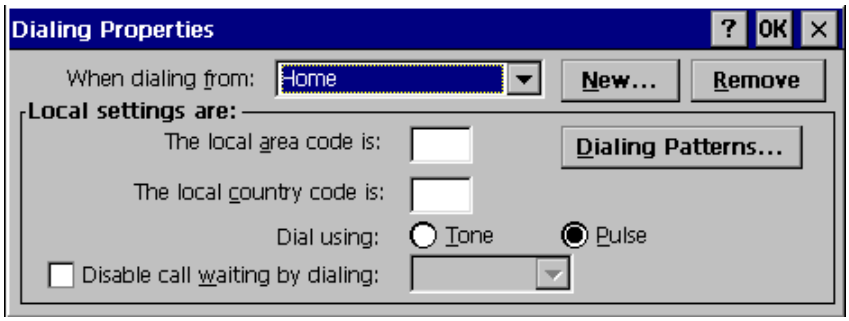
- **Cancel the call if not connected within … seconds**: If you want the call to be cancelled if it does not connect within a specified time limit, select this check-box and specify the duration.
- **Wait for dial tone before dialing**: Select this check-box if the dial-in device has to wait for a dial tone before dialing.
- **Wait for credit card tone**… **seconds**: Specify the duration for which the terminal has to wait for a credit card tone.
- **Extra Settings**: In this text field, you can provide special modem commands.

NOTE: IF YOU PROVIDE INPUT IN THIS FIELD, YOU **MUST** ALSO SELECT THE **MANUAL DIAL** CHECK-BOX IN THE **PORT SETTINGS** TAB.

9. After configuring call options, click **OK** to return to the **Modem Settings** dialog-box.

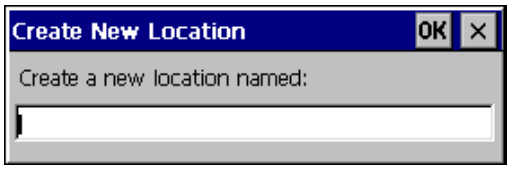


10. Click **Dialing Properties**. The following dialog-box is displayed.



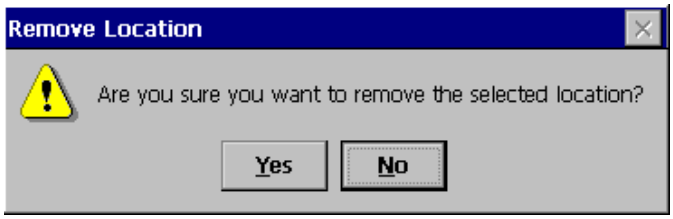
In the above dialog-box, you can create, delete and configure dialing locations.

- To create a **location**, click **New…**. The following dialog-box is displayed.



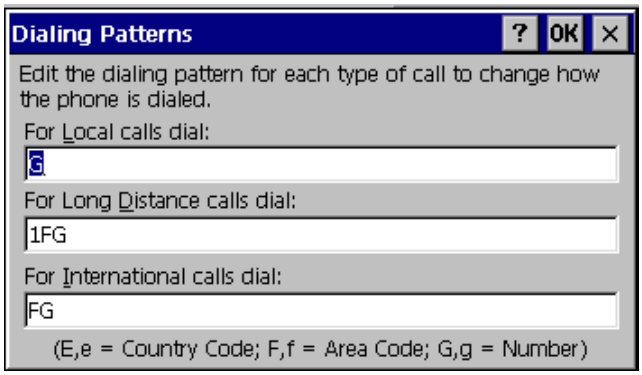
Provide a name for the new location and click **OK**.

- To remove a location click **Remove**. The following prompt is displayed.



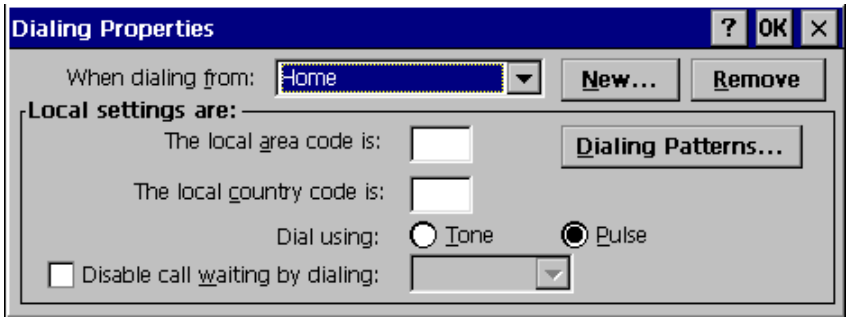
Click **Yes** to confirm deletion.

- You can configure dialing properties using the **Local Settings are…** group of fields. Provide the area code and country code and select a dial mode (***Tone*** *or* ***Pulse***). If you want to disable the 'call waiting' feature, select the **Disable call waiting by dialing** and either select from the options in the drop-down list or specify a new number.
- To edit dialing prefixes, click the **Dialing Patterns…** button. The following dialog-box is displayed.

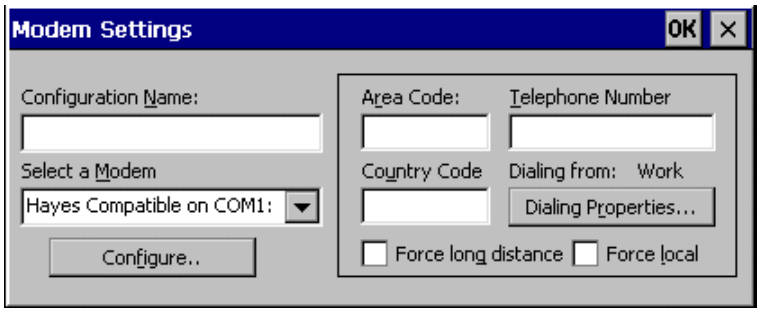


Enter appropriate dialing patterns for each local, long distance and international calls. Specify the dialing sequence by either entering a number-sequence or using the prefix-codes listed at the bottom of the dialog-box.

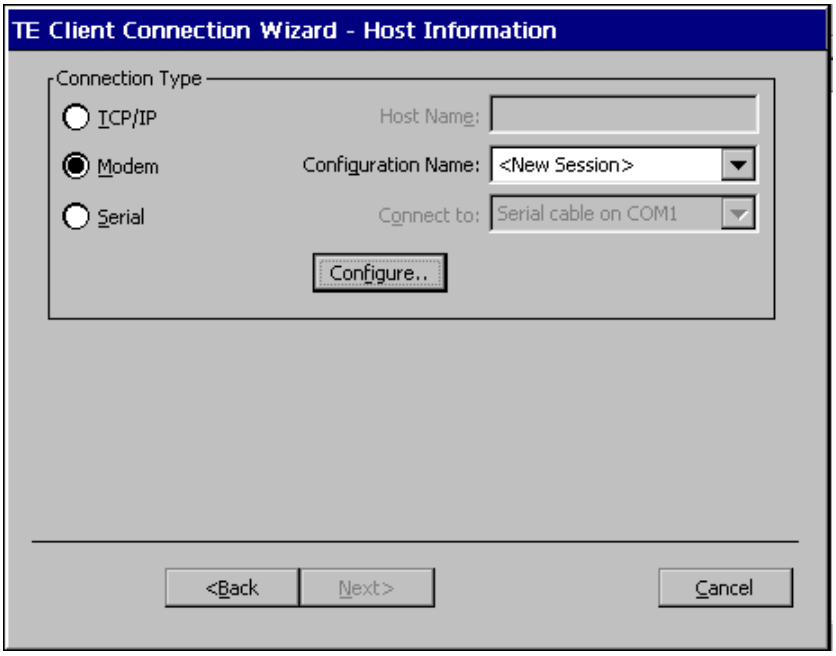
Click **OK** to return to the **Dialing Properties** dialog-box.



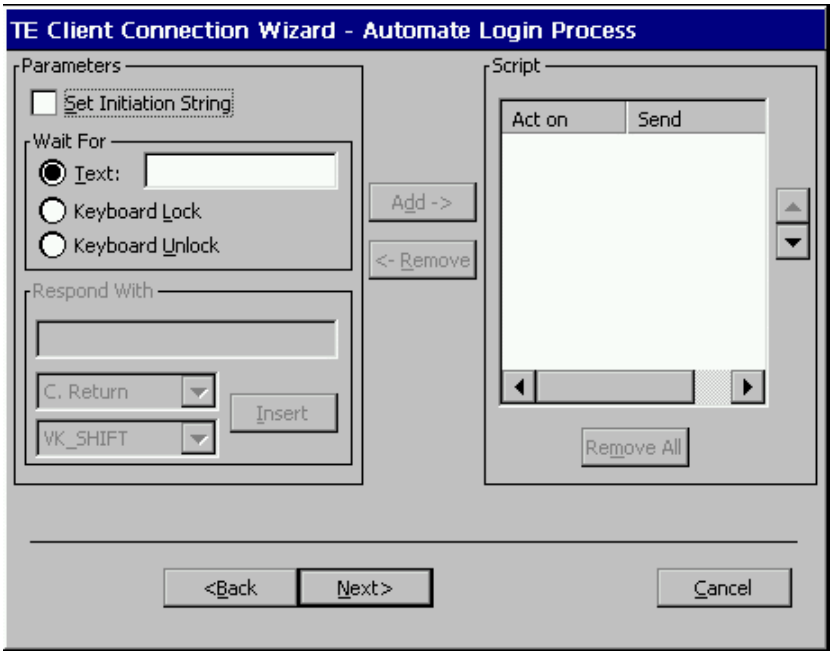
11. After configuring dialing properties, click **OK** to return to the **Modem Settings** dialog-box.



12. Provide the **Area Code**, **Telephone Number** and **Country Code**, select the **Force long distance** and **Force local** check-boxes if necessary, and click **OK** to return to the **TE Client Connection Wizard**.



13. Click the **Next** button to proceed. The following dialog-box is displayed.



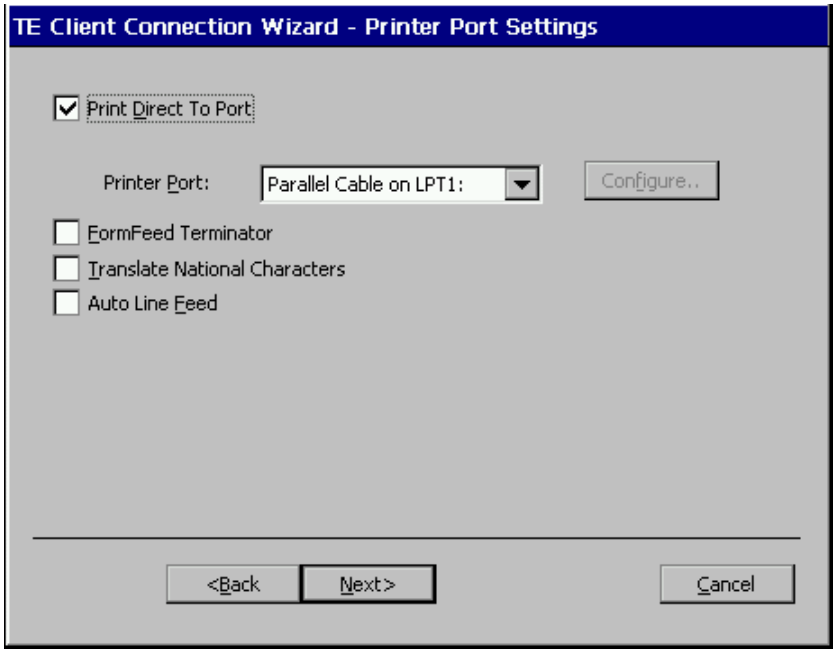
The above dialog-box allows you to partially/fully automate the login process.

- **Set Initiation String**: If the host requires an initialization string when you first connect to it, select this check-box. This will enable the **Initiate With** box in place of the **Respond With** box. Provide the required characters in this field and click the **Add** button. The initialization string will be added to the **Script** window.
- **Wait For**: With the **Text** or **Keyboard Lock** or **Keyboard Unlock** radio-button, you can specify the prompt or keyboard-status command that the automatic login process has to wait for. Some systems are case sensitive; so ensure that the **Text** entry follows the correct conventions for your system.

NOTE: WHILE RUNNING IBM3270 OR IBM5250 EMULATIONS, **TEXT** ENTRIES ARE ONLY APPLICABLE IN NVT (NETWORK VIRTUAL TERMINAL) MODE.

- **Respond With**: This group of fields is enabled only when one of the **Wait For** options is specified. With these fields, you can define responses for each **Wait For** option. You can either provide the text of the response in the text field or **Insert** a pre-defined response from the two drop-down lists below the text field. After providing or inserting a response, click **Add** to include the response in the **Script** window.
- **Script**: This window lists the defined initialization and response strings. The actions will be performed in the order in which they appear in this window. You can use the **up** and **down** arrow buttons adjacent to this window to change the order of actions.
- **Remove** / **Remove All**: With these buttons, you can remove selected or all entries from the **Script** window.

14. After configuring the above parameters, click **Next>** to proceed. The following dialog-box is displayed.

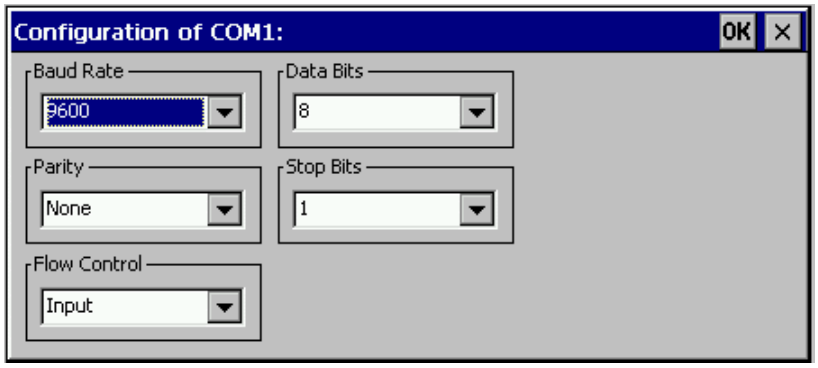


15. In the above dialog-box, you can configure your printer port.

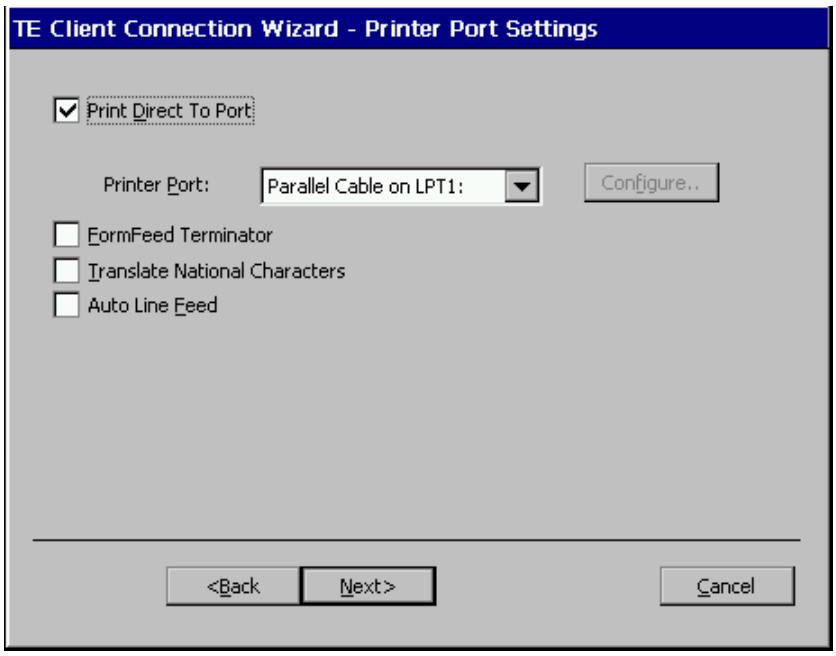
    Print Direct to Port: This check-box is selected by default indicating that a print-job fired from the emulation session will be sent directly to the printer-port of the client, bypassing the print manager (*overriding jobs in the print-queue*). This option is necessary when the host application sends control information (*for instance, 'escape' sequences sent in Print Controller and Autoprint modes in VT emulation*), which would be lost if the print-job is routed through the print manager. This option can be used when the printer-port of the client is dedicated to terminal emulation sessions.

    If on the other hand, the printer-port of the client is to be used for printing from RDP and ICA sessions as well, it is recommended that the **Print Direct to Port** check-box be deselected. In such cases, the only way to print from the emulation session is to configure the client as a print-server using LPD (*page35*) and configure the UNIX server for LPD printing (*page 166*).

16. Select the appropriate printer port from the **Printer Port** drop-down list. If you select one of the COM ports, the **Configure** button is enabled. Click this button. The following dialog-box is displayed.

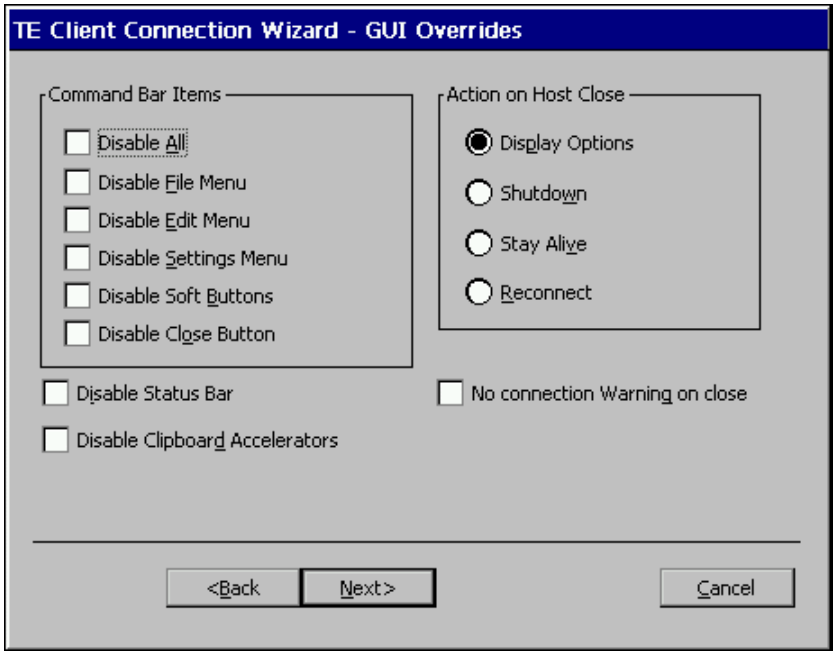


17. Configure settings (*Baud Rate, Parity, Flow Control, Data Bits and Stop Bits*) for the COM port and click **OK** to return to the **Printer Port Settings** dialog-box.



- **orm Feed Terminator**: Select this check-box if you want the printer to advance paper to the top of the form when it has finished printing.
- **Translate National Characters**: This option determines whether ISO Latin characters used by Microsoft Windows, or Roman 8 characters used in HP mode, are to be translated to IBM characters.
- **Auto Line Feed**: Select this check-box if you want the printer to start at the beginning of the next line when a carriage return command is received.

18. After configuring the above parameters, click **Next>**. The following dialog-box is displayed.



The options in the above dialog-box allow you to disable user access to settings that must not be changed. It also allows you to specify an emulator response when the connection is closed.

- **Command Bar Items**: Select appropriate options from this group of check-boxes to disable menus on the command-bar of the terminal emulation window.
- **Disable Status Bar**: Select this check-box to disable the status bar.
- **Disable Clipboard Accelerators**: Select this check-box to disable use of **Ctrl+C** and **Ctrl+V** shortcuts to copy to and paste from the clipboard while in the terminal emulation session.

  This feature is useful in certain emulations where Ctrl+C and Ctrl+V are used to send specific commands to the terminal. Besides, you must select this option if you plan to create keyboard macros for Ctrl+C and Ctrl+V using the **Settings->Keyboard Macros…** option of the terminal emulation screen. Even when the Ctrl+C and Ctrl+V shortcuts are disabled, you can use the **Edit->Copy** and **Edit->Paste** options of the terminal emulation screen for copying and pasting.
- **Action on Host Close**: Select one of these radio-buttons to specify a response when the connection is closed.

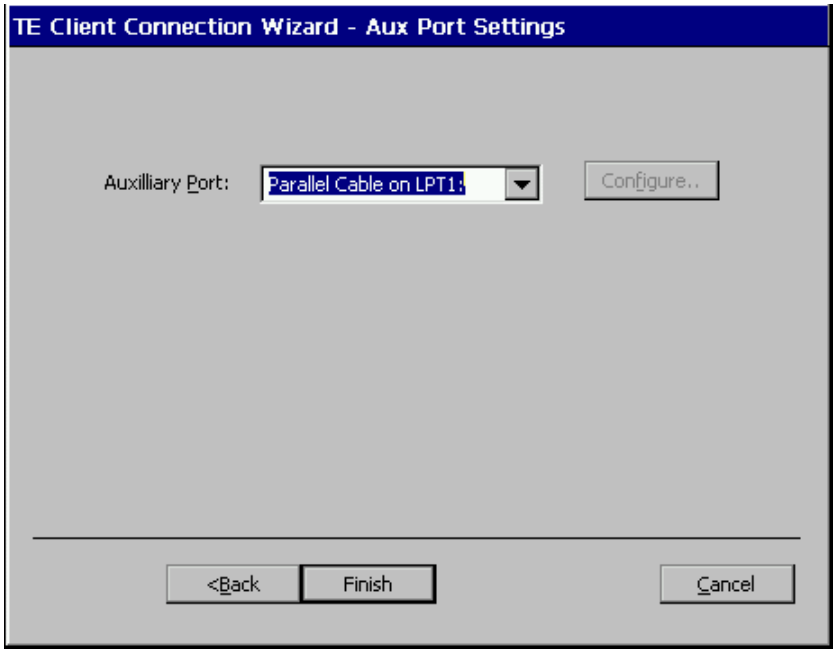
  Display Options: Select this radio-button if you want a dialog-box to be displayed with Shutdown, Stay Alive and Reconnect options.

  Shutdown: Select this radio-button if you want the emulation to close down.

  Stay Alive: Select this radio-button if you want to keep the emulation running.

  Reconnect: Select this radio-button if you want the emulation to attempt to reconnect to the host.
- **No Connection warning on close**: By default, the client will display a warning message if you attempt to exit the emulator while a host connection is active. You can disable the warning message by selecting this check-box.

19. Select the appropriate GUI overrides and click **Next>**. The following dialog-box is displayed.

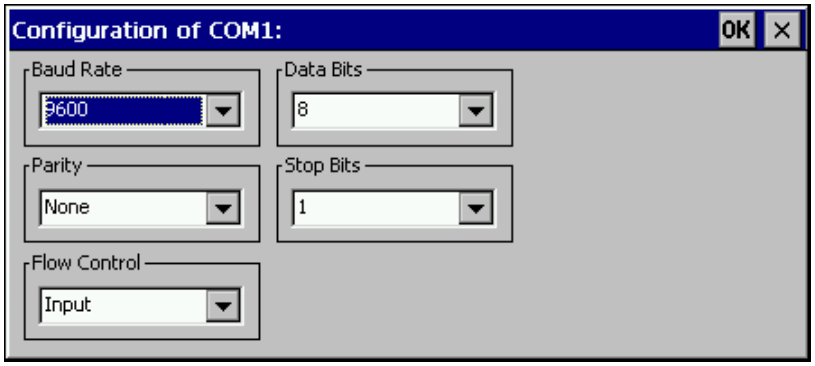


20. In the above dialog-box, you can specify a port through which external devices that require bi-directional flow of data can send data for further processing.

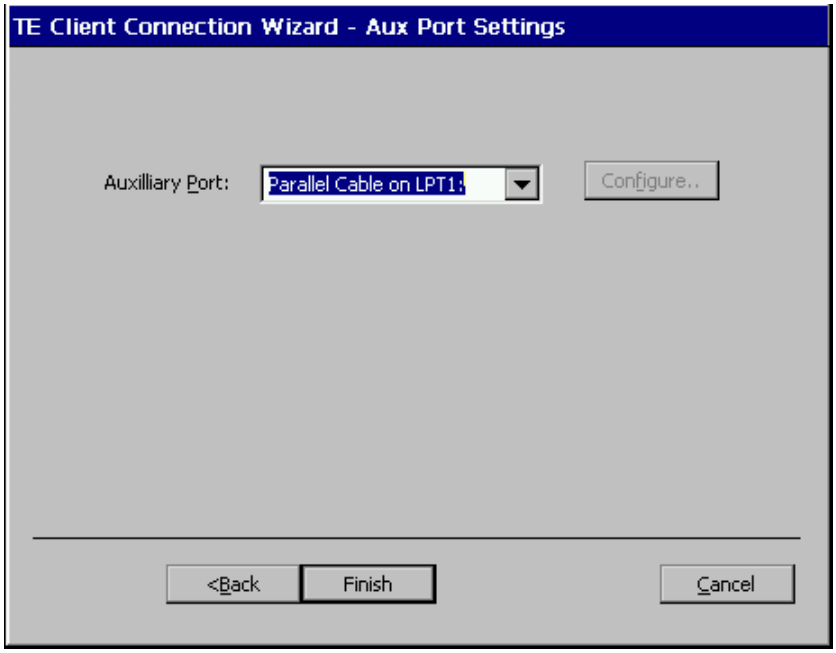
    For instance, the server pertaining to the Terminal Emulation connection may have an application that requires input from a serial device (say, a bar-code reader). In such a case, you can connect the bar-code reader to a COM port and specify that port as the auxiliary port.

NOTE: YOU MUST NOT SPECIFY THE SAME PORT AS BOTH PRINTER-PORT AS WELL AS AUXILIARY-PORT.

21. If you select a COM port, the **Configure..** button is enabled. Click this button. The following dialog-box is displayed.



22. Configure settings (*Baud Rate, Parity, Flow Control, Data Bits and Stop Bits*) for the COM port and click **OK** to return to the **Aux Port Settings** dialog-box.



23. Click **Finish**. The name of the connection you created will be added to the list of connections displayed in the **Terminal Connection Manager** window.

To start the connection, double-click on it, or highlight it and click the **Connect** button in the **Terminal Connection Manager**.

Creating Serial-Line Terminal Emulation Connections

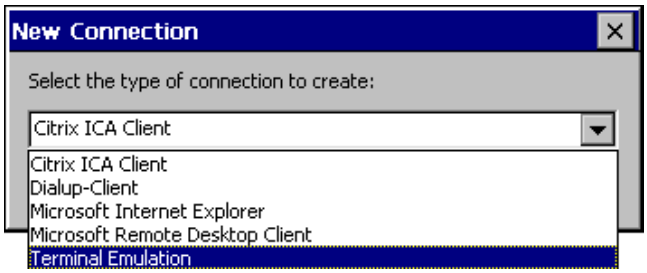
TIP: DETAILED INFORMATION ABOUT TERMINAL EMULATION SETTINGS IS PROVIDED IN THE ***PERICOM Windows CE Emulation User's Guide***, WHICH IS AVAILABLE IN THE CD SUPPLIED WITH THE PRODUCT.

This section describes the procedure to create a Terminal Emulation connection through a serial cable connected to one of the COM ports of the client.

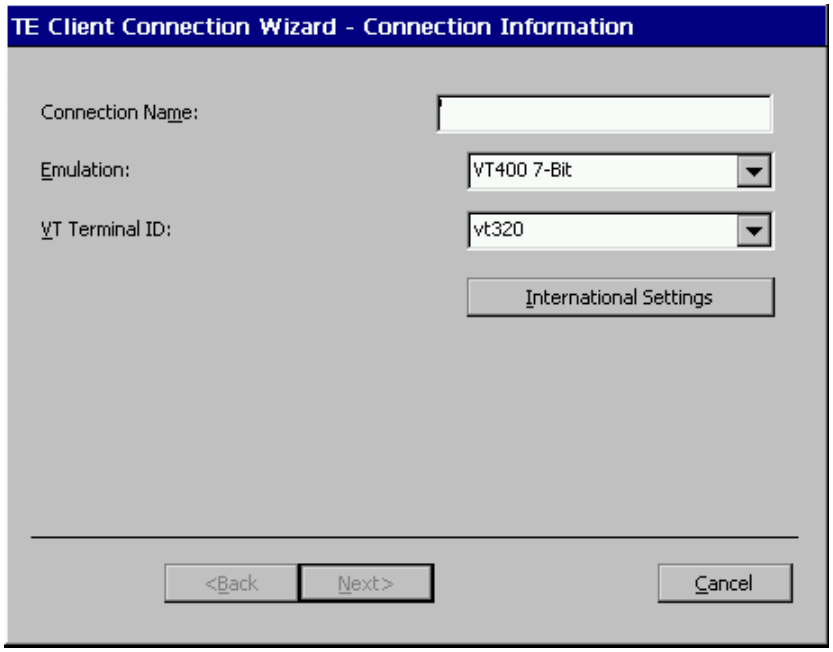
1. Select the **Configure** sheet of the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Click **Add…**. The **New Connection** dialog-box is displayed.



3. Select **Terminal Emulation** from the drop-down list and click **OK**. The first dialog-box of the **TE Client Connection Wizard** is displayed.



- **Connection Name**: Provide a name for the new connection. The connection-name can consist of a maximum of 42 characters (*including special characters*).
- **Emulation**: From this drop-down list, select the type of emulation. If you select **IBM3270** or **IBM5250** emulation-types, a few other options (*as mentioned in column-3 of the table on the following page*) will be displayed.
- **International Settings**: If you click this button, the **National Replacement Character** dialog-box is displayed. With this dialog-box you can configure the keyboard language, character set mode and other settings for the Terminal Emulation connection.

- The contents of this dialog-box vary depending on the **Emulation**-type selected.

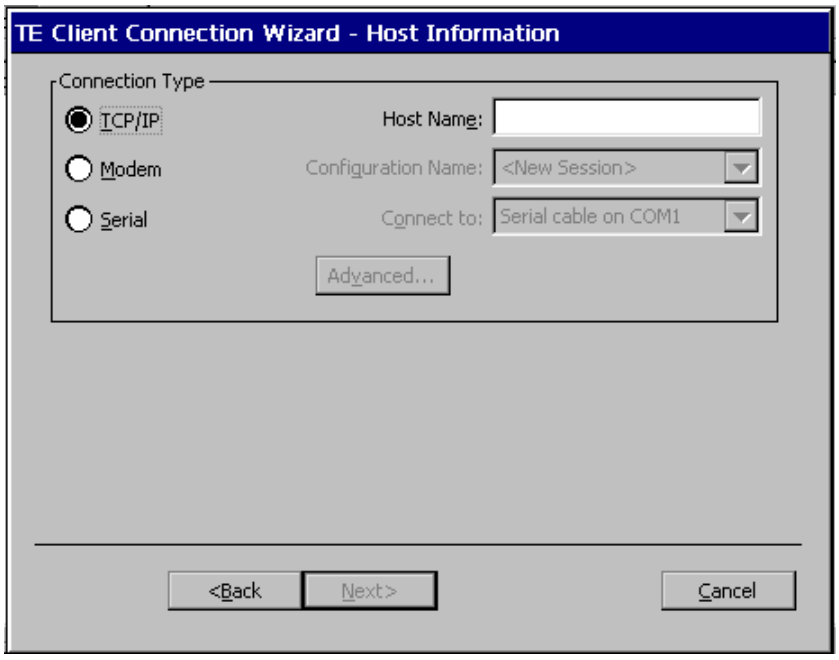
  Additional information is available in the *PERICOM Windows CE Emulation User's Guide*, which is in the CD supplied with the thin client. *Keyboard language settings are described in the **Emulation Settings** chapter on page 68 of the Emulation User's Guide. Character-set tables are available in pages 159-189 of the Emulation User's Guide*.

- **VT Terminal ID**: The name of this field will depend on the **Emulation-**type that is selected. Since the default emulation-type is **VT300 7-Bit**, the default name for this field is **VT Terminal ID**. From this drop-down list, select the type of the terminal.

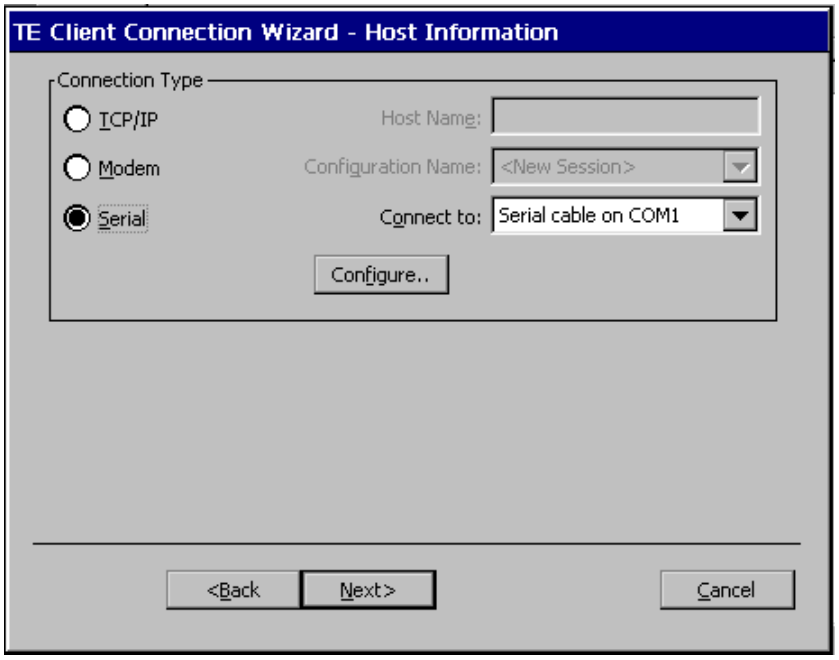
The following table contains the emulation and terminal types supported by the client.

Select one of the following from the **Emulation** *drop-down list.*	*Then…*		*And define other options (if any)*
Column-1	***Column-2***		***Column-3***
VT52, VT100, VT300 7-Bit (*default*) or VT300 8-Bit	Select one of the following from the **VT Terminal ID** drop-down list.	Vt100, vt101, vt102, vt125, vt220, vt240, vt320 (*default*), vt340, vt420, vt131 or vt132	
ANSI BBS, SCO Console, WY50, WY50+, WY60, TV1910, TV1920, TV1925, ADDS A2, or HZ1500			
IBM3151	Select one of the following from the **IBM 3151 Model** drop-down list.	11 (*default*) or 31	
IBM3270	Select one of the following from the **IBM 3270 Model** drop-down list.	3278-2, 3278-3, 3278-4, 3278-5, 3278-2-E (*default*), 3278-3-E, 3278-4-E, 3278-5-E, 3279-2, 3279-3, 3279-4, 3279-5 or 3287-1	Select the **Right Ctrl Acts as Enter Key** or the **Left Ctrl Acts as Reset Key** check-boxes if you want to enable these functions for 3270 emulation.
IBM5250	Select one of the following from the **IBM 5250 Model** drop-down list.	5291-1, 5292-2, 5251-11, 3179-2, 3196-A1, 3180-2, 3477-FC, 3477-FG, 3486-BA, 3487-HA or 3487-HC	Select the **Right Ctrl Acts as Enter Key**, **Left Ctrl Acts as Reset Key**, or **IBM5250 Monochrome** check-boxes if you want to enable these functions for 5250 emulation.

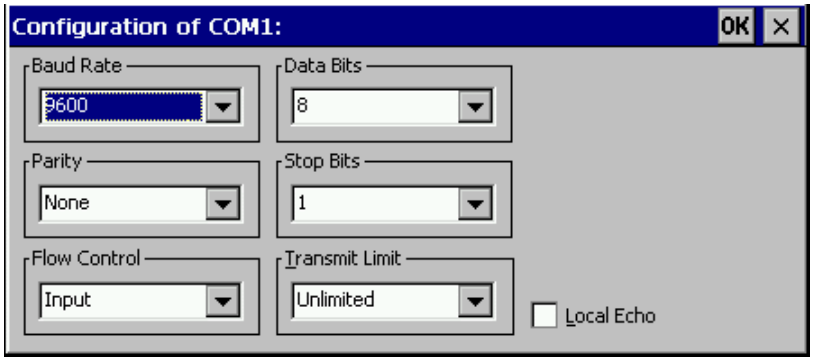
4. After providing a name and selecting the emulation/terminal type for the connection, click **Next>** to proceed. The following dialog-box is displayed.



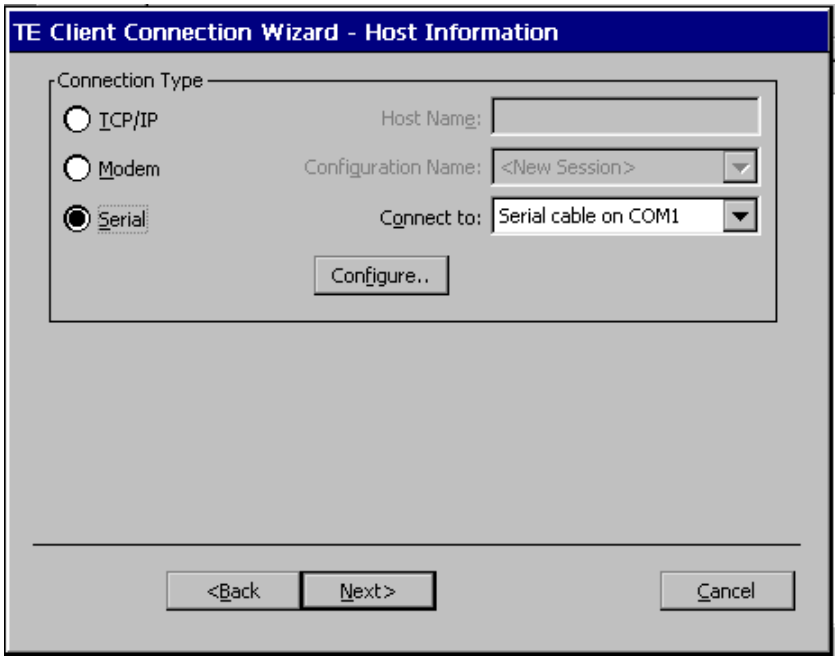
5. Select the **Serial** radio-button. The dialog-box changes as shown below.



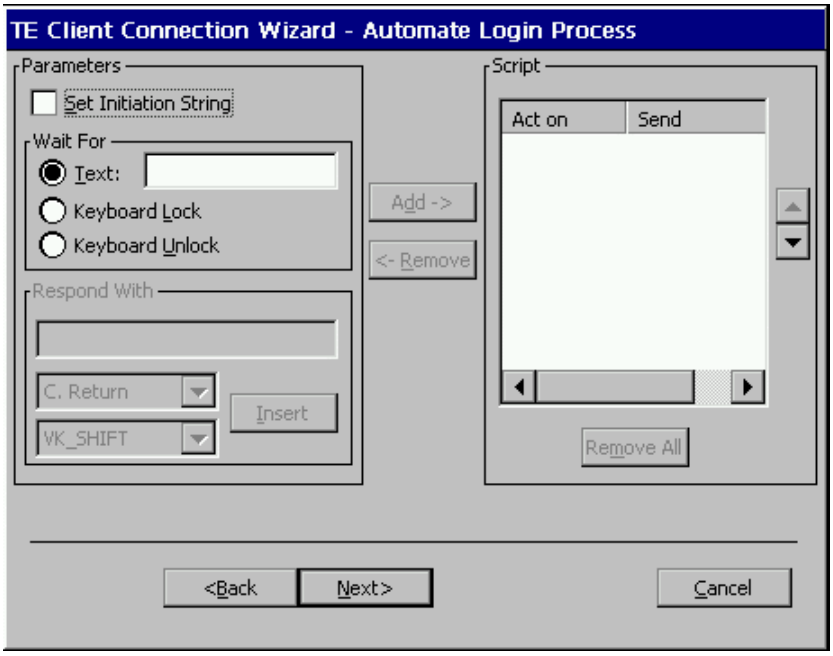
6. Select the port to which the serial cable is connected from the **Connect to** drop-down list, and click **Configure..**. The following dialog-box is displayed.



7. Configure settings (*Baud Rate, Parity, Flow Control, Data Bits, Stop Bits, Transmit Rate and Local Echo*) for the COM port to which the serial cable is connected, and click **OK** to return to the **Host Information** dialog-box.



8. Click **Next>** to proceed. The following dialog-box is displayed.



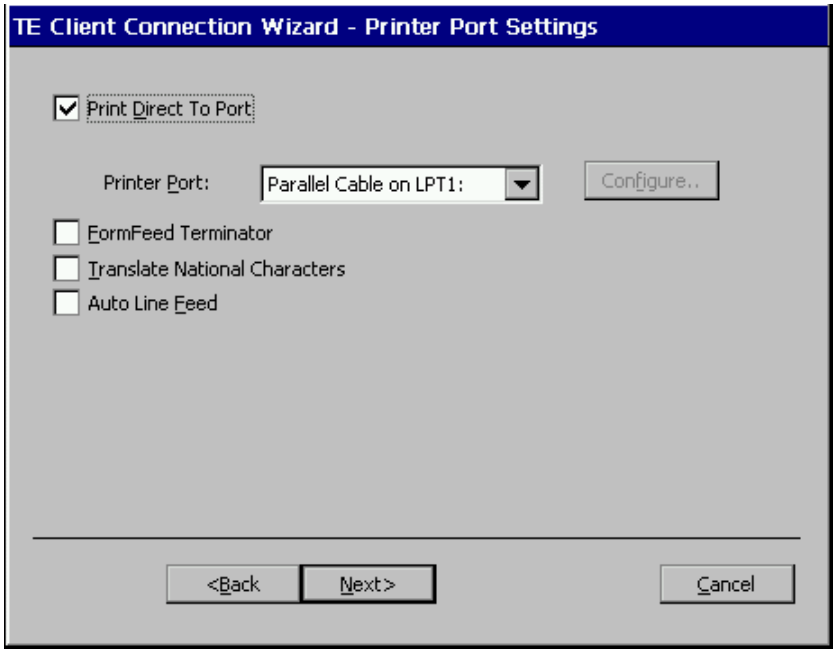
The above dialog-box allows you to partially/fully automate the login process.

- **Set Initiation String**: If the host requires an initialization string when you first connect to it, select this check-box. This will enable the **Initiate With** box in place of the **Respond With** box. Provide the required characters in this field and click the **Add** button. The initialization string will be added to the **Script** window.
- **Wait For**: With the **Text** or **Keyboard Lock** or **Keyboard Unlock** radio-button, you can specify the prompt or keyboard-status command that the automatic login process has to wait for. Some systems are case sensitive; so ensure that the **Text** entry follows the correct conventions for your system.

NOTE: WHILE RUNNING IBM3270 OR IBM5250 EMULATIONS, **TEXT** ENTRIES ARE ONLY APPLICABLE IN NVT (NETWORK VIRTUAL TERMINAL) MODE.

- **Respond With**: This group of fields is enabled only when one of the **Wait For** options is specified. With these fields, you can define responses for each **Wait For** option. You can either provide the text of the response in the text field or **Insert** a pre-defined response from the two drop-down lists below the text field. After providing or inserting a response, click **Add** to include the response in the **Script** window.
- **Script**: This window lists the defined initialization and response strings. The actions will be performed in the order in which they appear in this window. You can use the **up** and **down** arrow buttons adjacent to this window to change the order of actions.
- **Remove** / **Remove All**: With these buttons, you can remove selected or all entries from the **Script** window.

9. After configuring the above parameters, click **Next>** to proceed. The following dialog-box is displayed.

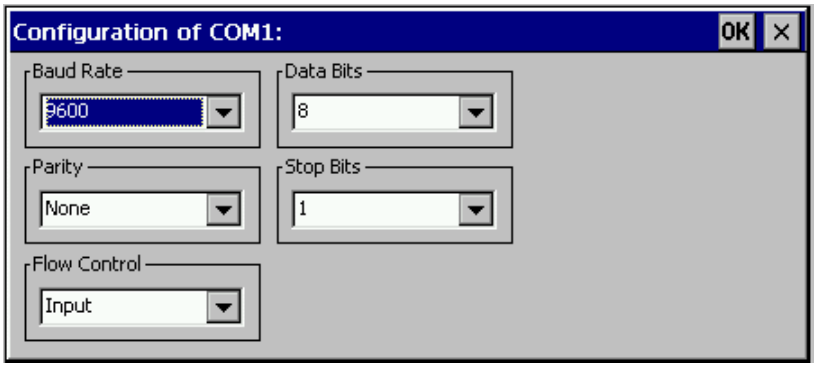


10. In the above dialog-box, you can configure your printer port.

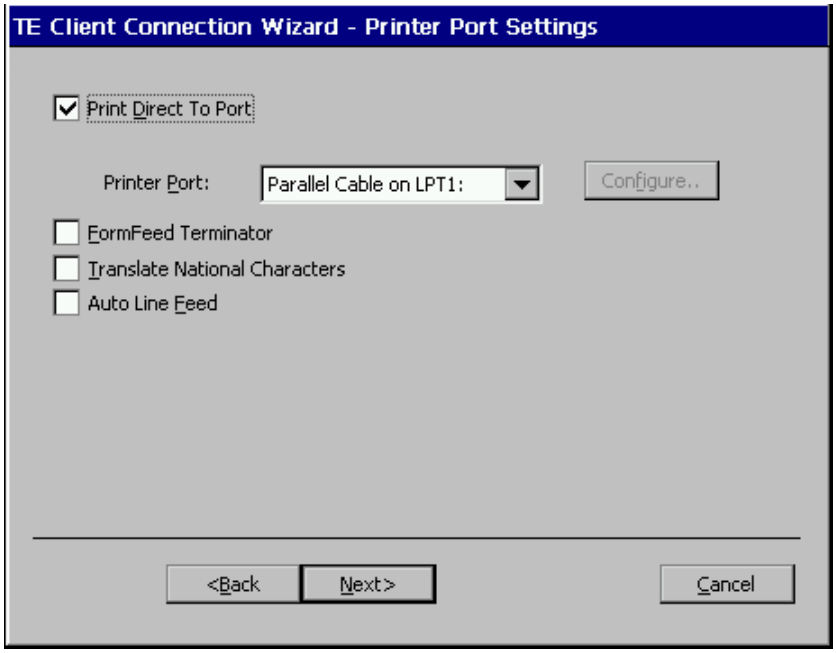
    Print Direct to Port: This check-box is selected by default indicating that a print-job fired from the emulation session will be sent directly to the printer-port of the client, bypassing the print manager (*overriding jobs in the print-queue*). This option is necessary when the host application sends control information (*for instance, 'escape' sequences sent in Print Controller and Autoprint modes in VT emulation*), which would be lost if the print-job is routed through the print manager. This option can be used when the printer-port of the client is dedicated to terminal emulation sessions.

    If on the other hand, the printer-port of the client is to be used for printing from RDP and ICA sessions as well, it is recommended that the **Print Direct to Port** check-box be deselected. In such cases, the only way to print from the emulation session is to configure the client as a print-server using LPD (*page* 35) and configure the UNIX server for LPD printing (*page 166*).

11. Select the appropriate printer port from the **Printer Port** drop-down list. If you select one of the COM ports, the **Configure** button is enabled. Click this button. The following dialog-box is displayed.



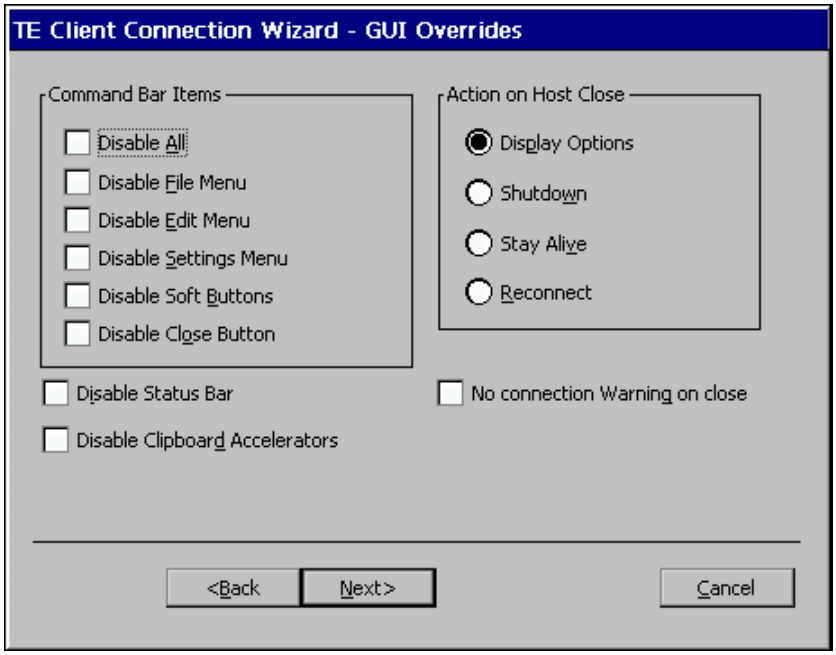
12. Configure settings (*Baud Rate, Parity, Flow Control, Data Bits and Stop Bits*) for the COM port and click **OK** to return to the **Printer Port Settings** dialog-box.



13. **Form Feed Terminator**: Select this check-box if you want the printer to advance paper to the top of the form when it has finished printing.

    - **Translate National Characters**: This option determines whether ISO Latin characters used by Microsoft Windows, or Roman 8 characters used in HP mode, are to be translated to IBM characters.
    - **Auto Line Feed**: Select this check-box if you want the printer to start at the beginning of the next line when a carriage return command is received.

14. After configuring the above parameters, click **Next>**. The following dialog-box is displayed.



The options in the above dialog-box allow you to disable user access to settings that must not be changed. It also allows you to specify an emulator response when the connection is closed.

- **Bar Items**: Select appropriate options from this group of check-boxes to disable menus on the command-bar of the terminal emulation window.
- **Disable Status Bar**: Select this check-box to disable the status bar.

- **Disable Clipboard Accelerators**: Select this check-box to disable use of **Ctrl+C** and **Ctrl+V** shortcuts to copy to and paste from the clipboard while in the terminal emulation session.

  This feature is useful in certain emulations where Ctrl+C and Ctrl+V are used to send specific commands to the terminal. Besides, you must select this option if you plan to create keyboard macros for Ctrl+C and Ctrl+V using the **Settings->Keyboard Macros…** option of the terminal emulation screen. Even when the Ctrl+C and Ctrl+V shortcuts are disabled, you can use the **Edit->Copy** and **Edit->Paste** options of the terminal emulation screen for copying and pasting.

- **Action on Host Close**: Select one of these radio-buttons to specify a response when the connection is closed.

  Display Options: Select this radio-button if you want a dialog-box to be displayed with Shutdown, Stay Alive and Reconnect options.

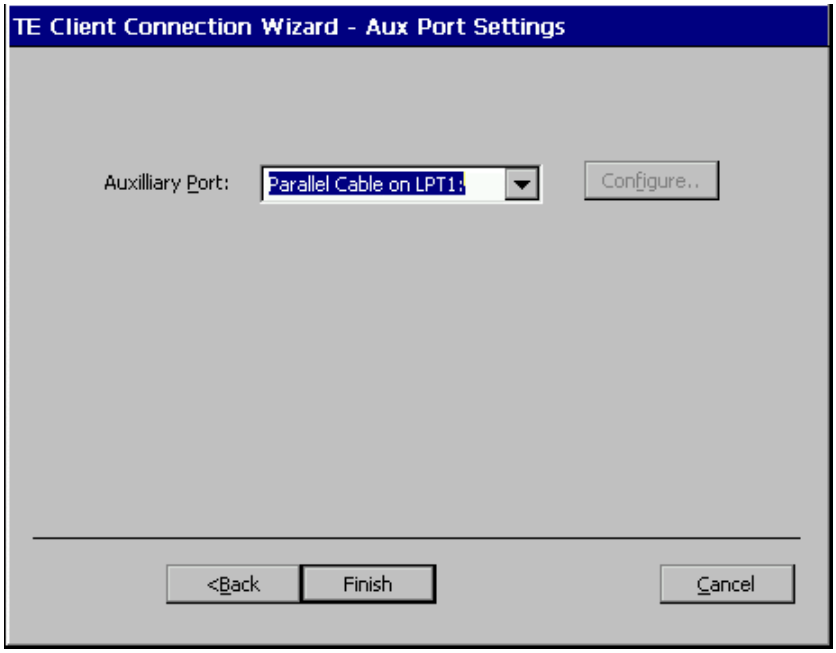
  Shutdown: Select this radio-button if you want the emulation to close down.

  Stay Alive: Select this radio-button if you want to keep the emulation running.

  Reconnect: Select this radio-button if you want the emulation to attempt to reconnect to the host.

- **No Connection warning on close**: By default, the client will display a warning message if you attempt to exit the emulator while a host connection is active. You can disable the warning message by selecting this check-box.

15. Select the appropriate GUI overrides and click **Next>**. The following dialog-box is displayed.

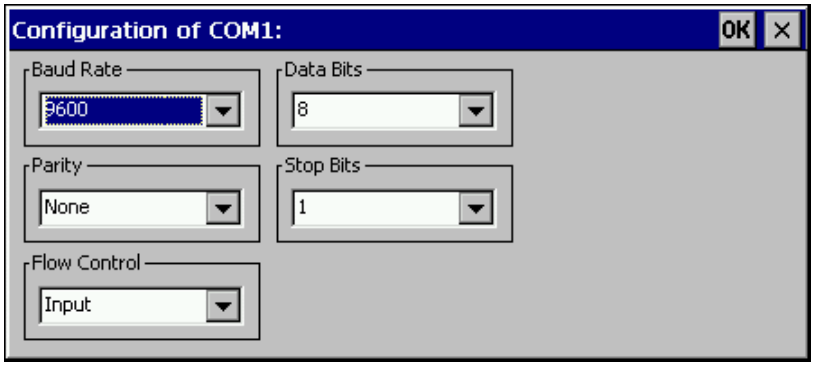


16. In the above dialog-box, you can specify a port through which external devices that require bi-directional flow of data can send data for further processing.

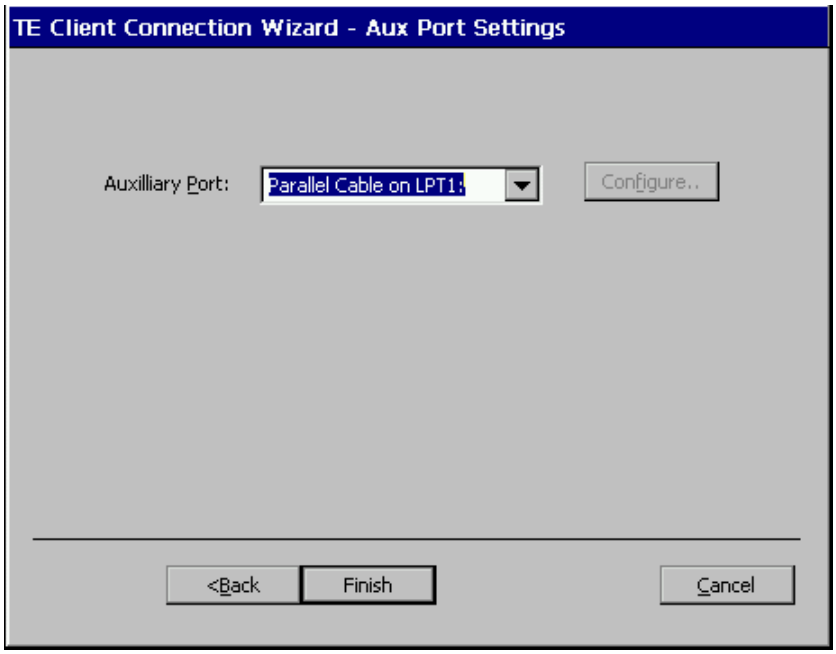
    For instance, the server pertaining to the Terminal Emulation connection may have an application that requires input from a serial device (say, a bar-code reader). In such a case, you can connect the bar-code reader to a COM port and specify that port as the auxiliary port.

NOTE: YOU MUST NOT SPECIFY THE SAME PORT AS BOTH PRINTER-PORT AS WELL AS AUXILIARY-PORT.

17. If you select a COM port, the **Configure..** button is enabled. Click this button. The following dialog-box is displayed.



18. Configure settings (*Baud Rate, Parity, Flow Control, Data Bits and Stop Bits*) for the COM port and click **OK** to return to the **Aux Port Settings** dialog-box.



19. Click **Finish**. The name of the connection you created will be added to the list of connections displayed in the **Terminal Connection Manager** window.

To start the connection, double-click on it, or highlight it and click the **Connect** button in the **Terminal Connection Manager**.

Editing Terminal Emulation Connections

TIP: DETAILED INFORMATION ABOUT TERMINAL EMULATION SETTINGS IS PROVIDED IN THE ***PERICOM Windows CE Emulation Software User's Guide***, WHICH IS AVAILABLE IN THE CD SUPPLIED WITH THE PRODUCT.

To edit a Terminal Emulation connection,

1. Select the **Configure** sheet from the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Highlight the Terminal Emulation connection to be edited.

TIP: THE 'TYPE' OF CONNECTION IS DISPLAYED IN THE **TYPE** COLUMN OF THE **TERMINAL CONNECTION MANAGER** WINDOW.

NOTE: CONNECTIONS CANNOT BE EDITED WHILE THEY ARE ACTIVE.

3. Click the **Edit…** button. A wizard, similar to the **TE Client Connection** wizard that has been described earlier in the guide, is displayed. The screens of the editing-wizard will contain an additional button to **Apply** changes. Select the appropriate hyperlink below for a description of the relevant editing-wizard.

   - TCP/IP Terminal Emulation connection: page 99.
   - Dial-up Terminal Emulation connection: page 109.
   - Serial-line Terminal Emulation connection: page 122.

Initiating Terminal Emulation Connection

1. Select the **Connections** sheet from the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Highlight the Terminal Emulation connection to start. Click **Connect.**

NOTE: YOU CAN ALSO DOUBLE-CLICK ON THE CONNECTION TO START/INITIATE THE CONNECTION.

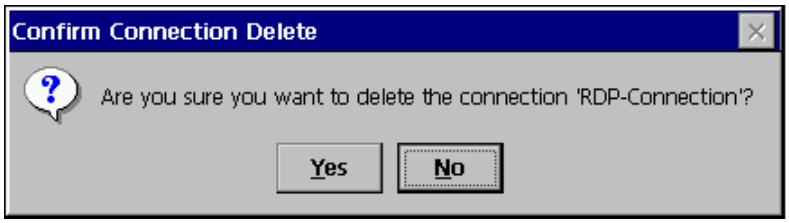
Deleting Terminal Emulation Connection

To delete a defined connection,

1. Select the Configure sheet from the Terminal Connection Manager window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Highlight the connection to be deleted, and click the **Delete** button. A **Confirm Connection Delete** prompt is displayed.



3. Click **Yes** to confirm deletion and **No** to cancel the delete command.

PPP

PPP (the Point-to-Point Protocol) is a mechanism for creating and running IP (the Internet Protocol) and other network protocols over a serial link. This link can be a direct serial connection (using a null-modem cable), over telnet-established link, or a link made using modems, telephone lines (using digital lines such as ISDN).

Using PPP, you can connect your client to a PPP server. You can then access the resources of the network where the server is connected (almost) as if you were directly connected to that network.

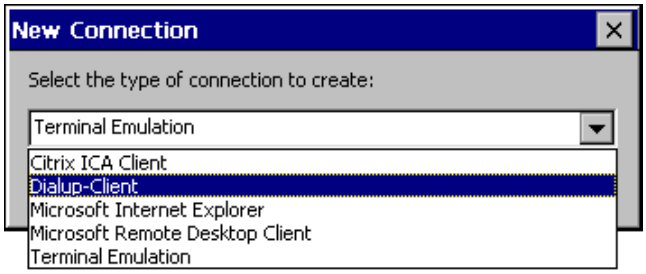
Creating PPP Connections

This section describes the procedure to configure dial-up parameters for PPP (*Point-to-Point Protocol*) connections using the RDP or ICA protocol.

1. Select the **Configure** sheet of the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

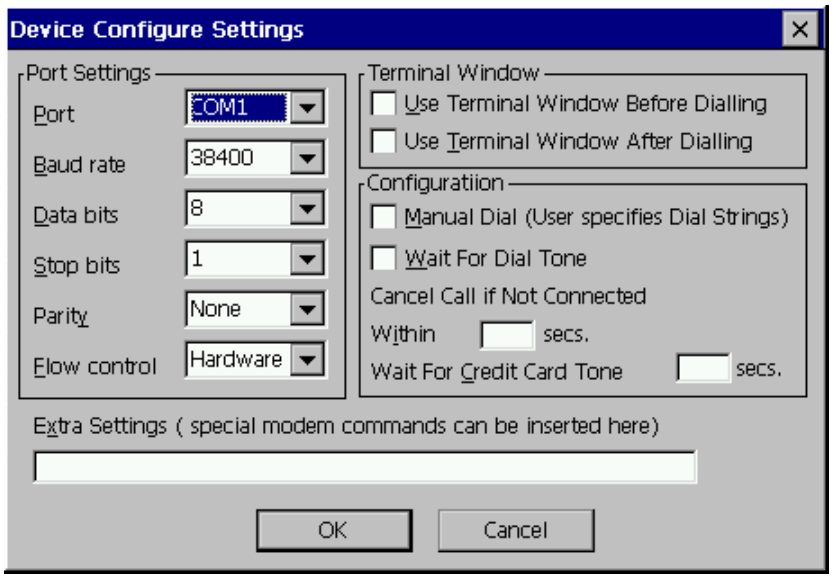
2. Click **Add…**. The **New Connection** dialog-box is displayed.



3. Select **Dialup-Client** from the drop-down list and click **OK**. The first dialog-box of the **Dial-Up Connection Wizard** is displayed.

4. Provide a name for the dial-up connection and click **Next>**. The following dialog-box is displayed.

- **Serial Device**: Select a serial device to be used for the PPP connection.
- **User Information**: In this group of fields, you can provide the **Username**, **Password** and **Domain** to be used to automatically logon to the server after the PPP connection is established. If you want the password to be saved, select the **Save Password** check-box. If you do not select the **Save Password** check-box, a password-prompt will be displayed every time you start the connection.
- **Dial Numbers**: Provide the telephone number to be dialed in the **Number** field. If you want to specify the country- and area- code, select the **User Country and Area Code** check-box and provide appropriate input in the **Area Code** and **Country Code** fields.
- Click **Configure** to define parameters for serial devices. The **Device Properties** dialog-box is displayed.



  - **Port Settings**: Select appropriate settings for the COM port (*Port, Baud Rate, Data Bits, Stop Bits, Parity and Flow Contro*l) from this group of drop-down lists.
  - **Use terminal window before dialing**: If you select this check-box, the terminal window is displayed *before* the connection is established.

- **Use terminal window after dialing**: If you select this check-box, the terminal window is displayed *after* the connection is established, prompting you for logon information.
- **Manual Dial (User Specifies Dial Strings)**: Select this check-box if you want to provide dial-strings while attempting a dial-up connection.

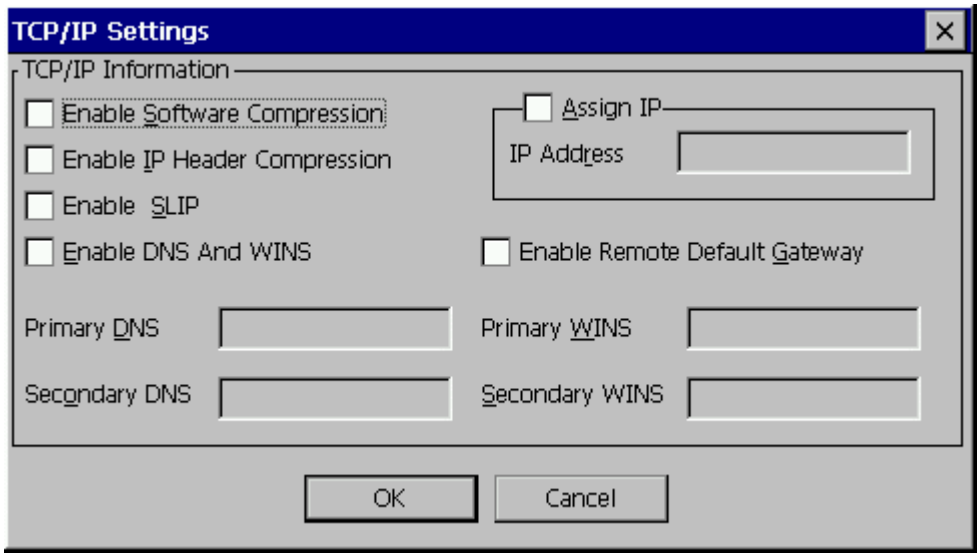
NOTE: MANUAL DIALING IS CURRENTLY NOT SUPPORTED.

- **Wait for dial tone**: Select this check-box if you want the dial-in device to wait for a dial tone before dialing.
- **Cancel the call if not connected within … seconds**: In this field, specify the time limit after which the call should be cancelled, if it does not connect.
- **Wait for credit card tone**… **seconds**: In this field, specify the duration for which the terminal has to wait for a credit card tone.
- **Extra Settings**: In this field, you can provide special modem commands.

NOTE: IF YOU PROVIDE INPUT IN THIS FIELD, YOU MUST ALSO SELECT THE **MANUAL DIAL** CHECK-BOX.

After configuring the serial device, click **OK** to return to the **Dial-Up Connection Wizard**.

- Click **TCP/IP** to configure the TCP/IP settings. The following dialog-box is displayed.



- **Enable Software Compression**: This setting causes data to be compressed before transmission, thus optimizing the bandwidth usage. Note that while data compression reduces the transmission time, it consumes more processor resources.
- **Enable IP Header Compression**: Select this check-box to enable compression of the IP header.
- **Enable SLIP**: Select this check-box to enable support for Serial Line Internet Protocol .
- **Assign IP**: If the remote system administrator has issued a fixed IP address for the connection, select this check-box and enter the IP address in the **IP Address** field. On the other hand, if the remote host provides IP addresses dynamically, do not select this check-box.
- **Enable Remote Default Gateway**: Select this check-box to enable use of the default gateway of the remote network.
- **Enable DNS And WINS**

  Select this check-box if your network has DNS or WINS servers and if want to use them. When this check-box is selected, the following fields will also be enabled.

  Primary DNS: provide the IP address of the primary DNS server in your network.

  Secondary DNS: provide the IP address of the secondary DNS server in your network.

  Primary WINS: Provide the IP address of the primary WINS Server.

  Secondary WINS: Provide the IP address of the secondary WINS Server.

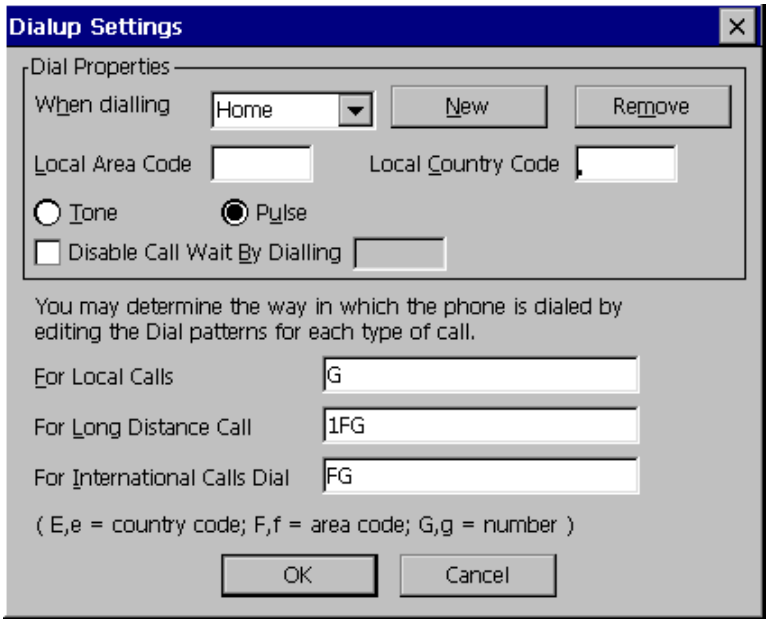
After configuring TCP/IP settings, click **OK** to return to the **Dial-Up Connection Wizard**.

- Click the **Security** button to configure settings for password encryption. The **Security** dialog-box is displayed.

  - **Authenticate Clear Text**: Select this radio-button if the password must be accepted as a string of normal characters.
  - **Accept Encrypted Password**: Select this radio-button if the password must be accepted in the standard encryption format.
  - **Accept Microsoft Password**: Select this radio-button if the password must be accepted in the Microsoft encryption format.

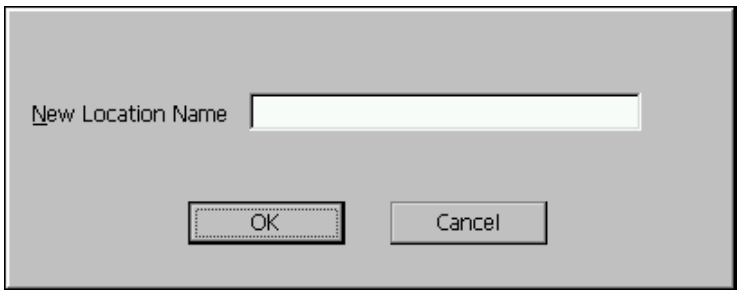
  Click **OK** to return to return to the **Dial-Up Connection Wizard**.

- Click the **Dial Properties** button to configure dialing properties. The **Dialup Settings** dialog-box is displayed.



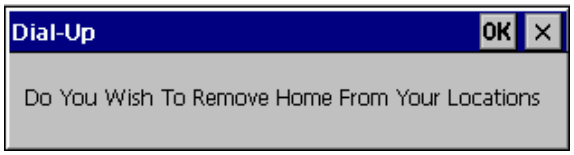
With the above dialog-box, you can create, configure and delete dialing locations.

- To create a location, click **New**. The following dialog-box is displayed.



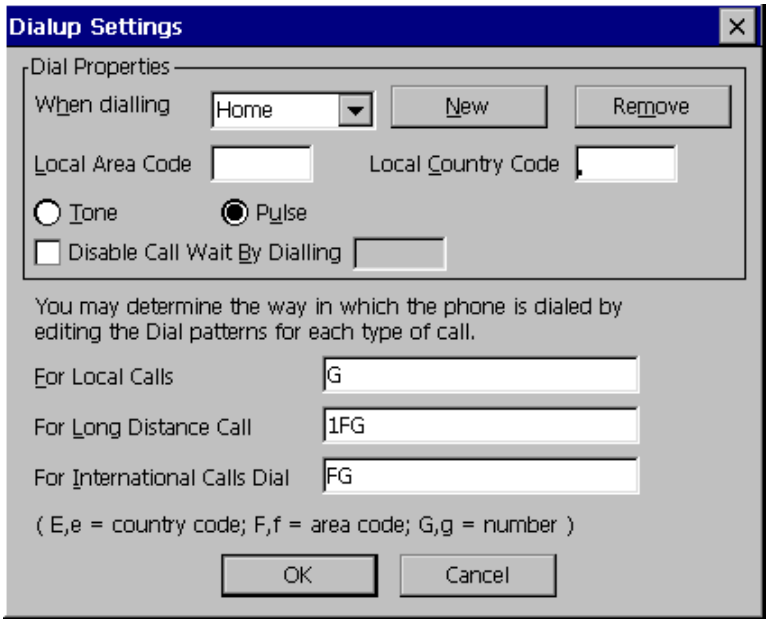
Provide a name for the new location and click **OK** to return to the **Dialup Settings** dialog-box.

- To remove a location, select it from the **When dialing** drop-down list and click **Remove**. The following prompt is displayed.



Click **OK** to confirm removal and return to the **Dialup Settings** dialog-box.

NOTE: YOU CANNOT REMOVE THE DEFAULT **HOME** AND **WORK** DIALING LOCATIONS.

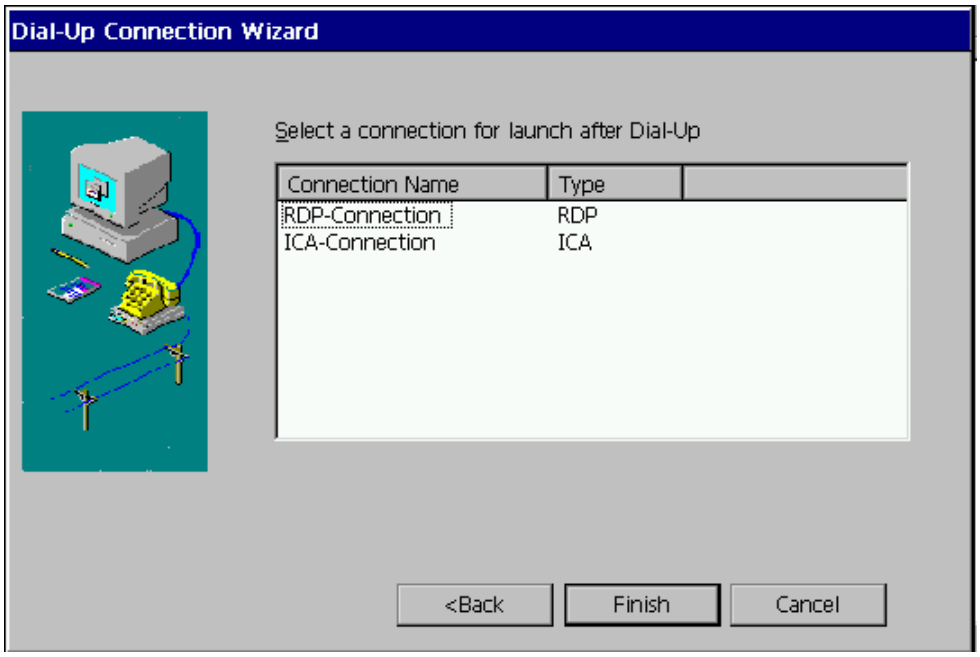


To configure properties of a dialing location,

- Select the required location from the **When dialing** drop-down list
- Enter the area code and country code in the **Local Area Code** and **Local Country Code** fields respectively.
- Specify whether the dial-up device should use **Tone** or **Pulse** dialing by selecting the appropriate radio-button.
- To disable the call-waiting function, select the **Disable Call Wait By Dialing** check-box and specify the number to be dialed.
- In the **For Local Calls**, **For Long Distance Call** and **For International Calls Dial** fields, specify the dialing sequence by either entering the appropriate number sequence, or by using the codes listed at the bottom of the dialog-box.

After configuring the dialing locations, click **OK** to return to the **Dial-Up Connection Wizard**.

5. Click **Next>** to proceed. The following dialog-box is displayed.



6. The above dialog-box lists the available connection entries. Highlight the connection that must be started using the dial-up link and click **Finish**.

The name of the connection you created will be added to the list of connections displayed in the **Terminal Connection Manager** window.

To start the connection, double-click on it, or highlight it and click the **Connect** button in the **Terminal Connection Manager**.

Editing Dial-up Parameters for PPP Connections

To edit a Dial-up connection,

1. Select the **Configure** sheet from the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Highlight the Dial-up connection to be edited.

TIP: THE 'TYPE' OF CONNECTION IS DISPLAYED IN THE **TYPE** COLUMN OF THE **TERMINAL CONNECTION MANAGER** WINDOW.

NOTE: CONNECTIONS CANNOT BE EDITED WHILE THEY ARE ACTIVE.

Click the **Edit…** button. The Dial-Up Connection Wizard (page 133) is displayed.

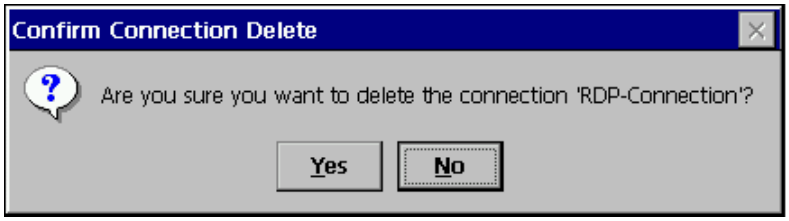
Deleting PPP Connection

To delete a defined connection,

1. Select the Configure sheet from the Terminal Connection Manager window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Highlight the connection to be deleted, and click the **Delete** button. A **Confirm Connection Delete** prompt is displayed.



3. Click **Yes** to confirm deletion and **No** to cancel the delete command.

Browser Session

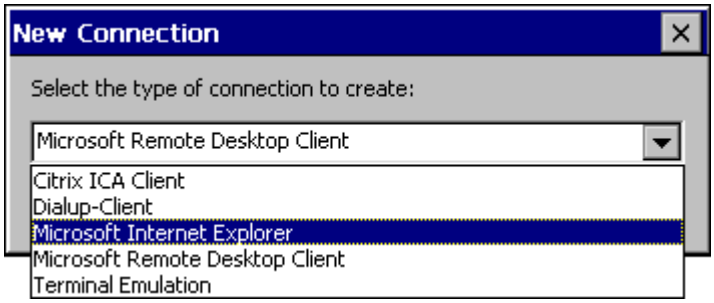
Creating Browser Sessions

The firmware of the client includes Microsoft Internet Explorer 4.01. To use the browser, you must create a browser-session as described in this section. For detailed information about capabilities of the browser, please visit www.cyscape.com. The site automatically evaluates and displays the capabilities.

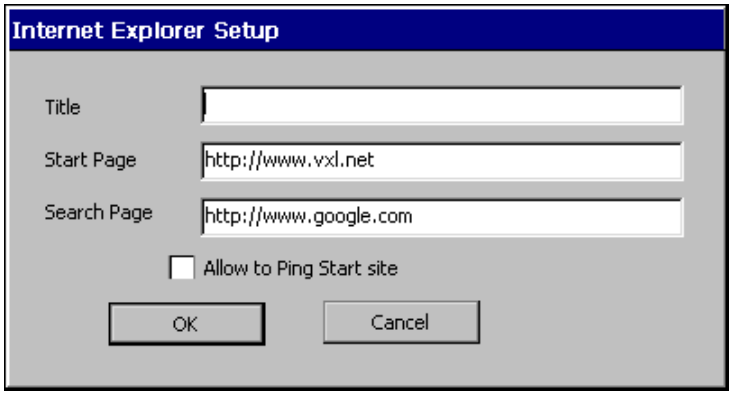
1. Select the **Configure** sheet of the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Click **Add….** The **New Connection** dialog-box is displayed.



3. Select **Microsoft Internet Explorer** from the drop-down list and click **OK**. The following dialog-box is displayed.



- Provide a name for the browser session in the **Title** field.
- In the **Start Page** field, specify the URL of the web page to be opened when the browser is launched.
- In the **Search Page** field, specify the name of the search engine to be launched when the user clicks on the 'search' icon on the tool-bar of the browser window.
- If you want the client to ping the start-site before connecting to it, select the **Allow to Ping Start Site** check-box.

4. After configuring the above parameters, click **OK**.

The name of the connection you created will be added to the list of connections displayed in the **Terminal Connection Manager** window.

NOTE: IF THE CLIENT USES A FIXED IP ADDRESS, THE GATEWAY AND THE DNS SERVER INFORMATION MUST BE SPECIFIED FOR THE CLIENT. IF THE CLIENT USES A DHCP-ASSIGNED IP ADDRESS, THE DHCP SERVER MUST BE CONFIGURED WITH APPROPRIATE DNS AND GATEWAY INFORMATION. THIS IS

ESSENTIAL FOR USERS TO BE ABLE TO SURF THE INTERNET USING THE IN-BUILT INTERNET EXPLORER BROWSER.

To start the browser connection, highlight the appropriate entry in the **Terminal Connection Manager** and click the **Connect** button.

Editing Browser Session Parameters

To edit a browser session,

1. Select the **Configure** sheet from the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Highlight the browser session to be edited.

TIP: THE TYPE OF CONNECTION (*ICA, RDP OR TEC*) IS DISPLAYED IN THE **TYPE** COLUMN OF THE **TERMINAL CONNECTION MANAGER** WINDOW.

Click the **Edit…** button. The Internet Explorer Setup dialog-box (page 142) is displayed.

Initiating Browser Session

1. Select the **Connections** sheet from the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Highlight the ICA connection to start. Click **Connect.**

NOTE: YOU CAN ALSO DOUBLE-CLICK ON THE CONNECTION TO START/INITIATE THE CONNECTION.

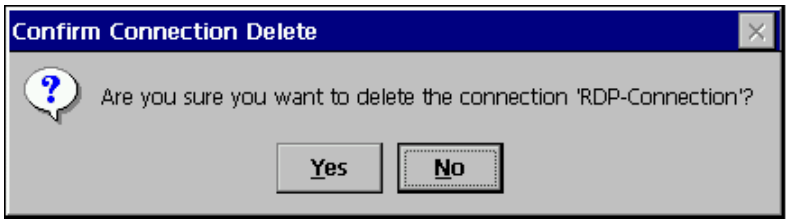
Deleting Connection Entries

To delete a defined connection,

1. Select the Configure sheet from the Terminal Connection Manager window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Highlight the connection to be deleted, and click the **Delete** button. A **Confirm Connection Delete** prompt is displayed.



3. Click **Yes** to confirm deletion and **No** to cancel the delete command.

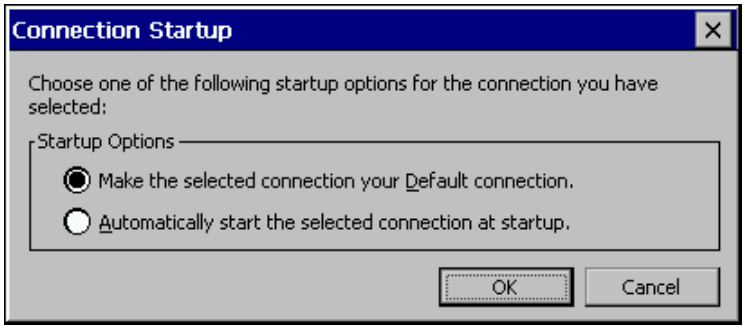
Specifying AutoStart / Default Connection

This section describes the procedure to configure the client to automatically start or highlight a particular connection when the client is switched on.

1. Select the **Configure** sheet from the **Terminal Connection Manager** window.

TIP: TO SWITCH TO THE TERMINAL CONNECTION MANAGER FROM AN OPEN SESSION, PRESS CTRL+ALT+END.

2. Select the connection for which you want to specify AutoStart or Default properties.
3. Click the **Startup…** button. The **Connection Startup** dialog-box is displayed.



The above dialog-box has two radio-buttons:

- **Make the selected connection your default connection**

  If you select this radio-button, the connection you selected in step 2 will be highlighted every time you switch on the client. The word **Default** will be displayed in the **Startup** column of the **Configure** tab of the **Terminal Connection Manager**.

- **Automatically start the selected connection at startup**

  If you select this radio-button, the connection you selected in step 2 will be automatically started every time you switch on the client. The word **AutoStart** will be displayed in the **Startup** column of the **Configure** tab of the **Terminal Connection Manager**.

4. After configuring the default and auto-start properties, click **OK** to return to the **Terminal Connection Manager**.

Server-side Configuration for LPD Printing

LPD (*Line Printer Daemon*) is a feature with which network users can access printers connected to the client. To implement this feature you must configure appropriate clients as print-servers (*as described on page 35*) and then configure the Windows NT 4.0 TSE, Windows 2000, UNIX and Linux servers as described in this chapter.

LPD printing provides the following advantages when compared to other local printing options (*see note below for the other local printing options*).

- In other local printing options, the client must be connected to the server to act as a print-server. Clients configured using the Line Printer Daemon, start functioning as print-servers as soon as they are switched on.
- During an ICA session, if a client receives a print-job from another ICA user, the receiving client may become slow and even temporarily unusable until the print-job has been completed. This is because in ICA-printing, the print-job and other client-server traffic use the same communication channel. On the other hand, if the client is configured as a print-server using LPD, the performance of the client is not affected while it is executing print-jobs. This is because, in the Line Printer Daemon uses a separate communication channel for printing.

NOTE: FOLLOWING ARE OTHER LOCAL PRINTING OPTIONS BESIDES THE LINE PRINTER DAEMON.

- WHEN A CLIENT IS CONNECTED TO A WINDOWS 2000 SERVER USING AN RDP CONNECTION, THE PRINTER PORT OF THE CLIENT CAN BE ACCESSED BY RDP USERS IN THE NETWORK. THE PROCEDURE TO IMPLEMENT THIS FEATURE IS DESCRIBED ON PAGE 32.
- DURING ICA SESSIONS, THE PRINTER PORTS OF CLIENTS CAN BE ACCESSED BY ICA USERS IN THE NETWORK IF THE USE PRINTER CONFIGURATION UTILITY OPTION (*PAGE 76*) IS APPROPRIATELY CONFIGURED WHILE CREATING THE ICA CONNECTION.

This chapter describes the procedure to configure the following servers for LPD printing.

Windows NT 4.0 Terminal Server Edition

This section describes the procedure to configure a Windows NT 4.0 TSE server to print on printers connected to LPD clients (*page35*).

1 Select the **Network Neighborhood** icon on the desktop.

2 Right-click and select **Properties**. The **Network** dialog-box is displayed.

3 Select the **Services** tab.

4 If **Microsoft TCP/IP Printing** is already displayed in the **Network Services** list, click **Cancel** to return to the desktop and proceed to step **10**.

5 If **Microsoft TCP/IP Printing** is not displayed in the **Network Services** list, click **Add**. The **Select Network Service** dialog-box is displayed.

6 Select **Microsoft TCP/IP Printing** and click **OK**.

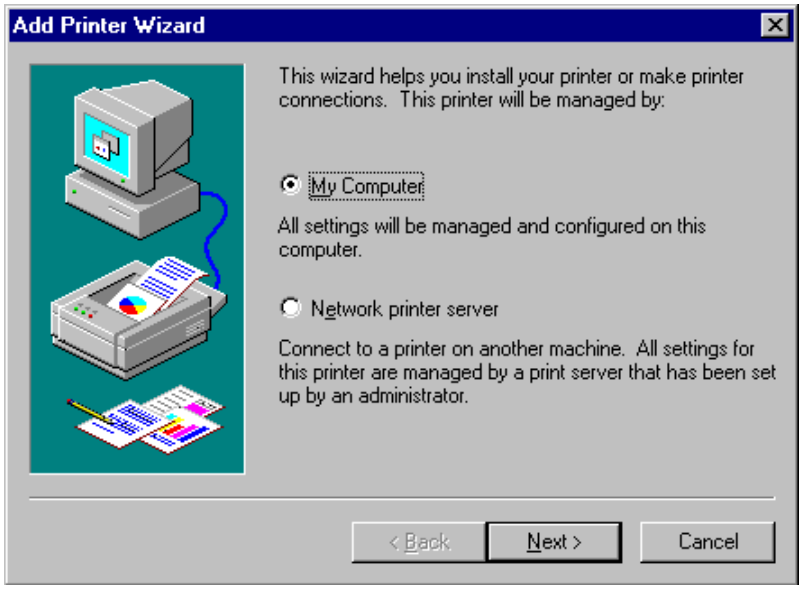
7 A prompt to insert the CD containing the Windows NT 4.0 TSE software is displayed. Insert the CD or type the path of the NTTSE-i386 directory and click **Continue**.

8 After copying required files, the **Network** dialog-box is displayed again. Click **Close**.

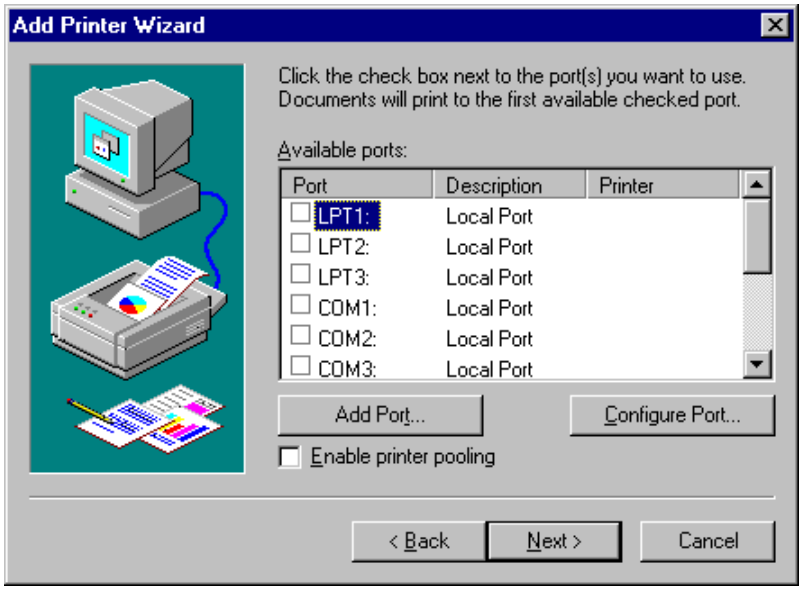
9 A prompt to shut down and restart the server is displayed. Click **Yes** to restart the server.

10 Select **Start**->**Settings**->**Printers**. The **Printers** window is displayed.

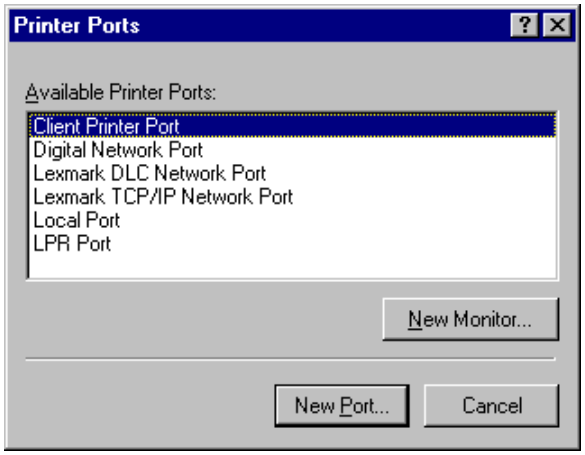
11 Double-click the **Add Printer** icon. The following dialog-box is displayed.



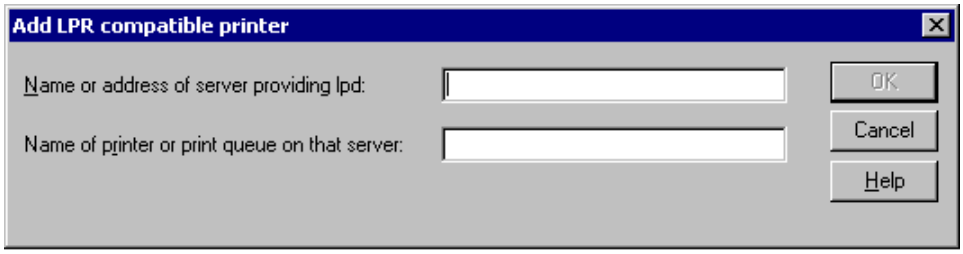
12 Select **My Computer** and click **Next>**. The following dialog-box is displayed.



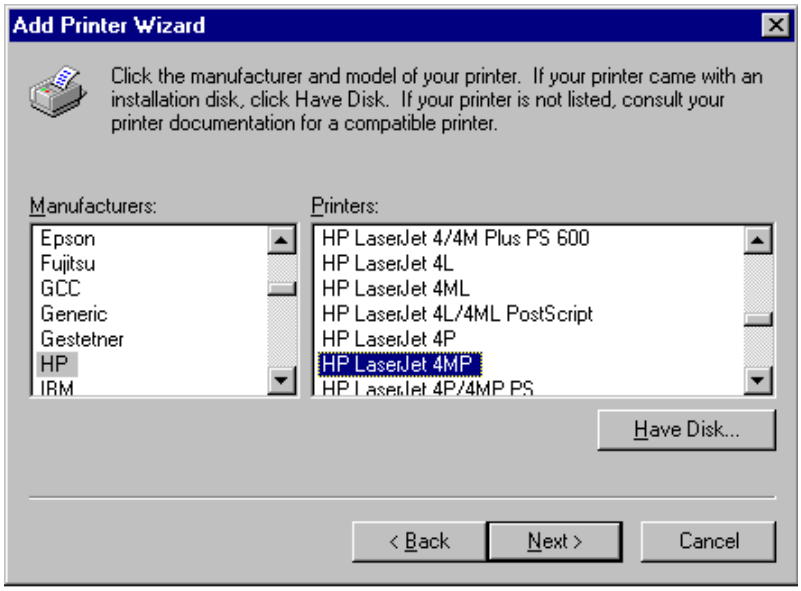
13 Click **Add Port…** The following dialog-box is displayed.



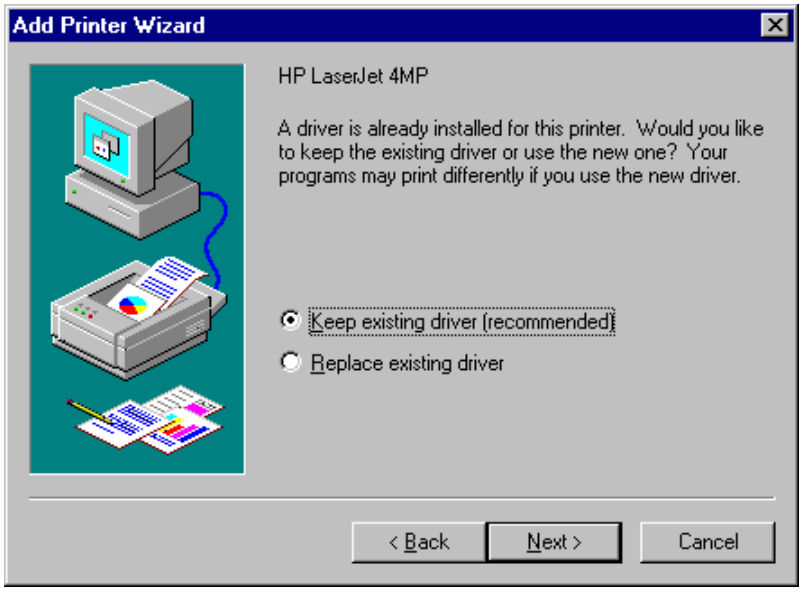
14 Select the **LPR Port** entry and click **New Port**. The following dialog-box is displayed.



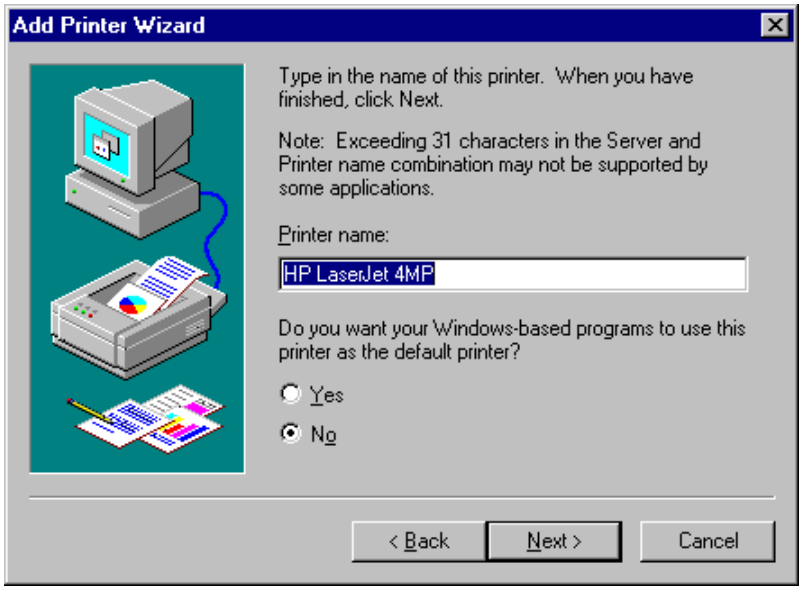
15 In the first text-field, specify the IP address of the client that is configured as a print-server using LPD. In the second text-field, enter the name of the printer connected to the LPD server. The name should be the same as that specified while configuring the client as an LPD server. Click **OK**. The following dialog-box is displayed.



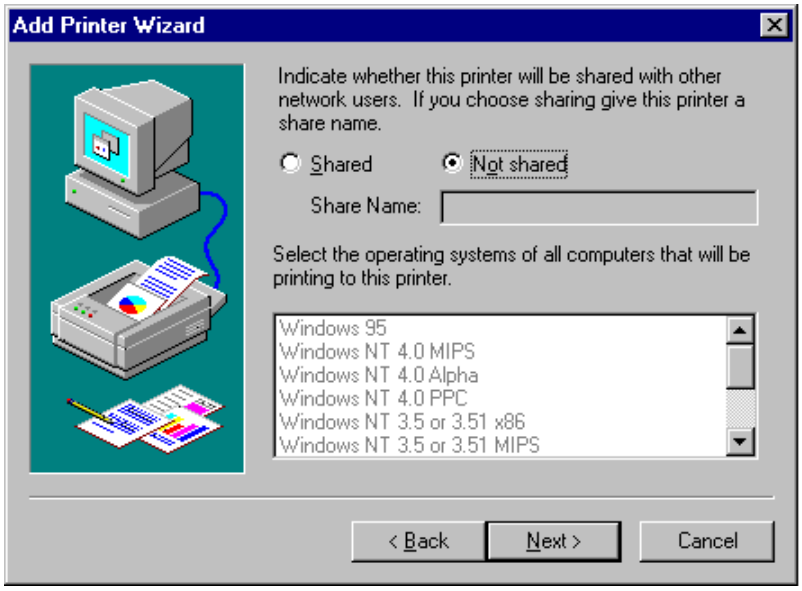
16 Select the make and model of the printer from the **Manufacturers** and **Printers** lists. Click **Next>** to continue. The following dialog-box is displayed.



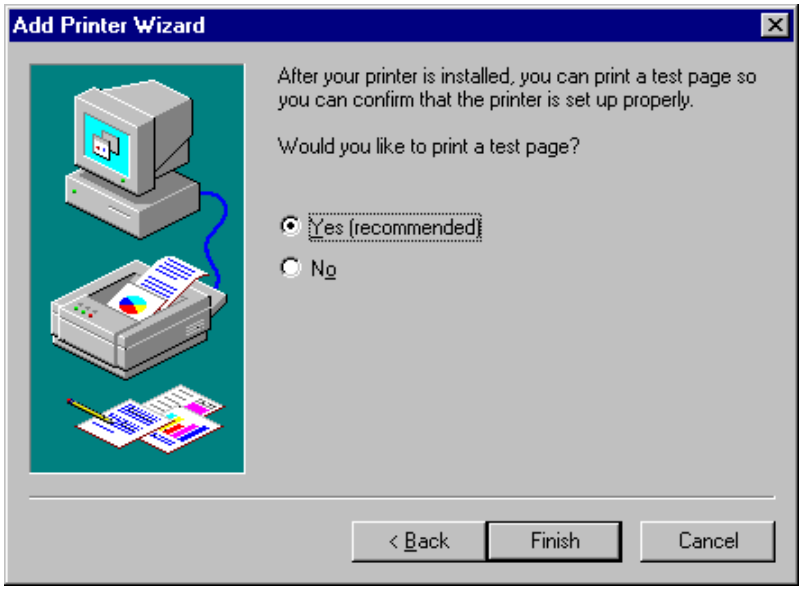
17 Select the appropriate radio-button to specify the printer driver and click **Next>**. The following dialog-box is displayed.



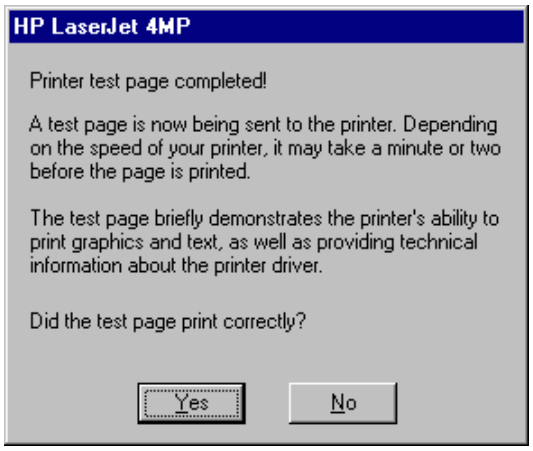
18 Enter a name for the printer and click **Next>**. The following dialog-box is displayed.



19 Specify the print-sharing parameters and click **Next>**. The following dialog-box is displayed.



20 Specify whether you want to print a test page and click **Finish**. If you chose to print a test page, the following dialog-box is displayed.



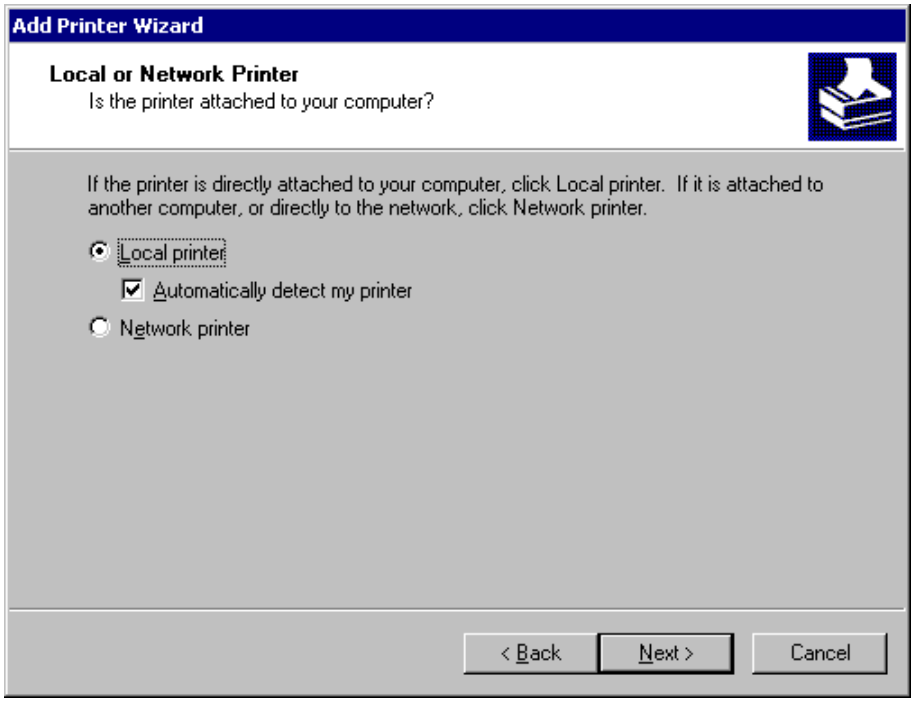
21 If the test page was printed properly, click **Yes**. Otherwise, click **No** to proceed with troubleshooting.

Windows 2000 Server

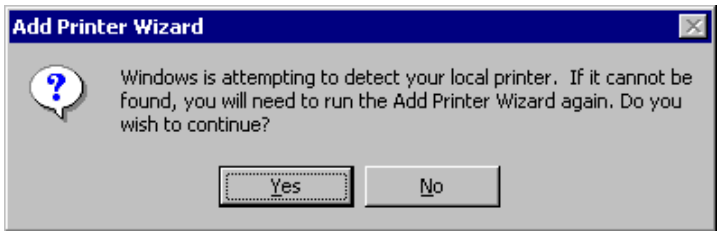
This section describes the procedure to configure a Windows 2000 Server to print on printers connected to LPD clients (*page 35*).

1. Select the **My Network Places** icon on the desktop.
2. Right-click and select **Properties**. The **Network and Dial-up Connections** dialog-box is displayed.
3. Select the **Local Area Connections** icon.
4. Right-click and select **Properties**. The **Local Area Connection Properties** dialog-box is displayed.
5. If **File and Print Sharing for Microsoft Networks** is already displayed in the dialog-box, return to the desktop and proceed to step **10**.
6. If **File and Print Sharing for Microsoft Networks** is not displayed in the dialog-box, click **Install**. The **Select Network Component Type** dialog-box is displayed.
7. Select the **Service** entry and click **Add**. The **Select Network Service** dialog-box is displayed.
8. Select the **File and Print Sharing for Microsoft Networks** option and click OK.
9. After copying required files, a prompt to shut down and restart the server is displayed. Confirm the prompt to restart the serer.
10. Select **Start**->**Settings**->**Printers**. The **Printers** window is displayed.
11. Double-click the **Add Printer** icon. The following dialog-box is displayed.

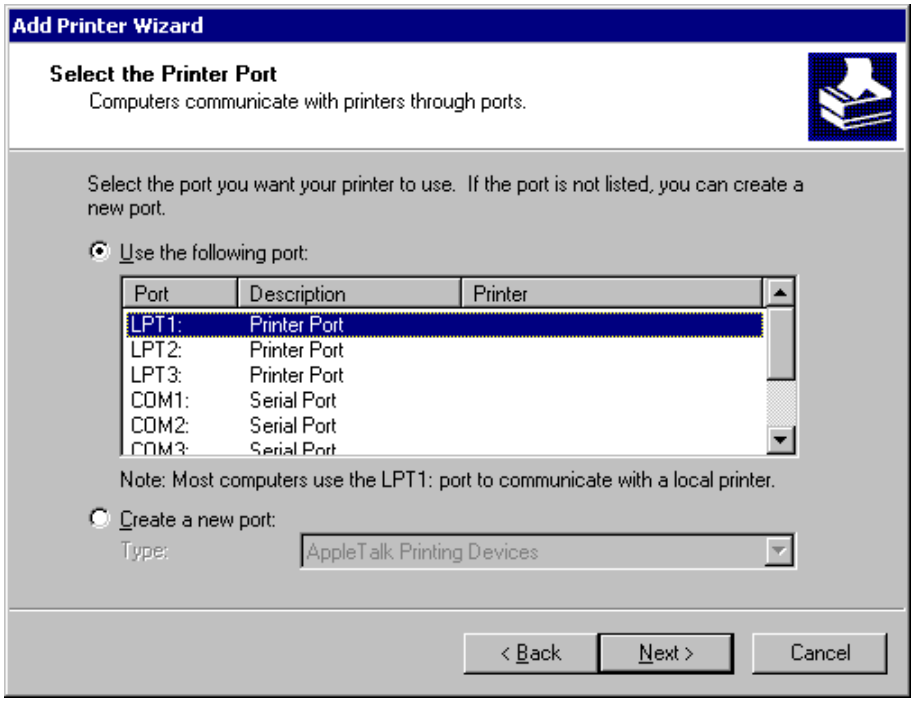
12. Click **Next>** to continue. The following dialog-box is displayed.



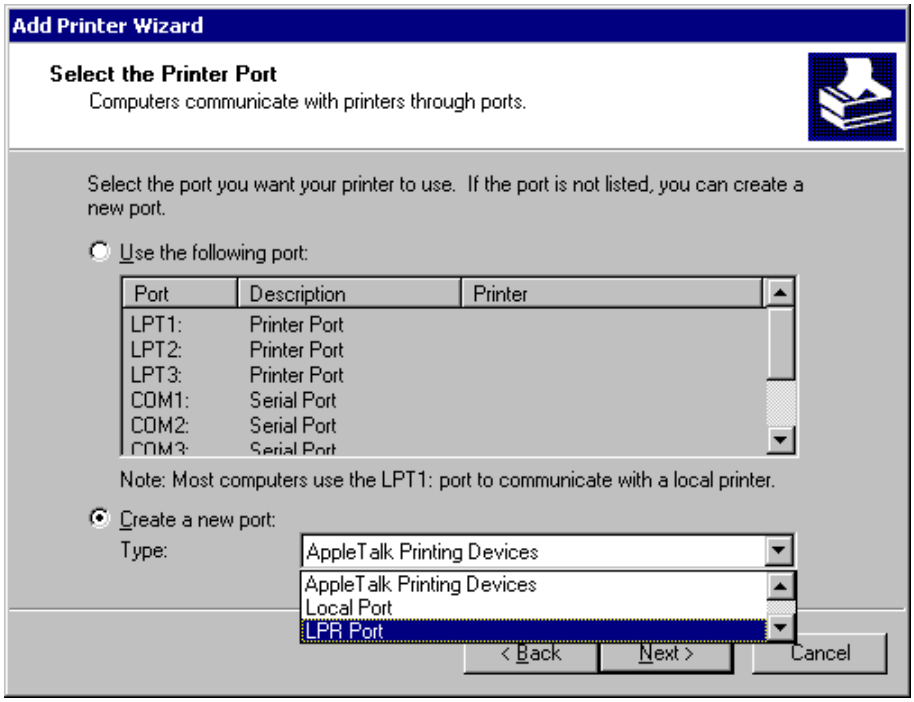
13. Select the **Local Printer** radio-button and the **Automatically detect my printer** check-box. Click **Next>** to proceed. The following prompt is displayed.



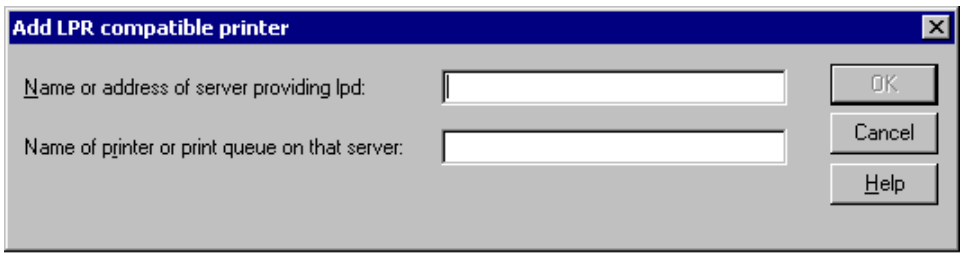
14. Click **Yes** to continue. The following dialog-box is displayed.



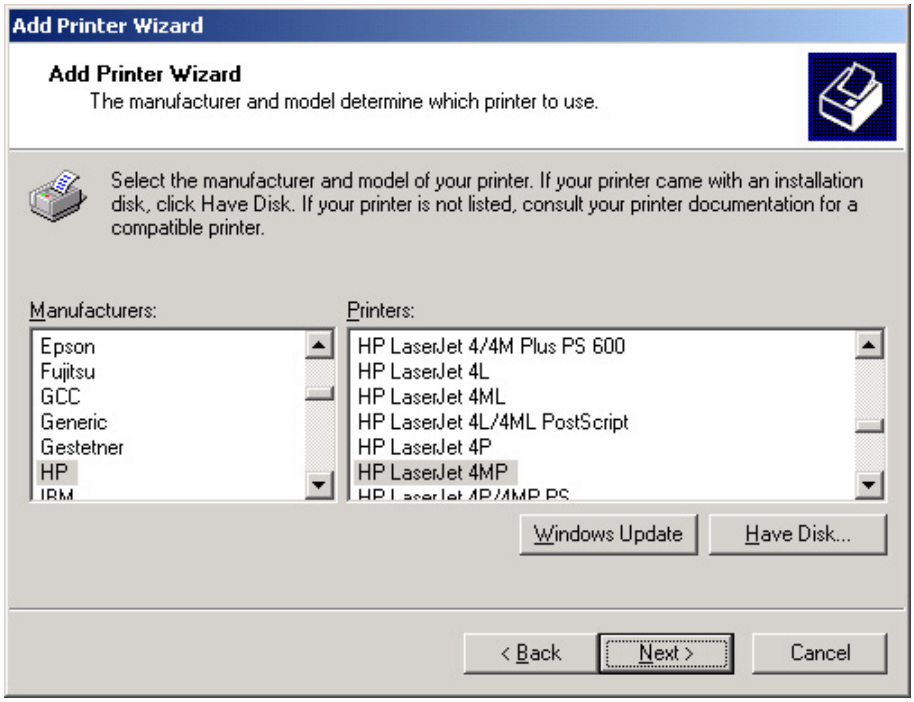
15. Select the **Create a new port** option and click on the **Type** drop-down list to view available options.



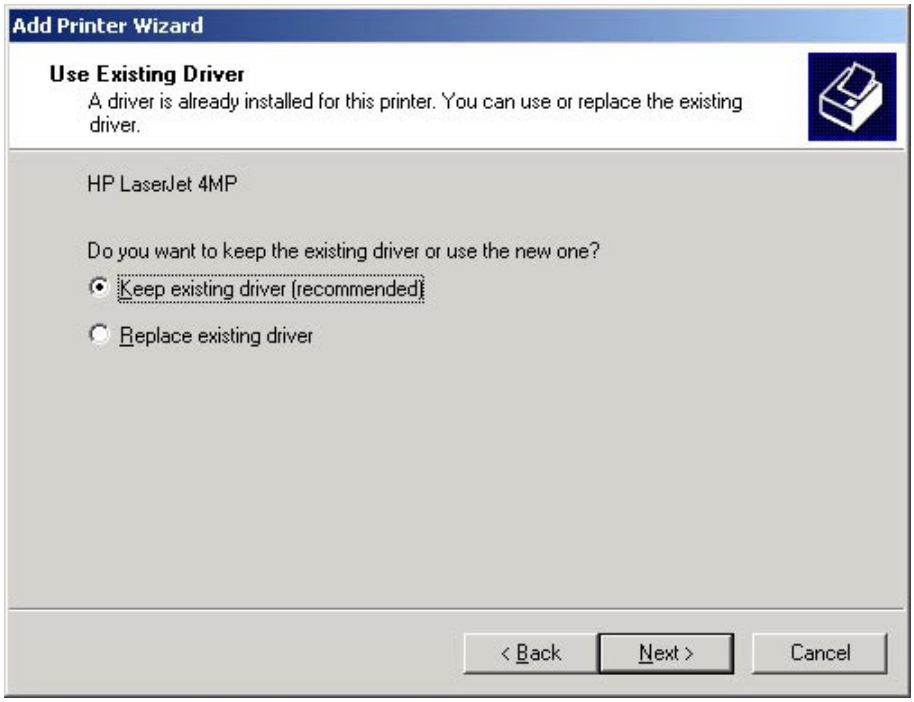
16. Select the **LPR Port** option and click **Next>** to proceed. The following dialog-box is displayed.



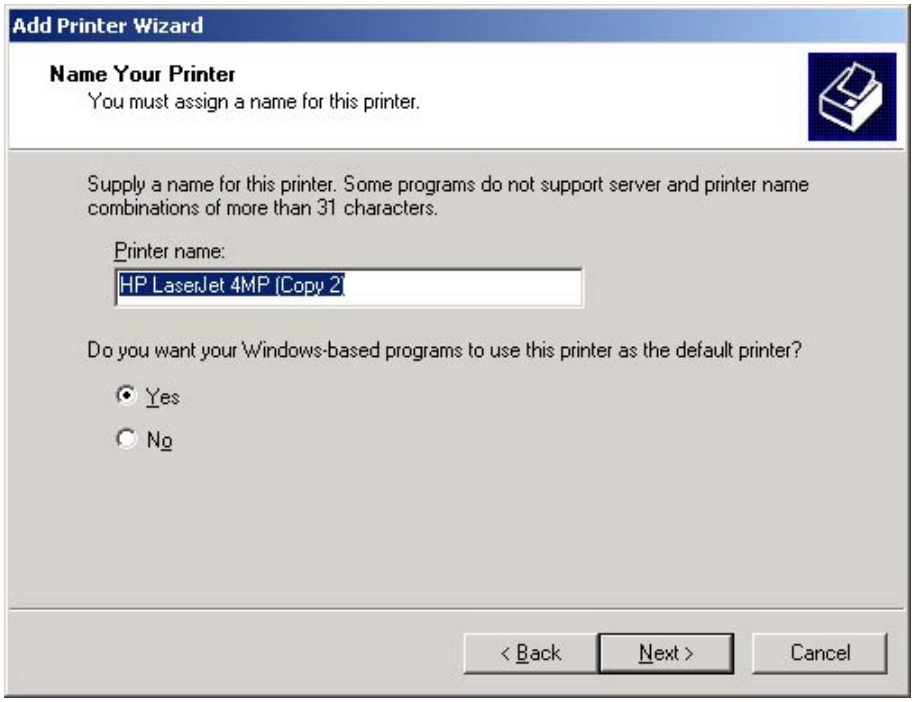
17. In the first text field, specify the IP address of the client that is configured as the LPD server. In the second text field, enter the name of the printer connected to the LPD server. The name should be the same as that specified while configuring the client as an LPD server. Click **OK**. The following dialog-box is displayed.



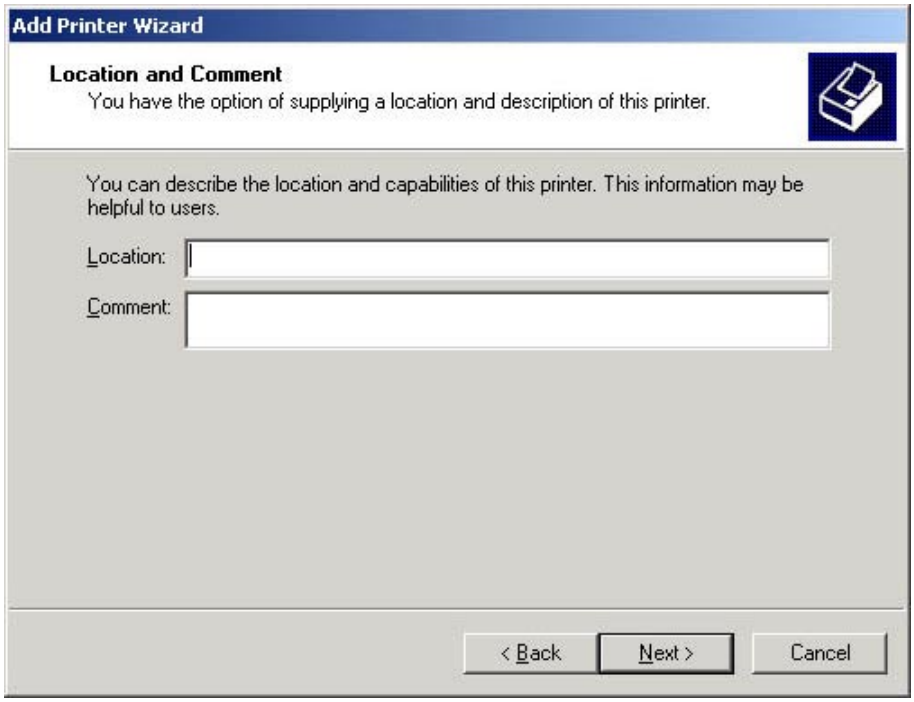
18. Select the make and model of the printer from the **Manufacturers** and **Printers** lists. Click **Next>** to continue. The following dialog-box is displayed.



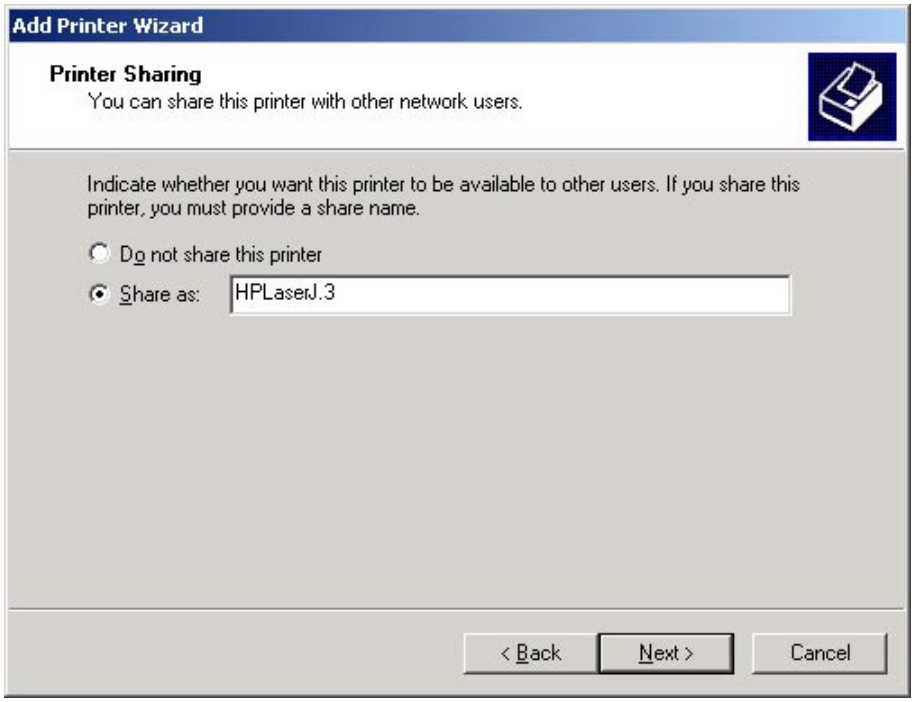
19. Select the appropriate radio-button to specify the printer driver and click **Next>**. The following dialog-box is displayed.



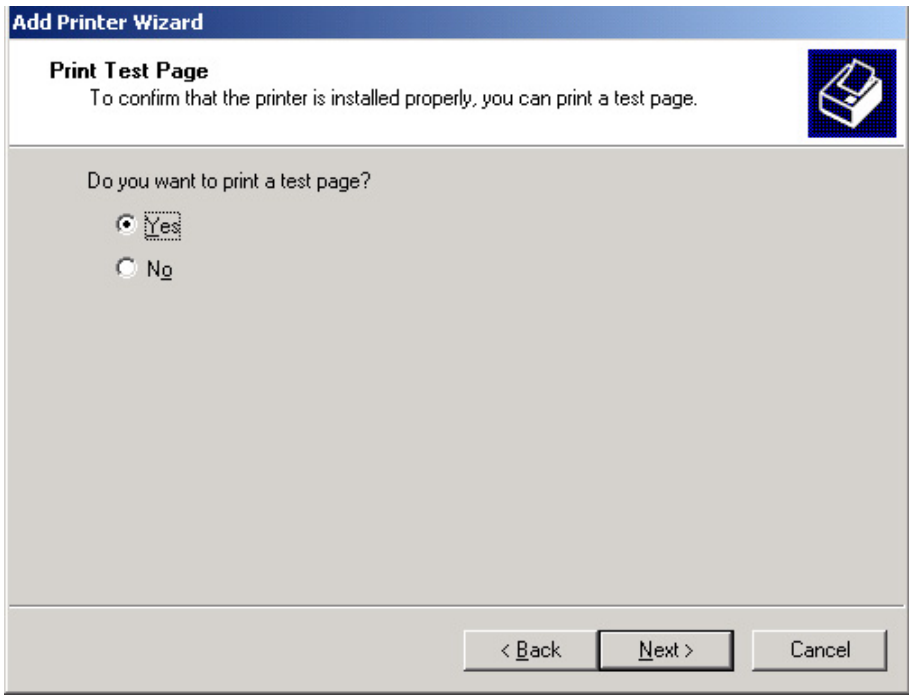
20. Specify a name for the printer and click **Next>**. The following dialog-box is displayed.



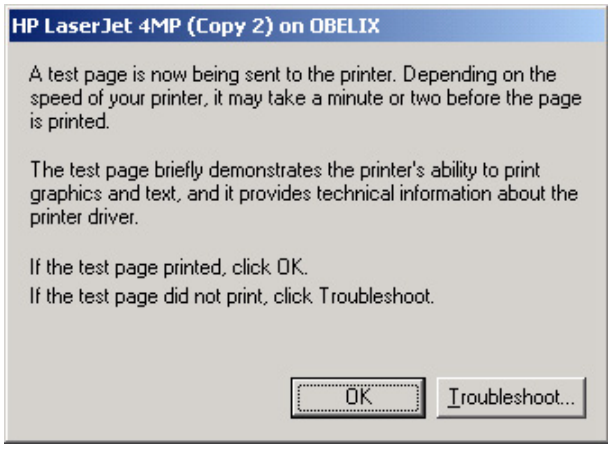
21. In the above dialog-box, you can enter the location of the printer and some comments describing the printer. These entries are optional. Click **Next>** to continue. The following dialog-box is displayed.



22. Specify the print-sharing parameters and click **Next>**. The following dialog-box is displayed.



23. Specify whether you want to print a test page and click **Finish**. If you chose to print a test page, the following dialog-box is displayed.



24. If the test page was not properly printed, click **Troubleshoot**. Otherwise, click **OK**. The following dialog-box is displayed.

25. The dialog-box displays the various settings specified in the wizard. Review the settings and click **Finish** to complete the process. To change settings, click **Back**.

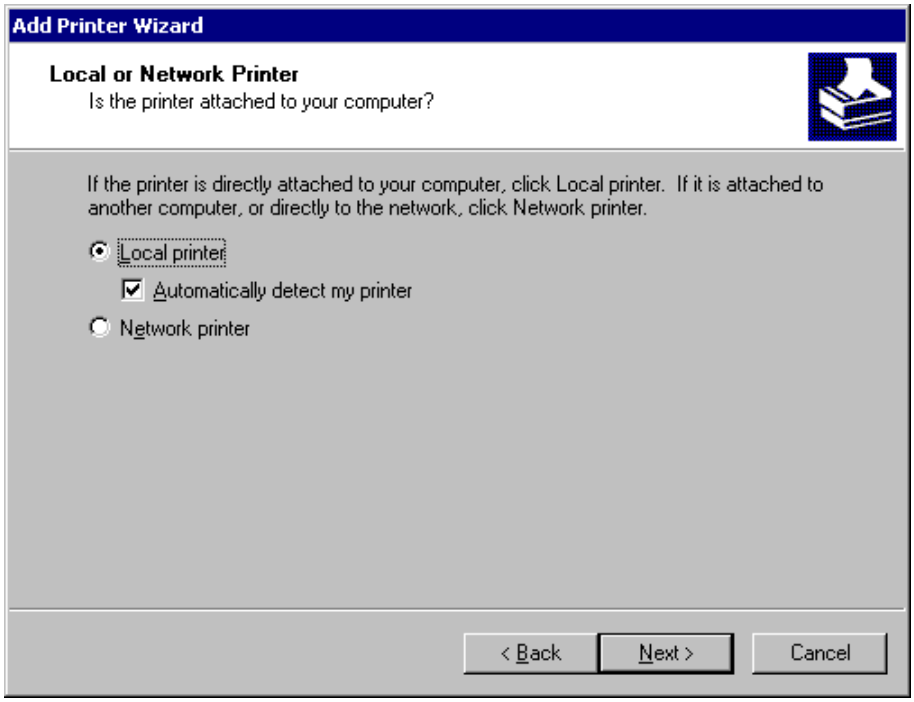
Windows 2000 Advanced Server

This section describes the procedure to configure a Windows 2000 Advanced Server to print on printers connected to LPD clients (*page 35*).

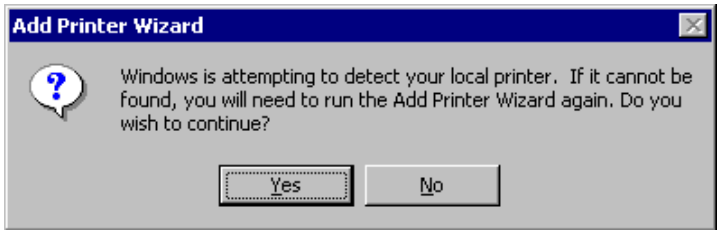
By default, the **File and Print Sharing for Microsoft Networks** service is installed along with the operating system. Perform the following procedure to add the LPD printer.

1. Select **Start**->**Settings**->**Printers**. The **Printers** window is displayed.
2. Double-click the **Add Printer** icon. The following dialog-box is displayed.

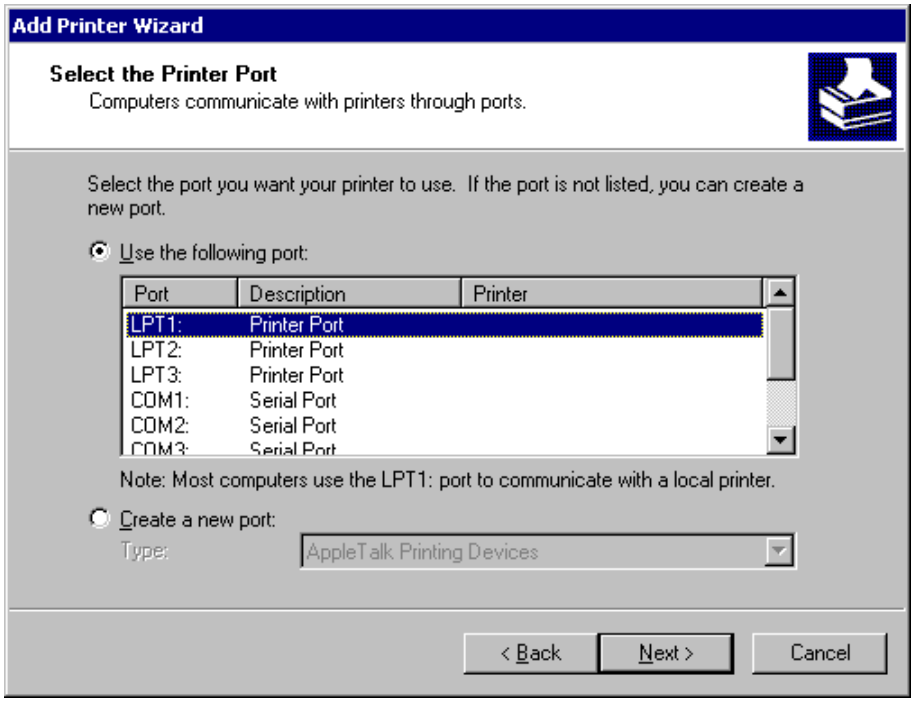
3. Click **Next>** to continue.



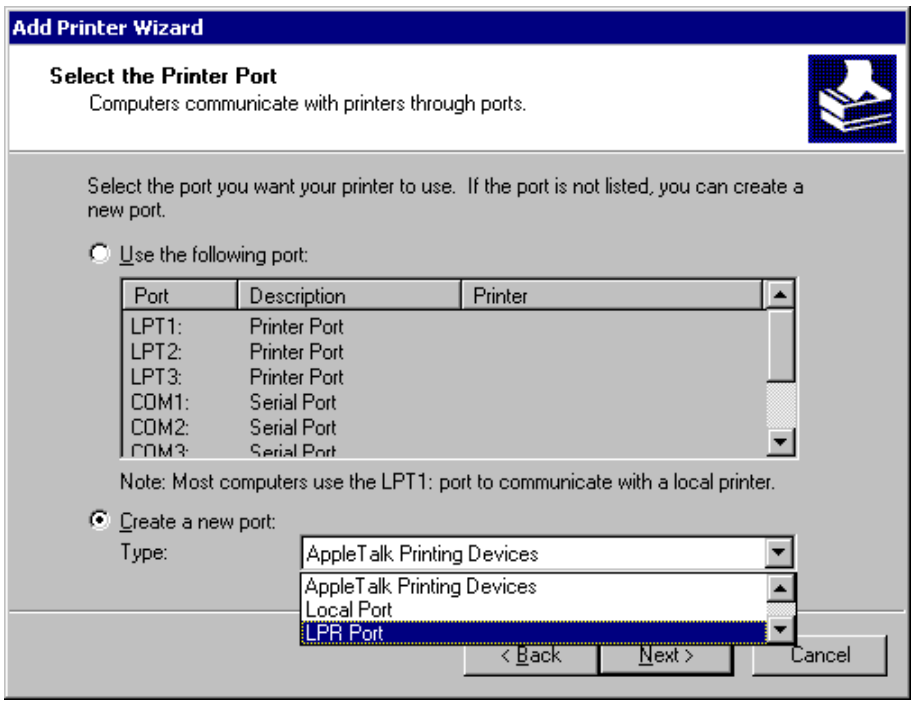
4. Select the **Local Printer** radio-button and the **Automatically detect my printer** check-box. Click **Next>** to proceed. The following prompt is displayed.



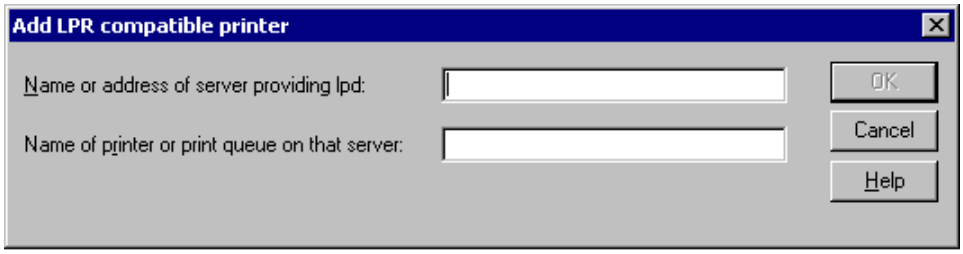
5. Click **Yes** to continue. The following dialog-box is displayed.



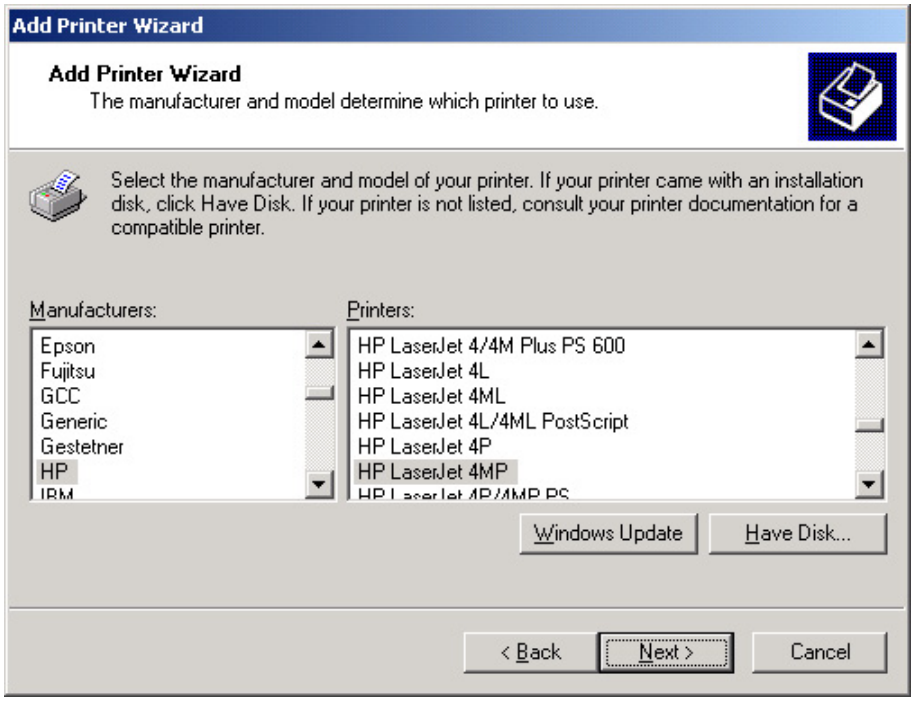
6. Select the **Create a new port** option and click on the **Type** drop-down list to view available options.



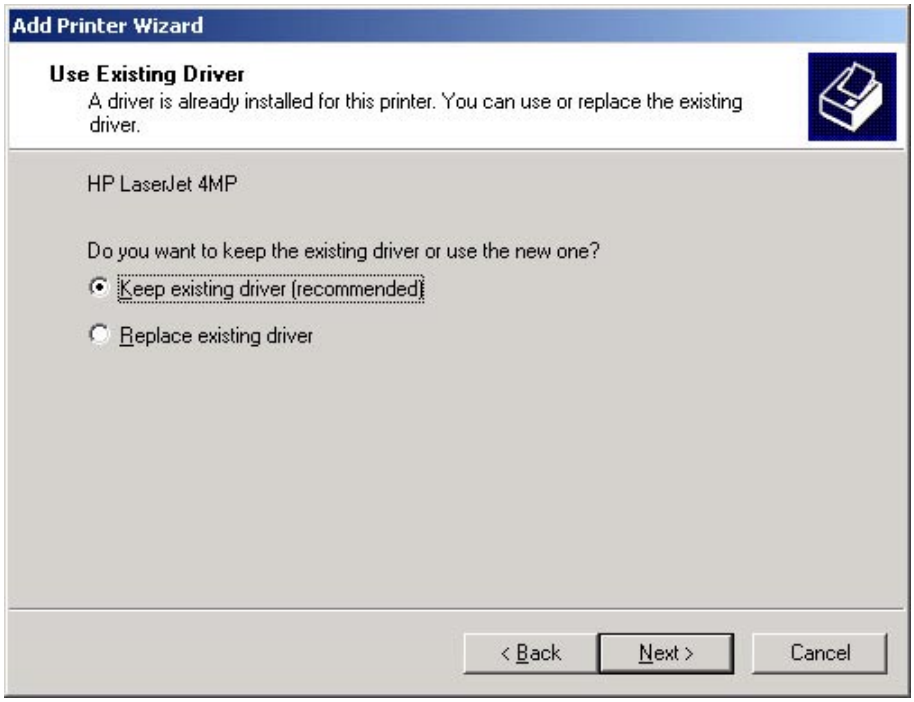
7. Select the **LPR Port** option and click **Next>** to proceed. The following dialog-box is displayed.



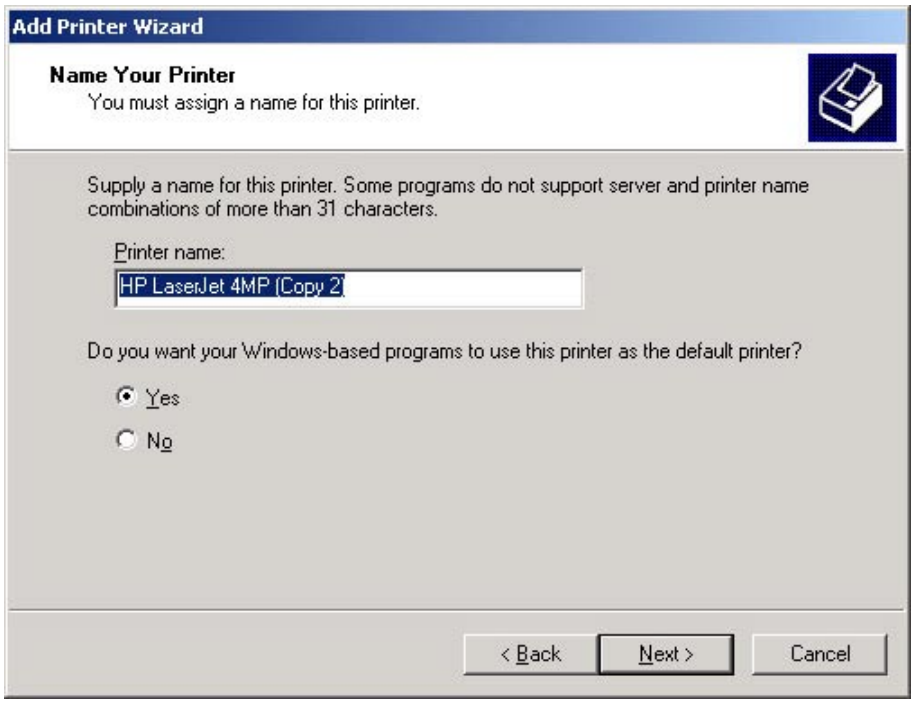
8. In the first text field, specify the IP address of the client that is configured as the LPD server. In the second text field, specify the name of the printer connected to the LPD server. The name should be the same as that specified while configuring the client as the LPD server. Click **OK**. The following dialog-box is displayed.



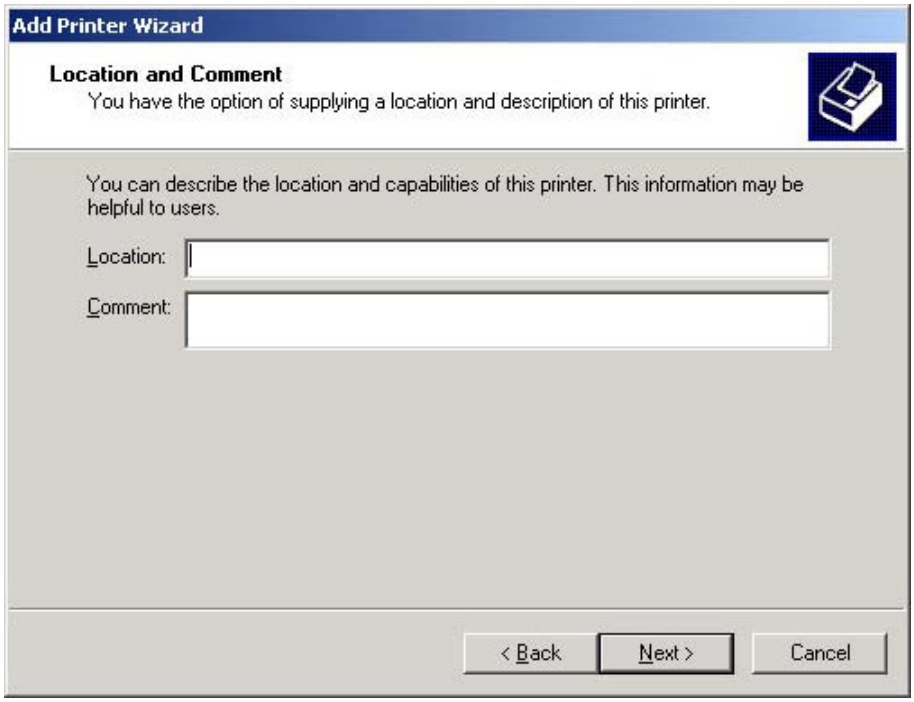
9. Select the make and model of the printer from the **Manufacturers** and **Printers** lists. Click **Next>** to continue. The following dialog-box is displayed.



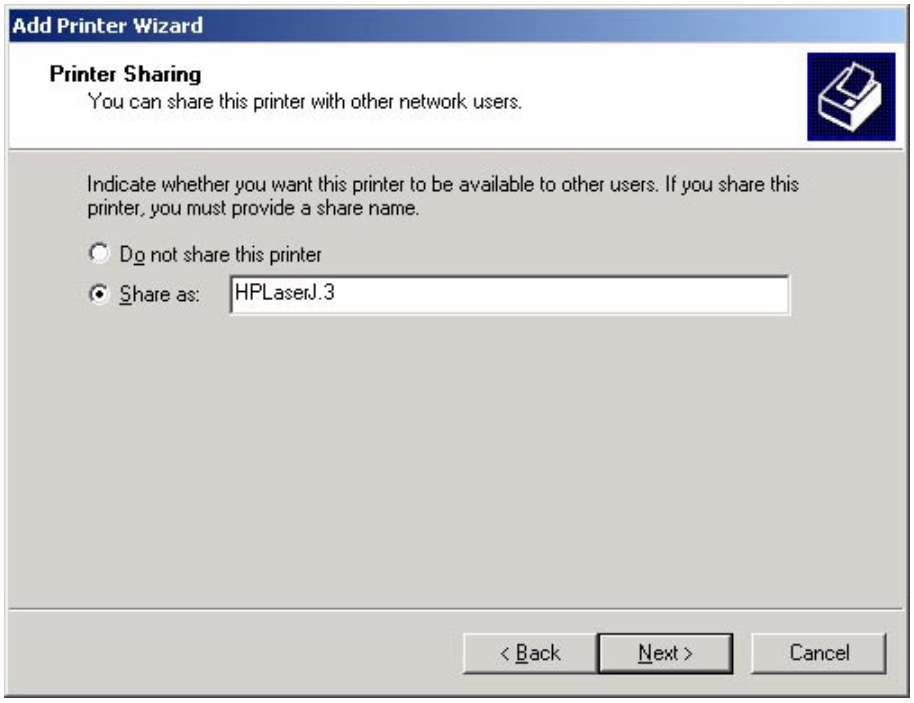
10. Select the appropriate radio-button to specify the printer driver and click **Next>**. The following dialog-box is displayed.



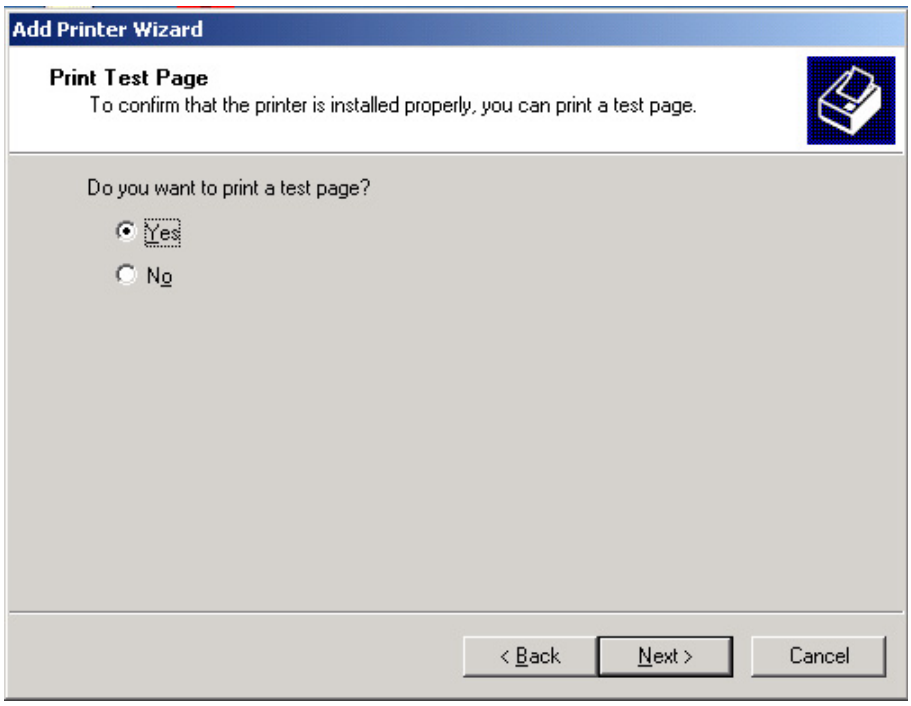
11. Specify a name for the printer and click **Next>**. The following dialog-box is displayed.



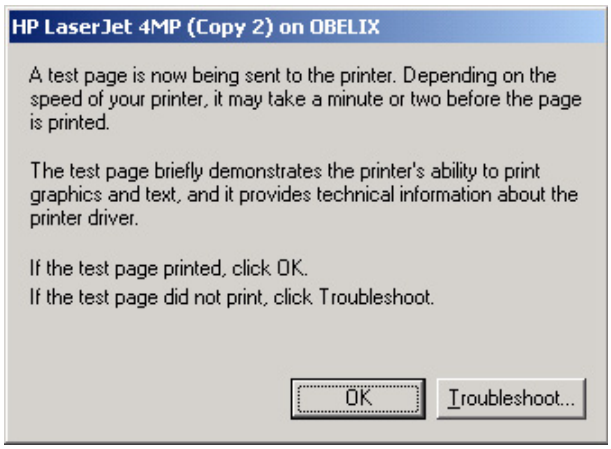
12. In the above dialog-box, you can enter the location of the printer and some comments describing the printer. These entries are optional. Click **Next>** to continue. The following dialog-box is displayed.



13. Specify the print-sharing parameters and click **Next>**. The following dialog-box is displayed.



14. Specify whether you want to print a test page and click **Finish**. If you chose to print a test page, the following dialog-box is displayed.



15. If the test page was not properly printed, click **Troubleshoot**. Otherwise, click **OK**. The following dialog-box is displayed.

16. The dialog-box displays the various settings specified in the wizard. Review the settings and click **Finish** to complete the process. To change settings, click **Back**.

SCO UNIX v.5.0.5 Server

This section describes the procedure to configure a SCO UNIX server to print on printers connected to LPD clients (*page 35*).

NOTE: TO PRINT POST-SCRIPT FILES TO NON-POST-SCRIPT PRINTERS (*FOR INSTANCE, DOT MATRIX PRINTERS*), ENSURE THAT THE UNIX HOST FROM WHICH THE PRINT COMMAND IS ISSUED HAS THE APPROPRIATE PRINTER-DRIVER.

1. Execute the following command at the shell prompt of the SCO UNIX server.

   scoadmin

2. From the resulting screen, select the **Printer** menu
3. Select the **Printer Manager->Printer->Add Remote->Unix** option.
4. Enter the IP address of the LPD server (*Windows CE client configured for LPD printing*) in the **Host** field.
5. Enter the name of the printer connected to the Windows CE client in the **Printer** field. This name must be same as the name specified while configuring the client as print-server.
6. Select **OK**.
7. From the **System** menu, select the **Print Services** option.
8. Select the **Remote Unix Print Service** option by pressing the spacebar.
9. Select **OK**.
10. Select **Host->Exit** and then **File->Exit** to return to the shell prompt.
11. Enter the IP address of the LPD server (*Windows CE client configured for LPD printing*) in the following files:

    /etc/hosts.lpd

    /etc/hosts.equiv

To print from the SCO UNIX server to the printer connected to the LPD client, execute the following command at the shell prompt: `lp -d <printer> <file>`

where <printer> is the name of the printer (*as specified in step 5 of the above procedure*) and <file> is the name of the file to be printed.

Red Hat Linux Server

This section describes the procedure to configure a Red Hat Linux server to print on printers connected to LPD clients (*page 35*).

NOTE: TO PRINT POST-SCRIPT FILES TO NON-POST-SCRIPT PRINTERS (*FOR INSTANCE, DOT MATRIX PRINTERS*), ENSURE THAT THE LINUX HOST FROM WHICH THE PRINT COMMAND IS ISSUED HAS THE APPROPRIATE PRINTER-DRIVER.

1. Execute the following command at the shell prompt:

   printtool

2. From the resulting screen, select the **Add** button.
3. Select the **Remote Unix (lpd) Queue** option.
4. Select **OK**.

5. Enter the IP address of the LPD server (*Windows CE client configured for LPD printing*) in the **Remote Host** field.
6. Enter the name of the printer connected to the Windows CE client in the **Queue** field. This name must be same as the name specified while configuring the client as print-server.
7. Click on the **Input Filter** button. After selecting the make/model of the printer, click **OK**.
8. From the **LPD** menu, select the **Restart lpd** option.

To print from the Linux server to the printer connected to the LPD client, execute the following command at the shell prompt: `lpr -P<printer> <file>`

where <printer> is the name of the printer (*as specified in step 6 of the above procedure*) and <file> is the name of the file to be printed.

Upgrading Client Firmware

Firmware of thin clients can be upgraded using **inControl for Terminals**, a powerful client-management utility that allows the system administrator to control and configure multiple clients from a remote server.

The software and relevant documentation for inControl is provided in the CD supplied with the product

Troubleshooting

This chapter contains basic solutions to problems you may encounter while using the client. If a problem persists even after you implement the solutions provided here, please contact your dealer, or I-O Corporation, 1490 North 2200 West, Suite 100, Salt Lake City, UT 84116 801-973-6767, visit our web site www.iocorp.com, or e-mail support@iocorp.com.

TIP: THE DIAGNOSTICS TAB OF THE **TERMINAL PROPERTIES** DIALOG-BOX CONTAINS IMPORTANT INFORMATION ABOUT CLIENT -HARDWARE AND -FIRMWARE THAT WOULD BE USEFUL TO SERVICE TECHNICIANS IN DIAGNOSING THE PROBLEM.

	Problem	*Solution*
1.	• The mouse does not work when the client is switched on, though the **Terminal Connection Manager** or the **Setup Wizard** is displayed.	✓ Ensure that the mouse is plugged into the PS/2 Mouse port on the rear panel of the client. ✓ Ensure that you are using the mouse provided with the client. The client supports only Logitech and Microsoft models.
2.	• The client cannot detect a keyboard.	✓ Ensure that you are using a PS/2 Windows keyboard.
3.	• The parallel printer connected to the client does not print.	✓ Check whether the protocol you are using supports printing. ✓ Ensure that the printer is plugged into the proper power outlet and switched on. ✓ Ensure that the printer is online. ✓ Check the connection between the printer and the client. ✓ Ensure that the printer is properly configured in the application-server's Print Manager ✓ Ensure that the printer has not been 'paused'. ✓ If you are using ICA as the connection protocol, ensure that you have correctly configured the Client Name.
4.	• The serial printer connected to the client does not print.	✓ Ensure that the printer is plugged into the proper power outlet. ✓ Ensure that the printer is switched on and online. ✓ Check the connection between the printer and the client. ✓ Ensure that client-serial-port and the printer are identically configured. They must use the same handshaking protocol. Refer to your printer manual for information about printing from a serial connection. ✓ Ensure that the printer is configured properly in the application server's Print Manager and that it has not been paused.

	Problem	Solution
5.	• The display is not satisfactory.	✓ Check whether your display unit supports the display setting selected. If it does not, perform one of the following procedures ✓ Request your system administrator to change the display setting of the client using the *inControl for Terminals* utility. OR ✓ Connect a display unit that supports the selected setting. Change the display setting to 800 x 600 @ 60 Hz. Disconnect the display unit and reconnect the previous display unit.
6.	• Mouse movement is out of control.	✓ Switch off and restart the system. Do not move the mouse until the **Terminal Connection Manager** is displayed.
7.	• A message "Insufficient Memory to Run application" is displayed.	✓ This happens when multiple connections are active. The system displays a list of all open programs. Select those that can be closed. This will free some memory and allow active applications to run.

Glossary

Cache

A place in memory where a copy of recently used or frequently accessed data is stored. For instance, web pages that you visit are stored in your browser's cache directory on the hard disk. That way, when you return to a page you've recently visited, the browser can get it from the cache rather than the remote server. This reduces access time and network traffic.

CDS

***C**itrix **D**evice **S**ervices* provides basic ICA connectivity of Windows-based terminals and other ICA devices to Microsoft Windows NT 4.0 TSE Server, Terminal Server Edition and Windows 2000 Server.

DHCP

***D**ynamic **H**ost **C**onfiguration **P**rotocol* is a protocol using which network administrators can centrally manage and automate the assignment of IP addresses in a network. Without DHCP, a fixed IP address must be assigned manually to each computer in the network.

DNS

***D**omain **N**ame **S**ystem* is the method using which Internet domain names are translated into IP addresses. An Internet domain name is a meaningful and easy-to-remember 'handle' for an IP address. The DNS method is based on DNS servers, which contain pre-defined and maintainable lists of domain names and IP addresses. Without this system, users would have to always remember and use IP addresses to access network computers or to browse the Internet.

Download

Downloading is the transmission of a file from one computer system to another, usually smaller computer system. From the Internet-user's point-of-view, to download a file is to request it from another computer (or from a Web page on another computer) and to receive it.

Encryption

A security measure that involves converting data to a form that cannot be easily understood by unauthorized systems. Simple encryption may involve substituting letters for numbers and rotating letters in the alphabet. More complex encryption is based on computer algorithms that rearrange the data bits in digital signals. To recover the contents of an encrypted transmission, the correct *decryption algorithm (key)* would be required.

EPROM

***E**rasable **P**rogrammable **R**ead-**O**nly **M**emory* is a special type of memory that retains its contents until it is exposed to ultraviolet light. The ultraviolet light clears its contents, making it possible to reprogram the memory. To write to and erase an EPROM, a special device called a PROM programmer or PROM burner would be required.

Firewall

A mechanism to protect resources of a private network from users from other networks. For instance, an enterprise with an Intranet could install a firewall to prevent outsiders from accessing its own data resources, and to restrict its own users' access to external resources.

A firewall typically consists of a set of rules incorporated in a router program, which is usually installed in a designated computer separate from the rest of the network. The firewall could also include a proxy-server that makes network requests on behalf of workstation users.

The destination and/or source of each network packet is screened for compliance with the firewall-rules before being forwarded.

Firmware

A computer-program or software stored in PROM or EPROM.

Flow control

The management of the flow of data between computers or devices or between nodes in a network so that the data can be handled at an efficient pace. Too much data arriving before a device can handle it causes data overflow, meaning either that the data is lost or must be retransmitted.

Flow control is usually implemented using a software protocol (Xon/Xoff signals) or hardware signals (CTS/RTS: Clear to Send/Ready to Send). In a network, flow control can also be applied by refusing additional device connections until the flow of traffic has subsided.

FTP

***F**ile **T**ransfer **P**rotocol* is a protocol to exchange files between computers on the Internet. Like HTTP (*HyperText Transfer Protocol*) which transfers web pages, and SMTP (*Simple Mail Transfer Protocol*) which transfers email, FTP is an application protocol that uses the TCP/IP protocol to transfer files from one computer to another.

Gateway

A point in the network that acts as the entrance to another network. Computers that control traffic within a network or at an Internet Service Provider are gateway nodes. In an enterprise network, gateway servers usually also act as proxy and firewall servers. A gateway server is often associated with a router that knows where an incoming packet must be directed, and a switch that furnishes the actual path in and out of the gateway for a given packet.

GUI

***G**raphical **U**ser **I**nterface* is a graphical (rather than purely textual) user interface to a computer.

Most major operating systems today provide a graphical user interface. Applications typically use the elements of the GUI that come with the operating system and add their own graphical user interface elements and ideas. Typically GUI includes elements of such as windows, pull-down menus, buttons, scroll bars, iconic images and wizards

Hz

Hertz is a unit of frequency (*change in state/cycle of a signal*) of one cycle per second.

ICA

***I**ndependent **C**omputing **A**rchitecture* is a technology (*developed by Citrix Systems, Inc*.), which provides the foundation for converting a client device to a Thin Client. ICA functions by separating the application logic from the user interface. While the application executes solely on the server, client-users can see and work with the application's interface, when in fact the application actually executes on the server.

Internet

(*or Net*) is a worldwide system of computer networks in which users at any one computer can get information from any other computer. Physically, the Internet uses a portion of the total resources of the currently existing public telecommunication networks. Technically, what distinguishes the Internet is its use of a set of protocols called TCP/IP.

The most widely used part of the Internet is the World Wide Web (*WWW or Web*). The outstanding feature of WWW is hypertext, a method of instant cross-referencing. Web pages can be viewed or browsed using browsers such as Netscape Navigator and Microsoft Internet Explorer.

Intranet

A private network within an enterprise that may consist of many inter-linked LANs and may use leased lines in a WAN. Typically, an Intranet includes connections through gateway to the outside Internet. The main purpose of an Intranet is to share company information and computing resources among employees. An Intranet can also be used to facilitate working in groups and for teleconferences.

An Intranet uses TCP/IP, HTTP and other Internet protocols and in general, looks like a private version of the Internet. When part of an Intranet is made accessible to users outside the enterprise, that part becomes part of an Extranet.

IP Address

A unique 32-bit number that identifies each sender or receiver of information that is sent in a packet across the Internet. When you request an HTML page or send e-mail, the IP part of TCP/IP includes your IP address in the message. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

The IP address is usually expressed as four decimal numbers, each representing eight bits, separated by periods. This is sometimes known as dot-address or dotted quad notation (Example: 192.16.4.12).

LAN

***L**ocal **A**rea **N**etwork* is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data that are shared in common by multiple computer users.

MAC Address

***M**edia **A**ccess **C**ontrol Address* is the unique hardware number of a computer in a network.

MetaFrame

An application-server software from Citrix, which incorporates Citrix's ICA protocol and provides a method to deploy, manage and access applications in a client-server networking environment.

Modem

A device that modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional telephone line, and demodulates the incoming analog signal and converts it to a digital signal for the digital device.

Network

A series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain subnetworks.

The most common configurations of networks include the bus, star and token ring topologies. Networks can also be characterized in terms of spatial distance as LANs, metropolitan area networks, and WANs.

OSD

***O**n-**S**creen **D**isplay* is a feature available in certain computer-monitors that allows users to view and configure display parameters using an on-screen user-interface.

Packet

A packet is the unit of data that is routed between an origin and a destination on the Internet. When any file is sent from one place to another on the Internet, the TCP layer of TCP/IP divides the file into chunks of an efficient size for routing. Each chunk (*or packet*) is separately numbered, and includes the IP address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file by the TCP layer at the receiving end.

Parallel Port

An interface that can transfer more than one bit of data simultaneously. Typically, parallel ports are used to connect printers, computers and other devices that need relatively high bandwidth. A parallel port is often called a Centronics interface after the company that designed the original standards for parallel communication between a computer and printer.

A newer type of parallel port, which supports the same connectors as the Centronics interface, is the EPP (Enhanced Parallel Port) or ECP (Extended Capabilities Port). Both of these parallel ports support bi-directional communication and transfer rates ten times as fast as the Centronics port.

Ping

A basic Internet program to verify whether a particular IP address exists and can accept requests. Ping can also be used to check the response-time of a host and to find out the IP address of a domain.

The ping utility operates by sending a packet to a designated address and waiting for a response.

Port Number

A number to identify the specific process to which an Internet- or other network-message is to be forwarded when it arrives at a server. For the TCP and UDP protocols, a port number is a 16-bit number that is included in the header appended to a message unit. This port number is passed logically between client and server transport layers and physically between the transport layer and the IP layer and forwarded on.

For example, a client might request a server for a file to be served from that server's File Transfer Protocol (FTP) process. To pass the request to the FTP process in the server, the TCP layer in the client appends the number 21 to the request (21, is by convention the 16-bit port number associated with an FTP request). At the server, the TCP layer reads the port number (21) and forwards the request to the FTP program at the server.

Some services or processes have conventionally assigned permanent port numbers. These are known as 'well-known port numbers'. In other cases, a port number is assigned temporarily (for the duration of the request and its completion) from a range of assigned port numbers. This is called an ephemeral port number.

PPP

***P**oint-to-**P**oint **P**rotocol* is a protocol for communication between two computers over a serial interface. For instance, an Internet Service Provider may provide a PPP connection for accepting and responding to requests from an Internet user.

PROM

***P**rogrammable **R**ead-**O**nly **M**emory* is a memory chip on which data can be written only once. Once data has been written onto a PROM, it remains there permanently. Unlike Random Access Memory (RAM), PROMs retain their contents when the device on which they are installed is turned off.

The difference between PROM and Read Only Memory (ROM) is that PROM is manufactured as blank memory, whereas ROM is programmed during the manufacturing process.

Data can be written onto PROM chips, using special devices called PROM-Programmers or PROM Burners.

Protocol

A special set of rules that end-points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection. There are hardware telephone protocols. There are protocols between each of several functional layers and the corresponding layers at the other end of a communication. Both end-points must recognize and observe a protocol. Examples: TCP/IP, HTTP and FTP.

Proxy Server A server in the network that acts as an intermediary between a user (computer) and the Internet. Enterprises can use proxy servers to implement security, administrative control, and caching. Depending on the network implementation, the proxy server may be associated with, or form part of, the gateway server, the firewall server and the cache server.

RDP ***R**emote **D**esktop **P**rotocol* a protocol developed by Microsoft to provide connectivity between Thin Clients and Windows NT 4.0 TSE/2000 Servers.

Serial Port An interface that can transmit only 1-bit at a time. Typically, serial ports are used to connect devices such as modems and serial printers.

Server A computer or program that provides services to other computers or programs. In the client/server context, a server is a program that awaits and fulfills requests from client programs in the same or other computers. A given application in a computer may function as a client, which requests for services from other programs and serves requests from other programs.

Server Farm A group of computers acting as a server and housed in a single location. A server farm is sometimes called a server cluster. A Web server farm is either a Web site that has more than one server, or an Internet service provider that provides Web hosting services using multiple servers.

In a business network, a server farm might provide centralized access control, file access, printer sharing, and backup for workstation users. The servers may have individual operating systems or a shared operating system. They may also be set up to provide load balancing when there are many server requests. Typically, in a server farm if one server fails, another can act as backup.

Socks A protocol used by proxy servers to accept requests from users in a network and forward them over the Internet. The protocol uses sockets to represent and keep track of individual connections. The client side of Socks is built into Web browsers and the server side can be added to a proxy server. The Socks server handles requests from clients within a company's firewall and either allows or rejects connection requests, based on the requested Internet destination or user identification.

Subnet An identifiably separate part of an organization's network: typically, all the computers at one geographic location, in one building, or on the same LAN. Networks divided into subnets can connect to the Internet with a single shared network address. Without subnets, each physical sub-network could have a separate connection to the Internet, resulting in unnecessary use of scarce network numbers that the Internet has to assign. Besides, in such cases, gateways outside the network would need to know about and manage routing that should ideally be handled within the organization.

Once a data-packet has arrived at a gateway, it is routed within the organization's internal gateways using the subnet number. Using a subnet mask, the router determines the subnet to which the packet must be directed.

TCP/IP ***T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol* is the basic communication language of the Internet. It can also be used as the communications protocol in a private network. The TCP layer converts outgoing messages or files into packets, and assembles incoming packets into the original messages or files. The IP layer handles the address part of each packet so that it gets to the right destination.

Telnet

A method to access one computer (*host*) from another. More technically, Telnet is a user command based on the TCP/IP protocol to access remote computers. While the HTTP and FTP protocols allow you to only request specific files from remote computers, Telnet allows you to actually logon as a user of that computer.

Terminal Emulation

The ability of a computer (which is programmable and therefore 'smart') to appear to be a 'dumb- (non-programmable) terminal', so that it can be used to interact with another computer with its own proprietary connection interface.

Typically, an enterprise with mainframe computers installs a terminal emulation program in all the computers in the network. Users can work locally with Windows-based or other workstation applications and also open a window and work directly with mainframe applications.

Thin Client

A low-cost, centrally managed computing device devoid of typical peripheral devices such as CD-ROM and diskette drives. The term derives from the fact that small computers in networks tend to be clients and not servers. Since the idea is to limit the capabilities of these computers to only essential applications, they tend to be remain 'thin' in terms of pre-loaded client-applications.

Touch screen

A touch screen is a touch-sensitive computer display screen that allows users to interact with the computer by touching specific areas on the screen. Touch screens are typically used in bank-ATM, information kiosk and computer-based training applications. They are also used in systems designed to help individuals who have difficulty using a mouse or keyboard.

UDP

***U**ser **D**atagram **P**rotocol* is a communications method that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol. UDP is an alternative to TCP and, together with IP, is sometimes referred to as UDP/IP.

UDP also uses the Internet Protocol to actually get a data unit (*Datagram*) from one computer to another. Unlike TCP however, UDP does not divide messages into packets and reassemble them at the other end. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP.

URL

***U**niform **R**esource **L**ocator* is the address of a resource accessible on the Internet. The type of resource depends on the Internet application protocol. Using the World Wide Web's protocol – HTTP - the resource can be an HTML, an image file, a Java applet or any other file supported by HTTP. The URL contains the name of the protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer.

For instance, the URL http://www.iocorp.com/ptrcon/ptrcon.htm describes a Web page located on a computer named www.iocorp.com . The specific resource is a file named 'ptrcon.htm'.

WAN

A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more LANs. Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

WinFrame WinFrame is a software product from Citrix that, together with a Windows NT 4.0 TSE operating system, allows a server to provide Windows applications and data to attached clients.

WINS ***W****indows* ***I****nternet* ***N****aming* ***S****ervice*, is a part of Microsoft Windows NT 4.0 TSE/2000 Servers that manages the association of computer-names with corresponding IP addresses. It automatically creates a computer name-IP address mapping entry in a table, ensuring that the name is unique. When a computer is moved to another geographic location, the subnet part of the IP address is likely to change. Using WINS, the new subnet information is automatically updated in the WINS table.

WTS ***W****indows* ***T****erminal* ***S****erver* is a server-program from Microsoft running on its Windows NT 4.0 TSE (or higher) operating system that provides the graphical user interface of the Windows desktop to user terminals. WTS has three parts: the multi-user core server, RDP that enables the Windows desktop interface to be sent to the terminals, and the Terminal Server Client that is available in each terminal.

Manufacturer's Warranty & Repair Policy

Manufacturer's Three Year Limited Warranty

(United States)

The following warranty applies only to products purchased and operated within the United States.

I-O Corporation (I-O) warrants this product against defects in material and workmanship for a period of three years commencing from date of purchase by the original customer, when operated and maintained in accordance with I-O's published specifications. I-O's liability shall be limited, at its option and expense, to refund to buyer the actual amount paid by buyer or to repair or replace any defective or nonconforming product or part thereof, F.O.B. I-O's authorized repair depot. Buyer may obtain a replacement product by meeting the terms of the I-O Customer On-Site Exchange Repair Policy in effect at the time of the request.

THE EXPRESS WARRANTY SET FORTH ABOVE IS IN LIEU OF ALL OTHER EXPRESS OR IMPLIED WARRANTIES. OTHERWISE, THE PRODUCTS ARE SOLD AS IS WITHOUT FURTHER OBLIGATION OR LIABILITY ON THE PART OF I-O. I-O EXPRESSLY EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

EXCEPT AS EXPRESSLY SET FORTH HEREIN, IN NO EVENT SHALL I-O BE LIABLE FOR ANY CLAIMS OR DAMAGE ARISING DIRECTLY OR INDIRECTLY FROM THE FURNISHING OR FAILURE TO FURNISH PRODUCTS, SPARE OR REPLACEMENT PARTS, INFORMATION OR SERVICES HEREUNDER. UNDER NO CIRCUMSTANCES SHALL I-O BE LIABLE IN ANY WAY FOR INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO LOST BUSINESS OR PROFITS, WHETHER OR NOT FORESEEABLE AND WHETHER OR NOT BASED ON BREACH OF WARRANTY, CONTRACT, OR NEGLIGENCE.

I-O shall not be liable for non-performance or delays hereunder due to causes beyond its control. These shall include, but not be limited to, acts of God, wars, strikes, fires, flood, storm, earthquake, shortages of labor or materials, labor disputes, transportation embargoes, acts of any government or agency thereof.

MODIFICATIONS OR RECONFIGURATION OF THE HARDWARE BY ANYONE OTHER THAN I-O OR I-O'S AUTHORIZED REPAIR FACILITY WILL VOID THIS HARDWARE WARRANTY.

Customer On-Site Exchange Repair Policy

Terms, Conditions, and Limitations
Effective May 1, 1994[a]

For products covered by the I-O Corporation (I-O) Manufacturer's Limited Warranty (United States), I-O's Customer On-Site Exchange (COE) Repair Policy provides customers with a replacement unit for a defective product, subject to the following terms and conditions:

Call Customer Support

If a product fails, call I-O Customer Support for assistance at (801) 972-1446.

Verify Product Failure

I-O will verify the product serial number, warranty coverage and product failure.

You are responsible for assisting in verifying the product failure.

When I-O Customer Support verifies a product failure they will issue a Return Merchandise Authorization (RMA) number for the failed product.

Replacement Units

Replacement units are shipped from I-O's stock of refurbished units, subject to availability.

Replacement units carry the same warranty as remaining on the original product.

I-O's COE Repair Policy applies only to warranted product failures. Buyer guarantees payment for non-warranted product repairs or replacement.

Return Your Failed Unit

When you return the failed product it must be shipped freight prepaid. Always note the RMA number on the outside of the package.

Buyer will pay reasonable labor and handling charges for each product returned for repair which is found to have no defect.

Install the Replacement Unit

You are responsible for installing the replacement unit.

After receiving the replacement unit please call I-O Customer Support if any assistance is required.

[a] I-O reserves the right to change the terms and conditions of this policy without notice.

Manufacturer's Three Year Limited Warranty
(International)

The following warranty applies only to products purchased or operated outside the United States.

I-O Corporation (I-O) warrants this product against defects in material and workmanship for a period of three years commencing from date of purchase by the original customer, when operated and maintained in accordance with I-O's published specifications. I-O's liability shall be limited, at its option and expense, to refund to buyer the actual amount paid by buyer or to repair or replace any defective or nonconforming product or part thereof, F.O.B. I-O's authorized repair depot. Buyer may obtain warranty service by meeting the terms of the I-O Return-to-Depot Repair Policy in effect at the time of the request.

THE EXPRESS WARRANTY SET FORTH ABOVE IS IN LIEU OF ALL OTHER EXPRESS OR IMPLIED WARRANTIES. OTHERWISE, THE PRODUCTS ARE SOLD AS IS WITHOUT FURTHER OBLIGATION OR LIABILITY ON THE PART OF I-O. I-O EXPRESSLY EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

EXCEPT AS EXPRESSLY SET FORTH HEREIN, IN NO EVENT SHALL I-O BE LIABLE FOR ANY CLAIMS OR DAMAGE ARISING DIRECTLY OR INDIRECTLY FROM THE FURNISHING OR FAILURE TO FURNISH PRODUCTS, SPARE OR REPLACEMENT PARTS, INFORMATION OR SERVICES HEREUNDER. UNDER NO CIRCUMSTANCES SHALL I-O BE LIABLE IN ANY WAY FOR INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO LOST BUSINESS OR PROFITS, WHETHER OR NOT FORESEEABLE AND WHETHER OR NOT BASED ON BREACH OF WARRANTY, CONTRACT, OR NEGLIGENCE.

I-O shall not be liable for non-performance or delays hereunder due to causes beyond its control. These shall include, but not be limited to, acts of God, wars, strikes, fires, flood, storm, earthquake, shortages of labor or materials, labor disputes, transportation embargoes, acts of any government or agency thereof.

MODIFICATIONS OR RECONFIGURATION OF THE HARDWARE BY ANYONE OTHER THAN I-O OR I-O'S AUTHORIZED REPAIR FACILITY WILL VOID THIS HARDWARE WARRANTY.

Return-to-Depot Repair Policy

Terms, Conditions, and Limitations

Effective May 1, 1994[a]

For products covered by the I-O Corporation (I-O) Manufacturer's Limited Warranty (International), I-O's Return-to-Depot (RTD) Repair Policy provides customers with warranty service for a defective product, subject to the following terms and conditions:

Call Customer Support

If a product fails, call I-O Customer Support for assistance at:

(801) 972-1446 for all locations outside the United States.

Verify Product Failure

I-O will verify the product serial number, warranty coverage and product failure.

You are responsible for assisting in verifying the product failure

When I-O Customer Support verifies a product failure they will issue a Return Merchandise Authorization (RMA) number to authorize return of the failed product.

Select Your Preferred Repair Location

I-O's Customer Support Representative will assist you in identifying the nearest I-O authorized repair depot.

I-O's Customer Support Representative will provide you with an RMA transmittal form referencing the assigned RMA number and the authorized repair depot address.

Return Your Failed Unit

Return the failed product to the I-O authorized repair depot previously identified, enclosing the RMA transmittal form. When you return the failed product it must be shipped freight prepaid.

I-O's RTD Repair Policy applies only to warranted product failures. Buyer guarantees payment for non-warranted product repairs.

Buyer will pay reasonable labor and handling charges for each product returned for repair which is found to have no defect.

Install Your Repaired Unit

I-O's authorized repair depot will service the faulty unit and return it to you, freight prepaid.

You are responsible for installing the returned unit.

After receiving the repaired unit please call I-O Customer Support if any assistance is required.

[a]I-O reserves the right to change the terms and conditions of this policy without notice.

Index

L

M

N

O

P

R

S

T

U

W