IBM Network Station

Version 2 Release 1 PTF 5

Using ICA for

Windows Application Access

February 18, 2000

IBM Copyright

Citrix Copyright and acknowledgment

Contents

Introduction and Overview

The ICA Client is a V2R1 IBM Network Station application that provides access to a Windows session running on high-performance Citrix servers. Once the connection to a Citrix server is established, you can access Windows applications and work with files in a similar way to working on a local PC.

The ICA Client displays the Windows session in a separate window on the IBM Network Station screen, and is fully integrated with your other IBM Network Station applications. You can cut and paste text and graphics between Windows applications in the ICA Client window and your other applications.

Your IBM Network Station's mouse and keyboard can be used with Windows applications in the usual way, and you can set up key mappings to enable you to enter PC keys not available on your IBM Network Station's keyboard.

Citrix Servers

Citrix WinFrame and Citrix MetaFrame are fast and easy Windows NT application server solutions for delivering Windows applications to the IBM Network Station and other desktops, including PCs, Apple Macintosh computers, X terminals, and UNIX workstations. Citrix server software usually runs on a high-performance PC, and a single-processor Citrix server will typically support up to 15 simultaneous client connections.

The Citrix server communicates with the ICA Client over a standard TCP/IP network connection.

Independent Computing Architecture (ICA) protocol

ICA is a general-purpose presentation services protocol owned by Citrix Systems. Conceptually similar to the UNIX X-Windows protocol, ICA allows an application's user interface to execute with minimal resource consumption on a client machine, while application logic executes on the WinFrame or MetaFrame multiuser application server.

The ICA protocol has been specially designed for transmitting Windows graphical display data, and keyboard and mouse input, over a network connection.

The key features of the ICA protocol that help to achieve the high performance are:

- Intelligent command and object-specific compression
- Intelligent caching of Windows objects including bitmaps, brushes, glyphs, and pointers
- Run length encoding

The ICA protocol is designed to be client independent.

More information about the ICA protocol is available from the Citrix World Wide Web page at http://www.citrix.com/

ICA Clients

An ICA Client application allows you to define and initiate ICA connections. On the IBM Network station, an ICA Remote Application Manager presents a list of the ICA connection definitions you have set up, and allows you to initiate an ICA connection to a Citrix Server.

Once you are connected to a Citrix server, the ICA Client application presents the ICA Client window to handle communication with the Citrix server and provide the display, keyboard, and mouse interface between the server and your IBM Network Station.

The ICA Remote Application Manager also allows you to create new connection definitions, or edit the definitions of existing connections.

For each connection you can define the following features:

Window size and borders

The ICA Client window size can be set to one of four predefined window sizes, full screen size, or a custom size (up to the greater of 1280x1024 or your IBM Network Station display size). Window borders and title bar can be turned off.

Number of colors

The ICA Client window can be set to 256 or 16 colors. This is an ICA Protocol limitation. At some future time, the ICA Protocol may be extended to support more than 256 colors, e.g., 16-bit TrueColor.

In addition, you can define default values for the window size and window colors, which are then used as the default for all new connection definitions.

Color approximation

Color approximation can be used if the IBM Network Station is running in PseudoColor mode. In this mode, differences in the palettes used between the ICA Client (and the Windows applications it displays) and the IBM Network Station may cause an annoying flashing that occurs when switching context. The ICA Client's color approximation scheme eliminates this flashing by using colors from the local desktop palette to display the ICA Windows sessions.

True Color

The ICA Client maps ICA protocol colors (16 or 256) to true color. Running the IBM Network Station in TrueColor mode provides the most compatible color management if the ICA Client is sharing screen space with any other program (including the window manager and desktop).

Remote Applications and Load Balancing

The ICA Client supports two types of connections: ICA connections and remote applications.

An ICA connection allows a user to access a Citrix desktop. The user can run any applications available on the desktop, in any order.

A remote application is a predefined application and its associated environment (for example directories and initialization files) that execute on a remote Citrix server.

There are several ways to define a remote application:

- By defining an ICA connection that directly executes an application.
- By defining an ICA connection that points to a published application created using the Published Application Manager on the Citrix server. This method also supports load balancing.

See Chapter 5, "Application Publishing," in the MetaFrame Administrator's Guide , or the WINFRAME System Guide for more information about application publishing.

The Load Balancing Services can be used with multiple Citrix servers to provide load balancing capabilities. Citrix load balancing support lets you define a remote application that runs on a predefined set of Citrix servers. When a user launches the remote application, the Citrix load balancing software uses a tunable algorithm to select a server to execute the application. The load balancing parameters are configurable and can be tuned to provide maximum throughput and system availability.

Another advantage of load balancing is increased reliability. By configuring a pool of servers that are capable of running your users' applications without your users ever needing to know which server is actually running the application, you can easily bring servers off-line for maintenance without affecting application availability, or add more servers for increased performance.

See Chapter 5, "Application Publishing," in the MetaFrame Administrator's Guide, or the WIN FRAME System Guide for more information about load balancing.

Printer mapping

You can redirect printing jobs from applications you are running on a Citrix server and print them to a printer connected to your IBM Network Station.

The ICA Client supports any spooled printer available from your IBM Network Station, as long as the associated printer driver is installed on the Citrix server.

If a Network Station printer has been defined with an associated NT printer device driver name then the ICA Client will automatically create the printer on the ICA Server during session logon and delete it when the session ends. Printers can also be explicitly created by using the NT Printer Wizard to add one or more printers for use in the ICA session.

Audio mapping

Audio mapping allows your client computer to play sounds generated by applications running on the Citrix server. ICA Client audio support includes configurable sound quality levels that allow you to customize sound quality based upon the amount of bandwidth available.

NT Server Audio

- Wave sound only (server may convert other formats to Wave)
- Midi music not supported
- CD audio not supported
- no sound card is required on the server

Supported audio characteristics

- linear PCM
- 8 and 16 bit
- 8, 11, 22, and 44 Khz
- mono and stereo

Device control (e.g. volume) is not supported

COM port mapping

Client COM port mapping allows devices attached to the client computer's COM ports to be used from ICA sessions on a Citrix server. This allows local serial devices to be used by applications running on the Citrix server.

Data compression

Data compression reduces the amount of data transferred across the ICA session to increase performance over bandwidth-limited connections.

Caching

Caching stores commonly used graphical objects such as icons in a local cache on the client computer to reduce the amount of data sent over the connection. Caching commonly used bitmaps tends to increase performance, especially for bandwidth-limited connections.

The ICA Client employs both an internal transient cache and an external persistent cache.

Since the IBM Network Station does not have a hard disk, the external persistent cache is implemented as an in-memory file system which is created each time the Network Station is re-booted. By default, this in-memory file system is not enabled due to the finite amount of memory in the Network Station. (In this release, persistent caching must be enabled by following the ICA persistent caching directions in the /.profile file.)

Drive Mapping

Client drive mapping makes selected directories on the IBM Network Station available to the users when they connect to a Citrix server. Access login and read/write permissions can be set for each selected directory.

SOCKS

ICA connections can use the SOCKS networking proxy protocol to enables hosts on one side of a SOCKS server to gain full access to hosts on the other side of the SOCKS server without requiring direct IP reachability. The SOCKS server address and port number can be set for each connection or for all connections.

Encryption

ICA sessions can be encrypted using 40, 56 or 128 bit encryption keys. The ICA Client must connect to an Citrix Server that supports an equal or higher number of bits for the encryption key.

User logon parameters

This feature allows you to set up the user's name, password and authenticating NT domain for an ICA session. The user name and password used to login in to the IBM Network Station can be reused automatically or these parameters can be configured for each connection. If these parameters are not provided, the user is prompted for them each time he connects to a NT multi-user server.

National language support

The ICA client supports all languages and keyboards supported by the IBM Network Station. In addition, an extended list of keyboards is supported by the ICA Client once a connection has been made to an ICA server.

External Interfaces

There are two executable programs in the IBM Network Station ICA package.

- The **ICA Remote Application Manager** program is a graphical user interface for selecting ICA servers or Windows applications to connect to. It presents connection records that it creates and connection records created by Network Station Manager. When a connection is initiated, the ICA Client program is fork'ed and exec'ed.

  When connecting to a description, the ICA Remote Application Manager created a new process and starts an instance of the ICA Client program. Using information passed by the ICA Remote Application Manager, the ICA Client connects to a Citrix server and establishes an ICA session.

- The **ICA Client** program connects to a Citrix application server and establishes a session. The application window is presented within an X11 window on the Network Station.

On-line help associated with panels, commands

The User Interface section has been translated into HTML and is presented when the user selects Help-->View detailed help.

Help files are located in the `$MRIPATH/$LANG/ICAClient` directory.

Using the ICA Remote Application Manager

The following sections describe how to use the ICA Remote Application Manager to connect to a Citrix server from your IBM Network Station:

Quick Start

To connect to a Citrix server you need to have a user name and password set up for you on the server, and you need to know the name of the server and domain.

To run the ICA Remote Application Manager

From the launch bar, select **Host Access - - -> ICA Remote Application Manager**.

From the command line, type the following command:

```
/usr/lib/ICAClient/wfcmgr  <Return>
```

where `/usr/lib/ICAClient` is the directory in which you installed the ICA Remote Application Manager.

Note: If the ICA Remote Application Manager has not been installed in the default installation directory, ensure that the environment variable ICAROOT is set to point to the actual installation directory.

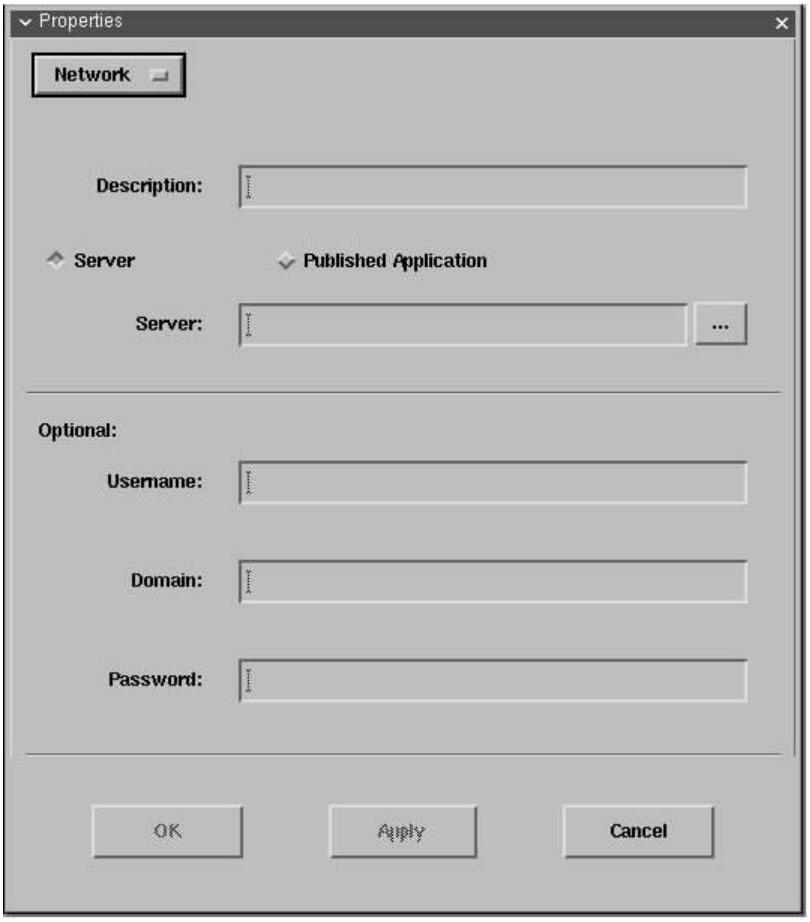
The ICA Remote Application Manager window is displayed:

To define a connection

Note: If Network Station Manager had been used to define ICA connection entries, they will be displayed. You may go to "**To open a connection**" or continue with defining a new connection entry.

1. Choose **New...** from the **Entry** menu, or click the New Entry icon.

   The **Properties** dialog box is displayed to allow you to define a new connection:



2. Edit the **Description** to describe the connection definition you are creating.

   The description is used to identify the connection definition in the **ICA Remote Application Manager** window.

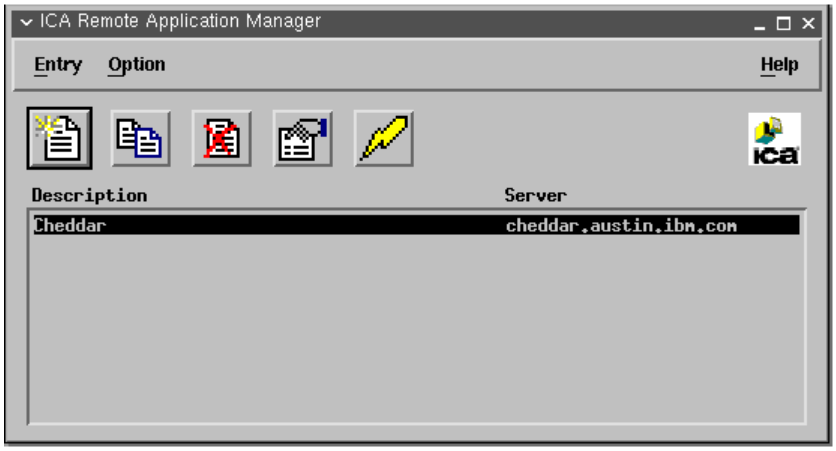
3. Select to connect to a Citrix **Server** or to a **Published Application** and then choose a Citrix server or published application from the pull-down list.

4. If you want to log in as a specific user enter the appropriate details in the **Username**, **Domain**, and **Password** fields.

   Alternatively, you can leave the fields blank, in which case you are prompted for them, if necessary, when you connect.

5. Click **OK** to create a connection definition containing the properties you have specified.

The **ICA Remote Application Manager** window shows the connection definition you have created:



To open a connection

Once you have created a connection file with the appropriate network connection properties set up, you can connect to the Citrix server as follows:

Double-click the name of the connection definition you want to open in the ICA Remote Application Manager window.

Alternatively, you can select the name of the connection definition and choose **Connect** from the **Entry** menu, or click the **Connect** button:

This connects to the server specified in the connection file with the user name and password details you have entered in the connection definition.

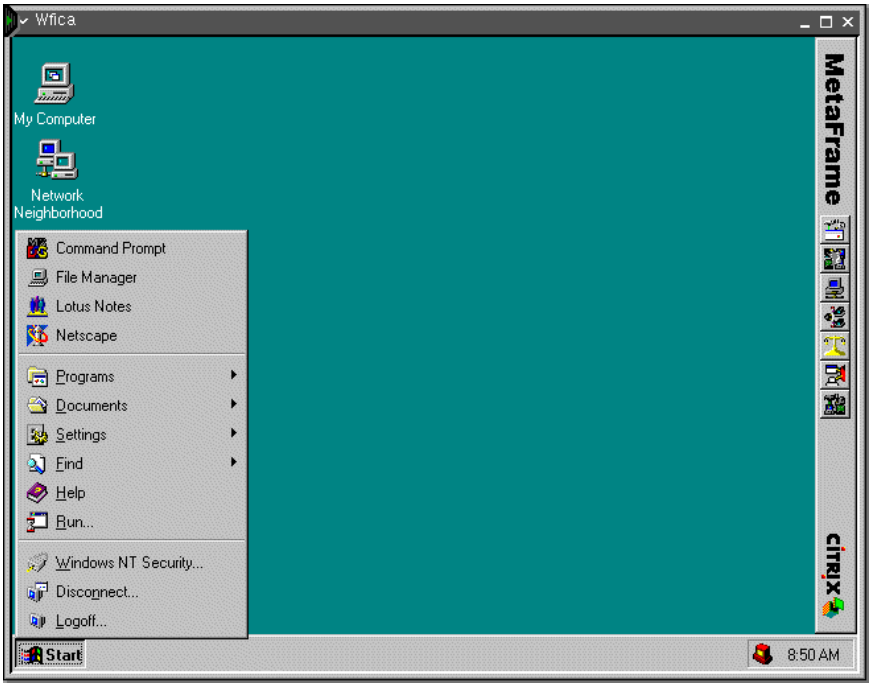
The following message then tells you which ICA server the ICA client is trying to connect to:

When the connection to the ICA server is complete, the following message is presented:

Connecting to Citrix MetaFrame Servers

If you have not specified a user name or password in the connection file, you are prompted to enter them if they are required by the server:

After a short delay the Windows desktop is displayed in a window on your IBM Network Station:



To log off from Windows

Choose **Logoff...** from the Windows **Start** menu or, if your connection is set up to run an application, choose **Exit** from the application's **File** menu. These two methods close the ICA session and terminates the ICA Client.

To disconnect from Windows

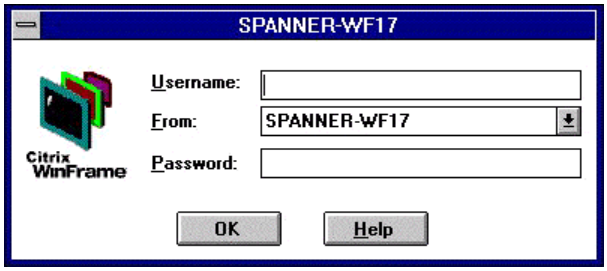
Choose **Disconnect...** (if available) from the Windows **Start** menu.

This leaves your session open on the Citrix server, and you can resume work where you left off next time you log on to the server with the same user name and password.

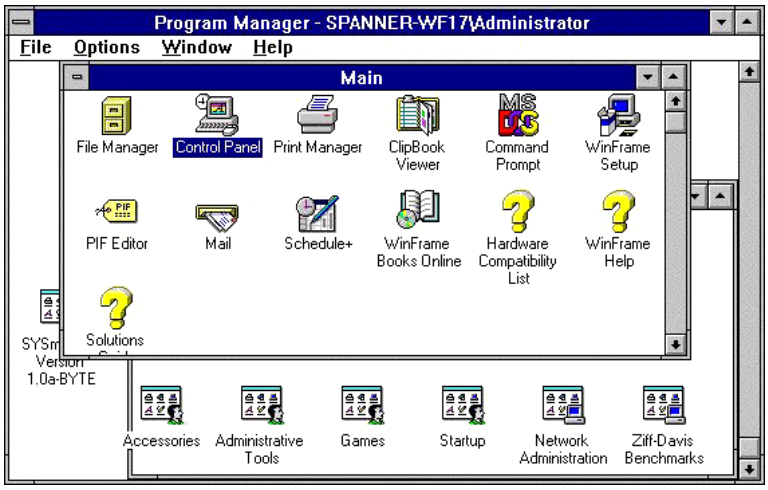
When you reconnect, the server forces the ICA Client window to be the same size and number of colors as in the original session.

Connecting to Citrix WinFrame Servers

If you are connecting to a Citrix WinFrame server, then the login window



and desktop window



have a different appearance.

To log off from Windows

Choose **Log off...** from the Windows Program Manager **File** menu or, if your connection is set up to run an application, choose **Exit** from the application's **File** menu. These two methods close the ICA session and terminates the ICA Client.

Alternatively, choose **Close** (if available) from the Window menu. This leaves the ICA Client application running so that you can open another session, if you want.

To disconnect from Windows

Choose **Disconnect...** (if available) from the Windows Program Manager File menu.

To quit from the ICA Remote Application Manager

Choose **Exit** from the **Entry** menu.

This leaves any connections to Citrix servers open.

To edit an existing connection definition

You can edit existing connection definitions, or create new connection definitions, in the ICA Remote Application Manager window.

When you create a new connection definition, the default window size and window color settings are those specified by the **Settings...** command on the **Option** menu.

For information about the properties you can specify for each connection see the section Editing connections.

To edit an existing connection definition

1. Select the name of the connection you want to edit in the ICA Remote Application Manager window.
2. Choose **Properties...** from the **Entry** menu, or click the **Properties** button.

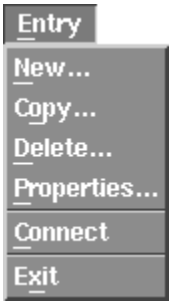
   

   The **Properties** dialog box shows the current properties of the selected connection.
3. Edit the properties you want to change, and then click **OK** to close the **Properties** window.

Menus

The ICA Remote Application Manager has three menu buttons for managing connection entries, setting options and presenting help.

Entry menu



New...

Opens the Properties dialog box to allow you to create a new connection definition.

Copy...

Duplicates the currently selected connection definition so that you can create a new connection based on an existing one.

Delete...

Deletes the currently selected connection definition.

Properties...

Displays the Properties dialog box to allow you to view or edit the properties of the currently selected connection definition.

Connect...

Makes a connection to the Citrix server specified in the currently selected connection definition.

Exit

Exits from the ICA Remote Application Manager application.

Option menu

Settings...

Displays the **Settings** dialog box to allow you to specify the default window settings for new connection definitions, and enter other general settings.

Help menu

About ICA Client...

Displays the ICA Client version number.

View detail help

Display help text for ICA Client.

Properties dialog box

This section explains in detail how to use the ICA Remote Application Manager to create and edit connection definitions, giving you total control over your access to Citrix servers.

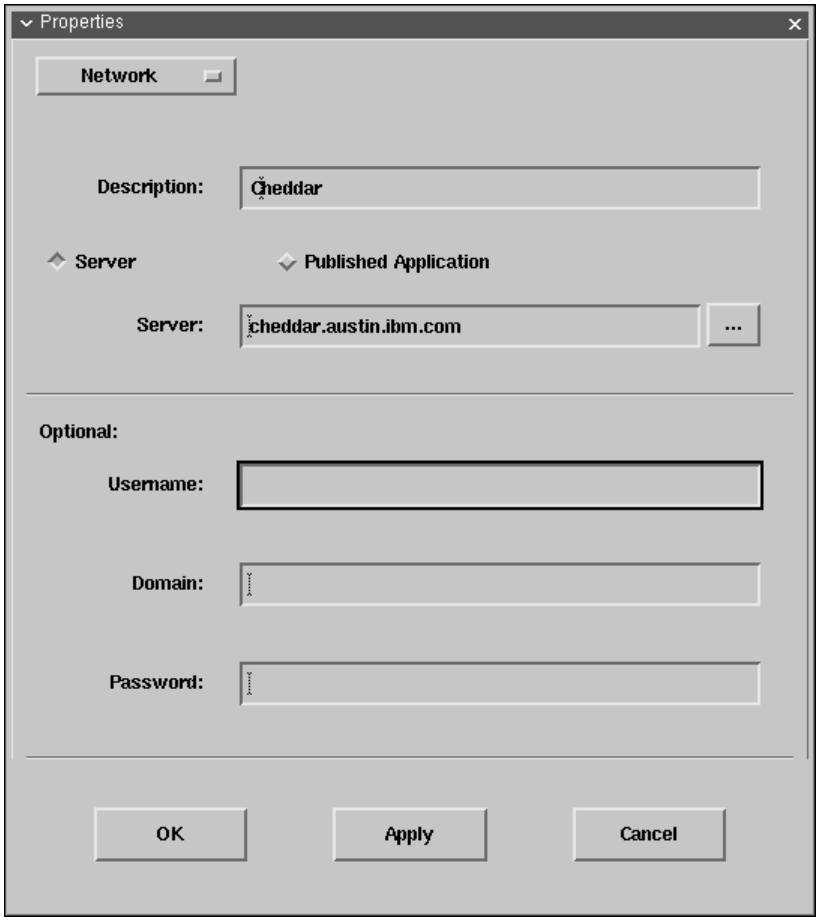
To display the connection properties

1. Select the name of the connection you want in the ICA Remote Application Manager window.
2. Choose **Properties...** from the **Entry** menu, or click the **Properties** button:

The **Properties** dialog box shows the current properties of the selected connection:

Network	description, server name, user name, password, domain
Connection	compression, caching, sound, encryption
Window	number of colors, color mapping, window size
Application	application name, working directory
Firewall Settings	SOCKS proxy

Network



Description is used to identify the connection definition. It is a required field. The characters **;=#[]-** are not allowed.

If **Server** is selected, enter the network name or address of the Citrix server. Selecting the **...** button will bring up a list of available Citrix servers. This make take some amount of time. The allowable characters are upper and lower case alphanumeric, plus the special characters period, underscore and dash. None of the special characters can be first or last.

If **Published Application** is selected, enter the name of the published application. The characters **;=#[]-** are not allowed. Selecting the **...** button will bring up a list of published applications. This make take some amount of time.

Either the **Server** name or the **Published Application** name is required.

The **Username**, **Domain**, and **Password** are used as login parameters and should match those set up on the specified Citrix server. If you do not provide these login parameters you are prompted for them each time you connect.

Connection

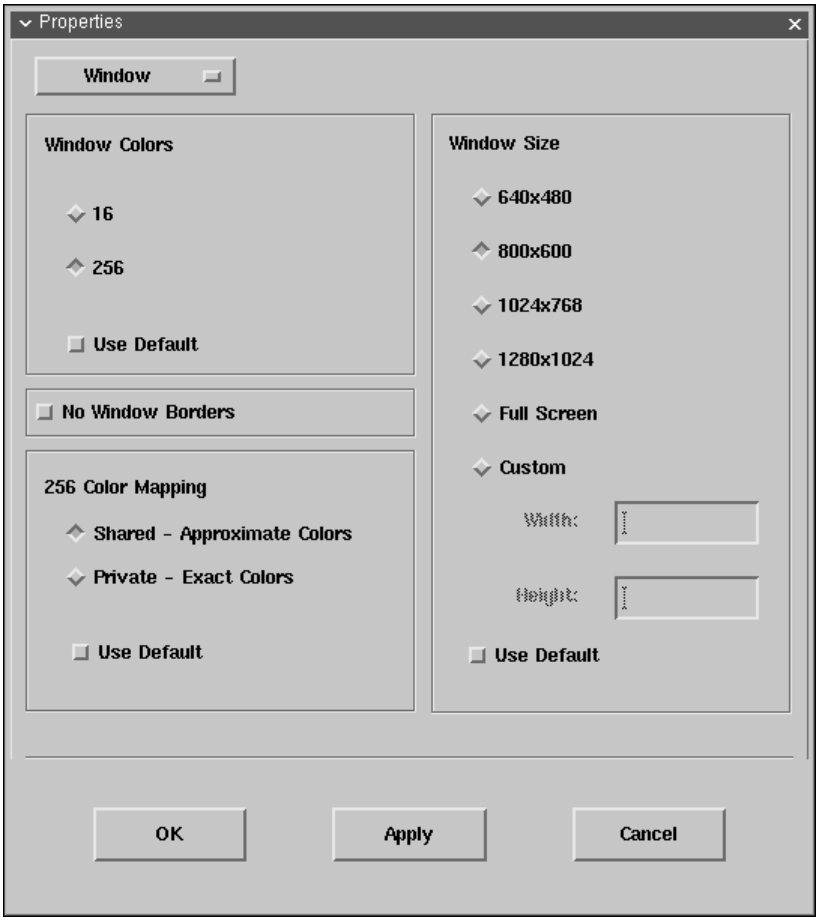
Select **Use Data Compression** to reduce the amount of data transferred across the ICA session. This requires additional processor resources to compress and decompress the data, but can increase performance over bandwidth-limited connections.

Select **Use Disk Cache for Bitmaps** to enable persistent caching of frequently used icons and bitmaps. The persistent cache is always cleared when the IBM Network Station is re-booted. Internal caching is not affected by this option. Persistent caching must be enabled by following the ICA persistent caching directions in the /.profile file.

Select **Enable Sound** to enable sound support. Select **High**, **Medium**, or **Low** quality depending on the available bandwidth. The higher the sound quality, the more bandwidth is used.

Select the **Encryption Level** for the ICA session. The default level is Basic. Strong encryption is available using RCA RC5 for 40, 56 and 128 bit session keys. Select RC5 128-bit Login Only to use encryption only during authentication. Selecting RC5 encryption disables automatic login to the Citrix server.

Window



Window Colors allows you to set the number of colors the Windows application should use to 16 or 256.

No Window Borders allows you to run the ICA Client in a window with out borders or title bar. Typically, the window manager will attach borders and a title bar to windows that appear on the desktop.

256 Color Mapping allows you to set up 256 color sessions to use approximate or exact colors. Use Approximate Colors to eliminate color flashing when switching context. Note that if other applications have allocated all 256 colors the client will fall back to using a private colormap.

Window Size allows you to select one of four standard window sizes, **Full Screen**, or a **Custom** size. If **Custom** is specified then **Width** must be between 300 and 1280 and **Height** is specified, is must be between 300 and 1024.

Select **Use Default** to use the default window size, window colors or 256 color mapping setting specified with the **Settings...** command on the **Option** menu; refer to Window Settings....

Application

Allows you to specify the pathname of an application to be run after connecting to the Citrix server. For example, to run Microsoft Word automatically after connecting to the Citrix server you might enter:

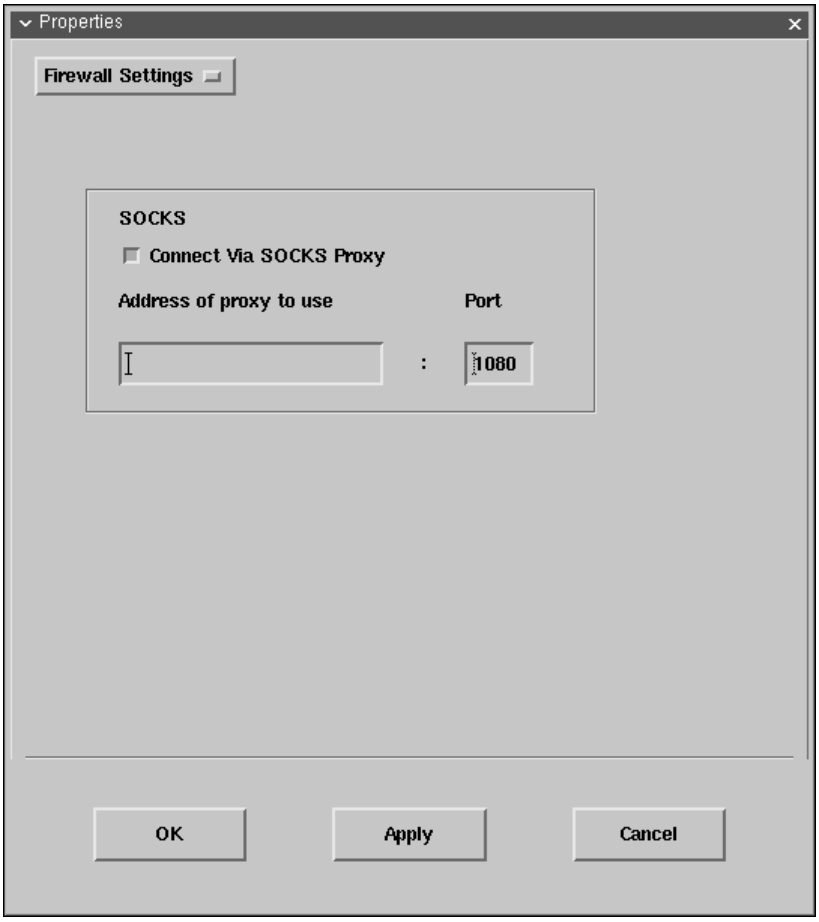
```
C:\WINWORD\WINWORD.EXE
```

If you specify an application then you do not see the Windows desktop, and the connection is closed when you quit from the application.

The **Working Directory** allows you to specify the pathname of a working directory to be used with the application.

Note: If you have selected to connect to a published application the Application dialog box will not be available.

Firewall Settings



Selecting **Connect Via SOCKS Proxy** allows your ICA session to connect to an ICA Server via a SOCKS Proxy Server.

Specify the **Address of proxy to use** (network name or network address) and the **Port** number to use.

Settings dialog box

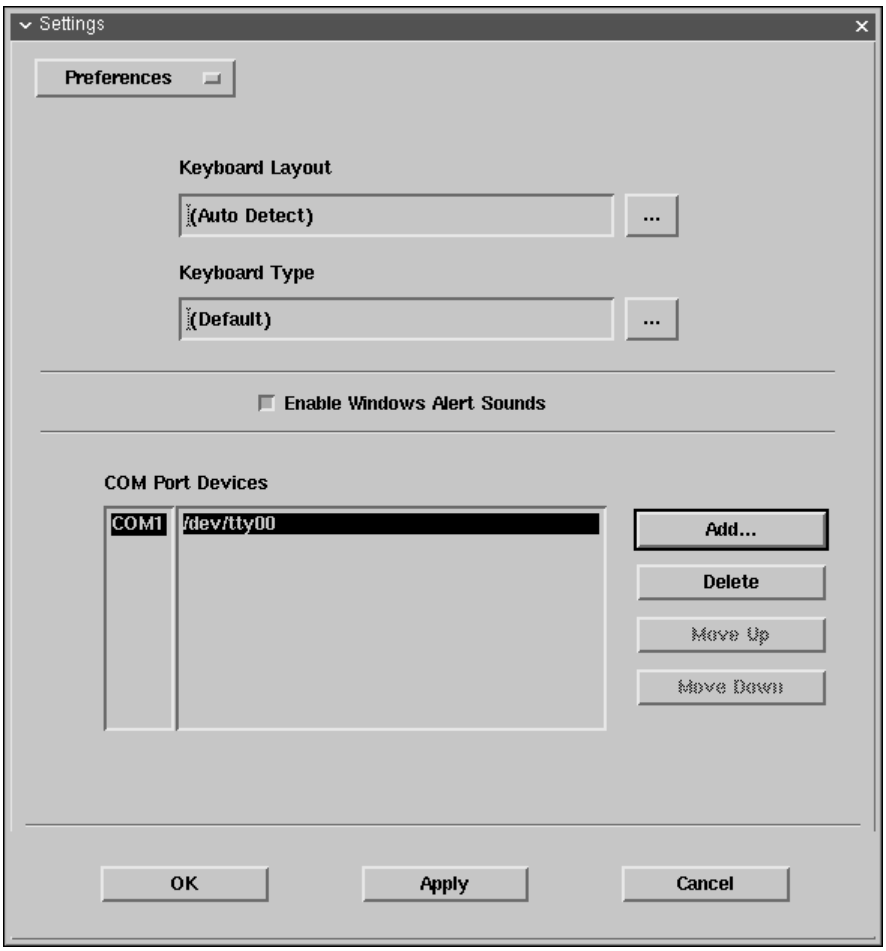
The **Settings** dialog box allows you to specify the default window settings used when you create a new connection file. It also allows you to enter a Citrix name server TCP/IP address.

To display the **Settings** dialog box choose **Settings...** from the Option menu.

It contains the following panels:

Preferences	keyboard type and layout, alert sounds, com port devices
Window	default color and size choices
Server Location	server groups, server lists
HotKeys	<Alt><F1-F12>, <Alt><Tab>
Drive Mapping	enable/read/write, directory to drive mapping
Firewall Settings	enable alternate network address, SOCKS proxy server

Preferences



Keyboard Layout specifies the keyboard layout used by the ICA Client.

If **(Auto Detect)** is selected then the ICA Client will automatically detect and use the keyboard layout configured by the IBM Network Station Boot Monitor.

If **(User Profile)** is selected then the Citrix server specifies the keyboard layout based on the user's Citrix server profile.

If neither of these options are suitable, one of the following explicit keyboard layouts can be selected:

Bulgarian	**French (Canadian 1992)**	**Polish (Programmer)**
Croatian	**French (Swiss)**	**Portuguese**
Czech	**German**	**Portuguese (Brazilian)**
Danish	**German (Swiss)**	**Romanian**
Dutch	**Greek**	**Russian**
Dutch (Belgian)	**Hungarian**	**Slovakian**
English (UK)	**Icelandic**	**Slovenian**
English (US)	**Italian**	**Spanish**
English (US ISO)	**Italian (Swiss)**	**Spanish (Latin American)**
Finnish	**Japanese (ATOK11)**	**Swedish**

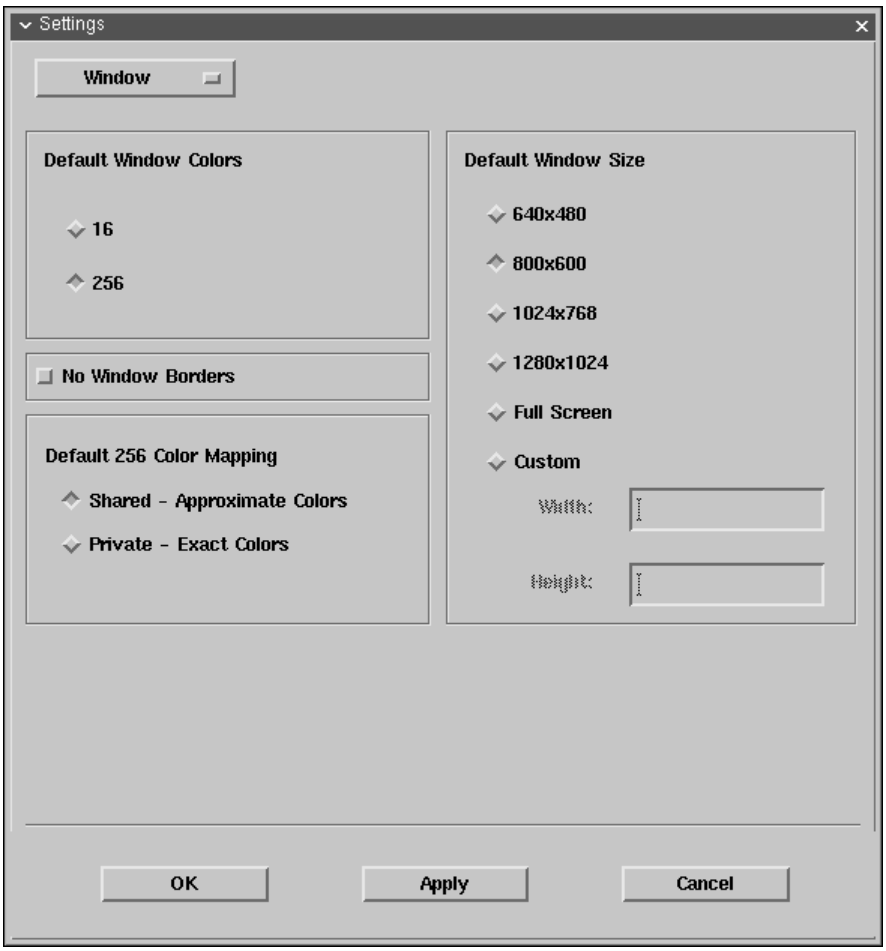
French	**Japanese (MS-IME98)**	**Turkish (F)**
French (Belgian)	**Norwegian**	**Turkish (Q)**
French (Canadian 1988)	**Polish**	

Keyboard Type specifies the keyboard type to be used with the ICA Client. Select **(Default)**.

Enable Windows Alert Sounds if selected causes Windows alert sounds to be played using the IBM Network Station sound system.

COM Port Devices allows bi-directional mapping of IBM Network Station serial devices, e.g. /dev/tty00, to Citrix Server COM ports.

Window



These settings are used as the default for all new connection files.

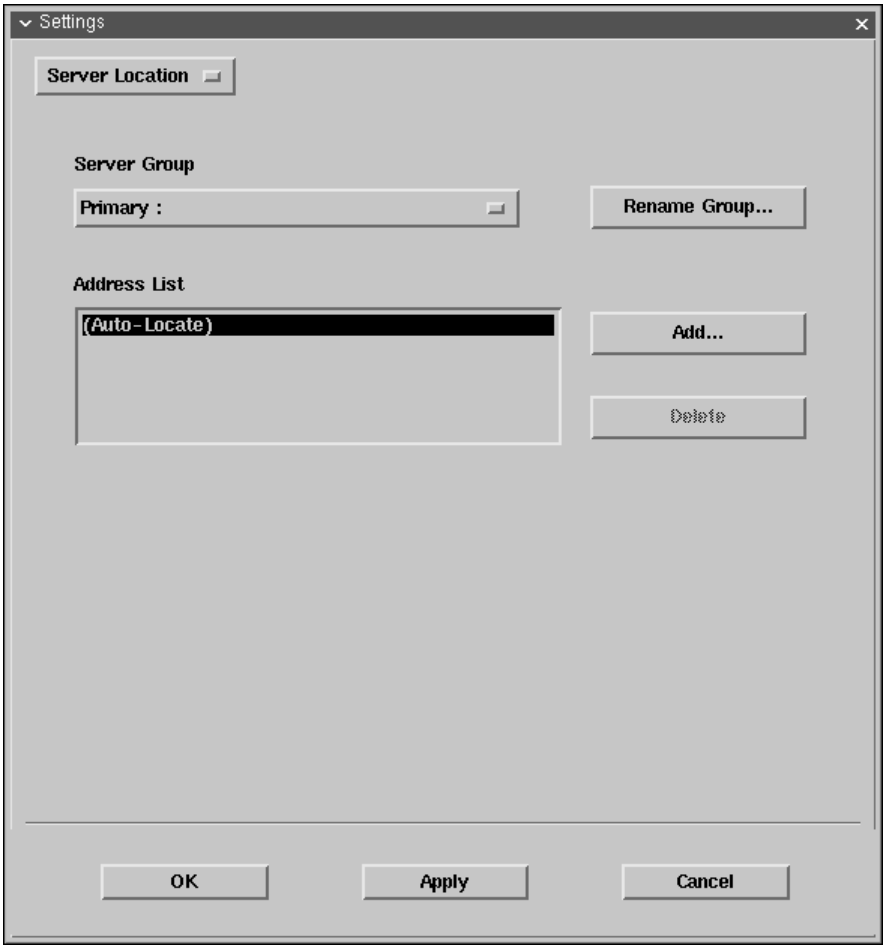
Window Colors allows you to set the number of colors the Windows application should use to 16 or 256.

No Window Borders allows to manage the window borders and title bar that surround an ICA session.

256 Color Mapping allows you to setup 256 color sessions to use approximate or exact colors.

Window Size allows you to select one of four standard window sizes, **Full Screen**, or a **Custom** size. If **Custom** is specified then **Width** must be between 300 and 1280 and **Height** is specified, is must be between 300 and 1024.

Server Location



Provides a more redundant method for locating the Master ICA Browser. The Master ICA Browser is queried to create a list of all Citrix servers and published applications on the network.

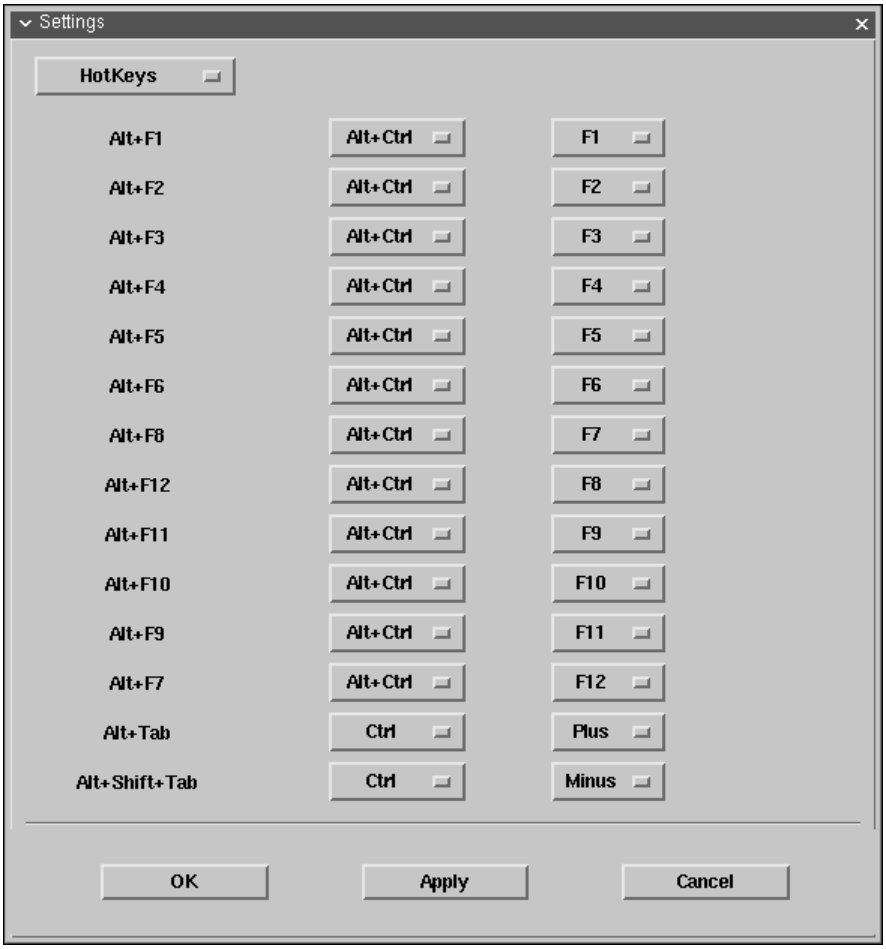
If **(Auto-Locate)** is specified in the **Address List** box, the ICA Client broadcasts a Get Nearest Citrix server packet. The first Citrix server to respond is queried for the address of the ICA Master Browser server.

If Citrix servers are specified in the **Address List** box, the ICA Client sends a request for the address of the Master ICA Browser to each of the servers listed in the Primary group. If there is no response, requests are sent to each of the servers listed in the Backup 1 group. If there is no response from the Backup 1 group, requests are sent to the servers listed in the Backup 2 group.

Some network configurations use routers or gateways to filter broadcast packets. Specifying Citrix servers allows the ICA Master Browser to be located on these types of networks.

Note: If the Master ICA Browser cannot be located, you can connect to Citrix servers directly by specifying the TCP/IP address as the server location.

Hotkeys



Allows you to define alternative key combinations for the hot keys. The following table shows the hot keys reserved for X Windows and the default alternative key combinations.

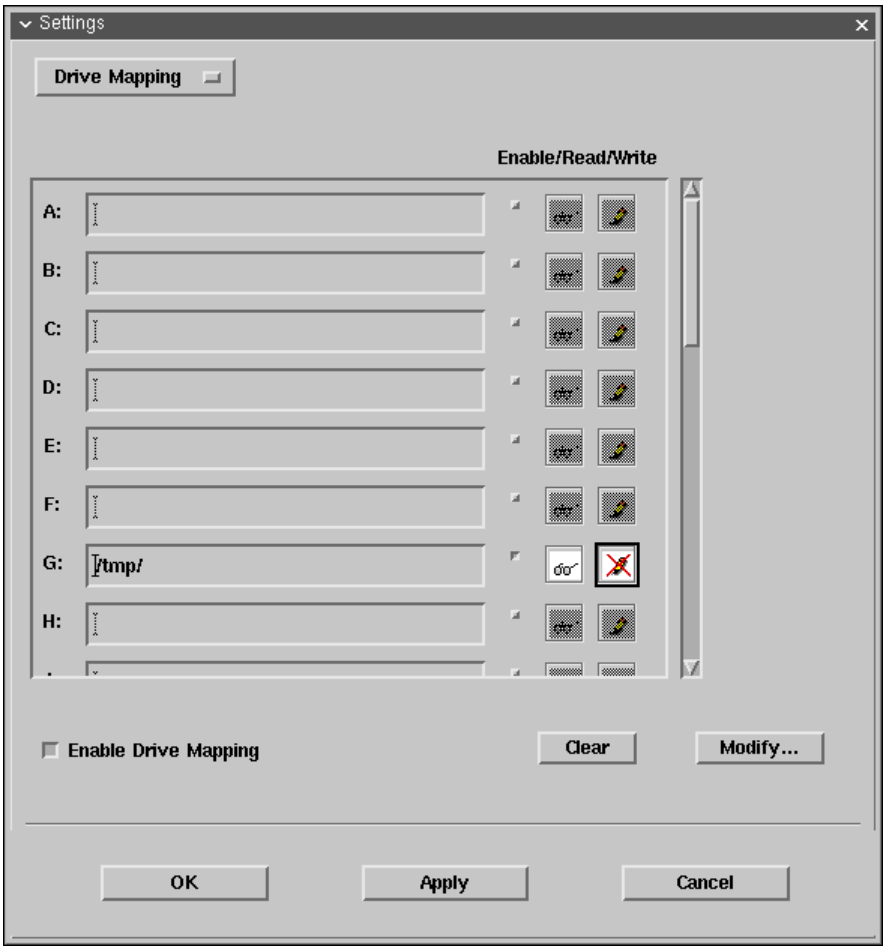
X Window Hot Key Combination	Default Alternative Key Combination
<Alt><F1> to <Alt><F12>	<Alt><Ctrl><F1> to <Alt><Ctrl><F12>
<Alt><Tab>	<Ctrl><Tab>
<Alt><Shift><Tab>	<Ctrl><Shift><Tab>

You can change the definitions by selecting alternative keys from the pop-up menus.

Any <Alt> key combinations not used by your X Window manager can be used as normal within your Citrix session.

In addition, the key combination <Ctrl><Alt><Enter> can be used to produce the PC key combination <Ctrl><Alt><Delete>.

Drive mappings



You can configure the ICA Client so that you can access any directory mounted on your IBM Network Station, including CD-ROMs, from the Citrix server session as PC drive letters.

After changing drive mapping settings you need to log off and reconnect to the Citrix server for the changes to take effect; simply disconnecting is not sufficient.

For each Windows NT drive letter, the Drive mapping list shows the disk or path name of the IBM Network Station directory mapped to the drive, and the **Enable/Read/Write** access.

To map a Citrix server drive to a directory on your IBM Network Station:

1. Select the drive you want to map; for example **G:**.

If the drive you have mapped is not available on the Citrix server, the directory you have specified is mapped to another free drive letter.

2. Click **Modify** to change the drive mapping. A file selection dialog is displayed to allow you to select the IBM Network Station directory to map.

3. Select the directory (e.g. **/tmp**) you want to map to and click **OK**. The directory is shown in the Drive mapping list.

To enable access to a specific drive, click the check box next to the corresponding drive.

To change the access to a drive, click the appropriate read/write icons corresponding to the drive. (Typically, only the $HOME and /tmp directories are writable.) The meaning of the icons areas follows:

Icon	Meaning
	Read access
	Prompt for read access on first access per session
	No read access
	Write access
	Prompt for write access on first access per session
	No write access

To enable drive mapping, select **Enable Drive Mapping**. This enables drive mapping for all your connection definitions.

Depending on the setup of the server, your mapped drives may or may not be immediately available. They may also be mapped to different server drive letters than those you specified in the **Drive Mapping** panel, because the drives you specified have already been assigned by the server.

For WinFrame

To find out the current status of your mapped drives, once connected to the Citrix server, open the **File Manager** and click the drive letter pull-down menu in the top left of the **File Manager** window.

This displays which local or client drives are mapped to which server drives.

Client drives are shown in the format `\\Client\drive` where drive is the drive letter specified in the **Drive Mapping** panel.

If a drive you specified in the **Drive Mapping** panel is not shown in this list you can connect it to a server driver letter as follows:

1. In the **File Manager** select **Connect Network Drive?** from the **Disk** menu.

2. In the **Connect Network Drive** dialog box, select the server drive you want to map the client drive to in the **Drive** pull-down menu.

3. If you want to have this drive available to you each time you log into this server, ensure that the **Reconnect at Logon** box is checked.

4. Double-click the **Client Network** icon in the **Shared Directories** list, then click the appropriate client icon for your IBM Network Station directory. This displays a list of the available local drives, previously set up in the **Drive Mapping** panel.

5. Select the drive you want to map to the selected server drive and click **OK**. Your local drive will now be available.

Repeat the above steps for each of the local drives you wish to attach to the server drives.

For MetaFrame

To find out the current status of your mapped drives, once connected to the Citrix server, open the **NT Explorer**. Client drives are shown in the format **<*drive*>$ on 'Client'(<*drive*>:)** where **<*drive*>** is the drive letter specified in the **Drive Mapping** panel.

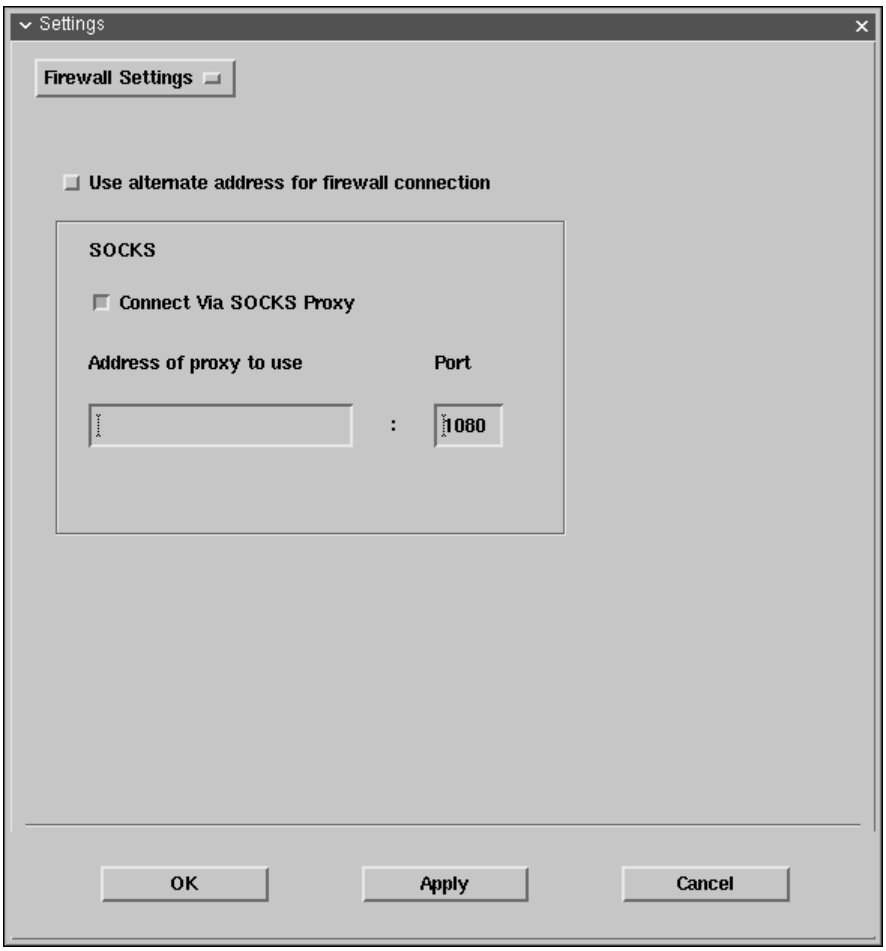
File naming conventions

As UNIX is a case sensitive file system and Windows NT is case insensitive, problems may occur if you use UNIX files within the ICA Client session whose names are identical except for their case. For example, ReadMe and README.

In such circumstances, although Windows NT displays the names correctly in a file listing, when a file is referred to, for example as a link in an HTML file, the first file found is used.

It is therefore recommended that any files you intend to use within the ICA Client session have unique names.

Firewall Settings



The **Use alternate address for firewall connection** feature is used to browse for Citrix servers or published applications that are inside a firewall from a client machine that is 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. Enter the external internet addresses in the Address List.

Do not use the **Use alternate address for firewall connection** check box except on the advice of your administrator.

Selecting **Connect Via SOCKS Proxy** allows your ICA session to connect to an ICA Server via a SOCKS Proxy Server.

Specify the **Address of proxy to use** (network name or network address) and the **Port** number to use.

Using the ICA Client

The following sections describe how to use the ICA Client to connect to a Citrix server from your IBM Network Station.

Quick Start

To connect to a Citrix server you need to have a user name and password set up for you on the server, and you need to know the name of the server and domain.

To run the ICA Client

Type the following command at the command line prompt:

```
/usr/lib/ICAClient/wfica  <Return>
```

where `/usr/lib/ICAClient` is the directory in which you installed the ICA Client.

Note: If the ICA Client has not been installed in the default installation directory, ensure that the environment variable ICAROOT is set to point to the actual installation directory.

The ICA Client host name dialog is displayed:

Enter the host name of the Citrix server that you want to connect to and press the Enter key or click the OK button.

After connecting to the Citrix server, the Citrix server may prompt you to enter your user id and password. After a short delay the Windows desktop is displayed in a window on your IBM Network Station.

Command Line Parameters

There are two executable programs in the IBM Network Station ICA package.

- The ICA Remote Application Manager program, **wfcmgr**, is a graphical user interface for selecting ICA servers or Windows applications to connect to. It presents connection records that it creates and connection records created by Network Station Manager. When a connection is initiated, the ICA Client program is fork'ed and exec'ed.

- The ICA Client program, **wfica**, connects to a Citrix application server and establishes a session. The application window is presented within an X11 window on the Network Station.

ICA Remote Application Manager - wfcmgr

There is a small set of command line parameters for the ICA Remote Application Manager. The **-description**, **-icaroot** and **-file** parameters came with the Citrix source code. The others have been added to provide addition value to the IBM Network Station.

```
Usage: wfcmgr [options]

Where [options] are:

  -help                     Show this message
  -noupdate                 Configuration/Connection updates not allowed
  -desc[ription] <string>   Connection description from connection file
  -icaroot <directory>      Installation directory (full path name)
  -file <filename>          Connection file name
  -g[eometry] <WxH±X±Y>     X11 window <Width x Height ± X_off ± Y_off>
  -UseFullScreen [<bool>]   X11 window full screen [ <true | false> ]
  -NoWindowManager [<bool>] X11 window without borders [ <true | false> ]
  -log                      Enable ASSERT logging
```

-help the usage text (as shown above) is sent to the console.

-noupdate when this option is specified, updates to the connection file and/or the configuration file are not allowed.

-description <*text*> the full text from the Description field of the connection definition dialog. If this argument is not specified, then the first description in the [ApplicationServers] section of the appsrv.ini file will be used.

-file <*name*> the fully qualified file name of the file that contains the connection description to be used. If the HOME environment variable is defined then the default file name is `$HOME/.ICAClient/appsrv.ini`. Otherwise, the default file name is `/usr/lib/ICAClient/config/appsrv.ini`.

-icaroot <*directory*> the fully qualified directory where the ICA client package was installed. If not specified then the ICAROOT environment variable is accessed to get the directory. If neither the -icaroot argument nor the ICAROOT environment variable are used to define the install directory, then by default, it is `/usr/lib/ICAClient`.

-geometry <*WxH±X±Y*> the X11 window Width, Height, X offset and Y offset. All values are in pixels. Positive X offsets are from the top of the screen, negative from the bottom. Positive Y offsets are from the left side of the screen, negative from the right. Variations of this specification include <*WxH*> and <±*X*±*Y*>.

By default, the **wfcmgr** window is centered on the screen. To position the **wfcmgr** window in the upper left corner of the screen, specify **-geometry +0+0**.

-UseFullScreen [<*bool*>] when this option is set to *True* then the **wfcmgr** window be the size of the full screen. Allowable values are *True* and *False*. Default value is *False*.

-NoWindowManager [<*bool*>] when this option is set to *True* then the **wfcmgr** window will not have borders nor title bar. Allowable values are *True* and *False*. Default value is *False*.

-log enables ASSERT logging. ASSERTs are program sanity tests that **wfcmgr** can make. Typically these test are not enabled because they tend to impact performance.

ICA Client - wfica

The Version 1 Release 3.0 ICA command line parameters will continue to be supported. This allows for Version 1 Release 3.0 ICA migration. The command line parameters have precedence over the .ini files.

```
Usage: wfica [ica_options] [ns_options [-- <application>]]

Where [ica_options] are:

  -help                    Show this message
  -version                 Show version information
  -quiet                   Suppress connection dialogs
  -desc[ription] <string>  Connection description from connection file
  -file <filename>         Connection file name
  -protocolfile <filename> Protocol file name
  -clientfile <filename>   Configuration file name
  -icaroot <directory>     Installation directory (full path name)

And [ns_options] are:

  -s[erver] <name>          NT server name
  -b[rowser] <namelist>     NT browser name list <name[:name: ... :name]>
  -u[sername] <name>        NT login user name
  -p[assword] [<password>]  NT login password
  -do[main] <name>          NT domain name
  -na[me] [<name>]          NT CLIENTNAME
  -c[olor] <16 | 256>       NT number of colors
  -en[cryption] <level>     NT encryption level <basic | login | 40 | 56 | 128>
  -WorkingDirectory <path>  NT working directory
  -g[eometry] <WxH±X±Y>     X11 window <Width x Height ± X_off ± Y_off>
  -UseFullScreen [<bool>]   X11 window full screen [ <true | false> ]
  -NoWindowManager [<bool>] X11 window without borders [ <true | false> ]
```

```
-ti[tle] <title>          X11 Window title
-ca[che] <size>           Cache size in Kbytes
-shm <size>               Shared memory size in Kbytes
-log                      Enable ASSERT logging
-<keyword> <value>        Override .ini files with "keyword=value"
-- <application>          Initial program OR published application
```

ICA Options

-help the usage text (as shown above) is sent to the console.

-version the following message is sent to the console:

```
IBM Network Station ICA Client
Version 2.0  (Build dd/mm/yyyy - hh:mm:ss)
Copyright International Business Machines Corp. 1999
All rights reserved

Citrix ICA Client for Unix
Version 3.00.15
Copyright 1998-1999 Citrix Systems, Inc.
All rights reserved
```

-quiet connection dialogs will not be presented to the user. By default, the ICA client will present a "connecting to" dialog followed by a "connected to" dialog. Both of these dialogs are informational and require no response by the user.

-description <*text*> the full text from the Description field of the connection definition dialog.

Either **-description** or **-server** or **-- <application>** must be specified. If neither of these parameters are specified then the user will be prompted for a server name.

-file <*name*> the fully qualified file name of the file that contains the connection description to be used. If the HOME environment variable is defined then the default file name is `$HOME/.ICAClient/appsrv.ini`. Otherwise, the default file name is `/usr/lib/ICAClient/config/appsrv.ini`.

-protocolfile <*name*> the fully qualified file name of the file that contains the protocols supported by the ICA client. By default, the file name is `/usr/lib/ICAClient/config/module.ini`. This is a system configuration file and not meant to be modified.

-clientfile <*name*> the fully qualified file name of the file that contains the options and defaults for all connection descriptions. If the HOME environment variable is defined then the default file name is `$HOME/.ICAClient/wfclient.ini`. Otherwise, the default file name is `/usr/lib/ICAClient/config/wfclient.ini`.

-icaroot <*directory*> the fully qualified directory where the ICA client package was installed. If not specified then the ICAROOT environment variable is accessed to get the directory. If neither the **-icaroot** argument nor

the ICAROOT environment variable are used to define the install directory, then by default, it is `/usr/lib/ICAClient`.

NS Options

Note: NS Options can not be combined with the **-description** parameter.

-server <*name*> specifies the ICA application server to connect to. The name can be a fully qualified network host name, an abbreviated network host name or a dotted decimal network address.

Either **-description** or **-server** or **-- <application>** must be specified. If neither of these parameters are specified then the user will be prompted for a server name.

-server and **-browser** are mutually exclusive.

-browser <*namelist*> specifies the name of a master browser. The master browser is an ICA server that tells the ICA client which ICA application server to connect to and which application to run on that server.

A colon "**:**" separated list of master browsers can be specified. Each name can be a fully qualified network host name, an abbreviated network host name or a dotted decimal network address.

If neither **-server** nor **-browser** is specified and **-- <application>** is specified then the ICA Client will broadcast (typically to the local subnet) to get a master browser name.

Either **-description** or **-server** or **-- <application>** must be specified.

-server and **-browser** are mutually exclusive.

-username <*name*> specifies the NT server login user name.

-password [<*password*>] specifies the NT server login password. The following password formats are supported:

NSM Format: The NSM format is checked first. This is a repeating sequence of the '%' character followed by two hexadecimal characters. For example, the following is an NSM encrypted password:

```
%B2%86%C8%78
```

ICA Format: The ICA format is checked second. This is a string of hexadecimal decimal characters. The first four characters specify the number of bytes required to contain the binary form of the remaining hexadecimal characters. For example, the following is an ICA encrypted password:

```
0005a986568f51
```

In-the-clear: If the password is neither an NSM password nor an ICA password then it is assumed to be an unencrypted password. For example, the following is neither an NSM nor an ICA encrypted password. Hence it is an unencrypted password:

```
mypw
```

If **-password** is specified without a ***<password>*** then an NSM formatted password is requested from the **actlogind** daemon.

-domain <*name*> specifies the NT server domain *name*.

-name <*clientname*> specifies the *client name* to be used by the ICA application server. If the client name is longer than 20 characters (an ICA protocol limitation) then it is truncated to 20 characters.

If **-name** is specified but is not followed by a host name then the fully qualified host name will be obtained from the system and converted to a simple host name. A simple host name is defined to be the first name in a fully qualified dotted name string. (In other words, everything is truncated after the first decimal point.) If the resulting string is longer than 20 bytes (an ICA protocol limitation) then it is truncated to 20 bytes.

If **-name** is not specified then the fully qualified host name is obtained from the system. If it is longer than 20 characters (an ICA protocol limitation) then the dotted decimal IP address string will be used.

-color <*number*> specifies the *number* of colors that the ICA application server should use to generate application graphics. Allowable values are *16* and *256*.

-encryption <*level*> specifies the *level* of encryption to be used between the ICA client and the ICA application server. Supported encryption levels are:

basic	simple encryption (this is the default)
login	128-bit RSA encryption for login only
40	40-bit RSA encryption
56	56-bit RSA encryption
128	128-bit RSA encryption

If any level of encryption is specified other than **basic**, then any client side specification of username, password and/or domain, whether from the command line or from an INI file, will not be used. (The intent here is to insure the user logs into the NT server via the NT login dialog.)

-WorkingDirectory <*path*> specifies the NT working directory path.

-geometry <*WxH±X±Y*> the X11 window Width, Height, X offset and Y offset. All values are in pixels. Positive X offsets are from the top of the screen, negative from the bottom. Positive Y offsets are from the left side of the

screen, negative from the right. Variations of this specification include <*WxH*> and <±*X*±*Y*>.

The window width may range from 300 to 1280. The window height may range from 300 to 1024.

By default, the **wfica** window is centered on the screen. To position the **wfica** window in the upper left corner of the screen, specify **-geometry +0+0**.

-UseFullScreen [<*bool*>] when this option is set to *True* then the **wfica** window be the size of the full screen. Allowable values are *True* and *False*. Default value is *False*.

-NoWindowManager [<*bool*>] when this option is set to *True* then the **wfica** window will not have borders nor title bar. Allowable values are *True* and *False*. Default value is *False*.

-title <*text*> puts the specified *text* into the X11 window title bar.

-cache <*size*> *size* in kilobytes of the internal ICA Client transient cache.

-shm <*size*> *size* in kilobytes of shared memory to be allocated. If size is greater than zero then the X11 Shared Memory extension is enabled.

-log enables ASSERT logging. ASSERTs are program sanity tests that **wfica** can make. Typically these test are not enabled because they tend to impact performance.

-<*keyword*> <*value*> any unrecognized arguments will be analyzed to see if they qualify as a command line *keyword=value* pair. Any such *keyword=value* pairs are assumed to be valid .INI file entries and will be concatenated with the *keyword=value* pairs extracted from the INI files.

<*keyword*>=<*value*> pairs are not checked for validity. Hence, the ability for the ICA client to detect and report command line errors is limited.

-- <*application*> specifies the program that the ICA application server should run if the **-server** argument is also specified. Otherwise it specifies a published application and a master browser will be contacted to get both the program to run and the ICA application server to run it on. This parameter must be last.

Either **-description** or **-server** or **-- <application>** must be specified. If neither of these parameters are specified then the user will be prompted for a server name.

If **-- <application>** is not specified then a default description must exist in an accessible connection file.

Deprecated Command Line Arguments

The following V1R3 command line arguments have been deprecated. They can still be used in the V1R3-to-V2R1 migration strategy but they should not be published.

-host <*name*>	same as **-server <name>** if **-lb** is specified. If **-lb** is specified then it is the same as **-browser <name>**
-lb	governs how the **-host** parameter will work.
-restart	ignored.
-geometry fullscreen	same as < *max_screen_width x max_screen_height + 0 + 0* >

FLASH Boot Support

When booting the IBM Network Station from a flash card, several Boot Monitor fields may be available. In particular, one of the three Boot Host fields can be used to specify the IP address of an ICA server or ICA master browser.

Additional unused Boot Monitor (text) fields may be also used to specify ICA command line parameters. The Boot Monitor storage for these additional ICA command line parameters is limited.

The ICA Client supports the following additional command line parameters to support flash boot:

-server1	indirectly specifies the **-server** parameter where the server <name> comes from the First Boot Host parameter in NVRAM.
-server2	indirectly specifies the **-server** parameter where the server <name> comes from the Second Boot Host parameter in NVRAM.
-server3	indirectly specifies the **-server** parameter where the server <name> comes from the Third Boot Host parameter in NVRAM.
-browser1	indirectly specifies the **-browser** parameter where the browser <namelist> comes from the First Boot Host parameter in NVRAM.
-browser2	indirectly specifies the **-browser** parameter where the browser <namelist> comes from the Second Boot Host parameter in NVRAM.
-browser3	indirectly specifies the **-browser** parameter where the browser <namelist> comes from the Third Boot Host parameter in NVRAM.
-nvram <*fieldname*>	specifies the name of a text field in nvram. The text field will be analyzed and, if the first non-blank character is a dash (**-**), then the text will be used to replace the **-nvram <*fieldname*>** specification. Use the Boot Monitor to enter text in selected fields. The table below give the NVRAM filed name for selected Boot Monitor fields which may be available.

Series 2xxx Boot Monitor Field Name	NVRAM Field Name
Boot file server dir and file name (second)	second-boot-path
Boot file server dir and file name (third)	third-boot-path
Workstation directory (second)	config-unix-directory2

Series 1xxx Boot Monitor Field Name	NVRAM Field Name
Configuration file	config-custom-file

For example, to specify multiple ICA browsers on a Series 2800, the following text could be entered in the Boot Monitor field called **Boot file server dir and file name (third)**:

-b 9.8.7.201:9.8.7.104:server2 -- MyApplication

Then the command

wfica -nvram third-boot-path

will actually be interpreted as

wfica -b 9.8.7.201:9.8.7.104:server2 -- MyApplication

The **-server1**, **-server2**, **-server3**, **-browser1** , **-browser2** and **-browser3** arguments are mutually exclusive.

Locking Keys

By default, the operator controls the locking state of the keyboard on the Network Station. When the operator presses a locking key (CapsLock or NumLock), the keyboard goes into the appropriate lock state. If the active window is the ICA client, then the locking key is sent to the active Windows application on the ICA server. Typically, this synchronizes the locking state and the LEDs between the Network Station and the ICA server.

However, a few Windows applications (notably VT100 emulators) process the NumLock key as a function key. As a result, the NumLock state of the ICA server is not changed and NumLock synchronization between the ICA server and the Network Station does not end until the NumLock key is pressed again.

To help control this situation, the ICA client (wfica) supports the following command line option:

-NumLockSync <*bool*> when this option is set to *False* then the ICA server controls the NumLock state of the **wfica** window. Default value is *True*.

The keyboard locking state will always be in sync with the active window. In effect, each Network Station window, including the window that ICA is running in, will perceive that the keyboard is in the correct lock state. However, the Network Station windowing system (X11) always toggles the NumLock LED every time the NumLock key is pressed. As a result, the NumLock LED may not always reflect the NumLock state of the ICA window if **-NumLockSync False** is specified.

Advanced Topics

Precedence order for ICA connection Records

The current schema for precedence of ICA connection records in the ICA Remote Application Manager is: NSM (NC Registry) first, then user's appsrv.ini file if it exists or if it does not exist, the system appsrv.ini file. This precedence information is important for understanding what connection records will appear in the Remote Application Manager (wfcmgr). Since the ICA code was designed to use the connection description as the unique field, two records cannot be added with the same description.

A problem will occur if/when NSM has a connection record with a description that is the same as one found in either of the appsrv.ini files. Currently the NSM connection record will take precedence and the duplicate will not be shown to the user.

Another problem could occur since NSM doesn't guarantee unique names for each connection record. So it is possible for 2 records to exist in NSM with the same description. In this case only the first record encountered will be shown to the user.

Copying and pasting text and graphics

The ICA Client automatically transfers simple text, RTF text and DIB/BMP graphics between the X Windows and Windows clipboards, so that you can copy or cut and paste freely between X Windows and Windows applications or between Windows applications on the same or different Citrix servers.

RTF	Rich Text Format. Both sending and receiving applications must be using the same code page.
DIB	Windows Device Independent Bitmap
BMP	Windows Bitmap

All applications involved with copy/paste operations must be capable of handling the data formats involved. The ICA Client does no data conversions.

To copy text or graphics from Windows to X Windows

1. Select the text or graphic you want to copy from the Windows application.
2. Choose **Copy** from the Windows application's **Edit** menu. The text or graphic is copied to the Windows clipboard.
3. Switch to the X application you want to use.
4. Choose the appropriate command from the X application to paste in the text or graphic you copied.

To copy text or graphics from X Windows to Windows

1. Select the text or graphics you want to copy.

2. Choose the appropriate command from the X application to copy the text or graphics. The text or graphic is copied to the Windows clipboard.

3. Switch to the ICA Client.

4. Choose **Paste** or **Paste Special...** from the **Edit** menu of the Windows application to paste the text or graphic.

Connecting to Local Printers

With the ICA Client you can print to any spooled printer available from your IBM Network Station. Such printers might be connected to the parallel port or the serial port. Printers can be connected automatically or manually.

Automatic Connection

Using Network Station manager (NSM), local printers need only be set up once to enable automatic connection to ICA sessions.

In order to automatically connect printers during the ICA logon two things need to happen. First, the ICA client needs to be able to provide the ICA server with the NT printer driver name for each of the Network Station printers. And second, the NT printer driver must be installed on the ICA server. The correct printer driver name can be found by using the Printer Wizard on the ICA server (see Note 1 below). The Network Station ICA client takes the NT printer driver name from the Network Station Manager (NSM) description field of the printer. The printer driver name is entered into the description field via the NSM printer configuration screens.

Once the printer driver name has been added via NSM and the Network Station in question has been rebooted, the user can log in to the ICA server and bring up the **Control Panel-> Printers** window and see the printers that were auto created. If they do not see the printers, they should bring up the **Programs->MetaFrame Tools->Client Printer Configuration** screen and make sure that the data they entered was correct and available to the ICA server.

Steps for determining the correct NT printer driver name:

1. On the ICA server computer, click **Start**, click **Settings**, then click **Printers**.

2. Double-click the **Add Printer** icon, select **My Computer**, then click **Next**.

3. In the **Available Ports** list box, select **LPT1**, then click **Next**.

4. In the left pane, select the **Manufacturer** of the printer you have installed on your Network Station. In the right panel, scroll to the model of the **Printer** you want the Terminal Server to load as the printer driver.

This is the server printer driver name that you want to use. Write this name down. This exact name will be entered via NSM into the description field of the printer you are configuring.

Manual Connection

Manual connections to local printers must be done each time an ICA session is established.

To print to a local printer in WinFrame

1. In the Main program group double-click the **Print Manager** icon.

   In the **Printer Manager** window you should see an icon, or open dialog box, for a network printer with a name similar to ***workstation#printer*** where ***workstation*** is the IBM Network Station name and ***printer*** is the IBM Network Station name for the printer.

2. If no client printer is available, select **Connect to Printer?** from the **Printer** menu.

3. Double-click the **Client Network** icon in the **Shared Printer** list.

4. Double-click the **Client** icon.

5. Select the client printer icon, which will have a name similar to ***workstation#printer***, and click **OK**.

6. If you want this printer to be your default printer select it in the **Default** menu at the top of the **Printers** window.

To print to a local printer in MetaFrame

1. Click **Start** on the taskbar, point to **Settings**, then click **Printers** on the submenu.

   In the **Printers** window you should see an icon for a network printer with a name similar to ***workstation#printer***, where ***workstation*** is the IBM Network Station name and ***printer*** is the IBM Network Station name for the printer.

2. If no client printer is available, double-click the **Add Printer** icon in the **Printers** window to run the **Add Printer Wizard**.

3. Click the **Network** printer server then click **Next**.

4. Double-click Client Network, and double-click **Client**.

5. Select the printer from the list displayed, and click **OK**.

   Spooled printers available on the IBM Network Station have a name similar to ***workstation#printer***.

6. If you want this printer to be your default printer, click **Yes** then click **Next**.

7. Click **Finish** to complete the process.

Note: The ICA Client printer support is not bi-directional. This means that the printer cannot answer or originate messages.

Connecting to Local Serial Devices

With the ICA Client you can use serial devices attached to any of the COM ports on your IBM Network Station.

COM port mapping does not happen automatically. To map a client COM port

1. Start the ICA Client and logon to the Citrix server.

2. Start a DOS command prompt: ...

At the prompt type net use ***comX: \\client\comZ***: where ***X*** is the number of the COM port on the server (ports 1 through 9 are available for mapping) and ***Z*** is the number of the client COM port you want to map to. Press ENTER.

3. To confirm the operation, type net use at the prompt. The list that appears contains mapped drives, LPT ports and mapped COM ports.

To use this COM port in a session on a Citrix server, install your device to the mapped name. For example, if you map COM1 on the client to COM5 on the server, install your COM port device on COM5 during the session on the server. Use this mapped COM port as you would a COM port on the client computer.

The IBM Network Station ICA Client can map any of the four virtual serial ports (com1 through com4) to any of the defined tty ports (/dev/tty00 through /dev/ttynn) on the Series 300, Series 1000 and Series 2800 Network Stations.

On the Series 2200 Network Station there are USB ports, not serial ports. However, USB to serial port boxes can be used and any of the four virtual serial ports (com1 through com4) can be mapped to any of the defined USB/tty ports (/dev/utty00 through /dev/uttynn).

Series 300 and Series 1000

/dev/tty00	base serial port on the planar board
/dev/tty01	A plug on the multiport serial card
/dev/tty02	B plug on the multiport serial card
/dev/tty03	C plug on the multiport serial card
/dev/tty04	D plug on the multiport serial card

Series 2200

/dev/utty00	A plug on USB to serial port box
/dev/utty01	B plug on USB to serial port box

...

Series 2800

/dev/tty00	serial port 1 on the planar board
/dev/tty01	serial port 2 on the planar board
/dev/tty02	A plug on the multiport serial card
/dev/tty03	B plug on the multiport serial card
/dev/tty04	C plug on the multiport serial card
/dev/tty05	D plug on the multiport serial card

Note: COM port mapping is not TAPI-compatable. TAPI devices cannot be mapped to client COM ports.

Low Bandwidth Considerations

The ICA Client has several performance tuning options that can be set, most of which address network traffic reduction. Network topologies vary greatly as does the instantaneous load they bear. You may need to experiment with the following tuning options to see how they best work in your network.

Number of colors

The ICA protocol supports 16 and 256 colors. Selecting 16 colors produces less network traffic than 256 colors. Operating the ICA server in the same color mode (16 or 256 colors) saves a color conversion on the server side. On the IBM Network Station, 16 color image data takes more processing power than 256 colors.

The default is 256 colors.

Tcp buffering

If your network topology involves any low bandwidth segments and you are noticing slow performance due to the large number of ica packets being sent over the wire, you can configure the ica connection to use a low bandwidth optimization algorithm for small packet transmissions. This will decrease the overall number of packets sent on the wire, which in some low bandwidth situations may improve the overall performance. This should not be used in high bandwidth environments since it can actually slow down the user interface performance.

To enable the low bandwidth optimization algorithm, add the following option to the extra options section of your connection in NSM or add it to your command line parameters if you are creating your own ICA Client commands:

-TcpNoDelay No

The default is **-TcpNoDelay Yes**.

Audio quality levels

There are three selectable audio quality levels - low, medium and high. These levels also represent the amount of network traffic that audio requires, i.e., low audio quality produces less network traffic than high audio quality.

The default is medium.

Persistent caching

Persistent caching only helps in very low bandwidth situations ,e.g., connecting through a modem. **In high bandwidth networks, persistent caching may actually decrease performance**.

The default is no persistent caching.

Compression

ICA protocol compression results in reduced network traffic at the expense of processing power required to run the compression algorithms.

The default is compression on.

Error messages

1: An internal error occurred in the ICA Client.

An internal error has occurred. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

2: unused

3: The option "..." is not valid.

Option "..." is not valid in this context.

4: Missing argument for the option "...".

Option "..." requires an argument.

5: The option "..." has an invalid argument: "...".

The configuration file has been edited directly, or is corrupt.

6: Insufficient memory available.

The client does not have enough memory to continue program execution.

7: Internal Error: E_CLIPPING

An internal error occurred in the ICA Client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

8: Invalid ICA Protocol data received.

This probably indicates a network error.

9: Internal Error: E_TOO_MANY_CALLS

An internal error occurred in the ICA Client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

10: Cannot read file: "..."

There was a problem reading a connection database file.

11: Error in configuration file: "..." Cannot find section "...".

The configuration file has been edited directly, or is corrupt.

12: Error in configuration file. Section "..." must contain an entry "...".

The configuration file has been edited directly, or is corrupt.

13: Internal Error: E_DESTROY_WITHOUT_INIT

An internal error occurred in the ICA Client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

14: Cannot open visual: ...

The visual (ID = ...) cannot support the required number of colors.

15: The visual (ID = "...") cannot support the required number of colors.

Cannot open visual.

16: Cannot allocate sufficient colors. Continuing in 16 color mode.

A suitable visual has been found but it can only support 16 colors.

17: Cannot find a suitable visual on this display.

Unable to allocate a private colormap on this display.

18: Unable to allocate a private colormap for this display.

Unable to get all the color cells needed for a private colormap on this display.

19: Internal Error: E_BUFFER_OVERFLOW

An internal error occurred in the ICA Client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

20: X Server cannot allocate sufficient resource. Request "..."

The X Server was unable to allocate the resources required by Request ... .

21: An error occurred in the graphics system.

There is a problem with the display. Try killing other applications such as Netscape Navigator to release the colors on your display.

22: Cannot find keyboard mapping file "...".

The keyboard mapping file specified in the **Preferences** page of the **Settings** dialog box is invalid or cannot be located.

23: A server must be entered.

A server name must be entered in the **Network** page of the **Properties** dialog box.

24: Window size must be between 300x300 and 1280x1024.

The Custom **Width** field in the **Window** page of the **Properties** and **Settings** dialog boxes can take values between 300 and 1280.

The Custom **Height** field in the **Window** page of the **Properties** and **Settings** dialog boxes can take values between 300 and 1024.

25: Data has been changed. Are you sure you want to quit?

You are quitting from the ICA Client without saving changes to the current connection entry.

26: Data has been changed. Are you sure you want to continue?

You are continuing to execute the ICA Client without saving changes to the current connection entry.

27: Invalid serial number.

Unable to obtain or generate a unique serial for this ICA client.

28: Cannot write file: "..."

There was a problem saving the connection database file; for example, no disk space.

29: Cannot create file: "..."

There was a problem creating a new connection database file

30: The X Request “...” caused error: "..."

An internal error occurred in the ICA Client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

31: Invalid error: Cannot start NCS with this connection.

The connection entry is invalid.

32: unused

33: Internal Error: E_HH_INVALID_DISPLAY

An internal error occurred in the ICA Client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

34: Internal Error: E_HH_UNSUPPORTED

An internal error occurred in the ICA Client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

35: Unable to start child program. Fork failed error: “...”.

The ICA Remote Application Manager was unable to start the ICA Client.

36: unused

37: Cannot read file: "..."

Unable to open an ICA configuration file.

39: Cannot find specified connection.

The configuration file is corrupt. Create a new configuration file.

38: Cannot find specified connection.

The configuration file is corrupt. Create a new configuration file.

40: Error in configuration file: "..." Missing section: "..."

The configuration file is corrupt. Create a new configuration file.

41: Inconsistency in configuration file: "..." Missing section: "..."

The configuration file is corrupt. Create a new configuration file.

42: This description is already in use. The Description must be unique.

The **Description** field in the **Network** page of the **Properties** dialog box must be unique.

43: This description is already in use. The Description must be unique.

The **Description** field in the **Network** page of the **Properties** dialog box must be unique.

44: You must enter a serial number for Net Client to run.

Enter serial number.

45: Invalid Demonstration License. Check that the Authorization Code and Expiry Date are correct.

Not used.

46: Cannot locate executable file "..." (...)

The executable file does not exist or the working directory/ path is incorrect.

47: Cannot execute file "..." (...)

The ICA Remote Application Manager was unable to start the ICA Client.

48: Cannot get address for server "..."

Unable to resolve the server name.

49: Cannot connect to server "..."

Unable to connect to server.

50: Your license does not allow you to connect to this server.

Not used.

51: A Master Browser cannot be located.

The query server cannot locate the Master Browser or the query server cannot be located**.**

52: No servers were found.

ICA servers were searched for but none were found. You may have to (re)set Server Locations in the Settings dialog.

53: Invalid Citrix Server Browser command header received.

An internal error occurred in the ICA Client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

54: Invalid Citrix Server Browser command received.

An internal error occurred in the ICA Client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

55: Invalid Citrix Server Browser command received on request.

An internal error occurred in the ICA Client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

56: Invalid Citrix Server Browser command sequence received.

An internal error occurred in the ICA Client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

57: Citrix Server Browser command contains an invalid parameter.

An internal error occurred in the ICA Client. Contact your IBM representative and report the problem. Provide a detailed description of the scenario that caused the problem.

58: Not enough memory.

The client does not have enough memory to continue program execution.

59: I/O Error.

One of the following problems occurred when attempting to contact a Citrix Master Browser: unable to bind socket, unable to get socket name, unable to set socket broadcast option, unable to set non-blocking option, connection refused, unable to connect.

60: Read Timeout.

Overdue response fro a Citrix Master Browser after multiple attempts. In addition, this may cause a request for the election of a new Citrix Master Browser.

61: IPX protocol is not available.

IPX protocol is not supported on the IBM Network Station.

62: TCP/IP protocol is not available.

Network error. Contact your system administrator.

63: NETBIOS protocol is not available.

NETBIOS protocol is not supported by the IBM Network Station.

64: The Citrix Server you have selected can not located.

The Citrix Server name cannot be resolved.

65: The Citrix Server cluster you have selected can not located.

Not used.

66: Unable to contact the Citrix Server Browser. Either your network is not functional, or you need to configure your an address under Server Browsing.

Either your network is not functional, or you need to configure your an address under Server Browsing.

67: Error in configuration file: "..." Bad Key "...".

The configuration file has been edited directly, or is corrupt.

68: Error in configuration file: "..." Bad Value "...".

The configuration file has been edited directly, or is corrupt.

69: Error in configuration file: "..." Bad Vendor Range "...".

The configuration file has been edited directly, or is corrupt.

70: Unable to perform update: not running as super user.

You must be running as super user to perform a client update.

71: Unable to perform update: client is not on local file system.

The client cannot update an installation on a non-local (e.g. NFS mounted) file system.

72: Unable to perform update: not running $ICAROOT/wfica.

The client cannot update an installation other than its own.

73: Error loading dynamic module: "..." ...

Not used.

74: Must specify proxy server address.

Enter proxy server address in the Firewall Settings under the Properties Box.

75: The option "..." is required.

Missing option “...” when using another option.

76: Cannot connect to the Citrix server. Your Citrix server does not support the encryption you required.

Your Citrix server does not support the encryption you required. Please change the encryption.

Citrix Copyright and acknowledgments