3 Advanced Features

This chapter covers more advanced aspects of the working environment of NCSA Telnet for the Macintosh. It describes how to use the mouse to position the session cursor, open multiple connections, implement commands from the **Connections** and **Network** menus, and use authentication and encryption.

Cursor Positioning with the Mouse

You can use the mouse to position the session cursor if you are using a full-screen editor that supports the arrow keys. One such editor is vi. When the mouse cursor is in a session window, holding down the OPTION key changes the mouse cursor into a rectangle. When the mouse cursor is in the session window, holding down the OPTION key and simultaneously pressing the mouse button instructs NCSA Telnet to send a sequence of arrow keys to move to that position on the screen.

NOTE: If your editor is EMACS rather than vi, you should either set the **EMACS arrow keys** option in the session configuration record or check the **EMACS arrow mapping** command in the **Session** menu

Multiple Connections

NCSA Telnet lets you use multiple connections, either to a single host or to several different hosts.

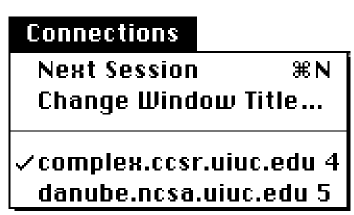
Opening More Than One Connection

To open another connection, follow either the opening-a-connection procedure presented in “Opening and Closing a Connection” on page 1–2 or the saved-set instructions in “Loading a Saved Set” on page 2–15.

The *active* session is the connection with which you are currently working. The active session’s window is generally frontmost on your desktop.

Moving between Connections

To switch between sessions and to make a new session window your active session, bringing it to the front, either click on the session window for the desired connection or select the desired session name from the **Connections** menu.



To activate the session window directly beneath the current session window, select **Next Session** from the **Connections** menu or press ⌘-N (for *next*).

NCSA Telnet opens new session windows on the screen relative to the number of windows currently opened. You can specify that these windows be staggered by just a few pixels or by the whole window title bar. See the description of the **Staggered Windows** option in“Global Preferences” on page 2–1.

Rules for Session Names

When you open multiple connections to a single host, it is useful to specify session names (other than the hostname) for the connections. You may use any of the following for session names:

- the host’s full Internet address, such as `192.17.22.20`
- any session configuration record alias (see “Editing Session Configuration Records” on page 2–5)
- any name, such as `sri-nic.arpa`, that can be resolved by the domain-based nameserver

NOTE: Some systems, such as MFENET, do not use the standard telnet port number 23. If you need access via the telnet protocol to a different port number, in the **Open Connection** dialog box enter the port number after the session name; the session name and port number must be separated by one or more spaces. For example, to open a connection to port 23 of `myhost.network.arpa`, in the **Host/Session Name** box of the **Open Connection** dialog box, enter **`myhost.network.arpa`**. To open a connection to port number 911 of the same host, enter **`myhost.network.arpa 911`**. You can also specify alternate port numbers in your session configuration records.

The Connections Menu

You can specify titles that are different from the session names for your session windows so that you can easily distinguish between multiple sessions and session windows.

Naming Windows

To specify a window title, enter the desired name in the **Window Name** box of the **Open Connection** dialog box.

NOTE: If the **Window Name** box is blank when you open a connection, NCSA Telnet automatically numbers the session. Each time you open a session, the number increases, no matter how many sessions are currently open.

Checking Session Status

The **Connections** menu contains the window names for current connections and the status of each session. A checkmark (✓) next to a *window* name indicates an active session, and a diamond (◆) or circle (·) next to a *session* name indicates an attempted connection that has not yet successfully opened. More specifically, a diamond indicates that NCSA Telnet is checking the nameserver to find the session name or hostname; a circle means NCSA Telnet is trying to open the session. Once the connection is established, the diamond or circle next to the session name goes away and the session window appears.

NOTE: If you do not remember the meaning of these symbols, select **Marked Connection** from the **Connections** menu. The **Connection Status** dialog box then reports the name and status of the connection. After you read the message, click the **OK** button (or press RETURN) to proceed with opening the connection, or click the **Abort** button to cancel the attempt.

Aborting Connection Attempts

To abort an attempted connection attempt:

1. Select the desired connection from the **Connections** menu. The **Connection Status** dialog box appears, reporting the name and status of the connection.
2. Click the **Abort** button in the **Connection Status** dialog box.

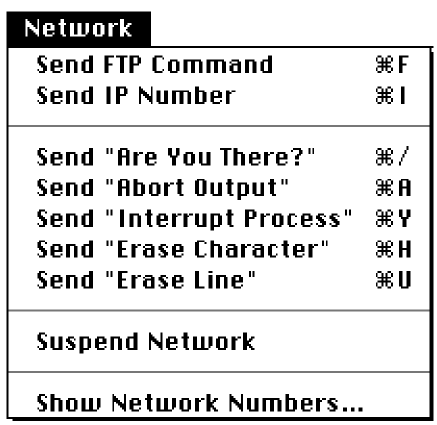
Changing a Window Title

Select **Change Window Title...** from the **Connections** menu to change the window title of the frontmost window.

The Network Menu

NCSA Telnet supports several special commands defined by the Internet standard telnet protocol. Each host telnet implementation treats these commands differently, so they may have no effect on some hosts.

The **Network** menu includes seven telnet commands as well as two network-related commands:



Telnet Commands

Command	Description
Send FTP Command	When you select this command, NCSA Telnet sends an FTP command to the remote machine. Normally the command is `ftp` *w.x.y.z* (where *w.x.y.z* is the IP address of your Macintosh) followed by a return character. However, if the FTP server is in anonymous mode, NCSA Telnet

sends the command `ftp -n` *w.x.y.z* followed by a return character. You can force NCSA Telnet to omit the `-n` option if you hold down the SHIFT key. For more information about FTP commands, see "File Transfer" on page 4–1.

Send IP Number When you select this command, NCSA Telnet sends the IP address of the Macintosh you are using to the remote machine as if you typed it in manually.

Send "Are You There?" Use this command whenever you are not sure whether the network and host are up. Every once in a while, especially when the host is bombarded with incoming information or tied up by a large number of users, the host doesn't seem to respond to your commands. When this happens and your terminal appears to have locked up, you can select this command to determine whether you are still connected to the host. The host is supposed to respond, if able, with a readable message. Some machines answer `Yes`; others answer with more informative messages.

Send "Abort Output" This command is supposed to throw away all output from the current process and then resume when there is a pause. Very few hosts implement this command correctly.

Send "Interrupt Process" Available on nearly every telnet host, this command stops the current process and throws away all pending data for the connection. It is equivalent to pressing CONTROL-C on most UNIX systems. You can set your Macintosh keyboard so that CONTROL-C sends the **Send "Interrupt Process"** command; select the **Setup Keys...** command in the **Session** menu, as described in "Changing Configuration after Session Connected" on page 2–9.

Send "Erase Character" *and*

Send "Erase Line" You can erase either the last character or the current line by selecting **Send "Erase Character"** or **Send "Erase Line"**, respectively. Many hosts do not implement these commands but use their own special characters instead.

Network-Related Commands

The **Network** menu includes two of NCSA Telnet's network-related commands:

Command	Description
Suspend Network	Select this command to temporarily suspend all network communications and disable all receive functions. All of your connections are kept alive, but you do not see any incoming text. **NOTE:** Generally you should use the `Suspend` and `Resume` commands rather than the `Suspend Network` command. See the discussion of the `Interrupt`, `Suspend`, and `Resume` commands in "Editing Session Configuration Records" on page 2–5.
Show Network Numbers	Because NCSA Telnet now uses MacTCP for all network communications, this command is largely unnecessary. However, for purposes of continuity, selecting this command displays your Macintosh's IP address in a dialog box but does not transmit the address. Click on the dialog box to remove it.

Authentication and Encryption

NCSA Telnet supports Kerberos Version 4 authentication (from Cornell University) and DES encryption.

Computer users traditionally have entered passwords to log on to their accounts on hosts. While passwords have provided some level of security, a proliferation of methods for snooping passwords off the Internet has greatly reduced the security provided by passwords.

Kerberos provides a system that *authenticates* a user to hosts. After you enter your password once, that password is usedto gain a *ticket* from a Kerberos server. You use this ticket to log on to Kerberos-aware hosts without entering your password: the ticket guarantees that the person making the connection is who you say you are (i.e., because you are the authentic person, you are authenticated). The method used to gain the ticket does not require that your password pass over the network in an easily snooped form.

Even with the authentication features of Kerberos, NCSA Telnet connections are still subject to snooping. Data you send and receive can be snatched from the network and viewed by others. However, when NCSA Telnet sets up an *encrypted* connection, data are scrambled before passing between your Macintosh and a remote host. Such data are significantly more protected than unencrypted data. Encryption is not foolproof, but it does stop the majority of attempts to snoop through your data.

NCSA Telnet requires that an authenticated connection be in place before using encryption.

Preparing Your Environment

NCSA Telnet uses Cornell University's Kerberos driver package (Kdriver) for Kerberos and encryption support routines. Kdriver, which supports Kerberos Version 4, requires that each Kerberos server host also run a UDP daytime server. KConfig (an application written by Rick Watson of the University of Texas) is used to configure Kdriver settings.

You can download the `Kerberos Client` extension and the KConfig application from NCSA's anonymous FTP server. (See "Anonymous FTP Server" on page C–1.) If you use a version of the Cornell Kerberos driver obtained from a source other than NCSA, encryption is not supported, some setting changes made by KConfig won't be saved in the `Preferences` file, and the ticket may display garbage for the user realm.

You also need to know pertinent information regarding your site's Kerberos server. If you are an administrator, you need to install a Kerberos server for your site. Installing a Kerberos server is beyond the scope of this manual.

NCSA Telnet for the Macintosh Version 2.6 supports the telnet authentication and encryption options described in the RFC1411/1416 and IETF drafts dated July 1991. Future versions may support the IETF draft AUTH_ENCRYPT option described in the draft dated April 1993.

Installing Software

To implement either authentication or encryption, you must install Kdriver in the `System` folder on your Macintosh. Drag the `Kerberos Client` extension to your closed `System` Folder. If you are running System 7, you are asked to verify that the file is to be placed in your `Extensions` folder.

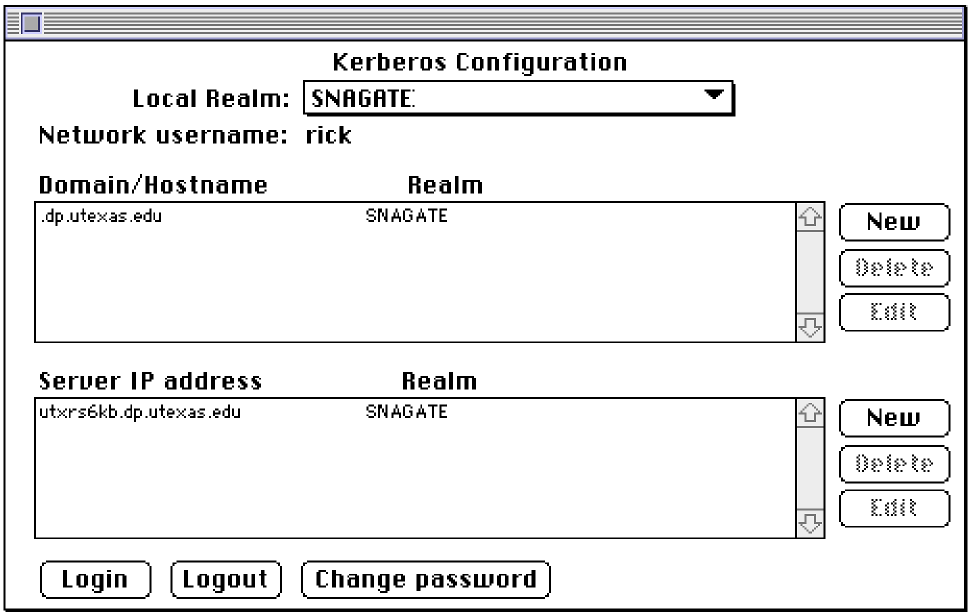
Reboot your Macintosh and use KConfig to configure settings for your Kerberos environment. All KConfig settings are made in the **Kerberos Configuration** window.

Mapping Kerberos Realms to IP Names

This section assumes you are familiar with Kerberos.

A domain/hostname-to-realm map attempts to match a Kerberos realm with IP domain names. Use KConfig to set up domain/hostname-to-realm maps, which are useful if you support more than one Kerberos realm.

You may (or may not) have to reboot after entering your initial settings in the **Kerberos Configuration** dialog box.



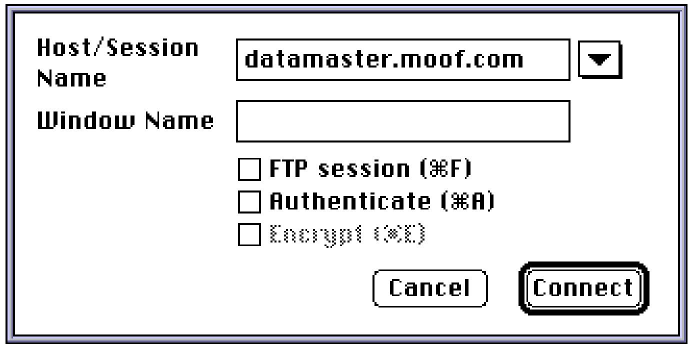
Option	Description
Domain/Hostname . . . Realm	Enter the domain or host name for each Kerberos host you are using.
Server IP address . . . Realm	Enter the Kerberos server's IP address or hostname for each Kerberos realm you are using. After entering your Kerberos servers, you can pick your local realm using the **Local Realm:** popup menu at the top of this dialog box.
Login	Click this button to authenticate to a Kerberos server and obtain an initial ticket-granting ticket for other services. You don't have to log on using KConfig; NCSA Telnet prompts you when a password is needed.
Logout	Click this button to destroy all tickets. Select **Show Credentials** from the **File** menu to display all your Kerberos tickets.
Change Password	Click this button to change your Kerberos password.

Activating Authentication and Encryption in NCSA Telnet

Authentication and/or encryption options appear in two places in NCSA Telnet:

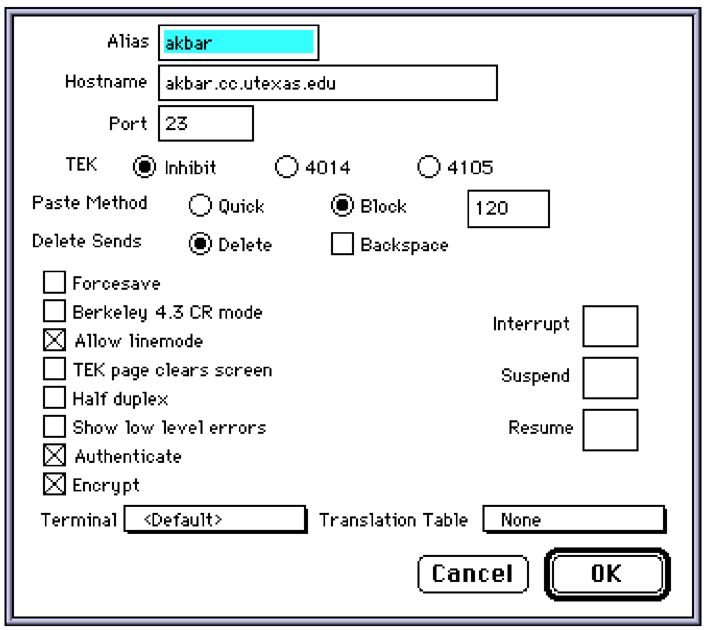
- In the **Open Connection** dialog box. See "Opening a Connection" on page 1–2.
- In the **Session Configuration Record** dialog box. See "Editing Session Configuration Records" on page 2–5.

In the **Open Connection** dialog box, you can select the **Authenticate** and **Encrypt** options when you open a session. These options apply to the default session.



NOTE: The **Authenticate** option is required for encryption. FTP sessions cannot currently be authenticated or encrypted.

In the **Session Configuration Record** dialog box, select the appropriate options for each session that you configure, including the default session.



Indicating Active Encryption

NCSA Telnet displays encryption icons next to the zoom box in the window's title bar. For example, see the padlock icon below:

A padlock icon indicates that a session is two-way encrypted, which means that data are encrypted both going to and coming from the server. If any other icon is displayed, the session is not two-way encrypted. An arrow indicates that the session is encrypted in one direction only—either boging to or coming from the server—and is probably evidence of a bug in either the NCSA Telnet code or in your telnet server. The absence of any icon means that no encryption is taking place.