# ANSWERS TO TOUGH QUESTIONS



---

**Can you summarize the Options/Preferences menu items?**

**Window style**

Designate a home page and specify the style of toolbar buttons and content area fonts.

**Link style**

Choose the underlining, color, and color longevity of highlighted text links.

**Network**

Specify the size in kilobytes of your memory cache and disk cache (Windows), the location of the Cache directory (Windows), the size of a network buffer (Macintosh), and the maximum number of network connections (Macintosh).

**Images**

Determine a priority for loading images and, depending on the platform, the manner that colors are approximated.

**Security**

Specify whether you receive notification dialog boxes regarding the state of a document's security.

**Directories**

Designate the Temporary directory (before a helper application launches a file, Netscape saves the file to disk in the Temporary directory). Also, designate the Cache directory (Macintosh).

**Applications**

Specify the location of these supporting applications: Telnet, HTML Source Viewer, and TN3270.

**News**

Specify the host name for the news server (that supplies Usenet newsgroups), a News RC file, and display criteria.

**Mail**

Specify a mail server, your user name, and your e-mail address to establish a viable incoming mail address (so others can respond to Netscape mail you send).

**Proxies**

Designate proxies and ports for FTP, HTTP, Gopher, News, and WAIS protocols, and depending on the platform, a SOCKS host.

**Helper Applications**

Map Mime types and extensions of external applications and, depending on the platform, actions to take.

---

**What does each part of an Internet address mean?**

The first part, **yourName**, identifies a user. The @ symbol (pronounced "at") separates the user name from the location of the server computer. The last part, **aserver.bserver.org**, identifies the location of the server computer. Addresses use lowercase letters without any spaces.

The name of a location contains at least a string and, typically, a three-letter suffix, set apart by a dot (the period symbol is pronounced "dot"). The name of a location might require several subparts to identify the server (a host name and zero or more subdomains), each separated by dots . The three-letter suffix in the location name helps identify the kind of organization operating the server. (Some locations use a two-letter geographical suffix.) Here are the common suffixes and organizational affiliation:

- **.com** (commercial)
- **.edu** (educational)
- **.gov** (government)
- **.mil** (military)
- **.net** (networking)
- **.org** (noncommercial)

E-mail addresses from outside the United States often use a two-letter suffix designating a country. Examples are:

- **.jp** (Japan)
- **.uk** (United Kingdom)
- **.nl** (The Netherlands)
- **.ca** (Canada)

---

**Where do I find helper applications?**

Choose the **Help/Release Notes** menu item to find sites for downloading helper application software. To install and configure helper applications (many are already configured), use the **Helper Applications** panel.

Helper applications expand Netscape's abilities. Netscape uses these applications to let you automatically decompress downloaded applications, listen to sounds, play movies, and get better display of images. Most can be obtained free or as shareware.

Compression: You may find that programs are stored on the Internet in formats that your computer doesn't understand. You may need to locate a helper application program like PKUNZIP (Windows) or Stuffit Expander (Macintosh) to translate and decompress downloaded software (and other helper applications).

Sounds: Most sound files aren't in a format that your computer can automatically play. To listen to the different types of sound files such as ULAW (common **.au** files), AIFF, and WAV, you'll need to install a helper application that understands them.

Pictures and Movies: Netscape can display **gif**, **jpeg**, and **xbm** files internally, but you may prefer to use a dedicated image viewer. To have Netscape automatically launch an external viewer, select the **Mime Type** in the list, then choose the radio button **Launch Application**. (On UNIX, you'll use a **.mailcap** file to supply a path and file name.) You'll need a player to view **mpeg** movies.

---

**What are the MIME types used by helper applications?**

HTTP (HyperText Transport Protocol) servers use HTML formatting. Netscape software has the built-in capability to read HTML-formatted pages (as well as the **gif**, **jpeg**, and **xbm** graphic file formats). Netscape can interpret many other file formats with the help of external helper applications. To accommodate the file formats requiring helper applications, Netscape keeps a mapping of file formats to helper applications.

MIME (Multipurpose Internet Mail Extensions) is a standardized method for organizing divergent file formats. The method organizes file formats according to the file's MIME type. When Netscape software retrieves a file from a server, the server provides the MIME type of the file. Netscape uses the MIME type to establish whether the file format can be read by the software's built-in capabilities or, if not, whether a suitable helper application is available to read the file.

For servers that do not provide a MIME type with a file, Netscape interprets the file's extension (a suffix appended to a file name). For example, the **.html** extension in the file name **welcome.html** suggests a file in the HTML format. Likewise, a **.zip** extension suggests a compressed file, an **.rtf** extension suggests a file in the Rich Text Format, and so on. You can view and configure the mapping of all MIME types to helper applications by using the **Helper Applications** panel. (On UNIX, edit your global or personal MIME types file whose pathname is designated.)

Technical note: The panel currently lacks a **Delete** button and the ability to assign arbitrary values to file types. If needed, advanced users might want to edit the preferences file directly.

---

**Can you summarize the Usenet newsgroup screens?**

Before you can use news for the first time you need to configure Netscape to point to your Usenet news server. Set the host name of your NNTP server in the **News** panel.

Your newsgroup subscription information is stored in a **News RC** file. If you have no previous **News RC** file, Netscape creates one that lists a couple of newsgroups designed for new users.

**Subscribed newsgroups**
Shows a listing of all the Usenet groups that you have subscribed to and lists the number of unread articles in each newsgroup. This view also allows you to subscribe and unsubscribe to newsgroups.

**Newsgroup listing**
Shows a list of all the unread articles in a threaded format. The threaded format groups all articles that are related to each other in a compact, ordered listing. Articles that are responses to previous articles are nested under the parent articles.

**Article listing**
Shows a single article. The article listing allows you to read the article, post a reply to the newsgroup, or send a mail reply to the original poster. The article may contain links to other articles or Internet pages.

**News posting**
Allows you to post a new article to a newsgroup.

**News followup**
Allows you to enter a reply to an existing news article and post the reply to the newsgroup.

---

**Why might I use Gopher?**

Some information on the Internet is offered through Gopher servers. When you want information that happens to be on a Gopher server, you'll click on a link whose URL begins with **gopher** (or enter the URL in the location field).

Netscape lets you access Gopher servers in the same way you access World Wide Web (**http**) pages. Though Gopher pages lack rich formatting, menu listings allow you to bring content pages or additional menu sublistings.

A menu is presented as a list of links, each link preceded by a small icon indicating the type of resource the link brings. For example, Gopher links can bring you:

- menus
- text files
- images
- indexes
- movie and binary files

Gopher indexes use form pages to allow you to find information on Gopher servers. An index page typically provides an editable field for you to enter a search string and a button for you to submit the form to the Gopher server. The results of the search are a Gopher menu listing items that match your search criteria.

Some files, such as short digital movies, require the use of Netscape's helper applications. If available, Netscape automatically launches the helper application required by a Gopher link.

---

**Why might I use FTP (file transfer protocol)?**

By clicking on a link whose URL begins with **ftp** (or by entering the URL in the location field), you can navigate directories, view files (including **html** and **gif** files), and download software. For example, the **Help/Release Notes** page offers several **ftp://pathname** links to FTP server sites for downloading helper application software.

Netscape lets you access FTP servers in the same way you access World Wide Web (**http**) servers. However, you may find the FTP directory and content pages have minimal formatting. When possible, Netscape shows the type, size, date and a short description of each file in a directory.

A directory is presented as a list of links, each link often preceded by a small icon indicating another directory or a file. Clicking on a directory link brings you a subdirectory. Typically, at the top of a subdirectory is link that brings you the parent directory.

Clicking on a text, **gif**, or **jpeg** file displays the file. Clicking on a binary file or program automatically downloads the software to a folder (designated in the **Directories** panel) on your computer. After downloading, Netscape automatically looks for a suitable helper applicationto launch the file. If the necessary helper application is not available, Netscape presents you with a dialog box asking whether you want to save or discard the downloaded software.

---

**What is a cache and how does it work?**

A cache temporarily stores the information on a page in your computer. If you request a page that is stored in a cache, Netscape can retrieve the page from the cache more quickly than retrieving the page again from its location out on the network.

The first time you ask for a page, Netscape retrieves the page from the network. No pages are permanently stored in a cache, but each page you bring is temporarily stored in a cache. If you request a page you have seen before, Netscape checks to see if the page is available in a cache. For example, if you use the **Back** button to bring a page, a cache can display the page more quickly than the network can retransmit it.

Sometimes you may not want a page to be retrieved from a cache. The page you brought initially may no longer be identical to the page currently offered by the network. If a modification to a particular URL has occurred, you may want the updated page rather than the copy (now stale) stored in a cache. Remember, you have no control over when a server updates its pages.

When you click on a link, choose a bookmark, enter a URL, or press the **Reload** button, Netscape checks with the server to see if an update has occurred before bringing a page from a cache. If any change to the page has occurred, a fresh version is transmitted over the network; otherwise, a copy is quickly retrieved from a cache.

When you press the **Back** button or choose a history item, Netscape does no such check. Since you are explicitly requesting a previously viewed page, Netscape tries first to retrieve the cached copy (if still present in the cache) even if the server offers a more recent version.

---

**What is the difference between memory cache and disk cache?**

Netscape supports two kinds of caches to improve performance and reduce network traffic. When you bring a page from the network, information is stored in both a memory cache and a disk cache. Netscape retrieves a page from the memory cache more quickly than from the disk cache, though retrieving from the disk cache is still faster than fetching from the network.

The disk cache has the advantage of persistence. When you exit a session (quit the Netscape application), the memory cache is emptied, but the disk cache is maintained (and takes up space on your hard disk).

Sometimes a cache can get confused (such as when servers provide inaccurate page modification dates). If you suspect a cache is acting improperly (such as providing stale pages) or just wish to free up space, you can clear the caches by pressing the **Clear Memory Cache Now** and **Clear Disk Cache Now** buttons in the **Network** panel (only **Clear Disk Cache Now** in the **Directories** panel on Macintosh).

---

**What is the recommended size for each cache?**

You can change the size of each cache to maximize its effectiveness. A larger cache may increase Netscape performance, though allocating too much space may constrict other applications. You might try to increase the size of the memory cache to whatever your system routinely has unused and increase the disk cache to between 2,000 and 5,000 kilobytes (2 and 5 megabytes).

You might find that a large disk cache increases the time required for the Netscape application to quit. If Netscape's cache maintenance causes undue delay when you exit the program, consider reducing size of the disk cache.

On Macintosh, the memory cache size is set (like other Macintosh applications) in the **Get Info** dialog box (from the Finder, select the Netscape application and choose the **File/Get Info** menu item); the disk cache size and location are set in the **Directories** panel. A **Browse** button in the dialog box allows you to set the directory location of the disk cache. By default, Netscape places the Macintosh disk cache inside the Netscape Preferences folder within the System Folder.

On UNIX, cache size and location preferences are set in the Cache panel. An editable field in the panel allows you to set the directory location of the disk cache.

---

**Where can I learn more about the company and its products?**

The **Welcome!** page provides links for getting started on the Internet and obtaining Netscape products. You'll find up-to-date information on sites offering Netscape software.

The **Netscape Communications Corporation** page offers links for news and information about the company. This page can direct you to most of the content pages produced by the company.

The **On Security** page contains links to a technical description of Netscape's approach to data security on the Internet and security protocol specifications.

The **Release Notes** page has current information particular to platform you are running, including answers to commonly asked questions, links for obtaining updated software and helper applications, and status reports on known bugs, available workarounds, compatibility issues, and forthcoming enhancements.

You may find substantial overlap in links from one page to another. You'll want to create bookmarks for the locations you consider valuable (or, without fear of blasphemy, write down the URL on paper). The roadside pundit who said "you can't get there from here" needs to change the old saw to "you can get there from anywhere if you know where there is."

---

**Where can I learn about Internet security?**

The Internet security technology developed by Netscape Communications to ensure private and authenticated communications (called SSL, short for Secure Sockets Layer protocol) is an open platform put into the public domain for the Internet community. Netscape Navigator and the Netsite Commerce Server are the first products to offer this nonproprietary technology.

Choose the **Help/On Security** menu item for links to:

**Netscape Navigator Handbook**
The introductory information in the handbook tells you why you need security on the Internet and how to recognize the security features built into Netscape Navigator.

**Internet Data Security**
This technical document provides an overview of security implementation and plans from Netscape Communications. You'll find a summary of SSL and details on how Netscape Navigator and the Netsite Commerce Server use SSL.

**Using RSA Public Key Cryptography**
This technical tutorial illustrates the basic tenets employed by Netscape's security technology, including public and private keys, message digests, digital signatures, and certificates. You can also obtain general security information and Netsite security product information directly from RSA Data Security, Inc.

**The SSL Protocol**
This comprehensive, highly technical document is the specification for the Secure Sockets Layer protocol. Appendices include a glossary and a description of potential security attacks.

---

**Can I safely transmit personal information such as credit card numbers?**

You can enter your credit card number on a secure (**https**) Netscape Navigator form and transmit the form over the Internet to a secure Netscape Commerce Server without risk of an intermediary obtaining your credit card information. The security features offered by Netscape Communications technology protects commercial transactions, as well as all other communications, from misappropriation and fraud that could otherwise occur as information passes through Internet computers.

Secure communications does not eliminate all of an Internet user's concerns. For example, you must be willing to trust the server administrator with your credit card number before you enter into a commercial transaction. Security technology secures the routes of Internet communication; security technology does not protect you from unreputable or careless people with whom you might choose to do business.

The situation is analogous to telling someone your credit card number over the telephone. You may be secure in knowing that no one has overheard your conversation (privacy) and that the person on the line works for the company you wish to buy from (authentication), but you must also be willing to trust the person and the company.

Server administrators must take additional precautions to prevent security breeches. To protect your information, they must maintain physical security of their server computers and control access to software passwords and private keys.

---

**How does Netscape's security technology protect me?**

The security features built into Netscape Navigator and the Netsite Commerce Server protect your

Internet communications with:

- Server authentication (thwarting impostors)
- Privacy using encryption (thwarting eavesdroppers)
- Data integrity (thwarting vandals)

Without thorough security, information transmitted over the Internet is susceptible to fraud and other misuse by intermediaries. Information traveling between your computer and a server uses a routing process that can extend over many computer systems. Any one of these computer systems represents an intermediary with the potential to access the flow of information between your computer and a trusted server. You need security to make sure that intermediaries cannot deceive you, eavesdrop on you, copy from you, or damage your communications. The Internet does not provide built-in security.

The SSL protocol delivers server authentication, data encryption, and message integrity. SSL is layered beneath application protocols such as HTTP, SMTP, Telnet, FTP, Gopher, and NNTP, and layered above the connection protocol TCP/IP. This strategy allows SSL to operate independently of the Internet application protocols.

With SSL implemented on both the client and server, your Internet communications are transmitted in encrypted form. Information you send can be trusted to arrive privately and unaltered to the server you specify (and no other).

---

**To what degree can SSL security protect me?**

SSL uses authentication and encryption technology developed by RSA Data Security Inc. For example, Netscape Navigator's export implementation of SSL (U.S. government approved) uses a medium-grade, 40-bit key size for the RC4 stream encryption algorithm. The encryption established between you and a server remains valid over multiple connections, yet the effort expended to defeat the encryption of one message cannot be leveraged to defeat the next message.

A message encrypted with 40-bit RC4 takes on average 64 MIPS-years to break (a 64-MIPS computer needs a year of dedicated processor time to break the message's encryption). The high-grade, 128-bit U.S. domestic version provides protection exponentially more vast. The effort required to break any given exchange of information is a formidable deterrent. Server authentication uses RSA public key cryptography in conjunction with ISO X.509 digital certificates.

Netscape Navigator and Netsite Commerce Server deliver server authentication using signed digital certificates issued by trusted third parties known as certificate authorities. A digital certificate verifies the connection between a server's public key and the server's identification (just as a driver's license verifies the connection between your photograph and your personal identification. Cryptographic checks, using digital signatures, ensure that information within a certificate can be trusted.

To evaluate the strategic and quantitative implications of the SSL implementation of certification and public key technology, consult the **SSL Protocol** specification.

---

**How can I tell when security is in effect?**

You can tell whether a document comes from a secure server by looking at the location (URL) field. If the URL begins with **https://** (instead of **http://**), the document comes from a secure server. To connect to an HTTP server that provides security using the SSL protocol, insert the letter "s" so that the URL begins with **https://**. You need to use **https://** for HTTP URLs with SSL and **http://** for HTTP URLs without SSL.

You can also verify the security of a document by examining the security icon in the bottom-left corner of the Netscape Navigator window and the colorbar across the top of the content area. The icon consists of a doorkey on a blue background to show secure documents and a broken doorkey on a gray background to show insecure documents. The doorkey has two teeth for high-grade encryption, one tooth for medium-grade. The colorbar across the top of the content area is blue for secure and gray for insecure.

A mixed document containing secure and insecure information is displayed as secure with insecure information replaced by a mixed security icon. Some servers may permit you access documents insecurely (using **http://**) to view mixed documents in full.

More detailed security information can be found by choosing the **File/Document Information** menu item. Several configurable notification dialog boxes inform you when you are entering or leaving a secure space, viewing a secure document that contains insecure information, and using an insecure submission process. You'll always be warned if a secure URL is redirected to an insecure location, or if you're submitting via a secure form using an insecure submission process.

---

**What does the Document Information dialog box tell me?**

Choosing the **File/Document Information** menu item produces a dialog box with a document's title, location (URL), date of last modification, character set encoding, and the security status of a document, Secure documents specify the type of encryption protecting the document and the version, serial number, issuer, and server subject of the certificate backing the document.

**Encryption Key**
States the type of public key supported. For example, the high-grade encryption key for U.S. domestic use only (RC4, 128-bit) refers to the 128-bit key size for the RC4 stream encryption algorithm.

**Subject (server id)**
The certification request process requires that each server administrator supply an e-mail address and certain identifying information. Identifying information may include:

- Country (C): two-character country code
- State or Province (ST): unabbreviated state/province name
- Organization (O): legal, registered organization name
- Organizational Unit (OU): optional department name
- Locality (L): city the organization resides or is registered in
- Common Name (CN): the server's fully qualified host name (such as: hostname.netscape.com)

**Issuer (certifier id)**

Identifies the certificate authority responsible for issuing the certification is identified. Identifying information is presented using the same abbreviations as those used to identify the server (C, for country, and so on).

**Are certificates required and where do you get one?**

Currently, certificates are issued to organizations running servers and are not issued to Netscape Navigator users. To operate using security features, the Netsite Commerce Server requires a digitally signed certificate. Without a certificate, the server can only operate insecurely. If you are a server administrator and want to obtain a signed certificate, you need to submit a certificate request to a certificate authority, a third-party organization that issues certificates, and pay an associated service fee.

Netscape Communications has engaged RSA Certificate Services, a division of RSA Data Security, Inc., to issue certificates to Netsite customers and will engage other certificate authorities over time. The process to obtain a certificate is explained in the Netsite Commerce Server manual. During the certificate request process, your server software generates a public key/private key pair and you choose a distinguished name. Online forms guide you through the process of submitting the form to RSA.

RSA verifies the authenticity of each certificate request (making sure requesters are who they claim to be). The approval process helps protect you, your organization, and the certificate authority. Upon approval, RSA digitally signs the request and returns the unique digitally signed certificate to you through e-mail. You can then install the signed, valid certificate and enable security. You'll need to establish adequate precautions to maintain the integrity of the signed certificate and your private key.

**Can one certificate be used on multiple servers?**

Technically, one certificate can be used on multiple servers, however risks are involved that would discourage this choice in many circumstances. If the same certificate is used on multiple servers, any compromise of one server's public key and private key pair endangers information on the other servers.

(Certificates are protected by public and private key pairs linked by a powerful cryptographic algorithm. These keys have the ability to encrypt and decrypt information. No one else's keys can decipher messages to you encrypted with your public key. And no one else's keys can be used to pose as you by sending messages encrypted with your private key.)

Similar risks would be incurred if you were to choose to secure your house, office, car, safety deposit box, and bike with the same key. You would only have to carry around a single key, but you would not have the flexibility to provide access to one item without providing access to all items. If security was compromised for one item, it would also be compromised for other items.

Multiple servers that are running on the same piece of hardware can technically use the same certificate. However, as your software installations expand, the need for different levels of security and individual keys increases. The security requirements for information served at remote locations or on separate hardware are best satisfied by unique certificates.

**Do security features impose any limitations on the ability to access sites?**

The security protocol works as an adjunct to other protocols without limiting access capabilities. You can use Netscape Navigator to bring either secure or insecure documents. Nor does security limit Netscape's Usenet news or electronic mail abilities.

If a document that is otherwise secure contains information that is insecure, the insecure information is replaced by a mixed security icon. However, a server may permit you to bypass this security feature by accessing the mixed security document through the insecure **http** protocol instead of the secure **https** protocol. The security aspects of SSL protect you from insecure transmissions, but do not limit your ability to receive insecure transmissions.

Online forms can be secure if the submit action is an **https://** URL to a secure server. Netscape Navigator uses dialog boxes to inform you about security status of the submission process when you submit a form.

You can save a secure document (though secure documents are not cached to disk among sessions). You can also view the HTML source of a secure document. Security affects the transmission of a document without affecting your ability to manipulate the document.

---

**How can I save files and images onto my hard disk?**

The **File/Save As** menu item produces a dialog box that permits you to save a page locally (onto your hard disk) in source format or text format. The source format produces a text file encoded with the HTML necessary to reproduce the formatted text or image faithfully; the text format saves text without HTML.

You can also save a page to disk without bringing the page to screen. Position the mouse over a link or image, then click the right-side mouse button (on Macintosh, hold down the mouse button) to produce a pop-up menu with the items **Save this Link as** and **Save this Image as**. These menu items produce a dialog box for saving a file. Clicking on any link with the shift key held down (option key on Macintosh) also produces a save dialog.

Saving a file onto your hard disk allows you to display the page's information without any network connection. You can choose **File/Open File** to display the HTML-formatted text or graphic image of any local file saved in source format (though a page's inline images are replaced with icons). For **gif**, **jpeg**, or other nontext files to show up in the **Open File** dialog, you'll need to select "All Files" or, on Macintosh, hold down the option key while selecting the **Open File** menu item.

The pop-up menu item **View this Image** lets you see an isolated image file. The pop-up menu item **Copy this Image Location** copies the URL of the image file to the clipboard. With the URL, you can choose to open the image at any time. Once open, you can save the image onto your hard disk in source format using **File/Save As** or the pop-up menu (more easily than using **View/View Source** to find the URL of an inline image embedded in HTML code).

---

**What is dithering and how is it used?**

Dithering is a software imaging process for arranging adjacent pixels of varying shades into order to achieve a visual effect. The process often enhances a computer's ability to display an image, particularly useful when the color or resolution of the original image must reproduced on computers with different display capabilities.

Netscape' display of inline **gif** and **jpeg** sometimes needs to translate an image's colors into similar colors available on your computer. If your computer doesn't have color capabilities that match the color information in an image, the image may look speckled.

On Windows, you can choose radio buttons in the **Images** panel to **Dither to Color Cube** or **Use Closest Color in Color Cube**. **jpeg** images, however, are always dithered.

When you choose to **Dither to Color Cube**, Netscape dithers the computer's available colors to most closely match the image's colors. When you choose **Use Closest Color in Color Cube**, Netscape substitutes an available color that most closely matches the image's colors. Images that are displayed with dithering take slightly more time to display than images using color substitution.

On Macintosh, dithering for all images is built-in and cannot be turned off.

---

**How do you organize bookmarks and create hierarchical menus?**

Hierarchical bookmarks allow you to thematically organize bookmarks using headers and their submenus. The name you choose for a header should describe a category of related pages. When you have a large number of bookmarks, a hierarchical arrangement allows you to effectively use limited screen space by spreading the display of bookmarks horizontally.

To manipulate bookmarks in general, choose the **Bookmarks/View Bookmarks** menu item and select the appropriate buttons in the **Bookmark List** dialog box. See the menu items section of the handbook for a complete description of bookmark options.

To create and manipulate hierarchical bookmarks, first define header items in the list in the **Bookmark List** dialog box, then insert bookmark items indented (in outline form) below each header. Items indented under headers in the bookmarks list become submenus under headers in a pull-down menu. The **Up** and **Down** buttons (arrows on the Macintosh) control the line position and indention of items. The actions of **Down**, described in parentheses below, perform the opposite of **Up**.

Typically, pressing the **Up** (**Down**) button swaps the positions of the current selection and the item directly above (below) the current selection. However, the **Up** (**Down**) button behaves as follows: if the current selection is a header, the header and its sub-items move as a single item; if the item directly above (below) the current selection is indented to the right (positioned to the left) of the current selection, pressing the **Up** button indents the current selection (reverses a single indent).

---

**How do you convert hotlists to bookmarks?**

Other browsers use hotlists similar to the way that Netscape uses bookmarks. Users of other browsers may wish to preserve the URLs they have accumulated as hotlists by converting them to bookmarks.

Netscape has an **Import** button in the **Bookmark List** dialog box (choose the **Bookmarks/View Bookmarks** menu item) that reads any HTML file containing links and converts those links into bookmarks. To import a hotlist into Netscape, you should first convert your hotlist to HTML. Several downloadable utilities perform this conversion. You may also be able to use another browser's mail command to transmit a hotlist in HTML format.

Consult **Help/Release Notes** for the name and location of a hotlist to HTML converter for your platform. Utilities include: **Winh2htm** on Windows, , **hotlist2HTML** or the Hypercard stack **HHConv** on Macintosh, and the **hot-convert.sh** shell script on UNIX.

---

**Are there any Macintosh-specific tips or tricks?**

**Bookmarks**
You can collapse and expand Bookmark headings by double-clicking on them. Currently, there is a limit of 37 hierarchical menus.

**Stop**
To interrupt the transfer of a page, press the **Stop** button or choose the **Go/Stop Loading** menu item. Interrupting by **command-.** might result in additional error messages.

**News**
Before posting news or sending mail, you must set up your name and e-mail address in the **News** panel. You might get an out-of-memory error message when trying to view a large newsgroup or newsgroup listing. The **News RC file** is stored in the Netscape preferences folder within the System folder.

**Printing**
If a page's display is too wide to be printed, use the resize box to shrink the window or, in the case of preformatted text, reduce the page size in the **Page Setup** dialog box.

**View Source**
This menu item runs the external application specified in the **Applications** panel (or the default Macintosh text editing program). When you use **Save As** to save a document as HTML, the creator is the same as the one set for **View Source**.

**Drag'n'drop support**
You can drag a URL onto the main window to load a page. You can also drag a URL from your history window.

**Multiple users on a single Macintosh**
Each user can have a personal preferences file by creating a separate copy of the **Netscape Preferences f** folder in the System Folder. Launch Netscape by double-clicking on the **Netscape Preferences** file.

---

### Any other Macintosh-specific tips or keyboard shortcuts?

**Selecting text on a grayscale monitor**

You may not be able to see selected text if the selected text color looks like Netscape's background color (light gray). To correct this, open your **Control Panels** and use the **Color** dialog to choose a lighter highlight color, such as yellow, or a darker one, such as red. These default to sufficiently lighter or darker grays to give contrast to selected text.

**URL in "Get Info" box**

Whenever you download a file to disk (using the pop-up menu item or clicking on a link with the option key held down), Netscape tries to set the comment field in the Finder's **Get Info** dialog box to the URL of the file.

**Keyboard shortcuts**

- Press **page-up**, **page-down**, **up-arrow** and **down-arrow** to vertically scroll the main window.
- Press **command-left arrow** to go **Back**. Press **command-right arrow** to go **Forward**.
- Press **tab** to move the cursor among form fields.
- Hold down **option** when clicking on a link to load a page to disk rather than to the screen.
- Hold down **option** when choosing the **File/Open File** menu item to allow Netscape to open any local file (files of all types are displayed in the file dialog).
- Hold down **option** when choosing the **Quote Document** button in the **Send Mail/Post News** dialog box to insert text without the angle bracket (**>** ) prefix.

---

### Are there any Windows-specific tips or tricks?

**Using INI files from another browser**

You may be able to copy your INI file from others browsers to the **netscape.ini** file. Be sure to add fields for **History File** and **File Location**. Be sure to convert your any hotlist entries to Netscape bookmarks.

**Viewing HTML source documents**

To use Netscape (rather than an external viewer) as the HTML source viewer, leave the **View Source** field blank in the **Options/Preferences/Applications** panel.

---

### Are there any UNIX-specific tips or tricks?

**Real-time decoding of audio or video files**

You can download a file in two ways: wait for the entire file and then launch an external viewer, or launch the viewer and then send the viewer data arriving from the network. With a viewer that can accept streaming input, you can play audio and video files directly off the network.

**Default window size**

To set the default size of the window, use the command-line option:

```
-geometry =620x950+630+40
```

or the X resource:

```
Netscape.TopLevelShell.geometry: =620x950+630+40
```

**What is the World Wide Web's place in the Internet?**

World Wide Web (WWW or Web) is one facet of the Internet consisting of client and server computers handling multimedia documents. Client computers use browser software (such as Netscape Navigator) to view documents (pages). Server computers use server software (such as the Netscape Commerce Server) to maintain documents for clients to access.

Web documents are created by authors using a language called HTML (HyperText Markup Language) that offers short codes (also called tags) to designate graphical elements and links. Clicking on links brings documents located on a server to a browser, irrespective of the server's geographic location. Documents may contain text, images, sounds, movies, or a combination.

Documents are addressed with a URL (Uniform Resource Locator or, for short, location). Clients and servers use a document's URL to find and distinguish among documents.

**How can I access the Internet?**

Some companies maintain a network that is linked to the Internet via dedicated communication lines. Those with less substantial resources, including most individuals, access the Internet via a service provider. A service provider is a company that offers use of its dedicated communication lines. If you have a modem, you can dial up a service provider whose computers will connect you to the Internet, typically for a fee. Dial-up access means that the modem on your computer can log in to another computer that is hooked up to the Internet.

The most popular dial-up access alternatives are shell accounts and SLIP/PPP accounts. When using a shell account, you dial into a service provider's computer and use the UNIX operating system to indirectly connect to the Internet. With an indirect connection, your computer does not interact with Internet computers. For example, if you download a file from an Internet site, the file is saved on the service provider's computer rather than on your computer. You then have to transfer the file from the service provider's computer to your home system. Shell accounts, while limited in features, have historically been less expensive than direct access accounts.

When using a SLIP or PPP account, you dial into a service provider's computer and run applications that directly connect to the Internet. With a direct connection, your computer can use browsers with user-friendly graphical interfaces to interact with Internet computers. A direct connection lets you download files directly to your system from remote sites. SLIP or PPP access to the Internet offers more performance and convenience than a shell account.

**What are SLIP and PPP?**

SLIP, short for Serial Line Internet Protocol, and PPP, short for Point-to-Point Protocol, are Internet standards for transmitting Internet Protocol (IP) packets over serial lines (phone lines). Internet information is packaged into IP packets, a method for enclosing data into small, transmittable units (wrapped up on one end, unbundled on the other).

A service provider may offer SLIP, PPP, or both. Your computer must use connection software (usually provided by the service provider) that matches the protocol of the server’s connection software. PPP is a more recent and robust protocol than SLIP.

**CSLIP**

CSLIP, Compressed Serial Line Internet Protocol, is a version of SLIP that supports compression.

**Dynamic SLIP and Static SLIP**

When you use a SLIP or PPP connection to the Internet, your service provider’s server identifies your computer by providing you with an IP address (a number like 192.34.32.81). Using dynamic SLIP, your computer is dynamically allocated a temporary IP address (just for the immediate session) from a set of IP addresses maintained by the server. Using static SLIP, your computer is allocated a one-time, permanent IP address (when your account is set up) for use in all your sessions. Static SLIP means you have a static IP address.

---

**What are TCP/IP and Winsocks?**

**TCP/IP**

TCP/IP, short for Transmission Control Protocol/Internet Protocol, is the standard communications protocol required for Internet computers. To communicate using TCP/IP, PCs need a set of software components called a TCP/IP stack. Macintoshes typically use a proprietary software called MacTCP. Most UNIX systems are built with TCP/IP capabilities.

**TCP/IP Stack**

Only the PC platform requires a TCP/IP stack. To make a successful connection to the Internet, your PC needs application software such as Netscape plus a TCP/IP stack consisting of TCP/IP software, sockets software (Winsock.DLL), and hardware driver software (packet drivers). Several popular TCP/IP stacks are available for Windows, including shareware stacks.

**Winsocks**

Winsock stands for Windows Sockets. Winsocks is a set of specifications or standards for programmers creating TCP/IP applications (communicating applications such as Netscape) for Windows.

---

**What should I know about firewalls?**

A firewall protects one or more computers with Internet connections from intrusion by external computers also with Internet connections. A firewall refers to an invisible boundary, created by software, that distinguishes networked computers within the firewall from those outside the firewall.

Those within the firewall possess internal access capabilities and shared resources not granted to those on the outside.

A firewall can be configured using proxies and SOCKS to specify which information remains internal and which is available to outsiders on the Internet. Typically, a firewall protects information such as e-mail and file archives of networked computers within a physical building or location. A firewall may also prevent, limit, or make more difficult, access to the Internet for computers protected within the firewall's boundaries.

---

**What are proxies and SOCKS?**

**Proxy or proxy server**

A proxy allows access to the Internet from within a firewall. A proxy is a special server that typically runs in conjunction with firewall software. The proxy server waits for a request from inside the firewall, forwards the request to the remote server outside the firewall, reads the response, then sends the response back to the client. Netscape lets you set the name and port number of proxy servers in the **Options/Preferences/Proxies** panel in order to resolve requests for access to Internet resources. Protocols such as HTTP, FTP, Gopher, News, and WAIS can have designated proxies.

**SOCKS**

SOCKS is software that allows computers inside a firewall to gain access to the Internet. SOCKS is usually installed on a server positioned either inside or on the firewall. Computers within the firewall access the SOCKS server as clients to reach the Internet. On Macintosh and UNIX computers, Netscape lets you set the name and port number of the SOCKS host (server) in the **Proxies** panel. On Windows, the host is specified in the INI file using the format:

```
[Services] SOCKS_Server=mysocks.domain.com
```

Sometimes you need to restart Netscape after changing the SOCKS host. Netscape supports version 4 of SOCKS defined by the socks.cstc.4.1 implementation.

Netscape Handbook: Table of Contents

---

*info@netscape.com*