NFS/Share

InterCon

■ **InterCon Systems Corporation**
950 Herndon Parkway ■ Herndon, Virginia 22070
703.709.9890 ■ 703.709.9896 (FAX)
comment@intercon.com (internet email)
AppleLink: D1988

NFS/Share

ONC/NFS Connectivity for the Macintosh

InterCon

InterCon Systems Corporation
950 Herndon Parkway
Herndon, VA 22070
703.709.9890 (Voice)
703.709.9896 (FAX)

comment@intercon.com
sales@intercon.com
tech@intercon.com

Chapter 1

■ ABOUT NFS/SHARE

1.1 What comes with it

The NFS/Share package comes with one 800K diskette, a product registration card and the NFS/Share documentation.

On your NFS/Share disk, you should find the **NFS/Share** Chooser document, the **NFS/Test**™ diagnostics application, the source code for **BWNFSD**, and Apple's **MacTCP**, along with an example hosts file for your Macintosh.

Send in your registration card! It is your ticket to further upgrades and technical support for NFS/Share. Please fill out this card completely and return it to InterCon immediately in order to ensure that product support is available to you.

1.2 Using this manual

The **NFS/Share** manual is divided into a number of chapters, each corresponding to a specific task or feature. Following is a brief description of each chapter. Depending on your knowledge and experience, you may find some chapters more interesting than others.

Chapter 1 **About NFS/Share** This chapter (you're halfway through it) is devoted to covering the manual's layout and the typographic conventions used througout this and every InterCon manual.

Chapter 2 **Getting Started** covers system requirements and simple concepts involved that you should note before installing and using NFS/Share on your network. This chapter also briefly covers how to install NFS/Share and mount a volume.

Chapter 3 **About TCP/IP** is a comprehensive chapter on the history and basics of TCP/IP networking. It is recommended that all users read this chapter, as it covers the basic concepts of TCP/IP and is very useful to seed a basis for understanding TCP/IP networking.

Chapter 4 **About MacTCP** covers the use and installation of Apple Computers' MacTCP. This chapter is included for informational use only, as the installation of MacTCP is handled automatically by the **Installer** application.

Chapter 5 **Using NFS/Share** covers all of the options available in NFS/Share.

Chapter 6 **Administration Notes** covers more technical matters such as server requirements and conventions used by NFS/Share.

Chapter 7 **Trouble Shooting** is a simple Q & A section that covers many topics that represent common questions for NFS/Share users.

Because NFS/Share is a product based on TCP/IP, it is recommended that you read the section on TCP/IP to obtain a better understanding on how your network operates. A basic understanding of TCP/IP will help you to better utilize the abilities of your TCP/IP network in an efficient manner.

1.3 Typographic Conventions

This section summarizes the typographic conventions that are used throughout this manual and throughout all InterCon manuals. In order to make references to commands, buttons, menus, screen displays and user input, we have adopted the following conventions:

The names of Macintosh applications, buttons, menu items, windows, dialogs and text boxes will be displayed in **this** (Univers Bold Condensed) font.

Text which is typed in by the user will be set in `this` (courier regular) typeface. This face is also used to indicate data that a user would see coming in from a data terminal or within a given text file, as well as a reference to Internet IP addresses and domain names.

Additionally, any string enclosed in broken brackets ('<' and '>') is intended as an implied variable and should be substituted with valid data if actually used. For

example, `<hostname>` could be replaced with `intercon.intercon.com` when referring to the primary host at InterCon Systems Corporation.

This symbol indicates an item of importance. Many common problems that users encounter with given features are answered by one of these items found in the manual.

This symbol indicates an item of interest. Many interesting workarounds, commands and items of trivia can be found in text marked by this symbol.

Chapter 2

GETTING STARTED

This chapter explains how to get a copy of NFS/Share up and running on your Macintosh as quickly as possible. This is not an in-depth tutorial, and it assumes a certain amount of familiarity with TCP/IP and the Macintosh Operating System; for more complete information, please read the chapters on installation and configuration.

2.1 What You Need To Have

2.1.1 Hardware

NFS/Share requires a Macintosh Plus or newer with at least 2 megabytes of memory, a floppy drive and 128K ROMs or newer. Additionally, NFS/Share requires one of the following types of network connections:

- ✓ **Direct Ethernet**: Either an expansion board (NuBus on the Macintosh II series, or Processor Direct Slot (PDS) on Macintosh computers with slots) or a SCSI attached Ethernet device.

- ✓ **LocalTalk**: A LocalTalk to Ethernet gateway connected to your Macintosh via LocalTalk (perhaps through one or more AppleTalk bridges). It is recommended that you set up your Gateway to use static addressing for each MacTCP client. It is possible to use NFS/Share with dynamic addressing, however it will usually require more overhead and conceptual knowledge of TCP/IP to administrate.

2.1.2 Software

- ✓ **Macintosh System Software**: NFS/Share requires version 6.0.5 or more recent of the Macintosh System file. InterCon strongly recommends that

you use the most recent version possible of Macintosh System Software.

NFS/Share requires **AppleShare** to be installed to facilitate certain operations of the Apple Desktop Manager. AppleShare is available on your Apple System Installer disks and must be installed with the Apple Installer application. Make sure that you run the Installer Application to install AppleShare, as simply copying the AppleShare document to your System Folder will not result in a complete installation.

✓ **Hardware Drivers** If you are using an Ethernet device, you must install the driver software provided by the manufacturer, although you do not need to turn on EtherTalk as your AppleTalk connection method under Network in the Control Panel.

✓ **Host Software** To run NFS/Share for the Macintosh, you need to have the following on your host machine: an NFS Server, a Domain Name Server (optional, but recommended), Sun's NIS (Yellow Pages), BWNFSD or PCNFSD (version 1 or 2), for password authentication.

2.1.3 Information

NFS/Share works best if you are able to configure **MacTCP** to provide "static" IP addressing. If you have not yet configured **MacTCP**, you will need to obtain the following information from your network administrator:

IP Address: The IP Address uniquely defines your Macintosh to other machines on the network. Your Macintosh needs to have an address in the range that has been assigned to your network but that is not in use by another host. (*Note: You can not use 192.0.0.x or 128.0.x.x as IP addresses with Apple's MacTCP. These addresses are considered illegal in accordance with RFC 1122.*)

Subnet Mask: If your network uses subnetting, you will need to know the subnet mask for the subnet to which you are attached.

Gateways: If you wish to connect to hosts that are not on your subnet, you will need to know the IP addresses of any IP gateways that connect your subnet to the rest of the Internet.

Name Servers: If your network has one or more Domain Name Servers, you should find out their IP addresses and domains. Domain Name Servers provide the service of mapping host names to IP numbers , allowing convenient access to a large number of hosts without extensive host configuration.

2.2 Installing and Using NFS/Share

✓ Start with a Macintosh computer running System 6.0.5 or greater.

✓ If you are running System 6, install AppleShare Workstation Software by running the Apple Installer from your Apple System Installer floppies and specifying a custom configuration. Please refer to your Apple System Installation documentation for more information on how to install AppleShare. (Note: You will want to check to see if AppleShare is already installed by opening the Chooser and checking to see if the AppleShare ICON is present.)

✓ Insert the **NFS/Share** distribution floppy and copy **NFS/Share** to your System folder. At this time, you should also copy the file **NFS/Test** to your hard drive. **NFS/Test** is an application, and it is not required specifically that it be in your System folder. Under System 7 you will need to put NFS/Share in the top level of the System Folder and not in the Extension Folder, as NFS/Share must load after MacTCP in order to function.

✓ Open the **MacTCP** folder on the **NFS/Share** distribution floppy and copy its contents into your System folder. You will need to open the Control Panel under the **Apple** Menu and configure MacTCP with your Macintosh's network information. (For more info on how to configure MacTCP, see the section on MacTCP later in this manual.)

✓ Reboot your machine and you will be ready to begin using **NFS/Share.**

2.2.1 NFS/Test™

Included with **NFS/Share** is the application **NFS/Test.** This application will assist you in configuring your host to properly operate as an NFS server. Copy **NFS/Test** to your boot volume and launch it. NFS/Test will display a window, showing your local hosts and what NFS related software they are running.

To check a remote host, type its name or IP number into the input area and click

the **Add** button. The new host and its configuration will be added to the list. Beside each host name will be a combination of up to five different icons. These icons indicate the existence of different NFS services.

As you can see in the example session, (Figure 2.1) host intercon.com is running all six servers. special.intercon.com is running NFS, LOCKD and PCNFSD. disco.intercon.com is running NFS, LOCKD, PCNFSD and PCNFSD Version 2. europa.asd.contel.com doesn't seem to have an NFS server and wuarchive.wustl.edu is only running an NFS server with no authentication damon. When you are through testing, click the **Done** button, and NFS/Test will quit.

In order to operate NFS/Share you need to be running NFS and one or any combination of the additional servers necessary for authentication and/or file locking capabilities. The available Authentication Servers are NIS, PCNFSD and BWNFSD. You will not have access to your NFS server without one of these daemons installed.

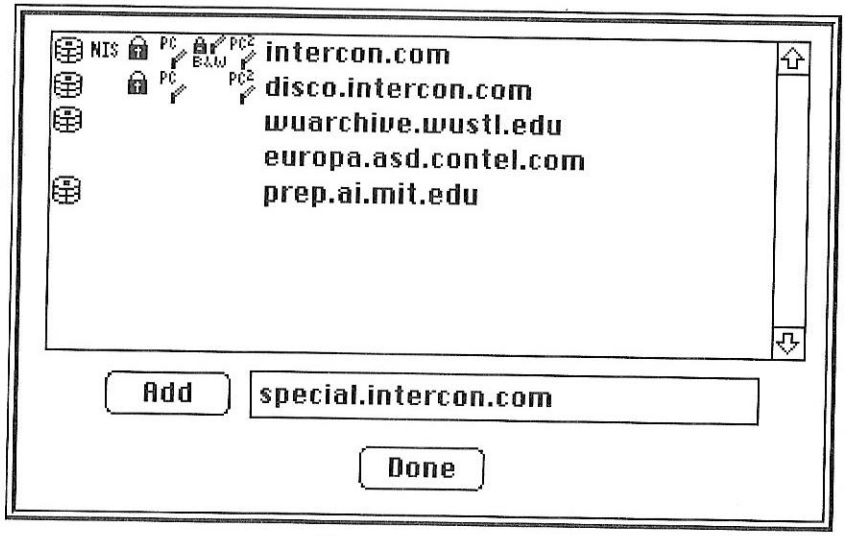


Figure 2.1 **NFS/Test**

2.3 NFS/Share Basics

NFS/Share's operation is quite simple. If you have an NFS server already set up

and running, you will probably need to do little to set up NFS/Share.

✓ Open the **Chooser** under the **Apple** Menu and select the **NFS/Share** icon. After a very short delay you should see a list of NFS servers in the list selector. These will appear as IP addresses or as names, depending on whether or not you are running a Domain Name Server or if you have a configured hosts file in your System folder.

If you do not have a Domain Name Server on your network, but would like to have your NFS servers identify themselves with names instead of IP addresses, please refer to the MacTCP section of this manual and set up a `hosts` file in your System folder.

✓ If you are running NIS (or YP) enter the default NIS domain by choosing NIS Domain in the pop-up menu and typing it there.

If you do not know your NIS Domain, ask your system administrator or enter the command `domainname` at a terminal prompt on the machine running the NIS daemon.

You must be running some authentication daemon in order to use NFS/Share. The daemons available for use are NIS, PCNFSD, or BWNFSD.

✓ Double click on the server that you want to access.

✓ Type in your username and password for that system, just as you would when signing on to a terminal, and hit the **log in** button. You will notice that a default entry appeared in your username area. **NFS/Share** copies your Macintosh's Chooser name into the username area. For convenience, you may want to change your Chooser name to match your normal login name.

✓ If the login was successful, a dialog will come up presenting you with a list of volumes that you can mount. Initially, this list will be blank and you will need to add entries to it. Click the **Other** button and enter a path name as the *Mount Point* and enter a desired *Volume Name* to identify your volume. The volume name will identify your NFS volume. Click the **Mount** button and the volume should appear on the desktop.

Chapter 3

ABOUT TCP/IP

TCP/IP is the common name for a set of widely used industry protocols for interconnecting across all implementations on different hardware platforms, allowing computers from different vendors to interoperate and share data and services, as long as they are capable of using TCP/IP.

TCP/IP development began when the U.S. Defense Advanced Research Projects Agency (DARPA) wanted more reliable communication protocols on the ARPANET, its packet-switched wide area network[1]. DARPA initiated a research project to define and implement a suite of protocols, and the researchers developed TCP/IP[2]. Eventually TCP/IP became the standard protocol suite used on the DARPA Internet, a collection of networks that includes the ARPANET, the U.S. Military Network (MILNET), the U.S. National Science Foundation Network (NSFNET), and networks at universities, research institutions, and military installations. Since then, hundreds of vendors have developed products that support TCP/IP and all kinds of networks around the world use it.

TCP/IP supports an architecture of multiple networks interconnected by gateways. This interconnected set of networks is called an internetwork or internet (the term "the Internet" refers to the DARPA Internet). For example, TCP/IP protocols can be used to connect networks on a college campus or geographically distant sites on a wide area network. "Figure 3.1 An Example Internet" on page 12 shows an example of an internet.

3.1 The Family Of Protocols

TCP/IP is a family of protocols named after the most widely used protocols in the suite, the Transmission Control Protocol (TCP) and the Internet Protocol (IP). The protocols described in this section are the ones most commonly supported by computers attached to TCP/IP networks. TCP, IP and the User Datagram Protocol (UDP) provide basic transmission facilities that are augmented by application services in higher-level protocols such as Telnet, the Network File Sharing

1. "A history of the ARPANET: The First Decade," Bolt, Beranek, and Newman, Inc., April 1981.
2. Selvaggi, Philip S., "The Development of Communications Standards in the DoD," *IEEE Communications Magazine*, no. 1, January 1985.

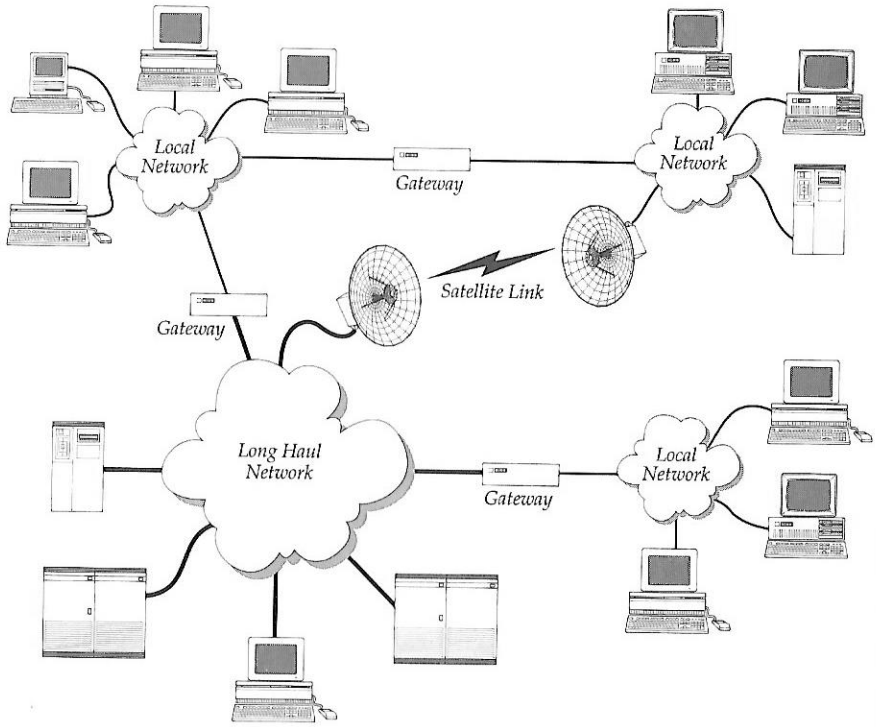


Figure 3.1 *An Example Internet*

protocol (NFS) which provide a means for sharing files across a network, the File Transfer Protocol (FTP), and the Simple Mail Transfer Protocol (SMTP).

Other Protocols in the TCP/IP family are described later in this chapter. The Address Resolution Protocol (ARP), the Reverse Address Resolution Protocol (RARP), and the Bootstrap Protocol (BOOTP) are described in "3.3.5 Address Resolution Protocol (ARP)" on page 20 and subsequent sections. The Routing Information Protocol (RIP) and the Internet Control Message Protocol (ICMP) are described in Section "3.3.4 The Domain Name System" on page 19.

3.1.1 Internet Protocol (IP)

The Internet Protocol (IP) is responsible for sending data across multiple networks. IP accepts segments of data from TCP or UPD, places the data in packets called datagrams, and determines the correct path for the datagram to take. The datagrams are sent across the Internet, through as many gateways as needed, until they reach the destination host.

IP provides an addressing mechanism that allows routing between networks. The header of an IP datagram contains source and destination internet addresses so that any host in a network can route a packet to a destination, either directly or through a gateway. IP has the ability to fragment a datagram as it is transmitted across a network. Since IP can be used with many different physical network implementations that specify different sizes for physical data frames, datagrams can be fragmented to fit into a small data frame. Fragments are reassembled as they arrive at the destination.

IP is often referred to as an unreliable delivery system because it makes a best-effort attempt to deliver all datagrams, but delivery is not guaranteed (TCP guarantees delivery). It is also called a connectionless delivery system because it routes each datagram separately. When IP receives a sequence of datagrams from TCP or UDP, it routes each datagram in the sequence individually and each datagram may travel over a different path to the destination.

3.1.2 Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) provides reliable transmission of data between processes. (Processes are application programs that communicate; for instance, a file transfer process on one host talks to a file transfer process on another host). It ensures that data is delivered error-free, without loss or duplication, and in sequence.

Upper-layer protocols such as Telnet pass data to TCP for delivery to peer processes. TCP encapsulates the data into segments and passes the segments to IP, which puts the segments into datagrams and passes them across the internet. TCP at the receiving end checks for errors, acknowledges error-free segments, and reassembles the segments for delivery to upper-layer protocols. If a segment is lost or damaged, it will not be acknowledged, and the sending process will retransmit.

TCP has a flow control mechanism so that computers of different speeds and sizes can communicate. When TCP at the receiving end sends acknowledgment, it also advertises how much data it is prepared to accept on the next transmission.

3.1.3 User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) provides unreliable transmission of data between processes. UDP's transport of data is unreliable because, unlike TCP, it does not provide error checking, it does not acknowledge that data has been successfully received, and it does not order incoming messages. UDP messages can be lost, duplicated, or arrive out of order. Like TCP, UDP messages are encapsulated

in IP datagrams for delivery.

The advantage of UDP is that the overhead associated with establishing and maintaining an error-free TCP session is avoided. Upper-layer protocols that don't require reliability use UDP to transmit data. For instance, the domain name system uses UDP because reliability is not critical; if there is no response to a domain name query, the resolver simply retransmits. (The domain name system is described in "3.3.4 The Domain Name System" on page 19).

3.2 Services

This section describes a few higher-level protocols which are implemented on most TCP/IP hosts. These protocols are used to provide network services to the user.

NFS: The Network File Sharing Protocol (NFS), developed by SUN Microsystems provides a transparent means to access shared files on a remote host across a network. The primary usefulness of the NFS protocol lies in the fact that unlike FTP (the File Transfer Protocol), NFS allows the client to request either an entire file or just a part of it. This flexibility allows a user to edit files and run applications found on remote hosts without having to transmit the entire file. Through the use of daemons such as PCNFSD, LOCKD, and NIS (formerly Yellow Pages or YP) NFS can support user authentication and file range locking.

NIS: (Formerly Yellow Pages or YP) NIS is another protocol developed by SUN. NIS is used for user authentication with NFS.

LOCKD: LOCKD is an authentication protocol for NFS that also allows for range locking with files, giving the user the ability to share files.

PCNFSD: A simple authentication protocol developed by SUN, PCNFSD allows for simple password authentication for non-UNIX NFS clients.

TELNET: Telnet is a remote access protocol that allows a terminal on one host to appear as if it were directly connected to a remote host on an internet. TELNET can also be used to make a personal computer act like a terminal. It is usually implemented as client software that initiates sessions to a remote location and server software that listens for connections from remote users.

FTP: The File Transfer Protocol (FTP) is used to transfer files. A host can connect to a remote host on an internet and send or receive files, list directories, and execute simple commands. Like TELNET, FTP is usually implemented with the user at a terminal and the server software receives requests from remote users to store or retrieve files.

SMTP: The Simple Mail Transfer Protocol (SMTP) is used to transfer electronic mail messages from one host to another. SMTP client programs are used by the operating system to connect to SMTP server programs in order to transfer mail.

POP: The Post Office Protocol (POP) is used to retrieve mail from a server host. The POP client exchanges authentication information with the POP server, and then can download mail messages from the server. POP is commonly used to provide mail service to hosts on which it is impractical or undesirable to run an SMTP server (such as a workstation or desktop computer).

SNMP: The Simple Network Management Protocol (SNMP) is used to provide client programs with information about how the network is operating and allow authorized clients to modify run-time parameters in the server hosts in order to adjust for network load and efficiency.

NNTP: The Network News Transfer Protocol (NNTP) is used to provide access to a local news database for client programs. Servers are usually run on large machines with plenty of disk space. The NNTP protocol is used widely on the Internet backbone of the Usenet network.

3.3 TCP/IP Addressing Conventions

In order for computers on an internet to be able to refer to each other, each machine must be assigned a universal address. This section describes the addressing scheme that was developed to allow each TCP/IP host in existence to be uniquely identified.

3.3.1 Internet addresses

Each host on a TCP/IP internet is assigned a unique 32-bit internet address, also sometimes called an IP number. The address is divided into fields, called the network field and the host field. The network field identifies a network on the inter-

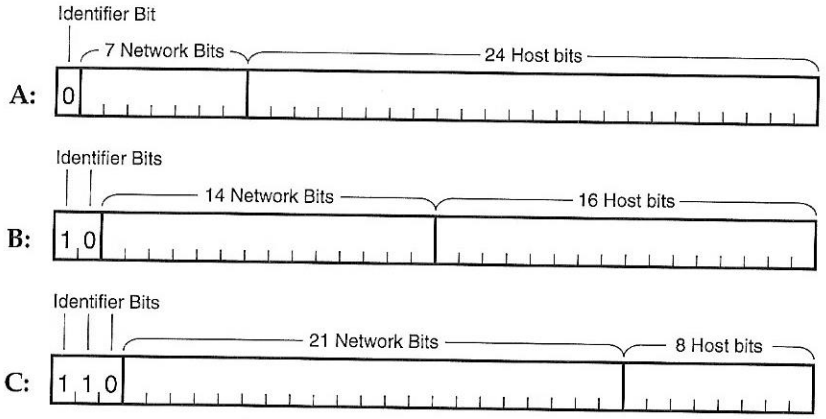


Figure 3.2 *IP Address Structure*

net to which the host attaches (such that all hosts on the same network share the same network field) and the host field identifies a particular host on that network.

The network field is assigned by central authority, the Network Information Center (NIC) located at SRI International. Local administrators assign the host field of the address. (Note that only networks that might attach to the DARPA Internet need to obtain the network address from the NIC, although it's generally considered a good idea anyway, since future connectivity can be hard to predict).

Three IP address classes–A, B, and C–provide for the following network configurations:

- Class A addresses are used for a few networks with many hosts; for instance, the ARPANET.
- Class B addresses are used for medium-sized networks; for instance, a large university network.
- Class C addresses are used for a large number of small networks; for instance, an Ethernet local area network (LAN).

The first bits of the address identify the address class, and the number of bits assigned to the network and host field of the address differs for each class. For instance, Class A addresses have 1 class identifier bit, 7 network identifier bits, and 24 host identifier bits. This allows for 128 Class A networks, where each network can support up to 16 million hosts. "Figure 3.2 IP Address Structure" on page 16 shows the class identifier bits and the number of bits allocated to the network and host fields for each address class.

To make the address easier to work with, the addresses are written in dotted decimal notation. Each octet ("byte") of the 32-bit address is assigned its decimal equivalent, and decimal points separate the integers. For example, the 32-bit address

10000100 00001101 00000010 00011110

is written in dotted decimal notation as `132.13.2.30`

3.3.2 Subnetwork addressing

The internet addressing scheme, designed for a few hundred networks, did not anticipate the proliferation of LAN technology. Organizations created large networks consisting of many LANs connected by gateways and there was an explosive growth in the number of networks on the Internet. Assigning every LAN on the Internet its own address created two problems:

- An immense administrative overhead was required to manage these addresses.
- Internet routing tables could not accommodate that many networks.

A technique called subnetwork addressing (or subnetting) was devised to deal with this problem. Subnetting allows multiple physical networks (called subnetworks) to share the same internet network number. For example, a university with two LANs can use subnet addressing so that both campus subnetworks share a single network number. The subnet structure is not visible to the rest of the Internet, thus the route to the network is the same no matter what subnet the host is on.

The last section stated that the internet address is divided into network and host fields. With subnetting, the address is conceptually divided into a network and local field of the address into subnet numbers; each internet site determines individually which scheme to implement.

Imagine Miskatonic University has subdivided its assigned Class B internet address, `190.10.0.0`, for the two LANs on campus. They divided the local field of the address into an 8-bit subnet identifier and an 8-bit host identifier. LAN_1 has the address `190.10.0.0` and LAN_2 has the address `190.10.2.0`. "Figure 3.3. Subnetting at Miskatonic University" on page 18 illustrates the addressing scheme at Miskatonic University.

In "Figure 3.3. Subnetting at Miskatonic University" on page 18, the rest of the internet perceives that it is sending data to one network. The gateway routes packets to the appropriate LAN by examining the upper half of the host bits in the address.

3.3.3 Subnetwork masks

An internet site that has implemented subnet addressing must choose a subnetwork mask (or subnet mask), which is used by network software to identify the host number field from the subnet number and network number fields. The portion of the address to be allocated to the subnet is defined (for example, Miskatonic University used the third octet of the address to identify the subnet). Then bits are set in the 32-bit subnet mask to correspond to the IP address. A subnet mask bit is set to 1 if the corresponding bit in the internet address is part of the network number and subnet number fields, and to 0 if the corresponding bit in the address is part of the host number field. The subnet mask for a Class A address might be

11111111 11111111 00000000 00000000

or `255.255.0.0` decimal. Since this is a Class A address, octet 1 identifies the network field and octets 3 and 4 identify the host number field; therefore, the system knows that octet 2 of the address identifies the subnet number.

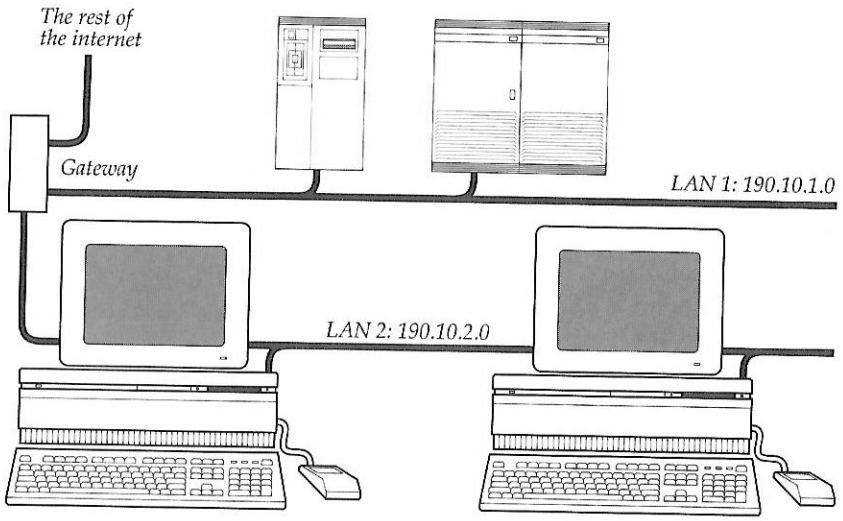


Figure 3.3. *Subnetting at Miskatonic University*

In theory, each LAN at the internet site could have a different number of bits allocated to its subnet field, and therefore have different subnet masks. However, it is generally recommended that a given network have a single subnet mask that is the same for all of its component LANs.

3.3.4 The Domain Name System

Because most users would rather refer to machines using meaningful, symbolic names rather than long strings of numbers, the Domain Name System (DNS) was created to map between internet addresses and names. The DNS's hierarchical naming scheme accommodates a large set of names and allows local autonomy in assigning names. A domain name is divided into subnames separated by periods, such as "`english.miskatonic.edu`".

In this example, `edu` is the top-level domain and each label further specifies a subdomain. The Network Information Center (NIC) administers the top-level domains and is responsible for assigning subdomains. "Figure 3.4 Top Level Domains on the Internet" on page 19 shows the top-level domains specified by the NIC.

After an organization obtains authority for a domain from the NIC, it can assign subordinate domain names. For instance, if Miskatonic University obtained authority for the domain `miskatonic.edu`, the English Department at Miskatonic University could subsequently obtain authority for the domain `english.miskatonic.edu`.

The organization with authority over a domain must maintain a domain name

COM	Commercial organizations
EDU	Educational institutions
GOV	Government institutions
MIL	Military group
NET	Major network support centers
ORG	Organization other than above
ARPA	Temporary ARPANET domain
ISO country code	Countries other than the USA[a]

Figure 3.4 Top Level Domains on the Internet

a. The ARPANET has been gradually phased out, and has been replaced by the Defense Research Internet (DRI).

server that maps domain names to internet addresses. If the English Department at Miskatonic obtained a new computer that they called "Lovecraft," the name `lovecraft.english.miskatonic.edu` would be added to a domain name server's database, along with the computer's internet address. Hosts participating in the domain name system must have name resolvers that request the information from name servers. The name resolver contacts a local name server to obtain the internet address associated with the domain name. The local name server may need to contact other domain name servers to obtain the internet address and assorted other information.

3.3.5 Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) is a protocol in the TCP/IP protocol suite that maps internet addresses to physical network addresses. If Host A wants to communicate with Host B and it only know B's internet address, it can use ARP to obtain B's physical address. Host A broadcasts an ARP request that contains Host B's internet address. All hosts on the network receive the request, but only Host B recognizes the internet address and replies with its physical address. Host A receives the reply, learns B's physical address, and delivers its packets directly to B.

3.3.6 Reverse Address Resolution Protocol (RARP)

The Reverse Address Resolution Protocol (RARP) maps physical network addresses to internet addresses (the opposite function of ARP). RARP provides a way for a host to obtain its internet address. The host broadcasts a RARP request that contains its physical network address. All hosts on the local network receive the request; however, only RARP servers can process the request and provide the internet address (RARP will work only if there's a RARP server on the network). The RARP server consults its database of internet addresses, then sends the information back to the host that made the request.

3.3.7 Bootstrap Protocol (BOOTP)

The Bootstrap Protocol (BOOTP), like RARP, provides a way for a host to find its internet address. A host running BOOTP broadcasts a BOOTP request. A BOOTP server returns a response that contains the host's internet address, the address of a bootserver, the address of an intervening gateway (if present), and other useful configuration information such as the subnet mask and addresses of domain name servers.

3.4 Routing

A packet transmitted by a host on the Internet may only need to take a short hop across the local network or it may have to cross many gateways and networks to reach its destination. The process of finding a path over which the packet can travel to reach its destination is called routing. This section describes how TCP/IP handles routing.

3.4.1 Gateways

If a host is transmitting to a destination on its own network, routing a packet involves finding the destination host's physical address (using ARP) and sending the packet over the physical network to its destination. When the destination is on a different network, the packet is routed to the nearest gateway. A gateway is a machine that interconnects two networks and passes packets from one network to another. If the local gateway is not connected to the destination, the packet is forwarded to other gateways until it reaches a gateway that is directly connected to the destination network.

3.4.2 Routing tables

All gateways in the internet have routing tables that contain pairs of network addresses and gateway addresses. Each network address is linked with the gateway address of the gateway to be used to get to that network. Routing decisions are based on the network number of the destination address rather than the host number to keep routing tables small.

3.4.3 Routing protocols

Routing protocols provide a way for gateways to find each other, keep up-to-date routing information, and report communication problems.

Routing Information Protocol (RIP) Some gateways use the Routing Information Protocol (RIP) to exchange network routing information. Gateways broadcast their routing tables to neighboring gateways. If a RIP message contains new information, gateways update their routing tables. RIP is intended for low-delay local area networks (although it is used in wide area networks). The most widely used version of RIP is the `routed` software that is released with the 4.3BSD UNIX system.

RIP can also be used to locate gateways on a LAN. Any computer broadcasting RIP packets is likely to be a gateway. While other routing protocols are used by gateway manufacturers, RIP is by far the most common protocol found in gateways.

Internet Control Message Protocol (ICMP) Gateways and hosts use the Internet Control Message Protocol (ICMP) to report communication problems. For instance, if a packet cannot be delivered because the destination host is disconnected from the network, an ICMP message may be returned to the sending host stating that the destination is unreachable. ICMP is primarily used by gateways to notify the source host of delivery or routing problems.

ICMP is an integral part of the Internet Protocol (IP). Successful IP routing requires ICMP services to report error conditions. ICMP messages are encapsulated in IP datagrams, transmitted to the destination gateway or host, and processed by IP software.

Chapter 4

■ ABOUT MACTCP

4.1 Overview

MacTCP is a software driver written by Apple Computers, Inc. for the Macintosh Operating System that implements the following TCP/IP protocols:

- Internet Protocol (IP)
- Internet Control Message Protocol (ICMP)
- User Datagram Protocol (UDP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- Routing Information Protocol (RIP)
- Bootstrap Protocol (BOOTP)
- Transmission Control Protocol (TCP)

These protocols provide core transmission services that are used by third-party products such as **TCP/Connect II**™, **TCP/Tools**™, **NFS/Share**™, remote printing, and database access. By providing these basic network protocols in a driver, **MacTCP** allows multiple pieces of software to use TCP/IP services at the same time. For example, you could be running **TCP/Connect II** in one MultiFinder layer and a HyperCard front end to a remote database in another, without having them interfere with each other.

The **Control Panel** is used to configure **MacTCP**, simplifying installation and setup procedures. Sections "4.5.2 Configuration tools in AdminTCP" on page 28 and "4.7.5 Bringing up the Administrator dialog box" on page 41, describe how to use the **Control Panel** to configure **MacTCP**.

4.2 Network Media

MacTCP runs over both Ethernet and LocalTalk-compatible cabling systems. A Macintosh Plus, Macintosh SE series, Macintosh II series, or Macintosh Portable computer can run **MacTCP** on LocalTalk-compatible cable. It will also run on any Macintosh with a compatible EtherNet card or connected SCSI EtherNet device.

MacTCP is co-resident with AppleTalk protocols so there can be concurrent TCP/IP and AppleTalk operation on a single network wire. For example, **MacTCP** can be run while a print job goes out to an Apple LaserWriter printer over LocalTalk cabling. AppleTalk and **MacTCP** can run over the same media, or one protocol can run over one media while the other protocol runs over a different media.

4.3 DDP-IP Gateways

To run **MacTCP** on LocalTalk cable (or any other AppleTalk compatible media), you need a Datagram Delivery Protocol to Internet Protocol (DDP-IP) gateway. This device takes a TCP/IP packet that is encapsulated in DDP, an AppleTalk protocol, and converts it to another format, such as Ethernet. DDP-IP gateways can also assign addresses to **MacTCP** nodes and handle routing to other networks.

InterCon has tested **MacTCP** with gateways from Compatible Systems, Shiva Corp. and Cayman Systems, although others may work as well.

If **MacTCP** is running on LocalTalk, a DDP-IP gateway must be provided on the network. By default, the DDP-IP gateway should be located in the same LocalTalk zone as the Macintosh computer running **MacTCP**. Alternatively, a single DDP-IP gateway can support Macintosh computers in multiple AppleTalk zones; in this case, the zone where the DDP-IP gateway resides must be selected by the user using the **MacTCP** Control Panel.

4.4 Installing Apple's MacTCP

This section describes how to install the **MacTCP** software before you perform the configuration tasks described in Section 4.5. The process differs somewhat for computers running system software version 6.0.x and those running version 7.0; therefore, this chapter includes procedures for both environments.

Note that MacTCP 1.1 is only recommended for Systems 6.0.5 and later. If you have an earlier version of the Macintosh Operating System, upgrade it to version 6.0.5 or later before continuing.

4.4.1 Included Software

The Software Distribution Disk contains one folder labeled **MacTCP Software**. This folder contains the following files:

- ✓ the **AdminTCP** file
- ✓ the **MacTCP** file
- ✓ a **Hosts** file

The **AdminTCP** file contains resources used by the administrator to configure the driver. You do not distribute it to the user. The **MacTCP** file contains the MacTCP driver as well as resources that allow the user to configure the driver. The **Hosts** file is a sample Hosts file. Section 4.6 describes how to edit the Hosts file.

4.4.2 System 7

To install the MacTCP software for version 7.0, perform the following steps:

1. Lock the Software Distribution Disk, then insert it into your floppy disk drive.
2. Open the disk icon by selecting the disk icon and choosing **Open** from the **File** menu, or double-click the icon. Open the folder named **MacTCP Software**. The **Hosts**, **MacTCP**, and **AdminTCP** files are displayed in the folder window.

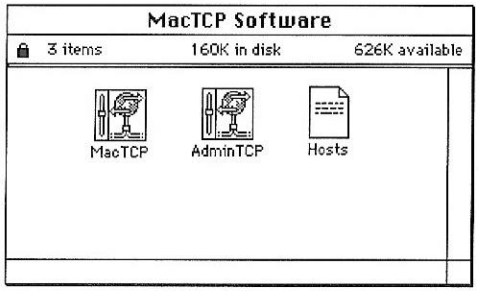


Figure 4.1 *MacTCP Software Folder*

3. Drag the **MacTCP** and **AdminTCP** icons into the System Folder on your hard disk by selecting both the **MacTCP** and **AdminTCP** icons (which is done by clicking one icon and then holding down the **Shift** key while clicking the other icon), and dragging them into the **System Folder.** A

dialog box will appear, asking if you want these control panels placed in the **Control Panels folder**. Click the **OK** button.

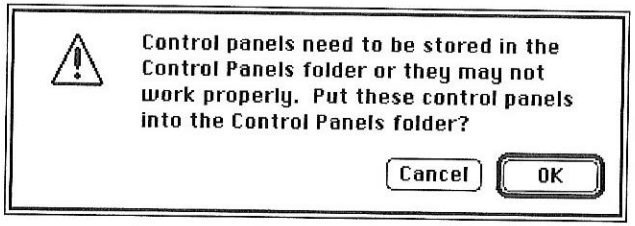


Figure 4.2 *System 7 "Auto-placement" Dialog*

4 If you want to use the **Hosts** file for name-to-address mapping, drag the **Hosts** file into the **System Folder** by selecting the **Hosts** file and draging it into the **System Folder**. To customize the contents of the **Hosts** file, refer to Section 4.6.

5 Close the **MacTCP Software** folder and the Software Distribution Disk folder, and Eject the disk.

6 Configure the MacTCP software as described in Section 4.5.

4.4.3 System 6

To install the MacTCP software for version 6.0.5 or greater, perform the following steps:

1 Lock the Software Distribution Disk.

2 Open the disk icon by selecting the disk icon and choosing **Open** from the **File** menu, or double-click the icon. Open the folder named **MacTCP Software**. The **Hosts**, **MacTCP**, and **AdminTCP** files are displayed in the folder window.

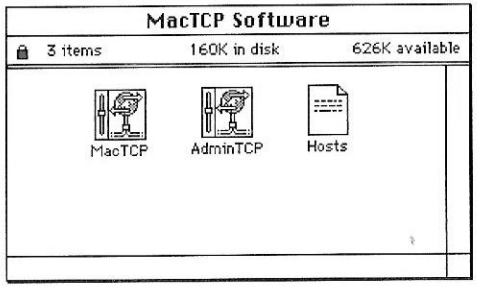


Figure 4.3 *MacTCP Software Folder*

3 Drag the **MacTCP** and **AdminTCP** icons into the **System Folder** on your hard disk by selecting both the **MacTCP** and **AdminTCP** icons (click one icon and then hold down the **Shift** key and click the other icon), and draging them into the **System Folder**.

4 If you want to use the **Hosts** file for name-to-address mapping, drag the **Hosts** file into the **System Folder** by selecting the **Hosts** file and dragging it into the **System Folder**. To customize the contents of the **Hosts** file, refer to Section 4.6.

5 Close the **MacTCP Software** folder and the Software Distribution Disk folder. Eject the disk, and put it away.

6 Configure the **MacTCP** software as described in Section 4.5.

4.5 Configuring MacTCP

You can configure the **MacTCP** software in several ways, depending on how much of the configuration you want to leave to your network users. Read the section "Configuration Scenarios" to determine your strategy.

These sections assume that you are bringing up the **MacTCP Control Panel** screens for the first time. If you have configured the driver once, the values that appear will be somewhat different from those depicted here.

Make sure that you have installed the **MacTCP** software according to the instructions in Section 4.4 before you proceed with the tasks described in this chapter.

4.5.1 The AdminTCP and MacTCP files

Recall from Section 4.4 that the Software Distribution Disk contains the **MacTCP** file and the **AdminTCP** file, which you have installed. The **MacTCP** and **AdminTCP** files both contain the configuration tools that modify resources in the **MacTCP** file and the **MacTCP Prep** file. However, one of the tools in the **AdminTCP** file includes an extra option, **Protected**, that leaves the resulting **MacTCP** file only partially configurable by the user.

Since the network administrator should control the option to protect or unprotect the configuration, you should not distribute the **AdminTCP** file to the user. Only the network administrator should use this file to configure the driver. The user can perform either full or partial configuration by running the **MacTCP** file. In its default state, the **MacTCP** file is unprotected, so if you plan to give the user full configuration authority, simply distribute the unprotected **MacTCP** file to the user. Otherwise, use **AdminTCP** to partially or completely configure the driver, protect the configuration, then distribute the **MacTCP** file to network users.

4.5.2 Configuration tools in AdminTCP

There are two MacTCP configuration tools in **AdminTCP**: The **MacTCP Control Panel** and the **Administrator dialog box**. The way you use these tools depends on the configuration scenario you choose to implement. (These scenarios are described in the section "Configuration Scenarios" later in this chapter.)

The top-level configuration tool is the **MacTCP Control Panel**. It is used to set link level information and, optionally, to enter the IP address in decimal notation. If you enter the IP address in the **MacTCP Control Panel**, portions of the Administrator dialog box are automatically filled out.

The appearance of the **MacTCP Control Panel** in the version 6.0.x environment (Figure 4.4 The MacTCP Control Panel Under System 6) differs from the Control Panel in version 7.0(Figure 4.5 The MacTCP Control Panel Under System 7). However, the function of the **MacTCP Control Panel** is the same in either environment.

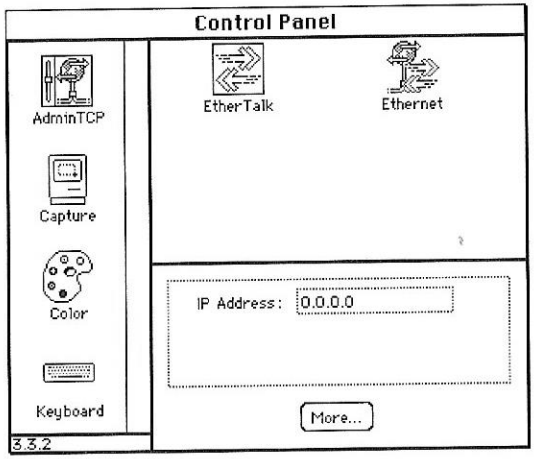


Figure 4.4 *The MacTCP Control Panel Under System 6*

The lower-level configuration tool is the **Administrator dialog box**, which is accessed through the **More** button on the **MacTCP Control Panel**.

You use the **Administrator dialog box** to enter detailed configuration information. The **Administrator dialog box** in the **AdminTCP** file also allows you to select the **Protected** checkbox, to protect the configuration from further modification. This option is not available through the **Administrator dialog box** in the **MacTCP** file; the checkbox is either dimmed (to indicate that the configuration has been protected) or does not appear.

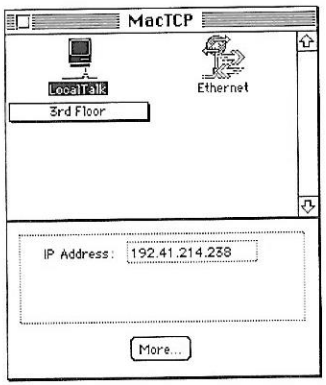


Figure 4.5 *The MacTCP Control Panel Under System 7*

The **Administrator dialog box** can be used by the network administrator and by users assigned full configuration authority. Users with partial configuration authority can view the dialog box but cannot modify it.

The following paragraphs give an overview of the **Administrator dialog box** features.

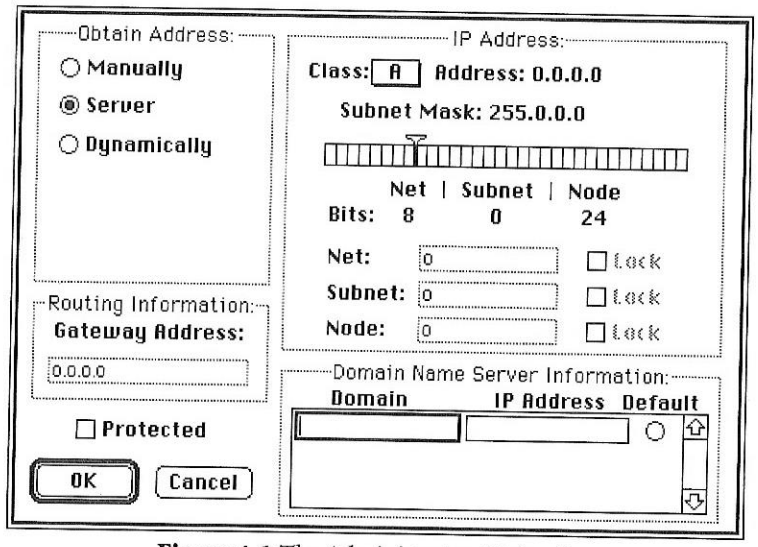


Figure 4.6 *The Administrator Dialog Box*

Obtain Address box

This is where you select the method with which you set the IP address. You have three options:

If you select the **Manually** button, you must fill in some or all of the fields in the **IP Address** box.

If you select the **Server** button, the IP address for the Macintosh computer is automatically obtained from a Server every time the user starts up the computer. This option requires a **RARP** or **BOOTP** server on an Ethernet, or a **KIP**-compatible Datagram Delivery Protocol-Internet Protocol (DDP-IP) gateway on an AppleTalk network.

If you select the **Dynamically** button, the node portion of the IP address for the Macintosh computer is set dynamically every time the user starts up the computer. If you use this option, you must also set some of the fields in the IP Address box.

IP Address box

This is where you set the address class, subnet mask, net, subnet, and node numbers. You can fill in some or all of these fields depending on the configuration scenario that you choose to implement.

Routing Information box

This is where you set the gateway address in dotted decimal notation if the Routing Information Protocol (RIP) is not implemented on your network.

If you leave this address set to `0.0.0.0`, MacTCP will use RIP to determine where your gateway is.

Domain Name Server Information box

This is where you enter the IP addresses of domain name servers and the domains over which they have authority. Make sure that whatever you enter here is valid, as invalid entries can cause sluggish behavior with MacTCP products.

Protected checkbox

If you click this checkbox, the user is not able to modify any of the fields in the **Administrator dialog box**. The screen is displayed with all the fields dimmed.

4.6 Configuration scenarios

You can configure the **MacTCP** driver in several ways; you must decide how much of the configuration you want to leave to network users. The following scenarios describe the possible strategies and summarize the configuration process for each.

Scenario A

Configure the **MacTCP** driver so that the user does not have to fill in any IP address information in the **MacTCP Control Panel**. If this is your strategy, you have two options. You can enter the IP address in the **MacTCP Control Panel** (in decimal notation) and then enter the subnet information in the **Administrator dialog box** (if appropriate). Or you can select the **Manually** button in the **Administrator dialog box** and then enter the address class, subnet mask, net, subnet, and node numbers. If you select the latter method, you must configure **MacTCP** software for each network user.

Scenario B

Configure the **MacTCP** driver so that the user must fill in the IP address in the **MacTCP Control Panel** (in decimal notation). If this is your strategy, select the **Manually** button in the **Administrator dialog box** and then enter the address class and subnet mask. Do not fill in the Net, Subnet, and Node boxes. If you select this method, you can distribute the configured **MacTCP** software to several users.

Scenario C

Configure the **MacTCP** driver so that the user must fill in the node portion of the IP address in the **MacTCP Control Panel**. If this is your strategy, select the **Manually** button in the **Administrator dialog box** and then enter the address class, subnet mask, net number, and subnet number. Do not enter the node number in the **Node** box. If you select this method, you can distribute the configured **MacTCP** software to several users.

Scenario D

Configure the **MacTCP** driver so that the address is automatically assigned. (The user does not have to fill in any IP address information in the **MacTCP Control Panel**.) If this is your strategy, select the **Server** button in the Administrator dialog box. If you select this method, you can distribute the configured **MacTCP** software to several users.

Scenario E

Configure the **MacTCP** driver so that the node portion of the address is assigned dynamically. (The user does not have to fill in any IP address information in the **MacTCP Control Panel.**) If this is your strategy, select the **Dynamically** button in the **Administrator dialog box** and then enter the address class, subnet mask, net, and subnet numbers. If you select this method, you can distribute the configured **MacTCP** software to several users.

Scenario F

The user is granted full configuration authority and can use the **Administrator dialog box** to configure the **MacTCP** software. The user will need to have knowledge of how to configure the **MacTCP** driver in order for this scenario to be successful.

4.7 Using MacTCP

This section describes how you bring up the MacTCP Control Panel in system software versions 6.0.x and System 7.0. Read the section that applies to your environment.

4.7.1 Activating under System 7

Choose **Control Panels** from the **Apple** menu, and the **Control Panels** window appears with a scrollable list of icons as shown in Figure 4.7.

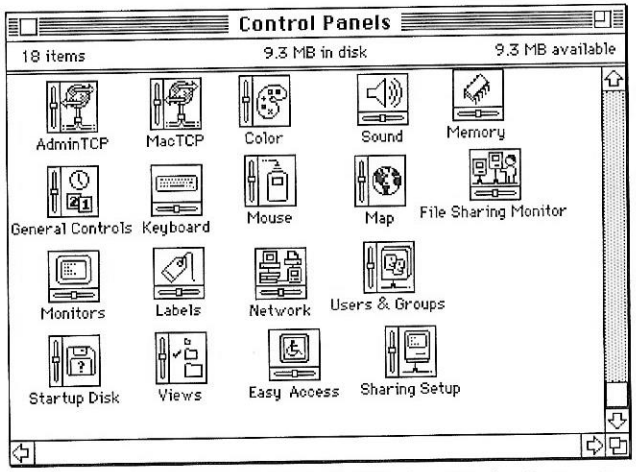


Figure 4.7 *The Control Panels Window Under System 7*

Click the **AdminTCP** icon (it may be necessary to use the scroll bar to bring the **AdminTCP** icon into view). The **AdminTCP** panel appears as shown in Figure 4.8. This panel serves as the **MacTCP Control Panel.**

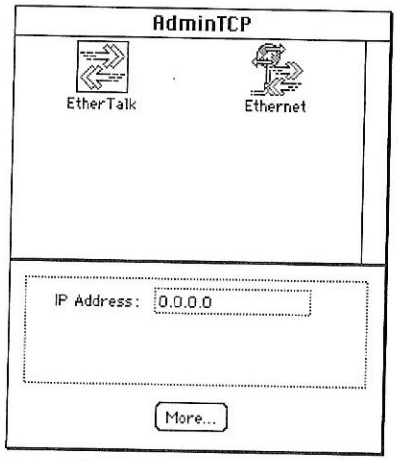


Figure 4.8 *The AdminTCP Control Panel*

4.7.2 Activating under System 6

Choose **Control Panel** from the **Apple** menu, and the panel appears with a scrollable list of icons at the left side of the window.

Click the **AdminTCP** icon (it may be necessary to use the scroll bar to bring the AdminTCP icon into view). The **MacTCP Control Panel** appears in the right three-quarters of the window as shown in Figure 4.9.

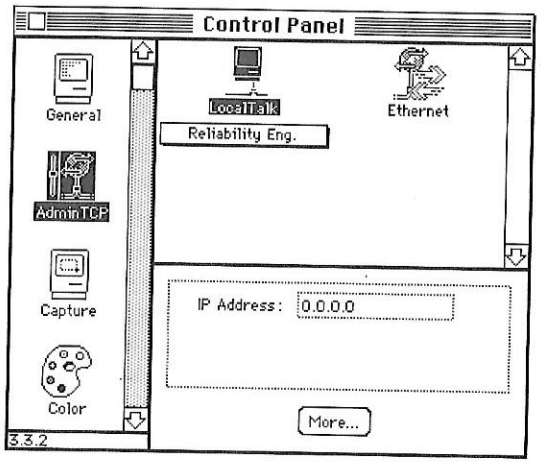


Figure 4.9 *The AdminTCP Control Panel Under System 6*

4.7.3 Setting link level information

The top half of the **MacTCP Control Panel** displays the available **link level protocols** on which the **MacTCP** driver can run. Different icons are displayed depending on your network configuration.

If your Macintosh computer is using an Ethernet interface card, make sure that the card's software is installed. The **MacTCP Control Panel** also provides a way for you to find out the hardware address of your Ethernet interface card, if you should need to do so for troubleshooting. Press and hold down the **option** key and click the **Ethernet** icon. The hardware address of the card is displayed beneath the icon, as shown in Figure 4.10.

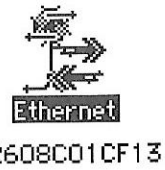


Figure 4.10 *Viewing Your Hardware Address*

Four possible network configurations are described on the following pages. Select the one that applies to your network and follow the instructions to set the link level information.

Note: This section is provided to help you set the link level information for your own computer. You cannot remotely perform this configuration task for users because it involves specific information that is reported to the MacTCP Control Panel by the computer.

Network configuration 1

Figure 4.11 illustrates one possible network configuration: a Macintosh computer on an AppleTalk network using LocalTalk cable with a gateway to an internet.

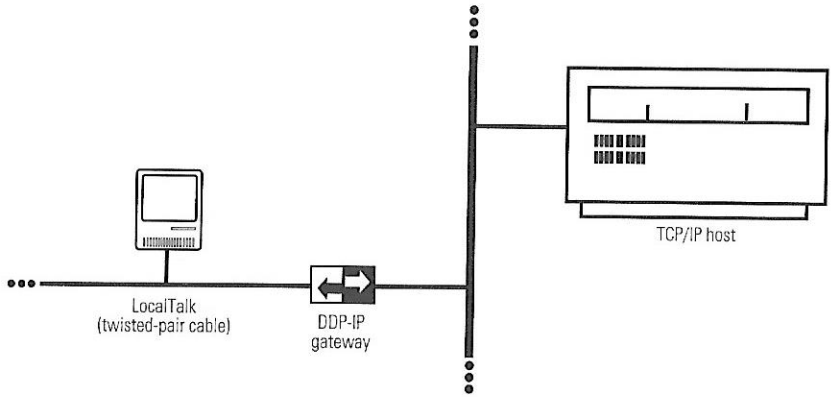


Figure 4.11 *A Macintosh on LocalTalk*

If this is your network configuration, the upper section of the **MacTCP Control Panel** contains the icon shown in Figure 4.12.

Figure 4.12 *Network Option For A LocalTalk Connected Macintosh*

The box beneath the icon displays the network zone where your DDP-IP gateway is located. If your gateway is located in another zone, direct the pointer to the zone box beneath the icon and press the mouse button. A pop-up menu appears with a list of zone names as shown in Figure 4.13. Keeping the mouse button down, drag the pointer to the list and highlight the appropriate zone. When you release the mouse button, the pop-up menu disappears, and the zone name you selected appears in the box.

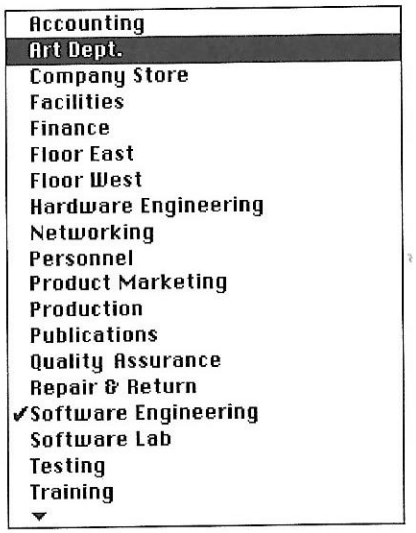


Figure 4.13 *An Example Zone List*

Network configuration 2

Figure 4.14 illustrates a second possible network configuration: a Macintosh computer with one Ethernet NB Card on an AppleTalk network using Ethernet cable.

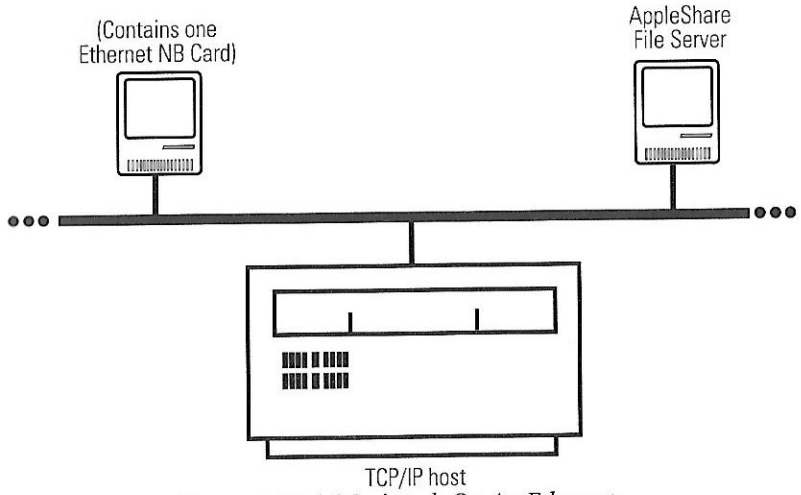


Figure 4.14 *A Macintosh On An Ethernet*

If this is your network configuration, the upper section of the **MacTCP Control Panel** contains the icons shown in Figure 4.15. Select the **Ethernet** icon to allow your Macintosh computer to use TCP/IP to communicate with other TCP/IP hosts on the network. (AppleTalk is already being used to communicate with the AppleShare® file server and LaserWriter printer.)

Figure 4.15 *Network Options For An Ethernetted Macintosh*

Network configuration 3

Figure 4.16 illustrates a third possible network configuration: a Macintosh II computer with two Ethernet NB Cards (located in slots 4 and 5) on an AppleTalk network using Ethernet cable.

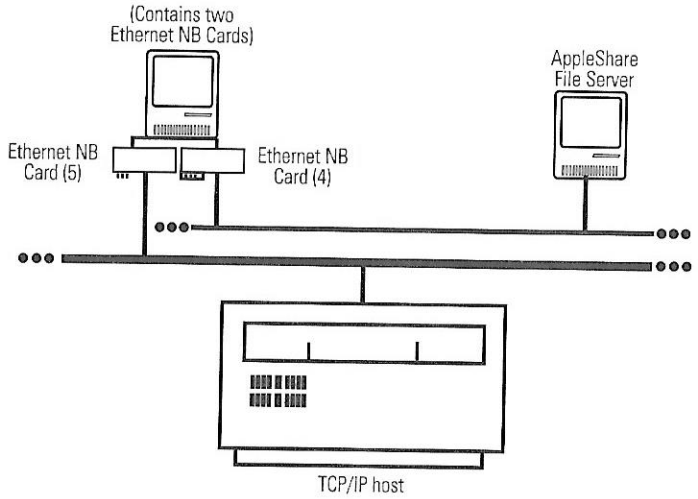


Figure 4.16 *A Dual–Ethernetted Macintosh*

If this is your network configuration, the upper section of the **MacTCP Control Panel** contains the icons shown in Figure 4.17. (If the Ethernet NB cards are located in slots other than 4 and 5, the numbers in the icon names will be different.) Select the **Ethernet (4)** icon to allow your Macintosh computer to use TCP/IP to communicate with other TCP/IP hosts on that network.

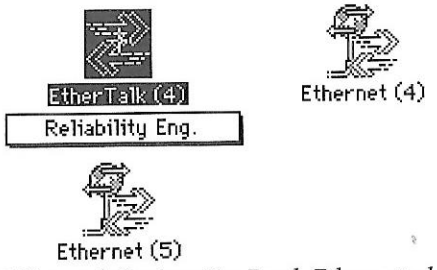


Figure 4.17 *Network Options For Dual–Ethernetted Macintoshes*

Network configuration 4

Figure 4.18 illustrates a fourth possible network configuration. Macintosh computers 1, 2, and 3 are on EtherTalk® cable segments separate from the TCP/IP host. These computers use AppleTalk protocols to communicate with the gateway, and the gateway uses TCP/IP protocols to communicate with the TCP/IP host. Macintosh computer 4, on the same Ethernet as the TCP/IP host, uses standard TCP/IP protocols to communicate directly with the TCP/IP host.

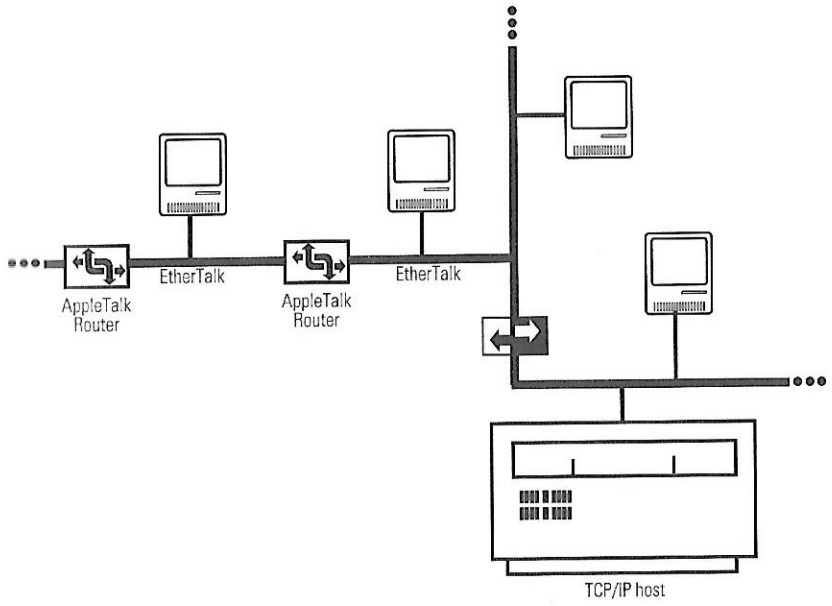


Figure 4.18 *A Complex Internetwork*

If this is your network configuration, the upper section of the **MacTCP Control Panel** contains the icons shown in Figure 4.19. If you must go through a gateway to reach a TCP/IP host (as computers 1, 2, and 3 do in Figure 4.18), make sure that the **EtherTalk** icon is selected. If you are on the same Ethernet as the TCP/IP host (as computer 4 is in Figure 4.17), select the **Ethernet** icon.

Figure 4.19 *Network Options for Complex Macintosh Networks*

4.7.4 Entering the IP address in decimal notation

If you have decided to enter the entire IP address for the user and you prefer to enter the address in dotted decimal notation (for example, 132.10.3.1), enter the address in the IP Address box as shown in Figure 4.20.

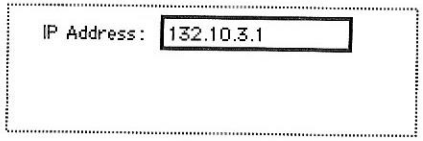


Figure 4.20 *Setting Your IP Address*

When you click the **More** button and the **Administrator dialog box** is displayed, the class, address, and net and node numbers are set as shown in Figure 4.21.

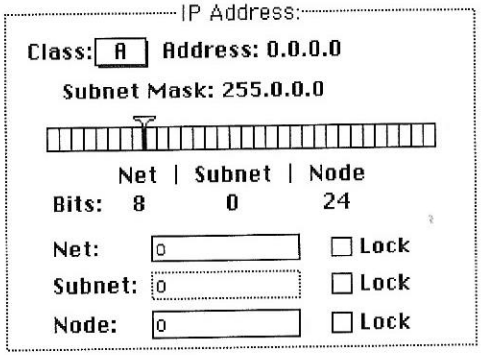


Figure 4.21 *The IP Address Section of the Administrator Dialog Box*

4.7.5 Bringing up the Administrator dialog box

Click the **More** button on the Control Panel to get to the **Administrator dialog box**, as shown in Figure 4.22. This panel is your main tool for configuring the **MacTCP** driver.

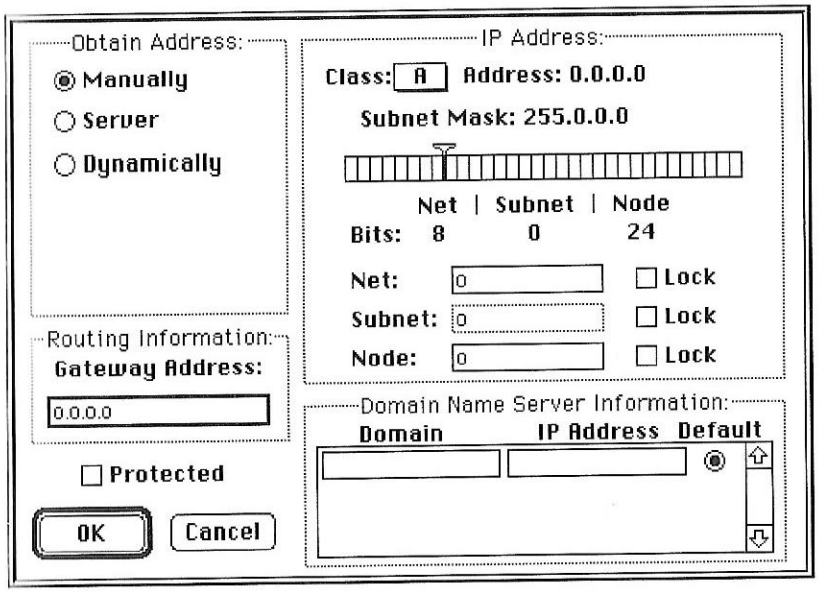


Figure 4.22 *The Administrator Dialog*

The **Administrator dialog box** provides you with three ways to set the IP address (if you did not enter the decimal address in the **MacTCP Control Panel**). The **Obtain Address** box in the upper-left corner of the panel (shown in Figure 4.23) allows you to select your preferred method for setting the address. Your selection determines whether the user must enter address information on the **MacTCP Control Panel**.

- If you select **Manually**, you must set the address manually using the fields in the IP Address box. See the next section "Setting the Address Manually."
- If you select **Server**, the address is obtained automatically from a Server. This option requires a RARP or BOOTP server on an Ethernet, or a KIP-compatible Datagram Delivery Protocol-Internet Protocol (DDP-IP) gateway on an AppleTalk network. See the section "Obtaining an Address from a Server" later in this chapter.
- If you select **Dynamically**, you must set the net and subnet portions of the address using the fields in the IP Address box, but the node portion of the address will be allocated dynamically (within the range of node numbers specified). See the section "Setting the Node Number Dynamically" later in this chapter.

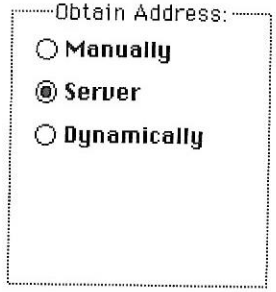


Figure 4.23 *The Obtain Address Section of the Administrator Dialog Box*

4.7.6 Setting the address manually

If you select **Manually**, you must set the address manually using the fields in the IP Address box. You can enter either the entire IP address, or the net and subnet portions. Entering the entire address causes the IP address to appear on the **MacTCP Control Panel**. The user does not need to enter any address information. Entering the net and subnet portions causes Net, Subnet, and Node boxes to appear on the **MacTCP Control Panel**. The user must enter the node number.

To set the address manually, click the **Manually** button located in the **Obtain Address** box. Then follow the steps described in the following sections.

4.7.7 Setting the address class

Move to the **IP Address** box and position the pointer on the **Class** box. Class A, the default setting, is currently in the box. Press the mouse button and a menu of classes appears as shown in Figure 4.24. The √ indicates which class is the current setting. If you want to change the class, drag the pointer to **B** or **C**.

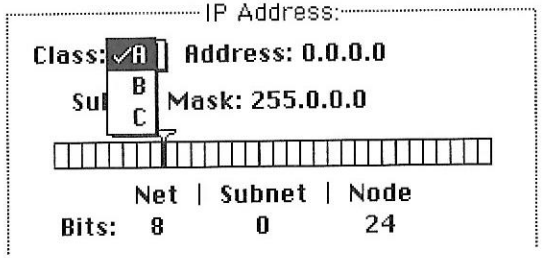


Figure 4.24 *Setting the Address Class*

If you change the class, the new value that appears in the **Net** box is the minimum value allowable for the selected address class. For instance, if you select class C, the value in the **Net** box changes to `12582912`, which is the minimum value that can be used for class C addresses.

Figure 4.25 *The Net Box*

Note that changing the class causes the slider on the ruler to move. The address, subnet mask, and bits allocated to net, subnet, and node also change. Figure 4.26 shows the address, subnet mask, position of the slider, and the bit allocation for each class selection.

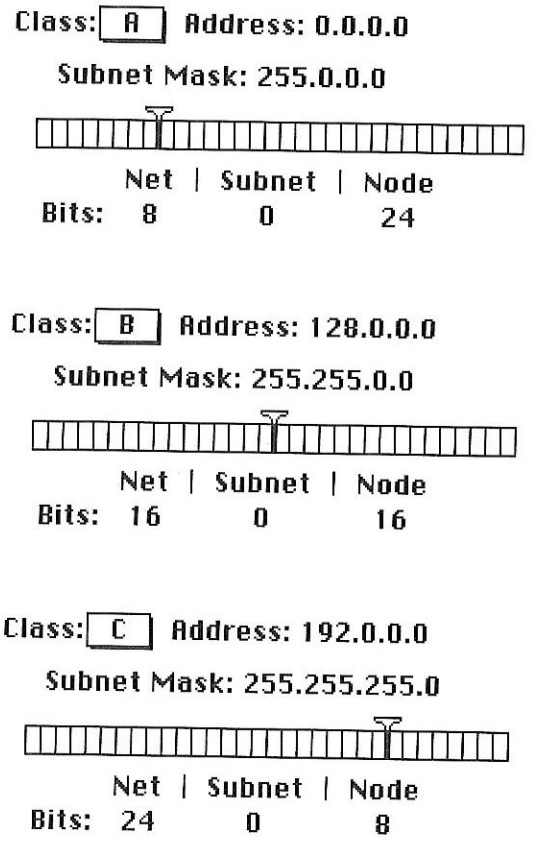


Figure 4.26 *Standard Subnet Masks*

4.7.8 Setting the subnet mask

Perform this step only if you have implemented subnet addressing on your network. Use the slider on the ruler to set the subnet mask. Each box in the ruler represents one bit of the 32-bit IP address. A dark line on the ruler indicates the number of bits allocated to the net portion of the address (as determined by the class selected). The slider can be moved anywhere along the ruler to the right of this darkened line. Place the pointer on the slider, hold down the mouse button, and drag the slider to the appropriate location on the ruler. When you move the slider, the subnet mask, the subnet bits, and the node bits change.
If you move the slider all the way to the left, the **Subnet** box is dimmed.

4.7.9 Setting the IP address (integer format)

If you want the user to enter the IP address in the **IP Address** box of the **MacTCP Control Panel** (scenario B in the earlier section "Configuration Scenarios"), skip this step. Continue with the configuration, referring to the section "Setting the Gateway Address" later in this chapter.

In integer format, the IP address is broken down into bits (four sets with eight bits per set). The bits are allocated to net, subnet, and node according to address class and subnet mask, then converted to a decimal number. For instance, the address `90.25.3.240` broken down into bits, looks like this: `01011010.00011001.00000011.11110000`

If the address class is A (8 bits compose the net portion of the address) and the subnet mask is `255.255.252.0` (or 14 bits of subnet address and 10 bits of node), then the integer form of the address is as follows:

```
Net: 90
Subnet: 1600
Node: 1008
```


If you want to enter the IP address in integer format, enter this information in the Net, Subnet, and Node boxes shown in Figure 4.27.

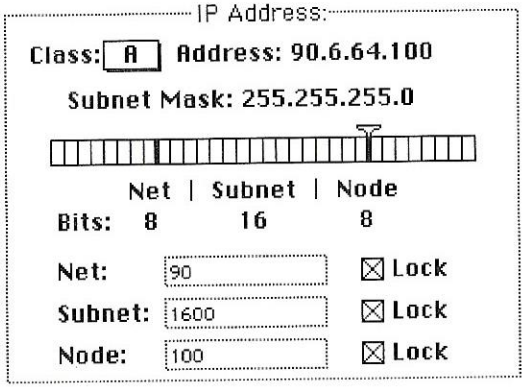


Figure 4.27 *An IP Address In Integer Format*

If you are configuring the **MacTCP** driver so that the user has to enter the **node** number in the **MacTCP Control Panel** (scenario C in the earlier section "Configuration Scenarios"), you must enter the net and subnet portion of the address in integer format in the Net and Subnet boxes.

Entering the net number

The **Net** box contains the lowest net number that can be used, determined by the address class that was selected. Click twice in the **Net** box and enter the net portion of the IP address in integer form. If you try to enter a number over the highest number allowed for the selected address class, the last digit in the number you enter isn't accepted; you must reenter a valid number. If you enter a number under the minimum allowed for the selected address class, a valid number is automatically assigned when you save your changes; therefore, be sure to enter a number over the minimum allowed for the selected address class.

If you click the **Lock** box to the right of the **Net** box, the net number is protected. The **Net** box is dimmed and you cannot change its value unless you click the **Lock** box to unlock it. If you lock the value in the **Net** box, the user will not be able to change this number on the **MacTCP Control Panel**.

Entering the subnet number

Note that you can enter the subnet number only if you set the subnet mask. Click the **Subnet** box and enter the subnet portion of the IP address in integer form. If you click the **Lock** box to the right of the **Subnet** box, the subnet number is protected. The **Subnet** box is dimmed, and you cannot change the value in the box unless you click the **Lock** box to unlock it. If you lock the value in the **Subnet** box, the user will not be able to change this number on the **MacTCP Control Panel**.

Entering the node number

You now have three choices: enter the node number, leave the **Node** box at the default and have the user enter the node number, or have the node number assigned dynamically.

If you decide to enter the node number, click the **Node** box and enter the node portion of the IP address in integer form. If you click the **Lock** box to the right of the **Node** box, the node number is protected. The **Node** box is dimmed and you cannot change the value in the box unless you click the **Lock** box to unlock it. If you lock the value in the **Node** box, the user will not be able to change this number on the **MacTCP Control Panel**.

If you decide to have the user enter the node number in the **MacTCP Control Panel**, leave the box at the default number and do not select the **Lock** box. Then continue with the configuration, starting with the section "Setting the Gateway Address" later in this chapter.

If you want the node number to be assigned dynamically every time the user starts up, see the section "Setting the Node Number Dynamically" later in this chapter.

Figure 4.27 shows values set and locked in the Net, Subnet, and Node boxes.

4.7.10 Obtaining an address from a server

If you select the **Server** button in the **Obtain Address** box, the network address is obtained automatically from a network server. On an Ethernet network, the protocols **BOOTP** or **RARP** are used to assign an address. On an AppleTalk network, a DDP-IP gateway sets the address.

To have a server provide the address, click the **Server** button in the **Obtain Address** box. (When you bring up the **Administrator dialog box** for the first time, Server is the default setting.) There is no need to enter class, subnet mask, or net, subnet, or node numbers; the **Server** button does it for you. The Macintosh computer that uses this configuration is assigned an address every time it starts up, as long as you have a properly configured server.

After you restart, the class, subnet mask, net, subnet, and node numbers assigned by the server are reflected in the Administrator dialog box and in the IP Address box. The user does not have to enter any address information.

4.7.11 Setting the node number dynamically

If you select the **Dynamically** button in the **Obtain Address** box, the node portion of the IP address is allocated dynamically within the range of node numbers specified.

An IP address has a range of valid node numbers that are determined by the address class and subnet mask. With dynamic addressing, the **MacTCP** software randomly selects a node address in that range and broadcasts to other nodes on the network, "Is there anyone out there using this address?" If there is no response, that node number is used; if there is a response, the software rebroadcasts until it finds a number that is not being used by other machines on the network.

To use dynamic addressing, enter the address class, subnet mask, and net and subnet numbers as described in the earlier section "4.7.6 Setting the address manually" on page 42. Click the **Dynamically** button in the **Obtain Address** box. Two boxes appear, showing the range of valid node numbers determined by the class and subnet mask (illustrated in Figure 4.28). After changes made to the **Administrator dialog box** are saved, a node number is assigned dynamically when the Macintosh computer is started up.

This choice causes the IP Address box to appear on the **MacTCP Control Panel** with the address already set. The user does not have to enter any address information.

If you know there are static addresses on your network, you can change the values in the **Node Range** boxes so that the addresses in the static range are not used. To change the minimum range value, double-click the **From** box and enter an appropriate number. To change the maximum range value, double-click the **To** box and enter an appropriate number.

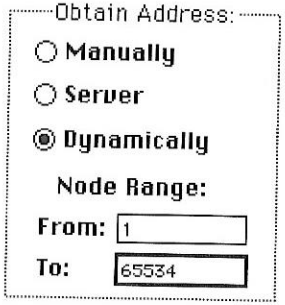


Figure 4.28 *Obtaining An Address Dynamically*

4.7.12 Setting the gateway address

Some gateways use the Routing Information Protocol (RIP) to exchange network routing information. The **MacTCP** software automatically monitors RIP traffic to determine active gateways. If your network does not use RIP, you must manually set the address of a gateway.

To manually set the gateway address, go to the **Routing Information** section of the **Administrator dialog box**. Click the pointer in the **Gateway Address** box and enter your gateway's decimal IP address as shown in Figure 4.29.

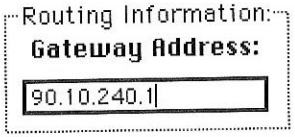


Figure 4.29 *Setting Your Gateway Address*

4.7.13 Setting domain name server information

This part of the **Administrator dialog box** allows you to enter the IP address of domain name servers and the domains over which they have authority. The box allows you to enter this information for your network's domain name server and other domain name servers on the internet.

Click the pointer in the **Domain** box and enter a domain name. Press the **Tab** key to move the pointer to the **IP Address** box and enter the address of that domain. As you enter the IP address, boxes appear (shown in Figure 4.30) to allow you to enter more domain name server information.

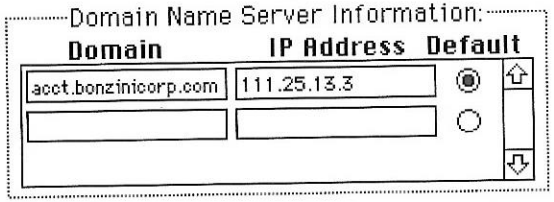


Figure 4.30 *Setting A Domain Name Server*

Click the **default** button to indicate your default domain name server and your default domain name extension. Generally, it should be a domain name server that has authority over your domain.

4.7.14 Protecting the configuration

To protect your configuration, click the **Protected** checkbox (shown in Figure 4.31). If you don't select the **Protected** checkbox, the user who receives the config-

ured user disk will be able to modify any of the fields in the **Administrator dialog box.**

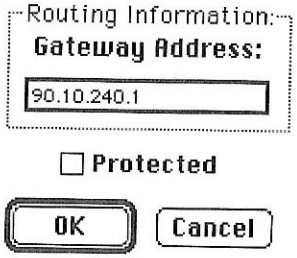


Figure 4.31 *Protecting Your Configuration*

4.7.15 Closing the Control Panel

When you have finished entering the appropriate information in the **Administrator dialog box**, the **MacTCP** driver is configured. The configuration settings are stored in the **MacTCP** driver and also in a file called **MacTCP Prep**.

Click the **OK** button in the **Administrator dialog box** and then click the **Close** box to close the **Control Panel** window. The configuration changes take effect the next time the driver is used. If the configuration changes cannot be made immediately, the alert message shown in Figure 4.32 is displayed.

This message alerts you that you must restart your Macintosh computer for the configuration changes to take effect. When you click the **OK** button, the Control Panel closes. When you restart, the **MacTCP** driver is configured on your computer.

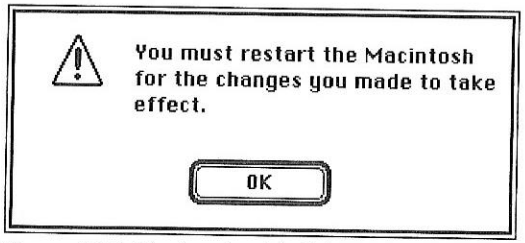


Figure 4.32 *Closing the Administrator Dialog Box*

4.8 The Hosts File

The **MacTCP** software includes a **Hosts** file that maps machine names to internet addresses, the same service provided by the domain name system. You can use the **Hosts** file if there is no domain name server on your network. It is also convenient to place frequently used name-to-address mappings in this file.

To use the **Hosts** file, you must edit the sample file that is included with the **MacTCP** software and add text that defines name-to-address mappings. Each host on your network that uses **Hosts** file services must have the file resident on the disk.

4.8.1 Hosts file syntax

The **Hosts** file syntax conforms to the master file syntax specified in Request for Comment (RFC) 1035. Refer to this RFC for more information.
(Note $INCLUDE has not been implemented.)

The syntax of the Hosts file is as follows:

```
<name><type><data>[;<comment>]
```

where `name` is the name assigned to a host or domain on the internet.

`type` is `A` (address), `NS` (name server), or `CNAME` (canonical name).

`data` is determined by the type specified:

- If `type` = `A`, the data field contains an internet address.
- If `type` = `NS`, the data field contains the name of the domain name server that has authority over the domain specified in the name field.
- If `type` = `CNAME`, the data field contains the canonical (or official) name for the name field.

`Comment` allows you to add a comment to the entry. A semicolon is used to start a comment.

Any combination of tabs and spaces can be used as a delimiter between each item in a line. Lines end with the return and line feed characters.

Example entries in a Hosts file are as follows:

```
acct.xco.comA128.8.1.1; address of host "acct"
xco.comNSserver.xco.com; name server for domain xco.com
fred.xco.comCNAMEbonzini.xco.com; canonical name for alias fred.xco.com
```

4.8.2 Editing the Hosts file

To create **Hosts** files for network users, modify the sample file using Apple's **TeachText**, adding text that defines name-to-address mappings for your particular network configuration.

To edit the Hosts file, perform the following steps:

1 Select the sample **Hosts** file icon entitled **Hosts**, included with your **MacTCP** software, and open it by choosing **Open** from the **File** menu or by double-clicking the icon.

2 Add names and internet addresses in the syntax specified in the previous section.

You can edit the **Hosts** file with any word processor as long as you save it as **Text Only** without formatting commands.

4.9 MacTCP Configuration Worksheet

The following table lists the information needed by a user to configure their copy of **MacTCP**. Each user should fill out this table and keep it handy in case they need technical support, or if they need to reconfigure **MacTCP** at some point. In case you are unsure of the meanings of the following terms, they have been redefined in the paragraphs following the table.

Settings	Value
Network Type	
IP Address[a]	
Gateway Address	
Subnet Mask	
Default Domain	
IP Address of Domain Name Server	

Figure 4.33 *Network parameters*

a. It should be noted that the IP Addresses 192.0.0.x and 128.0.x.x are considered to be invalid IP Addresses according to RFC 1122, and MacTCP will not allow you to assign your Macintosh one of these addresses. Because some TCP/IP stacks do allow you to set up you network with said network numbers, you will have to reassign your networks IP Addresses in order to use MacTCP on your network.

Network Type If you are using an Ethernet card, make sure that you select the Ethernet icon in MacTCP. LocalTalk users should verify that their Ethernet to LocalTalk gateway is set up to properly route IP packets.

IP Address This would be the assigned IP address for your Macintosh. If you are using Dynamic Addressing with a Ethernet to LocalTalk Router, you should write "dynamic" in this field.

Gateway Address This would be the IP Address of any IP gateway running the Routing Information Protocol (RIP), including Ethernet to LocalTalk routers, such as an Ether•Route or a FastPath. If you would like MacTCP to attempt to ascertain the appropriate value for your router, use the default Gateway Address of `0.0.0.0`.

Subnet Mask This is the subnet mask used by your particular network, and should be verified with your System Administrator. When you supply MacTCP with your IP Address, MacTCP will fill in the default SubnetMask for your particular network. Under most circumstances, this value will be correct, but you should verify it anyway.

Default Domain is the text descriptor for your particular network, if you are using Domain Names Services. For example, at MIT the machine named `zurich` is in the domain `ai.mit.edu`. Any other machine on this particular subnet would also have the default domain of `ai.mit.edu`.

IP Address of Domain Name Server is the IP address of a host on your subnet that is running the `named` daemon. If you do not have a domain name server on your network, do not enter any DNS information into **MacTCP**.

Chapter 5

USING NFS/SHARE

5.1 Setting up NFS/Share

Before using NFS/Share, make sure that you have installed and configured MacTCP. After MacTCP and NFS/Share have been installed on your machine, you should run the NFS/Test program to verify that your NFS server is up and running with the necessary daemons. Make sure that you have **AppleShare** installed, by looking for its document in the Chooser and checking to see if you have either **Get Privileges...** (System 6) or **Sharing...** (System 7) in your **File** menu. If you do not have AppleShare installed, install it from your Apple System Software installer disks by running the Installer application.

To use NFS/Share you must have at least one authentication daemon running on your machine. The choices are NIS, PCNFSD or BWNFSD.

If you are using NIS as your authentication daemon, select NIS Domain from the popup menu and enter its domain name in the dialog box. (The popup menu is located to the right of the Select button.) The NIS domain that you enter will be the default NIS domain for all the dynamically located hosts. Any hosts that you add manually (necessary for servers in other subnets or on the other side of a gateway) will require you to enter the NIS Domain in the respective **Add Host** dialog.

5.1.1 Adding remote hosts

Sometimes you may need to access a host that is not available locally. To add a host that does not automatically appear in NFS/Share's server list to your available hosts list, Select **Add Host** in NFS/Share's pop-up menu. In the Add Host dialog, fill in the **Name** text area with a descriptive string for the remote host, as you want it to appear in the Chooser's list, and fill in the **Server** text area with either the host name of the remote host or its IP address. If you are using NIS to authenticate, enter the correct **NIS Domain** in the last field of the dialog. Click **Add** to

return to the **Chooser** and your new NFS host will be listed in the host list. Remote hosts are mounted in the same manner as that of local hosts.

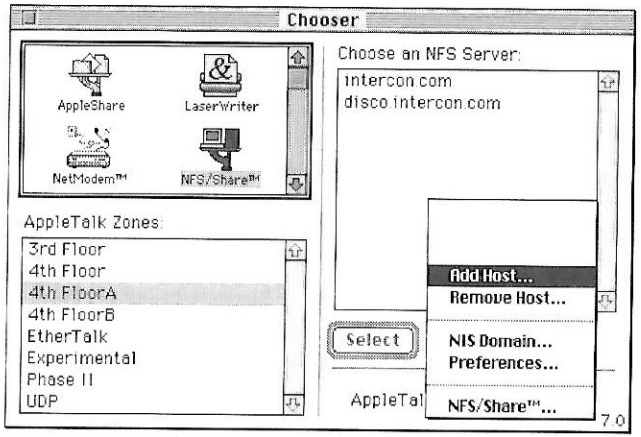


Figure 5.1 *NFS/Share's pop-up*

5.1.2 Mounting a volume

Mounting a volume with NFS/Share begins by opening the **Chooser** in the **Apple** menu and selecting the NFS/Share icon. After a brief pause, a list of local NFS hosts will come up in the list box. (A local host is defined as any host that resides in your IP Subnet and on your Macintosh's side of the Gateway.) If you do not have a Domain Name Server, you will see a list of IP addresses instead of host names. MacTCP will simulate a Domain Name Server automatically if you enter your NFS servers as "A" records in your hosts file, located in your System Folder.

Mounting a volume with NFS/Share is achieved through the following steps:

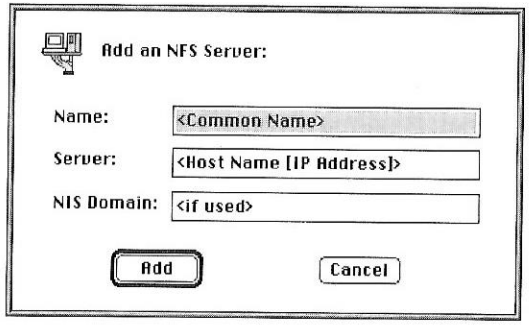


Figure 5.2 *Adding An NFS Server*

✓ Select the server you wish to mount and click **Select.** A dialog will come up asking for a **username** and **password.** This is the same username and password that you use to log on to a terminal session with the selected machine.

✓ The **Select a Volume To Mount** dialog is a user-definable volume list. Volumes are listed in this dialog by their volume name and are mounted by double clicking the entry. NFS/Share will only allow you to mount one volume at a time.

✓ To add a mount point, click the **Other** button. The **Mount Point** field is the path name on the NFS server that you intend to mount. The **Volume Name** field specifies the name of the NFS/Share icon that identifies the volume on the Macintosh.

✓ Click the **Mount** button and NFS/Share will mount the volume. (The other options found in the **Edit Mount Point** dialog will be covered in the following text.)

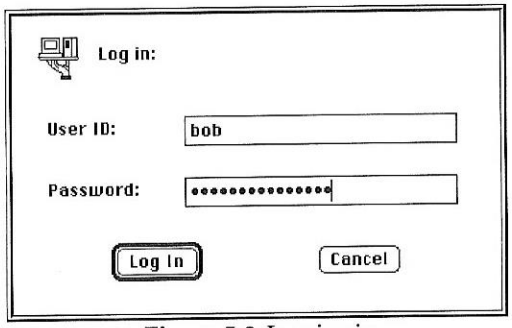


Figure 5.3 *Logging in*

5.1.3 Adding a volume

The **Select a Volume To Mount** dialog is a list of defined mount points relative to the chosen NFS server. To add a volume to this list, follow the steps below.

✓ Click **Other** in the **Select a Volume To Mount** dialog and the **Edit Mount Point** dialog will come up. If you are using NIS for authentication, the Mount Point text area will reflect the path to your default user directory.

✓ Enter/edit the **Mount Point** field for your volume and give it a name in the **Volume Name** field. (Note: The volume name which appears on your Macintosh desktop can only be edited in this dialog. You can not change it on the Macintosh desktop.)

✓ Click the **Save** button and the volume definition will be added to the **Select a Volume To Mount** dialog. Any options that you select before clicking **Save** will be attached to the volume definition.

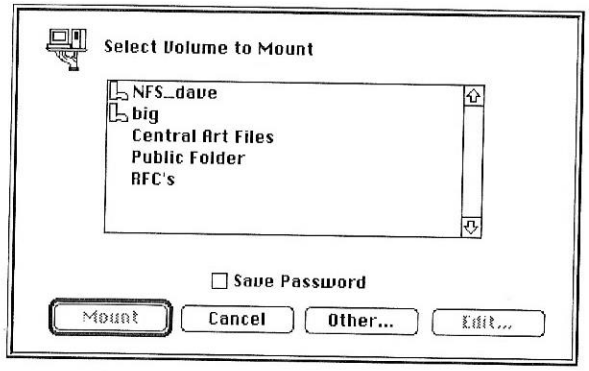


Figure 5.4 *Selecting a Volume To Mount*

The mount point can be any path that you desire as long as it is within an exportable file system. In other words, if you have `/usr` exported to you, you may directly mount any path within `/usr`.

It is not necessary to mount a volume in order to add its definition to the Volume List. If you have several volume definitions that you wish to add to NFS/Share's configuration, simply click **Other** and then click **Save** for each defined Mount Point. This will return you to the **Volume List** dialog without mounting the volume.

5.1.4 Maintaining Desktop Information

When adding or editing a volume definition, one of the available options is the **Maintain Desktop Information** checkbox. NFS/Share keeps your volumes desktop information in memory while the volume is mounted and if this option is selected, that information will be saved to disk when that volume is unmounted or when your machine is shut down.

When NFS/Share mounts a volume, it looks in the System Preferences Folder to see if there is any saved desktop information to be loaded in. If it is found, that information will be used to seed NFS/Share's desktop cache for that volume, regardless of whether or not the **Maintain Desktop Information** option is on. Because of this, a user can establish a default desktop for an NFS/Share volume that will always be the same every time the volume is mounted. To do this, mount the volume with the **Maintain Desktop Information** checkbox selected and arrange your folders and icons as desired. Unmount the volume by dragging it to the trash. Before you remount the volume, edit the mount point by selecting it in the **Select a Volume To Mount** dialog and clicking the **Edit** button. Turn off the **Maintain Desktop Information** option and click the **Save** button. Now when you remount the volume, all of the saved icon positions and window sizes will be as they were when you first set them, but any changes that you make to the desktop's appearance will not be saved when you unmount the volume.

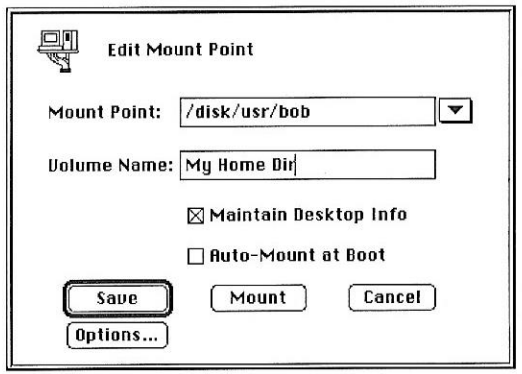


Figure 5.5 *Editing a Mount Point*

5.1.5 Auto-mounting

Selecting the **Auto-mount At Boot** option when editing a volume definition specifies that the volume will be automatically mounted when you start your machine. A volume designated for automounting will show a small boot icon beside it in the **Select a Volume To Mount** dialog. If the **Save Password** option is checked in this dialog, all automounting volumes from this host will be mounted using the log-on information that was last used to access this host with NFS/Share.

5.1.6 Filenaming options

The **Options** button will bring up a list of possible naming scheme options for translating Macintosh filenames to filenames suitable for your NFS server. The

default (**8-bit**) items in the pop-up menu indicates that NFS/Share will allow any legal 8-bit ASCII character to be used in a filename. Only the character "\" will be quoted when written to the NFS server as it is an illegal character for a filename. The **7-bit** option indicates that only 7-bit ASCII characters in a filename will be unmodified when they are written out to the NFS server. In practical terms, this option will never affect how you view the files with NFS/Share. Only when you view the files names from the host side will you notice that certain characters have been replaced with "quoted" characters.

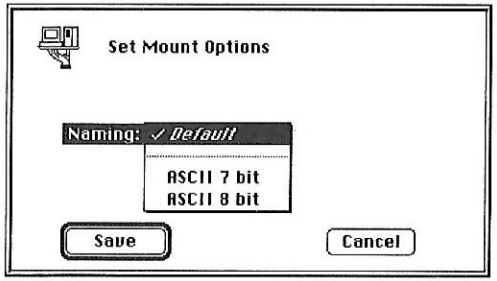


Figure 5.6 *Mount Options*

The conventions for a quoted character is a percent sign (%), followed by two digit hex codes representing the ASCII value for the original character. It should be noted that the 7-bit option will yield longer server-side filenames, as more characters that are common on the Macintosh will end up being quoted. The file-naming options should not be used unless you have specific limitations on your NFS server that require you to write 7-bit ASCII filenames.

5.1.7 Allocating memory for NFS/Share

NFS/Share allocates the memory it requires to operate at INIT time (when you start your machine). Initially, NFS/Share is configured to allocate enough memory to mount two volumes. If you need to mount more volumes, you can give NFS/Share more memory by selecting **Preferences** in NFS/Share's pop-up menu found in the Chooser and entering the number of volumes that you need to mount. NFS/Share will also tell you how much memory it will allocate. After

making changes to this area, you must restart your machine before the changes will be reflected.

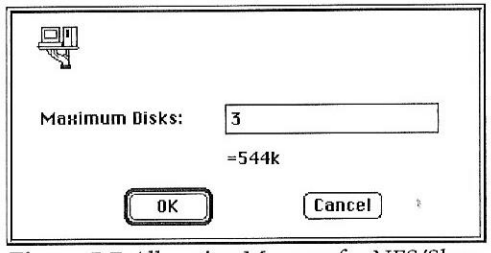


Figure 5.7 *Allocating Memory for NFS/Share*

5.2 Disabling NFS/Share

If you need to temporarily disable NFS/Share, start-up your Macintosh with the **Option** Key held down until you see the NFS/Share Disabled icon appear. (See Appendix A) Because the **Option** key is also used to disable many other inits, you may choose to press the Option key just before NFS/Share is ready to load. Inits in your system load in alphabetical order, so you need only wait for the icon of the init that comes before NFS/Share to display before depressing the **Option** key.

Also, during start-up, holding down the **A** key will prevent NFS/Share from mounting any volumes, but will still load NFS/Share.

5.3 User Tips

5.3.1 Automounting

NFS/Share will only remember a single user profile per selected server. What this means is that if you have a server named bob.mudfish.org, and you have set up a volume on that server to auto-mount, a subsequent mount of a volume on bob.-mudfish.org as another user will change the user and password that NFS/Share will use for the auto-mounted volume the next time you start your machine. To avoid such a conflict, manually add a second reference to your NFS server with the **Add Host** item in the popup menu. Assign this reference a unique name and use it when you intend to mount a volume with an alternate password.

5.3.2 Exporting file systems

On your NFS server, the file /etc/exports controls who may have access to certain directories or file systems. A /etc/exports file may look like this:

```
/etc    -access=dave.bob.mudfish.org

/usr    -access=SalesGroup

/free
```

In the above example, `/etc` may only be accessed by the machine named dave.bob.mudfish.org; `/usr` may be accessed by anyone who is a member of the netgroup SalesGroup, and `/free` is open to any NFS client.

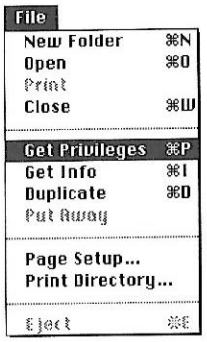
It is not possible to mount as the root user. If you attempt to do so, you will be assigned a UID of -2, which is the same as NFS's "nobody" user.

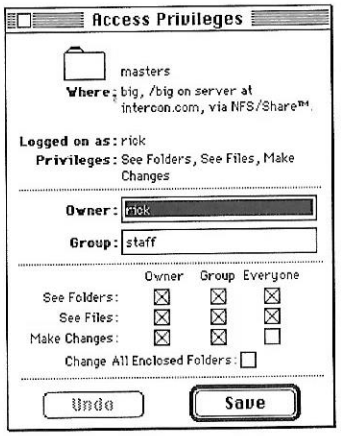
5.4 Permissions

NFS/Share provides access to server folder permissions via AppleShare's Privileges interface. Normally, folder and file permissions are modified from the host side via commands like UNIX's `chmod` command.

5.4.1 System 6

Under System 6, you can access the permissions interface by selecting **Get Privileges...** in the **File** menu. To access this menu item, select a folder within a mounted NFS volume and then select **Get Privileges...** in the **File** menu.





As in the example, an **Access Privileges** window will come up for the selected folder, presenting you with access information for the folder.

Where Indicates the name of the volume, the pathname as located on the server, the server's name and the fact that you are accessing the folder via NFS/Share.

Logged on as Indicates the username that privileges for this volume are based on.

Privileges This line will indicate the privileges that the user has to this folder.

Owner Indicates the user who owns this folder.

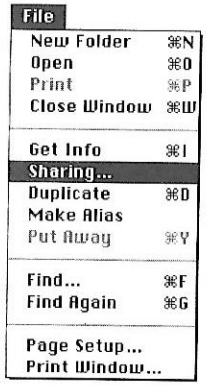
Group Indicates the group that this folder is assigned to.

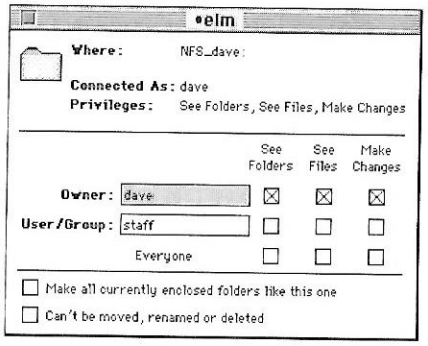
The check boxes in the lower section control the actual privileges to the folder and any enclosed folders. After modifying any of the check boxes, click the **Save** button and an `chmod` bits will be modified accordingly.

You can not change permissions for a folder unless you own it. Additionally, you must be using either NIS or PCNFSD2 in order to change the group of a folder.

5.4.2 System 7

Under System 7, the **Get Privileges...** menu item has been replaced with the **Sharing** menu item. The window that is displayed after selecting **Sharing** in the **File** menu is nearly identical to the System 6 **Access Privileges** window.

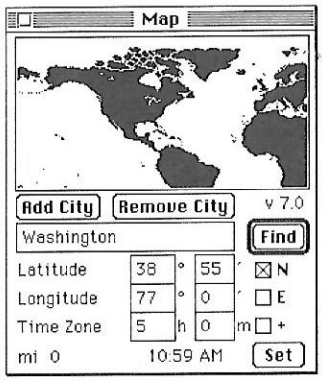




The only addition to the window is the **Can't be moved, renamed or deleted** check box. After making changes to this window, simply click the window's close box and you will be asked to confirm the changes. After confirmation, the appropriate `chmod` flags will be modified for the selected folder and enclosed folders, if required.

5.5 Time Zone

NFS reports file time-stamps in **GMT** time. If you want your times to view correctly when accessing files from **NFS/Share**, you must set your time zone with the **Map** Control Panel that is included with all Apple System Software.



The easiest way to set your time zone is to type the name of a major city, in your time zone into the text files and click the **Find** button. If the city is found, a small star will flash in the map area over the geographical location of the city. To set the location, click the **Set** button and close the **Control Panel** to save your changes.

It is important to note that time stamps are stored in GMT on the host. When you do an "ls," the host offsets the time stamp according to current Time Zone and also makes adjustments for Daylight Savings Time. NFS/Share currently makes adjustments for Time Zone only and none for DST. If you wish to have your time offset for Day Light Savings, modify the Time Zone value in the **Map** Control Panel.

5.6 Aliases

Under System 7, you may make aliases of NFS/Share's volumes, folders and files. If a volume is not mounted when you try to access an alias, the volume will automatically be mounted.

NFS/Share aliases contain your username and password and therefore can be copied to any System 7 Macintosh and function with *your* permissions. It should be noted, however, that if you change you password, existing aliases will cease to function.

It should also be noted that NFS/Share aliases do not load Saved Desktop info for the volume and they do not save Desktop Info when you unmount the volume either.

5.7 File Locking

Any file locking calls made by the Macintosh are translated in lock calls suitable for BWNFSD. If BWNFSD is not available on your NFS server, the command will not fail because there is no appropriate error condition available on the Macintosh to describe this situation. This should not be a concern unless you are running a multi-user database such as 4D or FoxBase, because file locking is only intended as a "safety feature" to prevent multiple applications/user from writing to the same section of the file. If you feel that you may be in a situation where successful file locking is a necessity, compile and run BWNFSD on your NFS server.

Chapter 6

ADMINISTRATION NOTES

6.1 Server Requirements

To use **NFS/Share** as an NFS Client, you must have an appropriate NFS server on your network. Attributes of the NFS server are the NFS server itself and an authentication server. It is also suggested that the server (or some host on the network) provide a Domain Name Service for host name to IP number mapping. Also, if you intend to share data between Macintosh clients, you should also have a file locking protocol available on your server.

6.1.1 User Authentication

NFS/Share supports three separate authentication methods: **NIS** (formerly Yellow Pages or YP), **PCNFSD** or **BWNFSD**. If available, NFS/Share will prefer NIS over the other methods.

NIS: `NIS` is provided by Sun Microsystems, Inc. and many other workstation manufacturers for use in network environments to provide centralized user authentication and information services. To use `NIS`, NFS/Share must be given the NIS domain name (not to be confused with the DNS (or Internet) domain name.) This can be entered for individual hosts at the time that the host is being added with the **Add Host** command, or as a default for automatic hosts by selecting **NIS Domain** from the pop-up menu and entering the NIS Domain name in the text dialog. NIS supports UID to name mapping, allowing you to view the owner and group name assigned to a folder when you view its permissions via AppleShare's permission interface.

If you are unsure of your NIS Domain, you can ascertain it by using the `domainname` command at the `TELNET` prompt of any host running NIS. Remember, the NIS Domain is *not* the same as your Internet Domain. They may have the same values, but this is not necessarily so. Use the `domainname` command if you have any doubts about your NIS Domain.

BWNFSD: BWNFSD is provided with **NFS/Share** and can be found in the BWNFSD folder on the distribution floppy. This protocol is basically a superset of PCNFSD with the locking features of LOCKD. BWNFSD is used for authentication if NIS fails to respond or is not present. BWNFSD supports UID to name mapping, allowing you to view the owner and group name assigned to a folder when you view its permissions via AppleShare's permission interface.

PCNFSD: PCNFSD is provided by workstation manufacturers or by NFS clients manufacturers to provide simple user authentication services for non-UNIX clients. If no NIS domain is specified, the selected NIS domain fails to respond, or if BWNFSD is not present, PCNFSD is automatically queried. PCNFSD version 1 does not support UID to name mapping, so the owner and group of a folder will be displayed as numerical data when viewed from the AppleShare interface.

6.1.2 Domain Name Service

It is strongly suggested that you have a functioning Domain Names Server in use on one of your hosts. Although not required, a Domain Name Server maps network IP addresses to host names and visa-versa. This is convenient, because it is easier to remember a meaningful host name than it is to remember an IP address. If a Domain Name Server is unavailable, use a `hosts` file as described in Chapter 4, "About MacTCP."

6.1.3 File locking

File and byte-range locking together provide the basis for Macintosh NFS clients to share data files and applications which are resident on an NFS volume. Without file locking capabilities, volumes which are to be accessed by multiple Macintosh clients simultaneously should be considered read only. **NFS/Share** supports two methods for file and byte range locking.

LOCKD: LOCKD is provided by SUN Microsystems, Inc. and many other workstation manufacturers for use in network environments to provide file and byte-range locking capabilities. Only versions 3 and above are supported by **NFS/Share**. If you have an older version, you will need to obtain a newer version to utilize its features with **NFS/Share**.

BWNFSD: BWNFSD provides file locking and byte-range locking capabilities for NFS clients. It is strongly suggested that you install BWNFSD to provide locking capabilities even if you are using another protocol.

Programs that make use of file and/or byte range locking will work over NFS/Share even if file locking services are not present. This is because the Macintosh File Manager does not have any error code to indicate the lack of file locking services and will therefore not return an error condition. However, this should not produce any negative effects for your operations unless you are using a program that depends on the calls being truly sucessful.

6.2 Technical Information

This section describes some of the procedures used by **NFS/Share** and by some NFS servers. The purpose of this section is to aid in debugging **NFS/Share** configurations.

6.2.1 Server display

When **NFS/Share** is selected in the **Chooser**, it attempts to find all of the NFS servers that are on its local network. This is achieved by sending a broadcast call to the portmapper for MOUNTD. If any machines respond, their IP numbers are converted to names (if a DNS is available) and they are displayed in the **Chooser** window along with hosts which have been added manually.

If no hosts are found during this search, **NFS/Share** does not see any NFS servers on the network. This occurs commonly with AppleTalk to Ethernet gateways, because the broadcast packets which are sent by the Macintosh are not received by the host because the gateway does not forward them.

If you need a host which does not show up by default, just add it using the **Add Host** item from the pop-up menu.

6.2.2 Mount point display

When you select **Other** from the **Select Volume To Mount** dialog, **NFS/Share** obtains a list of available mount points from the NFS server. These mount points are inserted into the pop-up menu to the right of the **Mount Point** text box. In order to keep the amount of clutter down in this menu, **NFS/Share** attempts to weed out entries which would not be accessible from the Macintosh client (most

commonly the root and swap partitions for diskless hosts.) The algorithm deletes all mount points which only have what it believes to be fully a qualified host name that does not match its name in the restrictions. If a mount point has ANY restriction entry which does not have a '.' in it, **NFS/Share** assumes it to be a net-group reference and treats it that way. Therefore, if you intend to use any restriction entries that refer to particular hosts, use the fully qualified name for that host.

6.2.3 NIS algorithms

NFS/Share keeps track of the NIS domains which are used to authenticate a user for NFS purposes. To find the NIS server, it first checks the internal cache to see if it has already been located. If this is the case, the same IP address and port are used unless the server does not respond. When the server is not in the cache, the NFS server is queried with the `Bind` protocol and then the `Serve` protocol if that is not successful. If neither of these methods work, a `Bind` broadcast is sent to search for the domain server/binder.

In light of this, we strongly suggest that you have `Bind` and `Serve` programs running on your NFS servers if you intend to use NIS.

6.2.4 File system shutdown information (rwall)

NFS/Share supports the `rwall` protocol for notification of system downtime or other crucial information. When an `rwall` call is received, NFS/Share brings up a dialog with the text of the message.

6.2.5 Packet size backoff

When **NFS/Share** senses a loss of communication with a server, it will attempt to reduce the size of the datagram packet and reestablish communication. In many instances, this will occur immediately when using **NFS/Share** over a LocalTalk to Ethernet gateway. In common NFS sessions, you should expect Ethernet devices to utilize 8K UDP packets, and unbuffered LocalTalk to Ethernet will normally use 1K UDP packets. Packet size backoff only occurs with reads.

6.3 Special Notes

6.3.1 INIT management utilities

INIT management utilities can cause numerous problems. Some symptoms to watch for include:

- The **NFS/Share** icon not showing up during start-up time. Check to see that **NFS/Share** has not been disabled by the init manager.
- **NFS/Share** comes up with an IP error. Make certain that MacTCP comes up before **NFS/Share** in the load order.
- **NFS/Share** comes up with a DNS error. This can be caused by init management utilities that change the TYPE and/or CREATOR of INIT's and CDEV's. If this happens, **MacTCP** (which contains the Domain Name Resolver) can not be found by **NFS/Share** or any other **MacTCP** application. Some init management utilities that do this will give you the option of not installing the INIT into the init manager. If this option exists, you should use it for both **MacTCP** and **NFS/Share**.

If you have any difficulties with NFS/Share and other inits, it may help if you place NFS/Share at the end of the load list by putting a tilde ('~') as the first character of the file name.

6.3.2 Configuration information

Configuration information for NFS/Share is kept in your System Folder in a folder named Preferences. The settings files within contain settings files and folders for each host that you have accessed. In each folder for a host are files for any defined mount point that is using the Save Desktop Information option.

6.4 Server-Side Conventions

6.4.1 Macintosh files

NFS/Share can read and write Apple Single and Apple Double format files. By default it creates Apple Double files because Apple Single Files can not be shared.

6.4.2 Text file conventions

NFS/Share converts CR's to LF's when necessary and when it can confirm the text contents in the file. As NFS/Share must read the first part of the file to check for Apple Single format, is also checks for non-ASCII characters at the same time.

6.4.3 Illegal file names

NFS/Share will by default escape '/' in a Macintosh file name by using a '%' and the appropriate hex digit. Server side files which have greater than 31 characters or contain colon characters (':') are currently omitted from view by the Macintosh. All other characters in a file name are passed through manually. Some machines do not allow the '%' used by the Apple Double File format to annotate the resource fork of a file. The machines may have options to "gobble" or remap these characters and therefore fool NFS/Share into thinking that the file was written with the expected file name. The "gobble" option will remember that the file is supposed to have a '%' prefix, and will report the correct file name to NFS/Share when it requests it.

NFS/Share supports a 7-bit file naming scheme that will quote any non 7-bit ASCII character. Using 7-bit file name restrictions may tend to yield longer file names on the NFS server, as more characters are potentially converted into their 3 character quote equivalents. The 7-bit option is available for any mount point via the **Add/Edit Mount Point** dialog.

6.4.4 Symbolic Links

Symbolic links are supported for both files and directories and are resolved based on the current mount point. Any relative link (including those which go above the mount point) should work fine. Absolute links will only resolve correctly if they are below the mount point. For example, to link `/usr/mac/joe` to `/usr/joe` when the mount point is currently `/usr/mac`, use `../../joe` not `/usr/joe`.

6.4.5 Host Authentication

As an NFS client, your Macintosh must be registered with the NFS server as a "trusted host," as RPC packets sent by an NFS client contain its host name to ensure that requests are only returned to authorized machines. In the UNIX world, NFS clients are listed in the `/etc/hosts` file by their IP Address and internet host name. Each Macintosh should be assigned a host name that is either

registered with the Domain Name Server, or is included as an "A" record in the MacTCP hosts file, located in the System Folder.

If you plan to use server-based addressing with a LocalTalk router, such as a FastPath™, you will need to assign each possible address a host name and enter each in the hosts control file on the NFS server, and register each host name with the Domain Name Server, or enter them as "A" records in MacTCP's hosts file. For more information on the MacTCP hosts file, see section "4.8 The Hosts File" on page 51.

6.5 Macintosh Conventions

6.5.1 Desktop Manager

NFS/Share uses the Desktop Manager (introduced with AppleShare) to store desktop information. This enables it to store said information in RAM and therefore eliminate contention problems. This approach is compatible with Apple's future directives.

6.5.2 Directory ID's

Since an NFS volume does not need to be mounted at the root level, assigning directory ID's on a global basis would be impossible. Therefore, each user establishes a local cache of file directory ID's which remain consistent as long as Desktop Information is saved.

6.6 BWNFSD

BWNFSD provides an alternative to using **PCNFSD** and **LOCKD** for user authentication and file locking on your NFS server. **BWNFSD** can be installed in place of **NIS**, **LOCKD**, and **PCNFSD**, or can be installed with these programs without conflict. **BWNFSD** is not an NFS server, however, and you will still need NFS server software to successfully use **NFS/Share**. If **NIS** is in place along with **BWNFSD**, **NIS** will be queried for user authentication and **BWNFSD** will be used for its file locking features.

The **BWNFSD** source code included with **NFS/Share** can be compiled on many UNIX®based workstations. You may, however, want to consult a knowledgeable UNIX programmer for assistance in compiling and installing **BWNFSD**. The source code was designed to work with BSD (Berkeley), Sun Microsystems, AT&T

System III and System V, Silicon Graphics, and SCO (Santa Cruz Organization) variations of UNIX.

6.6.1 Compiling BWNFSD

To build **BWNFSD** for your particular UNIX machine, you should create a directory for it, then copy the four files (`bwlock.c`, `bwprint.c`, `bwnfsd.c`, and `Makefile`) from the **bwnfs** folder on the NFS/Share disk to it. Once you have done so, you can `make` the program by typing one of the following lines:

`make sun` ; Sun or compatible running Sun-OS

`make bsd` ; Generic Berkeley Unix

`make sys5` ; Generic ATT System III or System V

`make sgi` ; Silicon Graphics machine

`make sco` ; Santa Cruz Organization (SCO)

`make aix` ; IBM AIX for RS/6000

6.6.2 Launching BWNFSD

If the compiling and linking process succeeds, an executable file called `bwnfs` is created. You will want to change the permissions on this file and execute it to start the **BWNFSD** program. You may also want to move it to a convenient directory (such as `/usr/local/bin`) and add it to your system start-up files so it will be executed every time your UNIX machine is restarted.

For the purposes of **NFS/Share**, the only parameter necessary to start **BWNFSD** is the name of any exportable file system. For example, one might launch **BWNFSD** with the following command:

```
bwnfsd /tmp
```

You may use any entry you found in your exports file as an exported filesystem, as long as that file system is exportable to the machine running **BWNFSD**. This parameter is necessary only to launch **BWNFSD** and has no effect on the operations of **NFS/Share** other than actually getting **BWNFSD** to run.

BWNFSD was written by Beame & Whiteside Software Ltd. of Ontario, Canada, and is currently distributed in the Public Domain.

Chapter 7

■ TROUBLE SHOOTING

This chapter covers many common problems that an NFS/Share user may run into when starting out with NFS/Share. Each topic is covered briefly, and therefore is not intended as a guide for the casual Macintosh user. Consult with your network administrator, or system specialist for assistance if you experience one of the symptoms that are covered in this chapter.

7.0 User Authentication

The message **Invalid user name or password** either indicates that you in fact have typed in an incorrect user name or password, or you do not have a proper authentication server installed on your host.

To use NFS/Share, you must have an authentication server running on your host in order for NFS/Share to "log-in." The possible authentication servers that are supported by NFS/Share are NIS (formerly YP), BWNFSD, and PCNFSD versions 1 or 2. If you do not have one of these services available, you will not be able to authenticate to your NFS server.

7.1 NIS Authentication Problems

If you intend to use NIS as your authentication service with NFS/Share, you must tell NFS/Share what your NIS Domain is. The NIS Domain is a string that is assigned to the NIS master server and is used by all NIS clients. If you are unsure of your NIS Domain, telnet to the host running NIS and type the command `domainname`. This command will return your current NIS Domain.

To configure NFS/Share to use this NIS Domain, select **NIS Domain...** in NFS/Share's pop-up menu and type the NIS Domain (verbatim) in the dialog.

If you manually add a host with the **Add Host...** item in the pop-up menu, you must enter the NIS Domain name there if it is used. NFS/Share will not apply the default NIS Domain when authenticating to manually added hosts.

7.2 Host Authentication Problems

The message **A permission error prevented mounting** indicates that the NFS client is not a "trusted host." To resolve this problem, enter the host name and IP address of the Macintosh in the hosts control file (/etc/hosts under UNIX). It is also recommended that you enter your Macintosh as an "A" record in MacTCP's hosts file, found in your System Folder. If you do not have a hosts file in your System Folder, you should create one with any text editor (such as Teach Text), and afterwards you should reboot your Macintosh to update MacTCP's DNS cache. See section "4.8 The Hosts File" on page 51 for information on the format of the host file.

7.3 Installation Problems Under System 7

To use NFS/Share on a Macintosh under System 7, you must have MacTCP 1.1 in your Control Panels Folder, and NFS/Share must be in the top level of your System Folder and not in the Extensions Folder. The reason this is necessary is that NFS/Share must load after MacTCP in order to function, and it will load before it if it is placed in the Extensions Folder.

7.4 Delays When Booting

If NFS/Share seems to take a unreasonable amount of time booting, the problem is probably due to misconfiguration of MacTCP—namely the Domain Name Server. When NFS/Share comes up at start-up time, it initializes MacTCP, which includes a "ping" of the Domain Name Server. Because MacTCP's Domain Name lookups are synchronous, you must wait for them to complete. If MacTCP is configured with a Domain Name Server that does not exist or is not currently up, MacTCP will try several times to contact the Domain Name Server before finally returning control to NFS/Share. This can translate into start-up delays of 20-30 seconds. If you are experiencing this problem, check your Domain Name Server's status on the network, or delete the entry in MacTCP.

7.5 Transmission Problems

NFS/Share uses UDP/IP via Apple's MacTCP, and it is the responsibility of the network connection device to be compatible with Apple's product to ensure reliable communications. If you experience any sort of transmission-related problems with NFS/Share, you may want to examine a traffic dump of the IP packets sent between the Macintosh and the NFS server.

One common transmission problem is caused by Ethernet devices that can not handle packet fragments, or the high speed of the IP traffic associated with NFS. A packet dump will illustrate that NFS's 8K UDP packets are split into 7 Ethernet fragments. If the Ethernet device drops one of these fragments, the entire 8K UDP packets will have to be transmitted again after a time-out period. You should consult with your Ethernet device's manufacturer or try a different Ethernet device if you experience these problems.

7.6 Rules For Exporting Filesystems

- Any filesystem, or its proper subset can be exported from an NFS server. A proper filesystem is a directory that begins below the mount point to the parent filesystem.
- A subdirectory of an exported filesystem can not be exported unless that subdirectory resides on a different physical device. Similarly, you can not export the parent directory of any exported filesystem unless the parent resides on a different filesystem.
- You can only export local filesystems.

7.7 Symbolic Links

NFS/Share supports symbolic links, however NFS does not support symbolic links across logical filesystems. In practical terms, this means that if you have two logical filesystems, `/bob` and `/fred`, a symbolic link on `/bob` that points to a folder or file on /fred can not be resolved.

Appendix A

ERROR CODES

When booting your Macintosh, take note of the NFS/Share icon, if there is a problem, NFS/Share will display an alternate icon to indicate the error condition. Below is a list of the possible icons that you may see if there is a problem.

MacTCP Initialization Error
This icon indicates that Apple's MacTCP had a problem starting up. Check your configuration in the Control Panel to ensure that MacTCP is properly configured. You will also get this message under System 7 if you put NFS/Share in the Extensions folder, as it is loading before MacTCP.

Domain Name Server Error
This icon indicates that MacTCP's Domain Name Resolver could not be initialized. If you are using MacTCP 1.0.x under System 7, this icon may indicate that MacTCP is in the Control Panels folder. If this is the case, move MacTCP 1.0.x to the top level of the System folder, or install MacTCP 1.1.

Out of Memory Error
This icon indicates that your Macintosh does not have enough memory to run NFS/Share.

NFS/Share Disabled
This icon indicates that the Option key was held down during boot, disabling NFS/Share.

Unknown Error
Check for possible INIT conflicts and call InterCon Technical Support at 703/709-9890 Ext 230.

Internal Error/Restart Machine
This icon indicates that NFS/Share needed to make internal configuration changes and must be restarted in order for them to take effect.

File System Loading Error
This icon indicates that a portion of the NFS/Share code could not be loaded during start-up.

Driver Load Error
This icon indicates that a portion of the NFS/Share code could not be loaded during start-up.

Table Expansion Error
This icon indicates that there is not enough memory for NFS/Share to run.

Key Error
This icon indicates that NFS/Share was unable to initialize your activation key on the network.

Appendix B

CHOOSER ERROR MESSAGES

When using NFS/Share in the Chooser, there are a number of diagnostics error messages that you may encounter.

No Such Host Exists
The host you are attempting to access does not exist on the network at this time.

The Host Couldn't Be Resolved
The requested domain name could not be resolved to an IP number. Check the spelling that you entered for the host and reenter it if necessary. This error may also be caused by your domian name service going down.

NFS/Share Is Not Loaded, Please Re-Boot Before Proceeding
The INIT portion of NFS/Share has not been initialized. This generally indicates an error condition in relation to MacTCP. Check your configuration of MacTCP and under System 7, make sure that NFS/Share is in the top level of the System Folder and not in the Extensions Folder.

Invalid User Name Or Password
The user name and/or password that you have entered can not be authenticated by the host. Try entering them again or confirm your name and password with your system administrator if you continue to have problems. This error will also occur if you do not have an authentication server on your host.

The Volume Could No Be Mounted
The volume that you have selected could not be mounted. Confirm that all necessary NFS servers are properly installed and configured on your host.

A Permission Error Prevented Mounting
You do not have permission to mount this volume. This error will occur if the specified mount point is not exportable to your machine (inappropriate listing in the /etc/exports file or not in the appropriate netgroup) or if your Macintosh is not a trusted host (Mac is not in the /etc/hosts file).

Couldn't Find Mount Port For
The specified server doesn't currently have the NFS mount protocol running on it. Check the host and make sure it is running the mount server (MOUNTD).

Couldn't Make Drive For
NFS/Share could not mount the volume because a drive could not be created. This should not occur.

Couln't Make Volume For
NFS/Share could not make the volume because a volume control block could not be created. This should not occur.

Not Enough Memory To Mount
NFS/Share has not been allocated enough memory to mount another volume. To add memory to NFS/Share's heap, select Preferences from NFS/Share's pop-up menu in the Chooser, enter the number of volumes that you need to simultaneously mount and restart the machine.

Please Enter a Name and a Host
NFS/Share requires both a common name and a host name or IP number to identify the host.

Need Both the Disk Name and Mount Point
To mount a volume, you must supply NFS/Share with a mount point (on your host), and a name to identify the mounted volume on the Macintosh's desktop.

Appendix C

GETTING HELP

If you need technical support, you can get it through four different sources.

- Call at 703/709-9890 Ext:230
- FAX to 703/709-9896 (Label ATTN: Technical Support)
- Internet e-mail to `tech@intercon.com`
- AppleLink to `D1988` (Label ATTN: Technical Support)

Before contacting Technical Support, please compile the following information:

Product Serial Number _____

Macintosh model in use _____

RAM (megabytes) _____

Operating System version _____

INITs in use _____

_____

_____

Network connection & Brand (EtherNet Card, router...) _____

_____

Host type (the computer you are connecting to) _____

_____

Host IP address _____

Network mask _____

Your Macintosh's IP address _____

The above information is considered to be standard information by InterCon Technical Support, so please try to have it available. You may want to verify the host information with your Systems Administrator to ensure accuracy.

Along with the above information, please write down any error messages as you see them.

Feature requests are also welcome for any of InterCon's products. Please send them either to our e-mail or AppleLink addresses.

If you send in your Technical Support request via FAX or e-mail, it would also be helpful if you included your compete mailing address and phone number. This will give the Technical Support team the option of calling you back to discuss your observations, and also to log you for *extra prompt* shipping of a future version of the program in question, if necessary.

GLOSSARY OF TERMS

active open The operation that a client performs to establish a TCP connection with a server at a known address.

Active window The frontmost window on the desktop; the window where the next action will take place. An active window's title bar is highlighted.

address resolution Conversion of an Internet address into a corresponding physical address. This may require broadcasting on a local network. See arp.

alert A warning or report of an error in the form of an alert box, a sound from the computer's speaker, or both.

alert box A box that appears on the screen to give a warning or to report an error message during use of an application.

ANSI (*American National Standards Institute*) A group that defines U.S. standards for the information processing industry. ansi participates in defining network protocol standards.

AppleTalk A multimedia network architecture developed by Apple Computer and implemented on Macintosh and other computers and peripherals.

application layer An iso layer of a network which performs services for the user, such as file transfer or mail services.

ARP (*Address Resolution Protocol*) Used to allow a host to find the physical address of a target host on the same physical network, given the target's Internet address.

arp hack When one machine, usually a gateway, answers an arp request intended for another machine by supplying its own physical address, thus accepting responsibility for routing packets to the correct machine. Proxy arp is used to allow a site to use a single Internet network address with more than one physical network. Also known as proxy arp.

ARPA (*Advanced Research Projects Agency*) Former name of darpa, a government agency that funded arpanet and later, the darpa Internet.

ARPANET A long haul network funded by arpa and built by bbn. It served as the basis for early networking research and acted as a central backbone during the development of Internet. It consists of packet switched nodes primarily located at U.S. universities, but includes connections at other sites as well.

ASCII (*American Standard Code for Information Interchange*) A code in which the numbers from 0 to 127 stand for text characters. ascii code is used for representing text inside a computer and for transmitting text between computers or between a computer and a peripheral device. Compare ebcdic.

baseband A method of using a single carrier frequency for data transfer in an Ethernet or similar network. All stations on a baseband network must take part in all transmissions. See broadband.

baud The number of times per second a signal can change on a transmission line.

BBN (*Bolt, Beranek, and Newman, Inc.*) The company responsible for the development, operation and monitoring of the arpanet and the later Internet Core Gateway System. A significant contributor to network and Internet development.

big-endian A binary data storage/transmission format in which the most significant byte (or bit) comes first. The darpa Internet's standard is big-endian.

BISYNC (*BInary SYNChronous Communication*) An early, low level protocol used to transmit data across a synchronous communication link. bisync uses special characters to mark the beginning and the end of data frames.

bit A contraction of binary digit. The smallest unit of information that a computer can hold. The value of a bit (1 or 0) represents a simple two-way choice, such as yes or no, on or off, positive or negative, something or nothing.

BITNET (*Because It's There NETwork*) A low speed, low cost network based at the City University of New York, connecting more than 200 universities and the European earn. It consists mostly of ibm mainframe computers connected by 9600 baud leased lines.

bps (*Bits Per Second*) A measure of the rate of data transmission.

bridge A routing device used to expand networks by transferring packets which are destined for non-local hosts to other networks. Bridges differ from repeaters because they "learn" about attached networks and forward packets accordingly. Same as smart repeater.

broadband A system in which many transmission signals are sent over a single cable after being multiplexed. This allows many simultaneous transmissions to occur including television and radio broadcasts over a single network.

broadcast A message delivery system which delivers a copy of a given packet to all hosts attached to the network. Ethernet is an example of a broadcast system.

BSC (*Binary Synchronous Communication*) An early, low level protocol used to transmit data across a synchronous communication link. bsc uses special characters to mark the beginning and the end of data packets. Same as bisync.

buffer A "holding area" of the computer's memory where information can be stored by one program or device and then read at a different rate by another; for example, a print buffer.

button A pushbutton-like image in dialog boxes where you click to designate, confirm, or cancel an action. See also mouse button.

byte A unit of information consisting of a fixed number of bits. On most systems, one byte consists of a series of eight bits, and can represent any value between 0 and 255.

CCITT (*Comite Consultaif Internationale de Telegraphie et Telephonie*) An international organization responsible for setting international communication standards. It defined the standards for the x.25 network protocols.

character Any symbol that has a widely understood meaning and thus can convey information. Some characters (such as letters, numbers, and punctuation) can be displayed on the monitor screen and printed on a printer. Compare control character.

character set The entire set of characters that can be either shown on a monitor or used to code computer instructions. In a printer, the entire set of characters that the printer is capable of printing.

check box A small box or circle associated with an option in a dialog box. When you click the check box, you may change the option or affect related options.

checksum A small integer value computed from data being transmitted and used to determine whether the data contains errors. The value is computed by treating a series of octets in the data as integers and computing the sum. Checksums are computed at the generation of a datagram and then stored in the header. When a host receives the datagram it recomputes the checksum and compares it to the one stored. If they do not match, the data has changed in transmission and therefore is corrupt.

choose To pick a command by dragging through a menu. You often choose a command after you've selected something for the program to act on.

client A program or machine that requests services from a network or server.

client-server The methodology of interaction between hosts in a distributed system where one host sends a request to another host and waits for a response. The client is the originator of the request, the server is the responder.

click To position the pointer on something, and then to press and quickly release the mouse button.

Clipboard The holding place for what you last cut or copied; a buffer area in memory. Information on the Clipboard can be inserted (pasted) into documents.

close box The small white box on the left side of the title bar of an active window. Clicking it closes the window.

collision detection A method of detecting when two network stations simultaneously attempt transmission, thus damaging both. Upon detecting a collision, a sender will stop transmitting and wait for the activity to subside before trying again.

Command key A key that, when held down while another key is pressed, causes a command to take effect. When held down in combination with dragging the mouse, the Command key lets you drag a window to a new location without activating it. The Command key is marked with a propeller-shaped symbol. On some machines, the Command key has both the propeller symbol and the Apple symbol on it.

connection The patch between two protocols that provides reliable delivery stream service.

connectionless service The packet delivery service offered by most hardware and by the Internet Protocol. It treats each packet or datagram as a separate entity that contains both the source and destination address. Connectionless service can lose packets or deliver them out of order.

control character A nonprinting character that controls or modifies the way information is printed or displayed. On most computers, control characters have ASCII values between 0 and 31, and are typed from a keyboard by holding down the Control key while pressing some other key. TCP/Connect II can generate control characters using the Control, Command, or Option keys.

Control Panel A desk accessory that lets you change the speaker volume, the keyboard repeat speed and delay, mouse tracking, and other features. This is where most of the MacTCP configuration is done. Under System 7, the Control Panel is simply a folder, found in the System Folder, that contains Control Panel Documents that now act like startup applications.

controller A peripheral device connected to a computer to perform a specific task.

core gateway One of a set of Internet gateways which exchange routing updates periodically to ensure consistency in routing tables. The core forms a central part of Internet routing because all groups must advertise their network paths to core gateways using the Exterior Gateway Protocol egp. Core gateways are operated by inoc at bbn.

CRC (*Cyclic Redundancy Check*) A small integer value computed from data being transmitted that is used to determine whether the data contains errors. Usually , packet switching hardware will compute a crc and attach it to a packet before transmitting the packet. When receiving a packet, the hardware will recalculate the crc and compare it with the value sent, to verify that the transmission was not damaged. crcs detect more errors than checksums but they take more time to compute.

CSMA (*Carrier Sense Multiple Access*) A characteristic of network hardware that listens to transmission media and transmits when the media is idle.

CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) A method of transmission using csma/cd with Positive Acknowledgement to avoid incidents of collision.

CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) A method of transmission using csma with a device for detecting if there is more than one transmission on the media at once. Ethernet is an example of a csma/cd network.

CSNET (*Computer Science NETwork*) A network providing Internet connections and mail delivery service using dialup. csnet also provides an Internet domain name server for members who cannot run their own. csnet was originally funded by the National Science Foundation, but is now self-sufficient.

DARPA (*Defense Advanced Research Projects Agency*) Formerly arpa. A government agency that funded the arpanet and later, the darpa Internet.

DARPA Internet The collection of gateways and networks, including the arpanet, milnet, and nsfnet, that use the tcp/ip protocol suite and operate as a single, virtual network. It provides reliable full duplex stream delivery and unreliable connectionless packet delivery. It also features universal connectivity and applications level services such as electronic mail.

data communications An interchange of information between systems.

data link layer The second layer of the osi Open Systems Interconnect communications model. It puts messages together and coordinates their flow. Also used to refer to a phone link connection between two computers.

database A collection of data organized to make accessing the data efficient and easy.

datagram The basic unit of information passed across packet-switched networks. Messages are transmitted in scattered order and the correct order is reestablished by the receiving host.

DCE (*Data Communication Equipment*) A term X.25 protocol standards use to refer to packet switching equipment in a network. It is the equipment located between data terminal equipment dte and the network which establishes, maintains and terminates data connections. In common usage, dce is synonymous with a modem.

DDCMP (*Digital Data Communication Message Protocol*) Digital Equipment Corporation's link level protocol. It uses serial lines, delimits frames with special characters and includes link level checksums. nsfnet incorporates ddcmp over its backbone lines.

DDN (*Defense Data Network*) milnet and associated parts of the darpa Internet which connect to military installations. ddn provides both local and long-haul data communications and interconnectivity for the Department of Defense systems and follows the DoD protocol suite. ddn is sometimes used to refer to milnet, arpanet and the tcp/ip protocols that they use.

DECNET A network architecture developed by DEC (Digital Equipment Corporation) which defines both protocols and specific physical implementations, including Ethernet.

desk accessories "Mini-applications" that are available from the Apple menu regardless of which application you're using (for example, the Calculator, Note Pad, Alarm Clock, Control Panel, Scrapbook, Key Caps, and Chooser.

desktop On the Macintosh, the computer's working environment, the menu bar and the gray area on the screen. You can have a number of documents on the desktop at the same time.

demultiplexor A hardware device which separates a single signal from a transmission line into several signals based on time or carrier frequency. It is used on broadband systems in combination with a multiplexor to allow multiple, simultaneous signal transmissions over a single medium. In general, it allows multiple hardware devices to use a single communication link at the same time.

device Frequently used as a short form for peripheral device.

device driver A program that manages the transfer of information between the computer and a peripheral device.

dialog box A box that contains a message requesting more information from you. Sometimes the message warns you that you're asking your computer to do something it can't do or that you're about to destroy some of your information. In these cases the message is often accompanied by a beep.

digit One of the characters 0 through 9, used to express numbers in decimal form.

dimmed command A command that appears gray rather than black in the menu. You can't choose a dimmed command, usually because the command would be unable to act on anything. For example, in a MacWrite document the Cut command is dimmed unless you have selected a piece of text.

dimmed icon An icon that represents a disk that has been ejected. You can select or open dimmed disk icons, but you cannot open the documents on them.

directory A pictorial, alphabetical, or chronological list of the contents of a folder or a disk. See also folder.

disk server A network device which gives client hosts access to space on a disk drive. Clients are usually given dedicated non-shared space.

distributed file server A system by which file systems residing on disks distributed throughout a network may be made available to workstations which are also distributed throughout the network.

domain A part of the Internet naming hierarchy consisting of a series of name separated by periods. For example, in the host name bar.vax.edu, bar is in the domain vax. vax is in the domain edu.

DNS (*Domain Name Service*) Also referred to as a Domain Name Server, a DNS is an on-line distributed database responsible for mapping host names to their respective IP addresses.

dotted decimal notation The method of representing a 32-bit number with four 8-bit numbers written in base ten and separated by periods. For example, 225.128.52.1.

double-click To position the pointer where you want an action to take place, and then press and release the mouse button twice in quick succession without moving the mouse.

drag To position the pointer on something, press and hold the mouse button, move the mouse, and release the mouse button. When you release the mouse button, you either confirm a selection or move an object to a new location.

driver A term for software used to control external devices and I/O.

DTE (*Data Terminal Equipment*) A term X.25 protocol standards use to refer to computers and terminals to distinguish them from the network to which they are connected.

duplex transmission Simultaneous two-way, independent transmission of data between two computers or between a computer and a terminal.

EACK (*Extended ACKnowledgement*) See SACK.

EARN (*European Academic Research Network*) A network which connects European universities and research facilities using BITNET technology.

EBCDIC (*Extended Binary-Coded Decimal Interchange Code*) A code used by IBM that represents each letter, number, special character, and control character as an 8-bit binary number. EBCDIC has a character set of 256 8-bit characters. Compare ascii.

EGP (*Exterior Gateway Protocol*) The protocol exchanged between external gateways of autonomous systems to advertise the Internet addresses of their respective system members. Every autonomous system must use EGP to advertise network reachability to the core gateway system.

EIA (*Electronic Industry Association*) A US trade organization which sets its own standards and contributes to ansi. They are known for RS-232-C and RS-422 standards for connection of terminals to computers and computers to computers.

Enter key A key that confirms or terminates an entry or sometimes a command.

escape character An ascii character that, with many programs and devices, allows you to perform special functions when used in combination keypresses.

Escape key A key that generates the escape character. The Escape key is labeled Esc.

escape sequence A sequence of keystrokes, beginning with the Esc key. Escape sequences are used as codes to control printers and terminals (such as the decvtxxx series).

Ethernet A best-effort delivery system using CSMA/CD technology developed by Xerox Corp., Digital Equipment Corp. and Intel Corp. Ethernet is one of the most popular LANs today.

FDM (*Frequency Division Multiplexing*) A method of transmitting multiple independent signals across a single medium by assigning each a unique carrier frequency. See multiplexor and demultiplexor.

file server A process running on a computer that provides network access to files residing on that computer to remote machines. File server is often used to refer to the computer running the server program itself.

file transfer The copying of a file from one host to another over a network.

Finder An application that's always available on the desktop. You use it to manage documents and applications, and to get information to and from disks.

floppy disk A disk made of flexible plastic, as compared to a hard disk, which is made of metal. The term floppy is now usually applied only to disks with thin, flexible disk jackets, such as 5.25-inch disks. With 3.5-inch disks, the disk itself is flexible, but the jacket is made of hard plastic; thus, 3.5-inch disks aren't particularly "floppy." See 5.25-inch disk, 3.5-inch disk.

folder A holder of documents and applications on the desktop. Folders, like subdirectories, allow you to organize information in any way you want.

font In typography, a complete set of type in one size and style of character. In computer usage, a collection of letters, numbers, punctuation marks, and other typographical symbols with a consistent appearance; the size can be changed readily.

font size The size of a font of characters in points; equivalent to the distance between the ascent line of one line of text and the ascent line of the next line of single-spaced text. Examples of font size are 12 point and 18 point.

fragment One of the pieces that results from an Internet Gateway dividing an ip datagram into smaller pieces for transmission across a network which cannot handle the original datagram size.

frame A packet as it is transmitted over a serial line; a physical level transmission. Derived from character oriented protocols which added start-of-frame characters and end-of-frame characters when sending packets.

FTP (*File Transfer Protocol*) The high level Internet standard protocol for transferring files from one machine to another. ftp is usually implemented at the application level.

full duplex A connection between hosts on a network which allows concurrent transfer in both directions. This is done with two independent data streams flowing in opposite directions with no apparent connection.

Fuzzball Term applied to both a piece of gateway software and the DEC LSI-11 computer on which it runs. Used as packet switches on the nsfnet backbone network.

gateway A special purpose dedicated computer attached to 2 or more networks, using unlike protocols, and routing packets between them. A gateway translates all protocol levels.

GBPS (**Giga Bits Per Second**) A measure of the rate of data transmission referring to billions of bits per second.

GGP (*Gateway to Gateway Protocol*) The protocol used by core gateways to exchange routing information. ggp uses a shortest path routing computation. Under normal conditions, all gateways using GGP will eventually agree on routing information.

half duplex A two-wire communication circuit or protocol designed for data transmission in either direction but not both directions simultaneously. Compare full duplex.

hardware address The low level addresses used by physical networks. Each type of hardware has its own addressing scheme.

HDLC (*High-level Data Link Control*) An Internet standard link level communication protocol. It is used in X.25 networks for link access protocol. It is increasingly used by psn interfaces to transfer frames between a host and psn.

hertz A unit of frequency equal to one cycle per second.

hierarchical routing Routing that is based on hierarchal addressing by dividing the routing procedure into steps based on portions of the address. A gateway will use only the network portion of the address unless it can deliver the packet, then it also uses the host portion. Subnetting is a method of adding additional levels of hierarchal routing.

host A computer that participates in a data communication network. Host computers may be a mainframes, minicomputers, or microcomputers.

Hz (*Hertz*) A unit of frequency equal to one cycle per second.

ICMP (*Internet Control Message Protocol*) The part of the Internet Protocol that handles error and control messages. It is used by gateways and hosts to report problems with datagrams to their source. icmp includes an echo request/reply to test the reachability and status of a destination.

icon An image that graphically represents an object, a concept, or a message. For example, an unopened MacWrite document looks like a sheet of paper with lines like writing on it; an unopened MacPaint document looks like a sheet of paper with a paint brush painting a line.

idling signal A signal used to communicate that no data is being transmitted but a connection is still established. Without idling signals, a pause in transmission could be determined to be a lost connection and hang up.

IEEE (*Institute of Electrical and Electronic Engineers*) An organization which makes and publishes standards used in LANs.

IGP (*Interior Gateway Protocol*) A term applied to any protocol used to communicate routing information and reachability within an autonomous system.

IMP (*Interfact Message Processor*) Former name for Packet Switched Nodes, the packet switches used in arpanet. See psn.

interactive Operating by means of a dialog between the computer system and a human user.

interactive protocol A protocol that lets you communicate interactively with a host computer. In this kind of protocol, part or all of the contents of the screen memory is sent to the host when you press the Return key. You do not have to communicate with the host by sending it disk files. telnet is an interactive protocol.

Internet See DARPA Internet.

internet A collection of interconnected packet switched networks which function as one large virtual network by adhering to common protocols.

Internet address The 32 bit address, consisting of an Internet address and a local address, assigned to a host that wants to participate with the darpa Internet using tcp/ip.

Internet Layer An iso network protocol layer providing host-to-host delivery over an internet. This layer encapsulates messages in ip datagrams and determines delivery pathway information. It is also responsible for handling these datagrams when they are received.

Internet Protocol The darpa Internet Standard Protocol which defines Internet Datagram as the unit of information passed across the Internet and provides the basis for connectionless, best-effort delivery service.

interoperability The ability of many types of hardware and software on many different machines from many different vendors to communicate meaningfully.

IP (*Internet Protocol*) See Internet Protocol.

IP datagram The basic unit of information passed across the internet containing source and destination address along with data.

ISDN (*Integrates Services Digital Network*) A proposed digital network providing voice and digital network services through a single medium. ccitt controls the protocol and technical standards for isdn.

ISO (*International Standards Organization*) An international organization which specifies international standards for many things, including networking protocols.

ISO layer A model containing 7 conceptual layers, each providing a set of services which are used in network operations.

KBPS (*Kilo Bits Per Second*) A measure of the rate of data transmission referring to thousands of bits per second.

kilobyte (*K*) A unit of measurement consisting of 1024 bytes. In this usage, kilo (from the Greek, meaning a thousand) stands for 1024. Thus, 64K memory equals 65,536 bytes. See also megabyte.

LAN (*Local Area Network*) Any physical network technology operating at high speed over a short distance. Operational speed ranges from tens of mbps to several gbps.

little-endian A binary data storage/transmission format in which the least significant byte (bit) comes first. See big-endian.

mail bridge A mail gateway which screens mail passing from one network to another for security and administrative purposes.

mail exploder A program which accepts a piece of mail and a list of addresses, then sends a copy of the message to each listed address.

mail gateway A machine which connects 2 or more mail systems and transfers mail among them. They are usually used between dissimilar systems on different networks, in which case it will reformat messages according to the destinations mailing system rules before forwarding the message.

Mail Server The software and machine which provides message transfer services on a network.

MAN (*Metropolitan Area Network*) Any physical network technology operating at high speed over distances sufficient to cover a metropolitan area. Operational speed ranges from hundreds of mbps to several gbps.

martians A term used for packets which unexpectedly turn up on the wrong network, usually because of incorrect routing.

MBPS (*Mega Bits Per Second*) A measure to the rate of data transmission referring to millions of bits per second.

MediumA point to point electronic communication pathway.

megabyte (*Mb*) A unit of measurement equal to 1024 kilobytes, or 1,048,576 bytes. See kilobyte.

menu A list of choices presented by a program, from which you can select an action. In Macintosh, menus appear when you point to and press menu titles in the menu bar. Dragging through the menu and releasing the mouse button while a command is highlighted chooses that command.

menu bar The horizontal strip at the top of the screen that contains menu titles.

menu title A word, phrase, or icon in the menu bar that designates one menu. Pressing on the menu title causes the title to be highlighted and its menu to appear below it.

microsecond One millionth of a second.

mid-level net One of the many networks funded by the nsf which operated autonomously but was connected to the nsfnet Backbone.

MILNET (*MILitary NETwork*) A network which was separated from arpanet in 1984 to provide reliable service to the military while arpanet was used for continued research.

millisecond (*ms*) One thousandth of a second.

modem (*MOdulator/DEModulator*) A device that converts serial digital data from a transmitting terminal to a signal suitable for transmission over telephone lines. The modem will also convert the telephone signal (analog) into a serial digital signal for use for another computer or terminal.

modem port A socket on the back of the computer marked by a telephone icon.

mouse A small device you move around on a flat surface next to your computer. The mouse controls a pointer on the screen whose movements correspond to those of the mouse. You use the pointer to select operations, to move data, and to draw with in graphics programs.

mouse button The button on the top of the mouse. In general, pressing the mouse button initiates some action on whatever is under the pointer, and releasing the button confirms the action.

multi-tasking A term used to refer to a computer which can execute more than one program simultaneously.

multi-user A term used to refer to a computer which can provide service to more than one user simultaneously.

multiplexor A hardware device which combines multiple signals from a transmission line based on time or carrier frequency. It is used on broadband systems in combination with a demultiplexor to allow multiple, simultaneous signal transmissions over a single medium. In general, it allows multiple hardware devices to use a single communication link at the same time.

mux See *multiplexor.*

NAK (*Negative AcKnowledgement*) A message sent from a receiver to a sender which indicates that the transmitted data contained errors from the transmission. Upon receiving a nak, the sender will usually retransmit the data.

name resolution The process of converting a host name into a corresponding network address.

network A system of computers and peripherals connected by some media and capable of communication.

network layer The network layer is responsible for accepting ip datagrams and transmitting them over a specific network.

NFS (*Network File System*) A SUN microsystems protocol which uses the Internet Protocol to allow sets of computers to access each others' files as if they were locally stored.

NIS (*Network Information Service*) Designed by SUN Microsystems, NIS (Formerly know as Yellow Pages or YP) provides centralized user authentication and information services.

node A point on a network where one or more communication devices are attached to the network, and where information can be sent, received, or forwarded.

NSF (*National Science Foundation*) A government agency which funded a cross country backbone network (see *nsfnet*) and many regional networks designed to internet scientific communities with available supercomputing facilities.

NSFNET (*National Science Foundation NETwork*) A term used to describe local supercomputing networks, mid-level networks, and their cross country backbone network, all of which were funded by the nsf. this network is used to increase access to supercomputing facilities throughout the academic community.

null An undefined value. Null is different from zero; zero is a value just like other numbers, whereas null means no value at all (of the expected type).

numeric keypad A calculator-style keypad, either built-in or peripheral, which you can use to type numbers. The layout of numbers on the keypad makes it easier and faster to use than the regular keyboard. Some application programs designate the keys of a numeric keypad as special function keys.

OSI (*Open Systems Interconnect*) A reference to iso protocols used for the interconnection of cooperating computer systems. See rsn.

operating system A program that organizes the actions of the parts of the computer and its peripheral devices.

Option key A modifier key that gives a different meaning or action to another key you type or mouse actions you perform. You use it to type foreign characters or special symbols contained in the optional character set.

packet A group of bits including address, data, and control elements that are transmitted over a packet switched network.

packet buffer A memory space set aside for storing a packet that is either waiting to be transmitted, or has been received. It may be located in either the network interface controller or the computer attached to the controller.

PAD (*Packet Assembler/Disassembler*) A term used for an interface device which connects non-X.25 devices to an X.25 network. It prepares output from a PC or a conventional terminal and prepares it for packet switched transmission, and conversely extracts characters from the network transmission and displays them on the terminal or PC.

peripheral device A piece of hardware (such as a video monitor, disk drive, printer, or modem) used in conjunction with a computer and under the computer's control. Peripheral devices are often (but not necessarily) physically separate from the computer and connected to it by wires, cables, or some other form of interface.

physical layer The term used to apply to the physical and machine characteristics of a network such as characteristics of voltage, current and wiring.

PING (*Packet Internet Grouper*). A program used in networks to test the reachability of a host by sending an icmp Echo request and waiting for a reply. It reports success or failure and statistics about the ``pinged'' host.

pixel Short for picture element. A point on the graphics screen; the visual representation of a bit on the screen (white if the bit is 0, black if it's 1). Also a location in video memory that maps to a point on the graphics screen when the viewing window includes that location. See also bit.

POP (*Post Office Protocol*). A protocol used to retrieve mail from a central mail repository. TCP/Connect II uses pop for mail reception.

port See *Protocol Port.*

positive acknowledgement See *acknowledgement.*

presentation layer The network layer which consists of many functions needed to make application programs work, such as operating system routines necessary for using a network.

print spooler A program which manages access to printers on a network. Users communicate with the spooler rather than directly to the printer.

promiscuous ARP When one machine, usually a gateway, answers an ARP request intended for another by supplying its own physical address, thus accepting responsibility for routing packets to the correct machine. Proxy ARP is used to allow a site to use a single Internet address for more than one physical network. Same as proxy ARP.

proportional font Any font in which different characters have different widths; thus, the space taken up by words having the same number of letters varies. For example, in the typeface used here the letter M is wider than the letter I, so that MMMMM produces a wider string than IIIII.

protocol A set of rules for communication between two or more machines.

protocol port A method used by transport protocols to tell the difference between many possible destinations within a single host. Operating systems usually allow an application program to specify what port it wants to be.

PSN (*Packet Switched Node*) The name for an arpanet packet switch. Each psn is connected to at least 2 others as well as up to 16 host computers.

queue A line of prioritized tasks waiting to be executed. High priority tasks will be executed before low priority tasks.

RARP (*Reverse Address Resolution Protocol*) The Internet Protocol used by a diskless machine to find its Internet Address at startup. The machine broadcasts its physical hardware address. A server then responds to it by sending the machine its network address.

remote job entry A service offered by many networks which allows a user to submit a batch job to a host from a remote site.

repeater A device used to duplicate electronic signals from one ethernet to another. Repeaters are also used to amplify signals and to clean up digital signals by regenerating them. Repeaters cannot regenerate analog signals because they cannot distinguish between the signal and electrical noise on the media.

Return key A key that causes the cursor or insertion point to move to the beginning of the next line. It's also used in some cases to confirm a command.

RFC (*Request for Comment*) A series of notes which contain information about the development of the darpa Internet, including proposed and accepted protocols for the Internet.

RIP (*Routing Information Protocol*) An interior gateway protocol (*igp*) used by Berkeley bsd 4.3 unix systems to exchange routing information between a small number of hosts.

RJE (*Remote Job Entry*) A service offered by many networks which allows a user to submit a batch job to a host from a remote site.

RLOGIN (*Remote LOGIN*) A service offered by Berkeley bsd 4.3 unix systems allowing a user on one machine to connect with other internetworked UNIX machines as if their terminal were directly attached.

round trip time See *rtt.*

route The path taken by data traffic within a network or through an internet.

ROUTED (*ROUTE Daemon*) A bsd 4.3 unix program which updates routing information on local area networks using rip protocols.

router A machine which makes decisions about which of several paths network traffic will flow over. For example, bridges and gateways.

RPC (*Remote Procedure Call*) A protocol that is used to support calls to remote machines. RPC is the basis for NFS and lockd.

RSN (*Real Soon Now*) A phrase coined by Jerry Pournelle, to satirize the tendency in the computer industry of discussing (or offering for sale) things that aren't actually available yet.

RS-232 An eia standard specifying electrical characteristics of low speed interconnections between terminals and computers or between 2 computers. The specifications limit speed to 20 kbps and 500 feet, though manufacturers support higher speeds and longer distances. This standard is actually RS-232-C, however, many prefer to call it RS-232.

RTT (*Round Trip Time*) The time it takes for a single packet or datagram to leave one machine, reach its destination, and return to the source machine.

scroll arrow An arrow at either end of a scroll bar. Clicking a scroll arrow moves a document or directory one line. Pressing a scroll arrow moves a document continuously.

scroll bar A rectangular bar that may be along the right or bottom of a window. Clicking or dragging in the scroll bar causes your view of the document to change.

scroll box The white box in a scroll bar. The position of the scroll box in the scroll bar indicates the position of what's in the window relative to the entire document.

SCSI (*Small Computer System Interface*) A specification of mechanical, electrical, and functional standards for connecting peripheral devices such as certain kinds of hard disks, printers, network devices, and optical disks to small computers.

SDLC (*Synchronous Data Link Control*) A predecessor of hdlc defined by IBM Corporation and used in their sna network products.

segment The unit of transfer between tcps on different machines. Each segment contains a stream of bytes being sent between the machines as well as additional fields for identifications, error checking, etc.

serial interface An interface in which information is transmitted sequentially, 1 bit at a time, over a single wire or channel.

serial port The connector for a peripheral device that uses a serial interface, commonly a modem.

server A machine or program designed to provide a service to a network.

session layer An osi data communication model layer which is responsible for log keeping, security, and administrative tasks.

size box A box on the bottom-right corner of some active windows. Dragging the size box resizes the window.

slot A narrow socket inside the computer where you can install peripheral cards. Also called an expansion slot.

smart repeater A routing device used to expand networks by transferring packets which are destined for non-local hosts to other networks. Bridges differ from repeaters because they "learn" about attached networks and forward packets accordingly. Same as bridge.

SLIP (*Serial Line Internet Protocol*) A specification for using the darpa standard Internet Protocol over a serial line for remote communication.

SMTP (*Simple Mail Transfer Protocol*) The darpa Internet standard protocol for transferring electronic mail messages from one machine to another. smtp specifies how two mail systems interact and the format of control messages they exchange to transfer mail.

SNA (*System Network Architecture*) The name applied to a class of network products offered by IBM Corporation.

SNMP (*Simple Network Management Protocol*) A network standard protocol used to monitor and control networks and network hosts. The snmp agent (or server) is run on machines which are monitored, and the snmp station (or client) is used to monitor those machines. TCP/Connect II has a built in snmp agent, so that it can be monitored and maintained by appropriate network hosts.

source route A route which is determined by the transmission source. The source establishes a sequence of machines that a datagram must visit along its trip to its destination.

SPOOL (*Simultaneous Peripheral Operations On Line*) A program or piece of hardware that controls a buffer of data going to some output device, usually a printer or tape drive. This allows users to send data to the device even when it is busy.

startup disk A disk with all the necessary program files (such as the Finder and System files contained in the System folder in Macintosh) to set the computer into operation. Sometimes called a boot disk.

subdirectory A directory within a directory; a file containing the names and locations of other files.

subnet A local area network which resides within another network.

subnet address An extension of the darpa Internet addressing scheme that allows a site to use a single internet address for many physical network. The subnet address is not looked at by the Internet portion of the routing, it is only used by local gateways and hosts to deliver the datagram to the correct physical address.

SYN (*SYNchronizing segment*) The first segment sent by the tco protocol. It is used to synchronize the two ends of a connection in preparation for opening a connection.

System file A file Macintosh computers use to start up and to provide system-wide information. The System file contains system programs.

system software The component of a computer system that supports application programs by managing system resources such as memory and I/O devices.

TCP (*Transmission Control Protocol*) The darpa Internet transport level protocol that provides reliable, full duplex stream service upon which many application protocols depend.

telnet A remote terminal connection service using darpa Internet standard protocols. It allows users at one site to interact with remote timesharing systems at another site as if the users' terminal was connected directly to the remote machine.

terminal emulator A program which runs at a workstation or terminal that makes it appear to be a specific type of data terminal to both the user and the software.

TFTP (*Trivial File Transfer Protocol*) The DARPA Internet standard protocol for file transfer with minimal overhead and capability. It depends only on the unreliable, connectionless datagram delivery service (*udp*) so that it can be used on diskless workstations that keep software in rom in order to bootstrap themselves.

title bar The horizontal bar at the top of a window that shows the name of the window's contents. You can move the window by dragging the title bar.

token A unique combination of bits which signals a workstation that it has been given permission to transmit.

topology The arrangement of connections, nodes, and pathways in a network. Examples are ring, bus, or star.

transparent The operation of a network in such a fashion that the user is unaware that the processes being carried out are remote rather than local to his machine.

transport layer The fourth layer of the iso model of data communication. The transport layer provides user to user communication, and is responsible for high level error checking and alternate routing of the packets.

UDP (*User Datagram Protocol*) The darpa Internet standard protocol that allows an application program on one machine to send a datagram to an application program on another machine. It uses Internet Protocol to deliver datagrams.

UNIX A popular operating system (and registered trademark) developed at AT&T Bell Laboratories which allows a computer to handle multiple users and programs simultaneously.

UUCP (*Unix to Unix Copy Program*) A unix application program that allows one unix timesharing system to copy files to or frame another unix timesharing system. uucp is the basis for unix electronic mail transfer, and its name is often used to revert to mail transfer in general.

virtual circuit A communication link that appears to be a dedicated point to point circuit. A virtual circuit system delivers data packets in sequential order by reorganizing and reassembling completed messages correctly at the receiving end before passing them on.

virtual disk A portion of physical disk drive appearing to be a dedicated host as a local disk resource.

VMS (*Virtual Memory System*) An operating system developed by Digital Equipment Corporation for the vms computer series.

well-known port Any set of protocol port numbers preassigned for specific uses by the transport layer protocols (i.e. tcp and udp). Clients can locate servers at well-known port assignments. File transfer servers, echo servers and time servers are some examples of servers using well-known port assignments.

window The area that displays information on a desktop; you view a document through a window. You can open or close a window, move it around on the desktop, and sometimes change its size, scroll through it, and edit its contents.

X.25 The ccitt standard protocol for transport level network service. Originally designed to connect terminals to computers, it provides a reliable stream transmission service that can support remote login.

XDR (*eXternal Data Representation*) The encoding scheme defined by SUN to permit exchange of typed data in a heterogeneous environment. Defined for use by RPC.

XMIT Transmit.

XNS (*Xerox Network Standards*) The term used to refer to the set of internet protocols developed at the Xerox Corporation. These are similar to darpa Internet standards, but use different packet formats and terminologies.

XON/XOFF (*Transmitter ON/Transmitter OFF*) A method of flow control used when a computer is attached to a slower device which cannot process information as fast as the computer sends it. A common device using xon/xoff is a printer. xon is sent as a control-Q, xoff is sent as a control-S.

zoom box A small box with a smaller box enclosed in it found on the right side of the title bar of some windows. Clicking the zoom box expands the window to its maximum size; clicking it again returns the window to its original size.

System 7 Note

When installing NFS/Share under System 7, put NFS/Share in the Top Level of the System Folder and not in the Extensions Folder. This is necessary to ensure that NFS/Share loads after MacTCP.

END USER SOFTWARE LICENSE

READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THE LICENSED PROGRAM. IF YOU DO NOT AGREE WITH THE FOLLOWING TERMS AND CONDITIONS, YOU SHOULD PROMPTLY RETURN THE DISKETTE PACKAGE UNOPENED AND YOUR MONEY WILL BE REFUNDED

InterCon Systems Corporation (InterCon) and/or its suppliers own these programs and their documentation, both of which are protected under applicable copyright and trade secret laws. Your right to use the programs and the documentation is limited to the terms and conditions described below:

1. LICENSE: YOU MAY: (a) use the enclosed programs on a single computer; (b) physically transfer the programs from one computer to another provided that the programs are used on only one computer at a time, and that you remove any copies of the programs from the computer from which the programs are being transferred; (c) make copies of the programs solely for purposes of backup. The copyright notice must be reproduced and included on a label on any backup copy.

YOU MAY NOT: (a) distribute copies of these programs or their documentation to others; (b) rent, lease or grant your rights to these programs; (c) translate, reverse engineer, decompile or disassemble, or otherwise alter the programs or their documentation without the prior written consent of InterCon; or (d) ship or transmit (directly or indirectly) any copies of the Program, or any technical data in the Program or its media, or any direct product thereof, to any country of destination prohibited by the United States Government.

2. TERM: Your license remains effective until terminated. You can terminate it at any time by destroying the Program together with all copies of the Program in any form. Your license will also automatically terminate without notice if you fail to comply with any term or condition of this License Agreement. Upon any termination you must destroy all copies of the Program in any form.

3. LIMITED WARRANTY, DISCLAIMER AND LIMITATIONS OF LIABILITY: Licensor warrants the media on which the Licensed Programs are provided to be free from defects in materials and workmanship for 30 days after delivery. Defective media may be returned for replacement without charge during the 30 day warranty period unless the media has been damaged by accident or misuse. Licensor warrants, for the 30 day warranty period that the unaltered Licensed Programs conform to the documentation and are without material defects. Due to the complex nature of computer software, Licensor does not warrant that the Licensed Programs are completely error-free, will operate without interruption, or are compatible with all equipment and software configurations. Do not use the Licensed Programs in any case where significant damage or injury to persons, property or business may happen if an error occurs. The Licensee expressly assumes all risk for such use. Repair, replacement or refund (at the option of Licensor) is the exclusive remedy if there is a defect. **LICENSOR MAKES NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, WITH RESPECT TO THE LICENSED PROGRAMS AND SPECIFICALLY DISCLAIMS THE WARRANTIES OF MERCHANTABILITY AND WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL LICENSOR BE LIABLE FOR INDIRECT OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATIONS, LOSS OF INCOME, USE OR INFORMATION, NOR SHALL THE LIABILITY OF LICENSOR EXCEED THE AMOUNT PAID FOR THE LICENSED PROGRAMS.** For personal, family or household use of the Licensed Programs, some states do not allow the exclusion or limitation of incidental or consequential damages or limitations on how long an implied warranty lasts, so the above limitation or exclusion may not apply to the Licensee. Any suit or other legal action related in any way to this agreement or to the Licensed Programs must be officially filed or officially commenced no later than one (1) year after the Licensed Programs are purchased by the Licensee. These warranties give the Licensee specific legal rights, and the Licensee may also have other rights which vary from state to state.

4. GENERAL TERMS: This License Agreement will be governed by the internal laws of the Commonwealth of Virginia. If you have any questions concerning this License Agreement, you can contact InterCon at the following address:

InterCon Systems Corporation
950 Herndon Parkway, Suite 420
Herndon, Virginia 22070

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT IT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN YOU AND INTERCON ("US") AND SUPERSEDES ANY EARLIER PROPOSAL OR PRIOR ARRANGEMENT, WHETHER ORAL OR WRITTEN, AND ANY OTHER COMMUNICATIONS BETWEEN US RELATIVE TO THE SUBJECT MATTER OF THIS AGREEMENT.

InterCon

NFS/Share

InterCon

NFS/Share

InterCon

InterCon Systems Corporation
950 Herndon Parkway ■ Herndon, Virginia 22070
703.709.9890 ■ 703.709.9896 (FAX)
comment@intercon.com (internet email)
AppleLink: D1988

Complete and return the attached registration card to become eligible for these InterCon services:

Standard Technical Support

You must be a registered user to receive standard technical support. Standard technical support is offered on an "as available" basis. Call 1 703-709-9890 ext 230, 9 a.m. to 7 p.m. E.S.T.; Fax 1 703-709-9896; or e-mail to tech @ intercon.com. Please have your registration number available on all correspondence. Standard technical support is provided with this product for 90 days. Additional support may be purchased by contacting InterCon's sales department at 1 703-709-9890 ext.231.

Diskette Replacements

Defective diskettes will be replaced at no charge within 90 days of purchase. Send disks to InterCon, 950 Herndon Parkway, Herndon, VA 22070.

Updates, Upgrades

As a registered user you may obtain an update to a new version within the 90 day standard support period at no cost. You are also eligible to receive an upgrade at a reduced price.

Update — A minor enhancement to an existing product, reflected in version changes. For example, 3.0a to 3.0b or 2.0 to 2.1.

Upgrade — A major enhancement to an existing product, reflected in version changes. For example, 2.0 to 3.0.

THIS IS YOUR PRODUCT LICENSE NUMBER

NFS/Share
0500-202636

We live each season as it passes; breathe the air, drink the drink, taste the fruit, and resign yourself to the influences of each. You will mourn when they are gone.

-Henry David Thoreau-

We at InterCon support the efforts of environmental groups, agencies and individual citizens who respect and work to save the natural resources of our planet. InterCon is a proud member of over 15 environmental groups and whole-heartedly embraces their cause: the preservation and improvement of the Earth.

All of InterCon's literature is printed on recycled paper. Our shrink wrap is of a bio-degradable plastic. For our software packaging, we have eliminated all of our plastic clamshell casing in favor of recycled cardboard. These, along with several other smaller efforts, demonstrate our allegiance to this cause.

If you discover that you have no future need for any part of this packaging, we ask you, our customer, to recycle it.

Thank you.

The employees of InterCon

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 9084 HERNDON VA.

POSTAGE WILL BE PAID BY ADDRESSEE

InterCon

950 Herndon Parkway
Herndon, Virginia 22070-9946

NFS/Share Registration Card

I have read the Product License Agreement and agree with the terms as expressed therein.

AUTHORIZED SIGNATURE _____ DATE _____

NAME _____ TITLE _____ COMPANY _____ DIVISION _____

ADDRESS _____ CITY _____ STATE _____ ZIP _____

PHONE _____ PRODUCT _____

I authorize Technical Support for two individuals:

NAME _____ NAME _____

SPECIFIER'S NAME _____ PURCHASED FROM _____ DATE _____ PRICE _____

What is your organization's primary business activity at this location? (check appropriate box)

☐ Aerospace ☐ Consumer Products ☐ Government ☐ Housing & Construction ☐ Office Equipment & Computers ☐ Telecommunications
☐ Automotive ☐ Containers/Packaging ☐ Food ☐ Manufacturing ☐ Paper & Forest Products ☐ Wholesale
☐ Banking ☐ Education ☐ Fuel ☐ Metal & Mining ☐ Retail
☐ Chemical ☐ Electrical/Electronics ☐ HealthCare ☐ Nonbank Financial ☐ Service Industries

Which of the following best describes your primary job function?

☐ Accounting/Finance ☐ Info /Microcomputer Center ☐ Purchasing ☐ Other (describe)
☐ Admin./Manag ☐ Manufacturing/Operations/Quality Control ☐ Research & Development
☐ Engineering ☐ MIS/DP ☐ Sales/Marketing

How many employees does your firm employ at this location? ☐ 10 or under ☐ 26-50 ☐ 51-100 ☐ 101-200 ☐ Over 200

How many Macs are located at your site? _____

How did you learn about this product? ☐ Computer Store Display ☐ Magazine Display ☐ User Recommendation ☐ Magazine Ad ☐ Trade Show

Publications you subscribe to or read regularly:

☐ Byte ☐ Digital News ☐ HP Professional ☐ PC Computing ☐ PC World ☐ MacWorld
☐ ComputerWorld ☐ Digital Review ☐ InfoWorld ☐ PC Magazine ☐ Systems Integration ☐ Other _____
☐ DEC Professional ☐ Gov't Computer News ☐ LAN Magazine ☐ PC Week ☐ MacWeek

Tradeshows you regularly attend:

☐ CeBIT ☐ DEXPO ☐ Networld ☐ COMDEX ☐ PC Expo ☐ MacWorld ☐ Unifourm ☐ Interop

Are you the contact to extend your support agreement? ☐ Yes ☐ No

NFS/Share
0500-202636

NOT
for
Resale

Product
Access Key

InterCon

NFS/Share

NFS/Share
0500-202636
Key:
z1yjKCM8XkB9y5cN

Do not lose this card!

NFS/Share

InterCon

NFS/Share

InterCon's NFS/Share™ provides the solution for Macintosh users wanting to take advantage of distributed file sharing within a multivendor environment.

InterCon has brought the ONC/NFS standard to your Macintosh desktop. Now Macintosh users can take full advantage of the storage and file sharing capabilities of your total NFS network providing access to VAX, SUN and UNIX computers.

Simple to use — Files from the remote systems take on the familiar format of the Mac documents you always use. There are no new operating procedures or software systems to learn. Certain text files, such as UNIX, are accessible from any Macintosh editor or word processor.

Macintosh resident — Once you have the physical link to the network and NFS/Share, you need nothing other than access to NFS servers on the network.

Access multiple remote machines easily — Just go through Apple's Chooser and you are there. A list of available servers or remote systems appear in a Pop-up window. You can access remote machines at the same time, and, just like your hard drive, they appear as icons on your desktop.

Apple Standard — NFS/Share uses Apple's defined standards (AppleSingle or AppleDouble) for representing files for foreign file systems.

Simultaneous access — Multiple users can easily access the same information at the same time without the need for different mounting points.

Security maintained — User identification is clarified through Sun Microsystems, NIS (Yellow Pages) or PCNFSD. Each user is presented with lists of access or mounting points automatically.

Requirements

- Macintosh Plus (or more recent model)
- 2 MB RAM
- Macintosh System 6.0.5
- MacTCP (included in package)
- Appropriate LocalTalk Gateway or Ethernet Board

90 Days Support — NFS/Share is provided with a 90 day period of product support which can be extended after the initial support period has expired.

InterCon Systems Corporation
950 Herndon Parkway ■ Herndon, Virginia 22070
703.709.9890 ■ 703.709.9896 (FAX)
comment@intercon.com (internet email)
AppleLink: D1988

ONC/NFS®

NFS/Share

InterCon