



SCO

SCO OpenServer[™]
Internet Services

SCO OpenServer

If this procurement is for a civilian government agency, this FAR Restricted Rights Legend applies:

RESTRICTED RIGHTS LEGEND: This computer software is submitted with restricted rights under Government Contract No. _____ (and Subcontract No. _____, if appropriate). It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (g)(3)(i) of FAR Clause 52.227-14 alt III or as otherwise expressly stated in the contract. Contractor/Manufacturer is The Santa Cruz Operation, Inc., 400 Encinal Street, Santa Cruz, CA 95060.

The copyrighted software that accompanies this publication is licensed to the End User only for use in strict accordance with the End User License Agreement, which should be read carefully before commencing use of the software.

Document Version: 5.0.4

30 May 1997

© 1983–1997 The Santa Cruz Operation, Inc. All rights reserved.

This publication is protected under copyright laws and international treaties.

© 1992–1994 AT&T Global Information Solutions Company; © 1987–1989 Computer Associates, Inc.; © 1987 Convergent Technologies, Inc.; © 1989 Digital Equipment Corporation; © 1987–1989 Hewlett-Packard Company; © 1993–1994 Platinum Technologies; © 1988 Massachusetts Institute of Technology; © 1985–1989 Metagraphics Software Corporation; © 1980–1989 Microsoft Corporation; © 1989 Open Software Foundation, Inc.; © 1993–1994 Programmed Logic Corporation; © 1994 Sun Microsystems, Inc.; © 1988 UNIX Systems Laboratories, Inc. All rights reserved.

Information in this document is subject to change without notice and does not represent a commitment on the part of The Santa Cruz Operation, Inc.

SCO, The Santa Cruz Operation, the SCO logos, VP/ix, SCO OpenServer, UnixWare, dbXtra, Panner, SCO Global Access, SCO MPX, SCO Doctor, SCO Doctor for Networks, SCO Doctor Lite, SCO Premier Motif, SCO Visual Tcl, SCO VisionFS, SCO ToolWare, SCO TermLite, SCO Vision 97, SCO CIFS Bridge, SCO WebTop, The Internet Way of Computing, and IWoC are trademarks or registered trademarks of The Santa Cruz Operation, Inc. in the USA and other countries. IXI, X.desktop, Deskworks, Wintif, IXI Panorama, Deskterm, and IXI Desktop are trademarks or registered trademarks of IXI Limited, a subsidiary of The Santa Cruz Operation, Inc. Visionware, Devkit.Vision, Esprit, Kodon, Super.Vision, Visionware Super.Vision, Term.Vision, Visionware Direction, the Visionware logo, Visionware SQL-Retriever, and XVision are registered trademarks of Visionware Limited, a subsidiary of The Santa Cruz Operation, Inc. SuperVision, TermVision, X-Visionware, SQL-Retriever, and Vision Builder are trademarks of Visionware Limited. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited. Cheyenne and ARCserve are registered trademarks of Cheyenne Software, Inc. Netscape, Netscape Navigator, Netscape Communications Server, Netscape Commerce Server, Netscape Proxy Server, Netscape FastTrack Server, Netscape Enterprise Server, Netscape SuiteSpot, Netscape Catalog Server, Netscape News Server, Netscape Mail Server, and Netscape Navigator Gold are trademarks of Netscape Communications Corporation. NFS was developed by Legent Corporation (formerly Lachman Associates, Inc.) based on LACHMAN SYSTEM V NFS. LACHMAN is a trademark of Legent Corporation. NFS is a trademark of Sun Microsystems, Inc. TCP/IP was developed by Legent Corporation (formerly Lachman Associates, Inc.) based on LACHMAN SYSTEM V STREAMS TCP, a joint development of Lachman Associates and Convergent Technologies. MPX was developed by Corollary, Inc. VP/ix is a product developed and licensed by Phoenix Technologies, Ltd/INTERACTIVE Systems Corporation. XRemote is a registered trademark of Network Computing Devices, Inc. Oracle is a registered trademark of Oracle Corporation, Redwood City, California. Java is a trademark of Sun Microsystems, Inc. All other brand and product names are or may be trademarks of, and are used to identify products or services of, their respective owners.

The Santa Cruz Operation, Inc. and SCO Skunkware are not related to, affiliated with or licensed by the famous Lockheed Martin Skunk Works®, the creator of the F-117 Stealth Fighter, SR-71, U-2, Venturestar™, Darkstar™, and other pioneering air and spacecraft.

The SCO software that accompanies this publication is commercial computer software and, together with any related documentation, is subject to the restrictions on US Government use as set forth below. If this procurement is for a DOD agency, the following DFAR Restricted Rights Legend applies:

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the US Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of Rights in Technical Data and Computer Software Clause at DFARS 252.227-7013. Contractor/Manufacturer is The Santa Cruz Operation, Inc., 400 Encinal Street, Santa Cruz, CA 95060.

About this book 1

How this book is organized	1
Related documentation	2
Typographical conventions	5
How can we improve this book?	6

Chapter 1

Introducing Internet FastStart 7

Internet FastStart features	8
The Internet	9
The World Wide Web	9
Intranets	11
Virtual domains	11
Network connections	11
Installing Internet components	12
Installing Netscape Navigator	12
Installing Netscape Navigator Gold	13
Installing the Netscape FastTrack server	13
Installing SendMail	13
Installing PPP from Morning Star	13
Installing additional SCO Internet Family products	14

Chapter 2

Configuring Internet services 15

Managing Internet services	16
Configuring network connections	17
Getting on the network	17
Configuring network cards	17
Using a modem to connect to the Internet	18
Configuring Internet services	24
Web	26
Mail	31
FTP	31
Net	32
Security	32
Directory structure before enabling virtual domains	33

Managing virtual domains	33
Enabling virtual domains	34
Configuring services	35
Viewing properties of virtual domains	37
Adding and deleting virtual domains	39
Filesystem layout for virtual domains	39
Remote administration of virtual domains	39

Chapter 3

Migrating from a previous Internet FastStart system **41**

Migrating sendmail configuration	42
Saving sendmail data from the IFS system	42
Configuring sendmail on your SCO OpenServer system	44
Migrating PPP configuration to SCO PPP from Morning Star	45
Migrating from an SCO PPP configuration	45
Migrating from an existing PPP from Morning Star configuration	45
Migrating server configuration and data	46
Saving server configuration and data: standard configuration	46
Saving server configuration and data: virtual domain configura- tion	47
Post-installation server configuration	48
Restoring server configuration files	48

Chapter 4

Features, limitations, and updates to Internet FastStart **51**

Read this before installing Internet FastStart	51
Read this after installing Internet FastStart	53
System notes and limitations	53
Configuring Domain Name Service (DNS)	55
SCO OpenServer and MMDF	56
Hardware notes	56
Software configuration	57
SCO Internet Manager notes	59
Netscape FastTrack notes	67
Netscape Navigator and Navigator Gold notes	70

Internet FastStart documentation	71
--	----

About this book

This book, *SCO OpenServer Internet Services*, contains information on configuring Internet services such as mail, web servers, dial-up networking, and network security.

You will find the information you need more quickly if you are familiar with:

- “How this book is organized” (this page)
- “Related documentation” (page 2)
- “Typographical conventions” (page 5)

Although we try to present information in the most useful way, you are the ultimate judge of how well we succeed. Please let us know how we can improve this book (page 6).

How this book is organized

This book introduces you to Internet concepts and features (page 7) and tells you how to install Internet FastStart components (page 12), then describes how to use the **Internet Manager** to:

- connect to the Internet (page 17) through a dialup connection or a LAN
- configure a web server (page 26) based on the Netscape™ FastTrack Server™
- modify mail configuration (page 31), including hiding your hostname on outgoing mail and re-directing outgoing mail to a central mail server
- enable file transfers (page 31), including anonymous **ftp**
- configure network parameters (page 32), including routing and gateway status

- restrict and grant access (page 32) by remote users to services on your system
- enable virtual domains (page 34) which allows your system to host multiple domains

It also describes limitations and updates (page 51) which apply to this release, and notes for those who are migrating from a previous release of Internet FastStart (page 41).

Related documentation

SCO OpenServer™ systems include comprehensive documentation. Depending on which SCO OpenServer system you have, books are available in online and/or printed form. Access online books by double-clicking on the Desktop **Help** icon. Additional printed versions of the books are also available. The Desktop and most SCO OpenServer programs and utilities are linked to extensive context-sensitive help, which in turn is linked to relevant sections in the online versions of the following books. See “Getting help” in the *SCO OpenServer Handbook*.

NOTE When you upgrade or supplement your SCO OpenServer software, you might also install online documentation that is more current than the printed books that came with the original system. For the most up-to-date information, check the online documentation.

Online documentation for some of the Internet FastStart components are not searchable via **scohelp**. These books are available via links from the **scohelp** Documentation Library, but are not accessible via the **scohelp** Search button.

For information about Internet Services books included with SCO OpenServer, see “Internet FastStart documentation” (page 71). The following SCO OpenServer books are available through **scohelp**:

Release Notes

Contains important late-breaking information about installation, hardware requirements, and known limitations.

SCO OpenServer Features and Limitations

The *SCO OpenServer Features and Limitations* highlight the new features added for this release.

SCO OpenServer Handbook

Provides the information needed to get your SCO OpenServer system up and running, including installation and configuration instructions, and introductions to the Desktop, online documentation, system administration, and troubleshooting.

Graphical Environment Guide

Describes how to customize and administer the Graphical Environment, including the X Window System server, the SCO® Panner™ window manager, the Desktop, and other X clients.

Graphical Environment help

Provides online context-sensitive help for Calendar, Edit, the Desktop, Help, Mail, Paint, the SCO Panner window manager, and the UNIX® command-line window.

Graphical Environment Reference

Contains the manual pages for the X server (section X), the Desktop, and X clients from SCO and MIT (section XC).

Guide to Gateways for LAN Servers

Describes how to set up SCO Gateway for NetWare and LAN Manager Client software on an SCO OpenServer system to access printers, file-systems, and other services provided by servers running Novell NetWare and by servers running LAN Manager over DOS, OS/2, or UNIX systems. This book contains the manual pages for LAN Manager Client commands (section LMC).

Mail and Messaging Guide

Describes how to configure and administer your mail system. Topics include **sendmail**, MMDF, SCO Shell Mail, **mailx**, and the Post Office Protocol (POP) server.

Networking Guide

Provides information on configuring and administering TCP/IP, NFS®, and IPX/SPX software to provide networked and distributed functionality, including system and network management, applications support, and file, name, and time services.

Networking Reference

Contains the command, file, protocol, and utility manual pages for the IPX/SPX (section PADM), NFS (sections NADM, NC, and NF), and TCP/IP (sections ADMN, ADMP, SFF, and TC) networking software.

Operating System Administrator's Reference

Contains the manual pages for system administration commands and utilities (section ADM), system file formats (section F), hardware-specific information (section HW), miscellaneous commands (section M), and SCO Visual Tcl™ commands (section TCL).

Operating System Tutorial

Provides a basic introduction to the SCO OpenServer operating system. This book can also be used as a refresher course or a quick-reference guide. Each chapter is a self-contained lesson designed to give hands-on experience using the SCO OpenServer operating system.

Operating System User's Guide

Provides an introduction to SCO OpenServer command-line utilities, the SCO Shell utilities, working with files and directories, editing files with the vi editor, transferring files to disks and tape, using DOS disks and files in the SCO OpenServer environment, managing processes, shell programming, regular expressions, **awk**, and **sed**.

Operating System User's Reference

Contains the manual pages for user-accessible operating system commands and utilities (section C).

PC-Interface Guide

Describes how to set up PC-Interface software on an SCO OpenServer system to provide print, file, and terminal emulation services to computers running PC-Interface client software under DOS or Microsoft Windows

Performance Guide

Describes performance tuning for uniprocessor, multiprocessor, and networked systems, including those with TCP/IP, NFS, and X clients. This book discusses how the various subsystems function, possible performance constraints due to hardware limitations, and optimizing system configuration for various uses. Concepts and strategies are illustrated with case studies.

SCO Merge User's Guide

Describes how to use and configure an SCO Merge system. Topics include installing Windows, installing DOS and Windows applications, using DOS with the SCO OpenServer operating system, configuring hardware and software resources, and using SCO Merge in an international environment.

System Administration Guide

Describes configuration and maintenance of the base operating system, including account, filesystem, printer, backup, security, UUCP, and virtual disk management.

The SCO OpenServer Development System includes extensive documentation of application development issues and tools.

Many other useful publications about SCO systems by independent authors are available from technical bookstores.

Typographical conventions

This publication presents commands, filenames, keystrokes, and other special elements as shown here:

Example:	Used for:
lp or lp(C)	commands, device drivers, programs, and utilities (names, icons, or windows); the letter in parentheses indicates the reference manual section in which the command, driver, program, or utility is documented
<i>/new/client.list</i>	files, directories, and desktops (names, icons, or windows)
<i>root</i>	system, network, or user names
<i>filename</i>	placeholders (replace with appropriate name or value)
<Esc>	keyboard keys
Exit program?	system output (prompts, messages)
yes or yes	user input
"Description"	field names or column headings (on screen or in database)
Cancel	button names
Edit	menu names
Copy	menu items
File ⇌ Find ⇌ Text	sequences of menus and menu items
open or open(S)	library routines, system calls, kernel functions, C keywords; the letter in parentheses indicates the reference manual section in which the file is documented
\$HOME	environment or shell variables
SIGHUP	named constants or signals
"adm3a"	data values
<i>employees</i>	database names
<i>orders</i>	database tables
buf	C program structures
b_b.errno	structure members

How can we improve this book?

What did you find particularly helpful in this book? Are there mistakes in this book? Could it be organized more usefully? Did we leave out information you need or include unnecessary material? If so, please tell us.

To help us implement your suggestions, include relevant details, such as book title, section name, page number, and system component. We would appreciate information on how to contact you in case we need additional explanation.

NOTE For answers to technical questions, please contact your software vendor or your support representative. Technical Publications is not qualified to give technical support.

To contact us, use the card at the back of the *SCO OpenServer Handbook* or write to us at:

Technical Publications
Attn: CFT
The Santa Cruz Operation, Inc.
PO Box 1900
Santa Cruz, California 95061-9969
USA

or e-mail us at:

techpubs@sco.com or ... *uunet!sco!techpubs*

Thank you.

Chapter 1

Introducing Internet FastStart

SCO OpenServer™ Release 5.0.4 Internet FastStart is an easily configured, general-purpose Internet server. Internet FastStart adds a rich set of features, described in “Internet FastStart features” (page 8), to enable:

- accessing and publishing information on the Internet (page 9)
- conducting electronic commerce on the Internet (page 9)
- sharing information through internal “intranets” (page 11)
- serving multiple virtual domains from one system (page 11)

After you install the appropriate components (page 12), you can configure and manage Internet services with the **SCO Internet Manager**, an HTML-based configuration utility that guides the system administrator through setup and maintenance. See “Managing Internet services” (page 16), “System notes and limitations” (page 53), and “SCO Internet Manager notes” (page 59).

Also available from SCO, on the SCO® Server Enhancement Products CD-ROM, are a number of useful add-on software packages that provide additional Internet or system capabilities, including:

- SCO® Internet to NetWare® Gateway, which provides Novell LANs with transparent access to the Internet
- Netscape Proxy Server™
- SCO® InterScan VirusWall®
- SCO® ARCserve®/Open from Cheyenne®
- SCO Doctor™

Internet FastStart features

SCO OpenServer Release 5.0.4 includes:

Netscape™ Navigator™ Gold 3.0

The leading premium web browser with an integral HTML editor and support for Java™, frames, and client-side SSL. The SCO OpenServer Desktop system contains Navigator 3.0, and the SCO OpenServer Enterprise and FreeUNIX systems contain Navigator Gold 3.0, which replaces Navigator 2.02 from SCO Internet FastStart 1.0.

Netscape FastTrack Server™ 2.0

The easy-to-use, high-performance new web (HTTP) server from Netscape with SSL 3.0 security, graphical server management tools, built-in reporting tools, One Button Publishing, and support for the Java and JavaScript™ programming languages. The Netscape FastTrack Server 2.0 replaces the Netscape Communications Server™ and the Netscape Commerce Server™ from SCO Internet FastStart 1.0.

SCO Internet Manager 1.2

Enhancements include **SCO Internet Manager 1.2** with improved packet filter configuration pages, support for IP address pooling for PPP connections, and control of PPP debugging log detail.

SCO SendMail 8.8.5

This version is fully 8-bit clean and incorporates improved security, support for 8-bit MIME messages (ESMTP's **8BITMIME** option), limited support for ESMTP Delivery Status Notification (DSN), improved configuration (more options in the *sendmail.cf* file), and bug fixes.

SCO PPP from Morning Star

This robust, high-performance PPP software from Morning Star Technologies provides support for 64 concurrent sessions, link-level error detection, enhanced modem support, link-level authentication of incoming calls by PAP/CHAP (Password Authentication Protocol and Challenge Handshake Authentication Protocol), callback (system disconnects incoming calls, then calls the originating system if that system is allowed access) full data compression, and dynamic IP (Internet Protocol) address negotiation.

New and revised documentation

New and updated documents are provided online in HTML format. PostScript images of some books are also available for downloading and printing (page 72).

The Internet

The Internet is the largest network in the world. Developed over 20 years ago as a US Defense Department network called ARPAnet, the Internet has grown to include other networks located around the world. The Internet was originally built primarily on UNIX systems, and has since diversified to include a variety of operating systems.

Services that run over the Internet include e-mail, file transfer between systems (FTP), remote use of systems (**telnet**), and the World Wide Web.

Organizations can use Web technologies and the Internet to make key information available to a worldwide audience of millions of people. It is an effective and inexpensive way to distribute information such as newsletters, financial reports, marketing information, and other important documents. These can be available 24 hours a day, and can easily be kept up-to-date. Because customers or clients download this information directly onto their own computers, printing, mailing, and distribution costs are reduced while service and response time are improved.

The Internet can be used as a tool to sell and market products and services. Organizations can leverage the Internet to provide valuable marketing and sales information to their traditional customers while expanding their reach into new markets. Customers can purchase product 24 hours a day at their own convenience, and the automated tasks of ordering products electronically can streamline the sales process, resulting in a higher level of customer satisfaction.

Providing your organization with access to Internet resources can enhance productivity. The Internet provides the largest library of useful information in the world. Employees can use the Internet to access a wealth of up-to-date information, including newsletters, reports, and online databases.

The World Wide Web

The World Wide Web is a global matrix (web) of interconnected documents on the Internet. Clicking on a cross-reference in one of these documents displays the referenced document, even though it might be located on a computer half-way around the world. This is possible because all systems connected to the World Wide Web use a common communication protocol, HTTP (Hypertext Transfer Protocol), to send and receive documents, and because all Web documents use the same method, HTML (Hypertext Markup Language), to define document formatting.

A collection of documents from one organization or individual on the Web is called a “Web site” (typically on a single system, although a large site can be supported by multiple systems or several sites could be located on one system). A Web site publishes these documents with software called a “Web server”, and they are viewed with a “Web browser”. Documents are typically divided into a number of short Web pages for convenient viewing. The top-level page at a site is referred to as a “home page”. Web activity is not limited to viewing pages: data can be exchanged by the server and browser and manipulated by either or passed on to other software. This makes it possible to run programs, conduct business, and manage remote computer systems over the Web.

Although the Internet has existed for some time, the introduction of the World Wide Web caused an explosive growth in its use. Prior to the Web, navigating the Internet required typing complicated paths and searching newsgroups for largely unformatted text. Moving about on the Web is a simple matter of clicking on interesting references. Searching the World Wide Web for information is also simple, and the support for graphics, sound, and motion makes the results of the search more rewarding. Encryption and other security features have made it possible to buy and sell services and products online. Increasingly, a presence on the Web is as much a part of doing business as being connected to the global telephone or e-mail networks.

Internet FastStart includes the premier Web browser, Netscape Navigator 3.0, which provides client-side image mapping, progressive JPEG and Java support, GIF animation, and support for multiple streaming of video, audio, and other data formats. It also features e-mail, news, and FTP file download capabilities.

For a Web server, Internet FastStart incorporates the powerful Netscape FastTrack Server. A specialized Web server, the Netscape Proxy Server™, is also available from the SCO Server Enhancement Products CD.

The Netscape FastTrack Server

is a high-performance Web server for publishing text or multimedia documents on the World Wide Web or on internal TCP/IP networks (“intranets”). It supports HTTP 1.0, HTML, MIME, GIF, JPEG, CGI 1.1, IP- and DNS-based access control, named group control, and NSAPI. The Netscape FastTrack Server has an intuitive, browser-based management utility. Dynamic Process Management minimizes the overhead in servicing multiple resource requests at the same time. Security features ensure protection of sensitive data, providing complete control over access to individual files, directories, or servers by user name and password, domain name, host name, IP address, and/or named groups.

The Netscape Proxy Server

features configurable caching of frequently accessed documents. It grants or limits access to specific external resources based on specified user and network information, and logs all HTTP, FTP, and Gopher transactions (including referrer, user agent, and completion status). Netscape Proxy Server can also enhance network security by providing a control point for all Internet traffic. All Netscape FastTrack Server capabilities are incorporated into the Netscape Proxy Server.

For more about the Netscape servers, see their manuals online.

Intranets

An “intranet” is an internal network that uses World Wide Web technologies for sharing work and information between departments and/or remote locations. Intranets can be used to facilitate teamwork and project collaboration through e-mail and other network-based applications. Company announcements, health insurance information, corporate policies, procedure manuals and the like can be made readily available from a central, easily updated Web site.

Virtual domains

Internet FastStart supports virtual domains (“multihoming”), which can be easily set up and managed with the **SCO Internet Manager** (page 33). Using virtual domains, one Internet FastStart server can act as the home for multiple individual or company Web sites or Internet domains (domains are named nodes or subsections of the Internet. SCO’s domain name, for example, is *sco.com*). Each virtual domain can receive e-mail and maintain its own list of e-mail users, make files available with anonymous FTP, and publish its own set of Web pages.

Network connections

In addition to the strong networking capabilities of SCO OpenServer Release 5 (including TCP/IP, IPX/SPX, NFS, DNS, SMTP, and POP), Internet FastStart offers enhanced PPP support with SCO PPP from Morning Star Technologies, which is included on your SCO OpenServer Release 5.0.4 CD-ROM.

PPP (Point-to-Point Protocol) allows two systems to communicate with each another through modems or a serial connection. PPP is typically used to connect remote sites together into a TCP/IP network. SCO PPP from Morning Star Technologies is robust, high-performance PPP software with support for 256 concurrent sessions, link-level error detection, enhanced modem support, link-level authentication of incoming calls by PAP/CHAP (Password Authentication Protocol and Challenge Handshake Authentication Protocol), callback

(system disconnects incoming calls, then calls the originating system if that system is allowed access), full data compression, and dynamic IP (Internet Protocol) address negotiation.

SCO PPP from Morning Star Technologies must be installed as a layered product after installing SCO OpenServer. For more information, see the *SCO PPP from Morning Star User's Guide* and "Migrating PPP configuration to SCO PPP from Morning Star" (page 45).

PPP and other network connections can be configured with the **SCO Internet Manager** (page 18) and other SCO utilities.

For more about general networking issues, see the *Networking Guide*.

Installing Internet components

Before installing Internet FastStart components, see "Read this before installing Internet FastStart" (page 51) and "Read this after installing Internet FastStart" (page 53).

Your SCO OpenServer system media contains the following Internet FastStart components:

Desktop system	Netscape Navigator, Internet Manager, enhanced PPP from Morning Star Technologies, and SendMail.
Enterprise system	Netscape Navigator Gold, Netscape FastTrack server, Internet Manager, enhanced PPP from Morning Star Technologies, and SendMail.
FreeUNIX system	Netscape Navigator Gold, Netscape FastTrack server, Internet Manager, enhanced PPP from Morning Star Technologies, and SendMail.

Installing Netscape Navigator

If you selected a full installation when you installed your SCO OpenServer Desktop system, Netscape Navigator was installed automatically.

If you did not select a full installation, you need to install the SCO Netscape Navigator (NAVIGATOR) component. See Chapter 4, "Installing and managing software components" in the *SCO OpenServer Handbook*. See "Netscape Navigator and Navigator Gold notes" (page 70) for notes about configuring and using Netscape Navigator.

Installing Netscape Navigator Gold

If you selected a full installation when you installed your SCO OpenServer, Enterprise, or FreeUNIX system, Netscape Navigator Gold was installed automatically.

If you did not select a full installation, you need to install the SCO Netscape Navigator Gold (NAVIGATORAu) component. See Chapter 4, “Installing and managing software components” in the *SCO OpenServer Handbook* for information on installing components. See “Netscape Navigator and Navigator Gold notes” (page 70) for notes about configuring and using Netscape Navigator Gold.

Installing the Netscape FastTrack server

If you selected a full installation when you installed your SCO OpenServer system, the Netscape FastTrack server was installed automatically.

If you did not select a full installation, you need to install the SCO FastTrack Server (FASTTRACK) component. See Chapter 4, “Installing and managing software components” in the *SCO OpenServer Handbook* for information on installing components. See “Netscape FastTrack notes” (page 67) for notes about configuring and using the Netscape FastTrack server.

Installing SendMail

When you installed your SCO OpenServer system, you were given a choice of Mail Transport Agents: SendMail or MMDF. If you chose SendMail, you can use the **Internet Manager** to configure your mail system and can make use of advanced features such as virtual domain naming. If you chose MMDF, you cannot use the **Internet Manager** to configure mail.

You can switch mail systems by removing the SCO MMDF (MMDF) package and adding the SCO **SendMail** (SendMail) package. For more information, see Chapter 4, “Installing and managing software components” in the *SCO OpenServer Handbook*.

Once you install SendMail, use the **Internet Manager** to configure it (page 31).

Installing PPP from Morning Star

By default, PPP from Morning Star is not installed when you install your SCO OpenServer system. Using PPP from Morning Star allows you to use the **Internet Manager** to configure your dial-up connections.

To install and use PPP from Morning Star, you need to remove the SCO PPP (tcp:PPP) package and add the SCO PPP from Morning Star (mstppp) package, then configure connections with the **Internet Manager**. For more information, see Chapter 4, "Installing and managing software components" in the *SCO OpenServer Handbook* and "Getting on the network" (page 17).

Installing additional SCO Internet Family products

The SCO Server Enhancement Products CD-ROM, available from SCO, contains these products, which can be licensed for use with SCO OpenServer and Internet FastStart:

- Netscape Proxy Server
- SCO Advanced File and Print Server
- SCO ARCserve/Open from Cheyenne
- SCO Doctor for Networks
- SCO Doctor 5-Client Connection
- SCO Internet to NetWare Gateway
- SCO InterScan VirusWall
- SCO Strong Encryption Supplement
(available in the United States and Canada only; obtain a license from your authorized reseller)

For information on ordering the SCO Server Enhancement Products CD, contact your authorized reseller.

Chapter 2

Configuring Internet services

Use the **SCO Internet Manager** (page 16) and other utilities to:

- configure network connections (page 17)
- configure Internet services (page 24)
- manage virtual domains (page 33)

NOTE When you install SCO OpenServer, you are given a choice of choosing MMDF or SendMail as your Mail Transport Agent (MTA). To use the **Internet Manager** to configure electronic mail, you must choose SendMail. If you choose SendMail, you will have full access to multihoming and other advanced mail features not available if you choose MMDF.

If you installed MMDF, but now want to use SendMail as your MTA, use the **Software Manager** and the instructions in “Removing software” and “Installing software” in the *SCO OpenServer Handbook* to remove the MMDF package, then add the **sendmail** package.

See also:

- Chapter 9, “Administering SCO systems” in the *SCO OpenServer Handbook*

Managing Internet services

Use the **SCO Internet Manager** to configure and manage World Wide Web access, e-mail forwarding, remote file transfer access, routing to/from the Internet, point-to-point connections with other systems, and network security (including data packet filtering, and local or remote administrative access). Also use the **SCO Internet Manager** to create and manage virtual domains (or "multihomes").

NOTE You must be running an X session to configure Internet services.

To start the Internet Manager on the local system:

1. As *root*, do one of the following:
 - From the Desktop, double-click on the **Internet Configuration** icon.
 - From a UNIX window (**SCOterm** or **xterm**), enter:
`scoadmin internet`
2. In the "User ID" field, enter *admin*. In the "Password" field, enter the **Internet Manager** password.

This is set to the first eight characters of the *root* password by default. To change the Internet *admin* password, click on the **Security** button on the Internet Services page, then choose **Set Internet Manager Password** (or log in as *root* and enter `/etc/internetpw`).

NOTE If you defer setting the *root* password during the initial installation procedure, the *admin* user's password is set to (Enter).

To start the Internet Manager from a remote system:

NOTE Only systems which have been specifically permitted remote access can use the **Internet Manager** on the local system.

To permit remote access by a system, select **SYSTEM-WIDE** on the Internet Services page of the **SCO Internet Manager**, click on the **Security** button, then click on the **Control Access From Remote Sites** button. (Or add the remote system's IP address to the `/usr/internet/admin/access/site` file on the local system.)

1. With a Web browser that supports tables (such as Netscape Navigator), open this URL:

`http://system-name:615/mana/mana/menu.mana`

For *system-name*, substitute the fully-qualified name of the system that you want to configure.

2. In the “User ID” field, enter *admin*. In the “Password” field, enter the **Internet Manager** password.

Configuring network connections

Configuring network connections involves:

- “Getting on the network” (this page)
- “Configuring network cards ” (this page)
- “Using a modem to connect to the Internet” (page 18)

Getting on the network

When you start the **Internet Manager** for the first time, it prompts for which interface connects your system to the Internet. The **Internet Manager** lists all network cards that you have configured and offers you the option of creating a PPP connection. If you are planning to use a network card to connect to the Internet or your LAN, select that card from the list. If you are using a modem to connect your system to the Internet, choose to add a PPP connection (page 19).

In addition to selecting an interface, you are given the option of whether the system should test your connection. It will do this by attempting to contact a known system on the Internet. If you do not want the system to perform this test (if, for example, you are configuring your system for use on a LAN that has no Internet connection), deselect the **Test Internet connection** checkbox.

Once you click **OK**, the system tests your connection (unless you’ve chosen not to have it do so) and configures several system services, such as the Domain Name System (DNS). If the test was successful, your system is on the Internet, and you are ready to configure specific system services, as described in “Configuring Internet services” (page 24). If the test is unsuccessful, you can chose to **Reconfigure** the settings. If the system timed out before the connection/dial completed, click on **Try Again**.

Configuring network cards

The **Internet Manager** does not support the installation or configuration of network cards directly. If you install a new network card or need to reconfigure it (for example, to change its IP address), you need to run the **Network Configuration Manager**. For more information about installing and configuring network cards, see Chapter 1, “Configuring network connections” in *Configuring Network Connections* and **netconfig**(ADM).

Using a modem to connect to the Internet

If you plan to use a modem to connect to the Internet, you must configure an outbound PPP connection. To do this, you should have a PPP account with an Internet Service Provider (ISP). Your ISP will provide you with a telephone number to dial as well as other important information necessary to configure your link.

NOTE The Internet Manager is designed to configure SCO PPP from Morning Star Technologies, which you must install separately after installing SCO OpenServer. See “Installing PPP from Morning Star” (page 13).

At a minimum, you need the following information to create a PPP connection:

- modem type
- phone number
- login account name
- password
- the IP address assigned to your system
- the IP address of the remote system
- In addition, you must verify that the netmask of 255.255.255.0 is correct.

If your ISP does not provide you with these IP addresses, then the addresses are assigned to you dynamically each time you dial in, and you do not need to know them. However, you must enter the IP addresses when you create the link (the addresses you enter will be replaced with the correct ones when you dial in). If your ISP does not provide you with initial addresses to use, use 127.0.0.2 for the local site and 127.0.0.3 for the remote site.

You might also need to know the following additional security information:

- PAP/CHAP name
- PAP/CHAP secret
- chat script login sequences

Again, your ISP will give you this information if it is required to create the connection. In many cases, it is not required.

See also:

- “Creating an outbound PPP connection” (page 19)

- “Configuring an inbound PPP Connection” (page 21)
- “Troubleshooting your PPP connection” (page 23)

Creating an outbound PPP connection

Once you have the information described in “Using a modem to connect to the Internet” (page 18), you are ready to create a PPP connection. The information required is the same whether you are connecting to an ISP or if you simply want to dial in to another system.

The **Internet Manager** page for configuring an outbound PPP connection contains three sections.

Create new PPP dial-out connection:

Local PPP IP address:		☐ Dynamic
Remote PPP IP address:		☐ Dynamic
Remote PPP account login name:		
Remote PPP account password:		
Remote phone number:		

Creating a new PPP dial-out connection

If your ISP or network administrator has given you IP addresses for your system and/or the remote system, enter them here; otherwise, choose default addresses and select **Dynamic** to indicate that IP addresses are to be reassigned dynamically. You must also enter your login name and password. If you are using a modem to make the connection, enter the remote phone number.

Modem and connection type:

Connect via: ☒ Direct serial line ☐ Modem

Connection times out in: seconds

Dial at boot time and maintain link? ☒ Yes ☐ No

Serial port speed (baud rate):

Serial device:

Modem type:

AT&T 2296
Best Data 28.8
Codex 3260
Dataflex HyperGEM V.34
Digicom Systems 9624E+

Modem and connection type

If you are using a modem to make the connection, select the modem type from the list provided. If your modem does not appear in the list, try one of the generic settings.

You also need to specify whether the line should stay up all the time, or if it should only come up automatically when packets need to be routed across the link. Do this by setting how many seconds the connection needs to be idle before it times out and hangs up. If you are using a part-time connection, the correct time out value depends on the cost of your phone connection; for many situations, a value of 120 is reasonable. Entering a value of zero (the default) causes the line to stay up continuously. You can also instruct the system to dial the connection every time the system boots.

Optional security information:

Chat scripts are modified on the Advanced PPP connections page.

PAP/CHAP name:

PAP/CHAP secret:

Address parsing information:

Netmask for PPP connection:

Optional information

You might also want to specify certain optional parameters. If your ISP or network administrator gives you PAP/CHAP authentication information, enter it here. Finally, you must verify the netmask, which is necessary for the system to properly route packets. A default value of 255.255.255.0 is appropriate for a class C network and is commonly used; you should change it only if your ISP or network administrator instructs you to do so.

Configuring an inbound PPP Connection

Configuring an inbound PPP connection is similar to creating an outbound connection. You must set the account name and password for each PPP connection, typically one per user. The user account is created for you, using system account defaults (except for the shell, which is specifically for PPP users. You also must specify the IP address used on your system's side of the connection. You can specify that a fixed IP address be used by the remote system each time it connects. If you select the **Dynamic** checkbox, the system uses the IP address given to it by the remote side of the connection during link negotiation. You must specify a default IP address even if you select the **Dynamic** checkbox.

Create new PPP dial-in connection:

Local PPP account login name:

Local PPP account password:

Local PPP IP address:

Remote PPP IP address: ☐ Dynamic

Seconds until connection times out:

Optional security information:

PAP/CHAP name:

PAP/CHAP secret:

Address parsing information:

Netmask for PPP connection:

Creating an inbound PPP connection

Enter the number of seconds you want to allow the link to be idle before the system drops the connection. If you enter zero, the system will not drop the connection because it is idle; if you want a part-time connection, enter the timeout period (120 seconds is a reasonable value).

If you require that the remote system authenticate itself using PAP/CHAP, enter the PAP/CHAP name and secret. Finally, enter the appropriate netmask to use for this link; a value of 255.255.255.0 is appropriate for class C networks and is commonly used. If your network uses a different netmask, enter it here.

Once you click on **OK**, the PPP link is ready to use, and a remote system should be able to connect almost immediately.

Troubleshooting your PPP connection

Even though the configuration of a PPP connection appears to be simple, problems often arise. These are most often the result of making the wrong modem selection for the modem you are using, or when the two sides of the connection do not agree on all the necessary parameters.

Determine that the configurations for both sides of the connection are consistent. For example, they must agree on the account name and password, and the netmask for the connection must agree. Check your IP addresses to make sure they are consistent. If this is an incoming connection, be sure that you do not make the IP address for a system as specified on both sides of the connection dynamic, as neither system will tell the other which IP address to use.

It is often useful to watch what the PPP daemon is doing on your system when it attempts to make the connection. To do this:

1. If you are configuring an outgoing connection, edit the `/usr/lib/mstppp/Autostart` file. If you are configuring an incoming connection, edit the `/usr/lib/mstppp/Accounts` file.
2. Look for the entry corresponding to the connection you are trying to debug. Incoming entries can be identified by account name. Outgoing connections can be identified by the IP addresses of the local and remote systems (dynamic IP addresses are specified by a “~” character).
3. Add `debug #` to the end of the line, where `#` is a number between 1 and 11 (higher numbers produce more debug information). **debug 5** is a recommended starting point.
4. Save and close the file. If you are debugging an outgoing link, you must kill and restart the PPP daemon:
 - To kill the PPP daemon, enter these commands:


```
ps -ef | grep pppd | grep -v grep
kill processID
```

 where *processID* is the second column of the output from the `grep` command.
 - To restart the PPP daemon, enter these commands:


```
cd /usr/lib/mstppp
./Autostart
```
5. Enter these commands at the UNIX prompt:

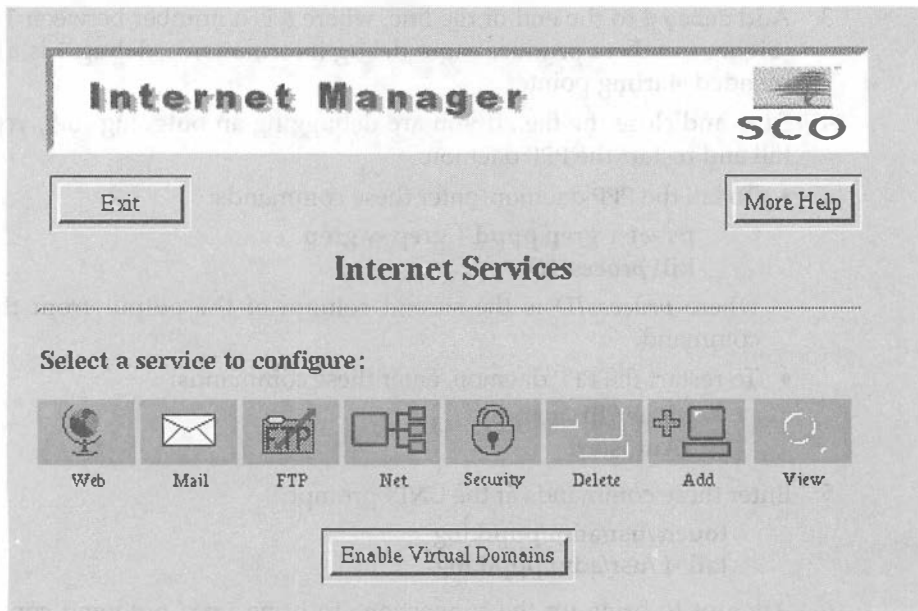

```
touch /usr/adm/pppd.log
tail -f /usr/adm/pppd.log
```
6. Attempt to bring up the connection. To bring up a outgoing connection, use **ping(ADMN)** to contact the remote system’s IP address. To bring up an incoming connection, have the remote system dial in.

7. Watch the output of the **tail** command for debug information.

Particular things to watch for are account names and passwords that are incorrect. Also, if one end of the connection is expecting a string to be sent by the other (for example, login:) and the other side sends something else (for example, username:), this is a problem. If you have such a problem, you can use the **Internet Manager** to modify the chat script by clicking on the **Net** button on the Internet Services page, then clicking on the **PPP Connections** button. If more than one dial-out connection is configured, select the dial-out PPP connection you are debugging, then click on the **Advanced** button. The login chat script can be modified from that page. Alternatively, you can modify the `/usr/lib/mstppp/Systems` file, where the chat script is stored. The format of each of the configuration files is described in the corresponding man page: `ppp.Accounts(MST_PPP)`, `ppp.Auth(MST_PPP)`, `ppp.Devices(MST_PPP)`, `ppp.Dialers(MST_PPP)`, or `ppp.Systems(MST_PPP)`. If you have a complicated chat script, the **Internet Manager** might not be able to configure the connection after the chat script is modified.

Configuring Internet services

Once you have successfully connected to the Internet, the **Internet Manager** displays its main menu, the Internet Services page.



Internet Manager main menu

When you reach the Internet Services page, important Internet services have already been configured for you:

Caching Domain Name Service

DNS enables your system to act as a name server for your local network, minimizing delay and network traffic.

World Wide Web

The Netscape FastTrack Server serves a default home page on the Web.

E-mail

Your system can send and receive e-mail, and any users on your system have POP accounts automatically set up for them.

File transfer

The system allows password-protected FTP access for users on the system.

These services can be configured by clicking on the appropriate icon:

Web	Configure Netscape FastTrack Server, as well as Netscape Proxy Server if it is installed. See "Web" (page 26).
Mail	Specify e-mail forwarding, the domain used in addresses, and the postmaster and hostmaster. See "Mail" (page 31).
FTP	Enable and disable file transfer using the FTP protocol. See "FTP" (page 31).
Net	Configure network routing and PPP connections. See "Net" (page 32).
Security	Set the Internet Manager password and specify which systems can use it remotely. If the optional SCO Internet Security Package is installed, control all network traffic flowing in and out of the system. See "Security" (page 32).

The configuration of each of these subsystems has been simplified to make it easy to configure the system for common uses. When configuring any of these subsystems, you can click on the **More Help** button and the **Internet Manager** will display more information about how to configure it.

See also:

- "Directory structure before enabling virtual domains" (page 33)

Web

When you click on the **Web** button, the **Internet Manager** displays a list of Web servers you have installed.

Clicking on a server enables you to configure it using the Netscape administration utility for that server. This utility prompts you for a user name and password, which are initially set to be the same as that for the **Internet Manager** (the user name is always *admin* and the password is initially set to the first eight characters of the *root* password set during the initial system load).

NOTE If you change the password for the **Internet Manager**, the passwords for the Netscape administration utilities are not changed. To change the passwords for the Netscape administration utilities, you must change them from within those utilities.

The Netscape administration utilities enable you to change many attributes of your servers' behavior. Some attributes, however, should not be changed, or the **Internet Manager** might not work properly. Specifically, these attributes are:

- port
- document root
- bind to address
- server name

See also:

- "Netscape Web server installation defaults" (page 27)
- "Starting and restarting Netscape servers" (page 28)
- "Deferring or reconfiguring network configuration" (page 28)
- "Manually configuring Netscape servers" (page 30)

Netscape Web server installation defaults

The installation of the SCO OpenServer Netscape Web servers uses the following default values. You can alter these values once you complete the installation.

Server name	the string returned by hostname Do not change unless you change the system name (or are configuring multiple servers).
Server IP address	the first (non-loopback) returned by netstat -in , or 127.0.0.1 if TCP/IP is not configured Do not change unless you change the system's IP address.
Server port	Netscape FastTrack Server listens on port 80, is administered on port 620 Netscape Proxy Server listens on port 8080, is administered on port 446
Server home	Netscape FastTrack Server <i>/usr/internet/ns_httpd</i> Netscape Proxy Server <i>/usr/internet/ns_proxy</i>
Server document root	Netscape FastTrack Server <i>/usr/internet/ns_httpd/docs</i>
Server processes	Number of server processes: Minimum 2 Maximum 32 (25 for Netscape Proxy Server)
Home page	Netscape FastTrack Server <i>/usr/internet/ns_httpd/docs/index.html</i>
Index files	<i>index.html</i> or <i>home.html</i> recorded in the server's root (rather than <i>syslog</i>)
administration username	set to <i>admin</i>
administration password	set to the <i>root</i> user's password at installation of server product

- The servers run as user *nouser*.
- The servers always attempt to resolve IP addresses into host names.
- All accesses to the servers are logged.

- Administration access is limited to the local host.
- The servers use fancy directory indexing.

The Netscape Proxy Server is set to the following additional defaults:

- timeout (maximum time between successive network data packets) set to 2 minutes
- use extended access log format
- by default, HTTP, FTP, and Gopher are proxied (SSL and HTTPS are not)
- no caching

Starting and restarting Netscape servers

Once installed, the Netscape FastTrack and Netscape Proxy Servers start automatically on reboot.

NOTE If you have configured a secure server, starting the server requires a password, and therefore must be done manually.

If you have configured virtual domains, see “Configuring interfaces” (page 35).

To stop and restart the Netscape servers, use the following commands as *root*:

Netscape FastTrack Server

```
/usr/internet/ns_httpd/httpd-80/stop and  
/usr/internet/ns_httpd/httpd-80/start
```

If a secure server is configured:

```
/usr/internet/ns_https/https-443/stop and  
/usr/internet/ns_https/https-443/start
```

Netscape Proxy Server

```
/usr/internet/ns_proxy/proxy-8080/stop and  
/usr/internet/ns_proxy/proxy-8080/start
```

For more information, see “Starting and stopping the server” in Chapter 5 of the *Netscape FastTrack Server Administrator's Guide* (**noting this correction to that book:** the server files have been installed in */usr/internet/ns-httpd* in SCO OpenServer).

Deferring or reconfiguring network configuration

During SCO OpenServer installation, Netscape servers are configured with settings for Server Name, Hosts, and Addresses by default. If you defer TCP/IP configuration during initial system installation or you reconfigure TCP/IP, any Netscape servers installed on your system might be improperly configured.

To configure your Netscape server after deferring or reconfiguring networking configuration, edit the following files:

Netscape FastTrack Server:

- In `/usr/internet/ns_httpd/admserv/ns-admin.conf`, set "ServerName" to the string returned by `hostname(ADMN)`. Set "Hosts" and "Addresses" to the hostnames and IP addresses allowed to administer this server. After you set these configuration variables, you can use the Netscape administration server to further configure the server.

In `/usr/internet/ns_httpd/httpd-80/config/magnus.conf`, set "ServerName" to the string returned by `hostname`. Then copy this file to `/usr/internet/ns_httpd/admserv/httpd-80/magnus.conf`. The timestamp on the former file must be the same or earlier than that on the latter.

- If you have enabled virtual domains, edit `/usr/internet/ns_httpd/httpd-80.ipaddress/config/magnus.conf`, where *ipaddress* is the primary IP address for the system. Set "ServerName" to the string returned by `hostname`. Then copy this file to `/usr/internet/ns_httpd/admserv/httpd-80.ipaddress/magnus.conf`. The timestamp on the former file must be the same or earlier than that on the latter.

If you changed the system's primary IP address, rename these directories:

```
mv /usr/internet/ns_httpd/httpd-80.OldIPAddress \
    /usr/internet/ns_httpd/httpd-80.NewIPAddress
mv /usr/internet/ns_httpd/admserv/httpd-80.OldIPAddress \
    /usr/internet/ns_httpd/admserv/httpd-80.NewIPAddress
```

- If a secure server is configured, with no virtual domains, in `/usr/internet/ns_https/https-443/config/magnus.conf`, set "ServerName" to the string returned by `hostname`. Then copy this file to `/usr/internet/ns_httpd/admserv/https-443/magnus.conf`. The timestamp on the former file must be the same or earlier than that on the latter.
- If a secure server is configured, with virtual domains enabled, edit `/usr/internet/ns_https/https-443.ipaddress/config/magnus.conf`, where *ipaddress* is the primary IP address for the system. Set "ServerName" to the string returned by `hostname`. Then copy this file to `/usr/internet/ns_httpd/admserv/https-443.ipaddress/magnus.conf`. The timestamp on the former file must be the same or earlier than that on the latter.

If you changed the system's primary IP address, rename these directories:

```
mv /usr/internet/ns_https/https-443.OldIPAddress \  
/usr/internet/ns_https/https-443.NewIPAddress  
mv /usr/internet/ns_httpd/admserv/https-443.OldIPAddress \  
/usr/internet/ns_httpd/admserv/https-443.NewIPAddress
```

Netscape Proxy Server:

In `/usr/internet/ns_proxy/proxy-8080/config/magnus.conf` set "ServerName" to the string returned by `hostname`. Then copy this file to `/usr/internet/ns_proxy/admserv/proxy-8080/magnus.conf`. The timestamp on the former file must be the same or earlier than that on the latter.

Manually configuring Netscape servers

NOTE Configuring new servers directly with the FastTrack Administration Server might cause them to not be seen by the **Internet Manager**.

To configure Netscape servers manually without using the **Internet Manager**:

1. Start the appropriate administration server by entering one of these commands as *root*:

Netscape FastTrack Server

```
/usr/internet/ns_httpd/start-admin
```

Netscape Proxy Server

```
/usr/internet/ns_proxy/start-admin
```

2. Access the administration server by opening one of these URLs, on the server being configured, with any forms-capable Web browser:

Netscape FastTrack Server

```
http://localhost:620/
```

Netscape Proxy Server

```
http://localhost:446/
```

3. Log into the administration server as user *admin*.

At installation, the *admin* password was set to the first eight characters of the *root* password.

4. Select the server to administer.
5. When you are finished, stop the administration server by entering:

Netscape FastTrack Server

```
/usr/internet/ns_httpd/stop-admin
```

Netscape Proxy Server

```
/usr/internet/ns_proxy/stop-admin
```

Mail

When you install SCO OpenServer, you are given a choice of choosing MMDF or SendMail as your Mail Transport Agent (MTA). To use the **Internet Manager** for configuring electronic mail, you must choose SendMail. If you choose SendMail, you will have full access to multihoming and other advanced mail features not available if you choose MMDF.

If you installed MMDF, but now want to use SendMail as your MTA, use the **Software Manager** and the instructions in "Removing software" and "Installing software" in the *SCO OpenServer Handbook* to remove the MMDF package, then add the **sendmail** package.

A Post Office Protocol (POP) server is configured at installation time so that many popular mail programs on PCs and Macintoshes (including Netscape Navigator and other POP clients) can receive mail using your system as the server.

The system is configured so that any incoming mail destined for your system is either delivered locally (if the destination user exists) or is rejected; if the system receives any mail destined for another system, it forwards it on to that system. Any mail addressed to *postmaster* is delivered to the *root* user as well as to those users you have designated *postmaster*.

Outgoing mail is delivered directly to the system to which it is addressed. Mail sent by local users will have the fully qualified domain name of the system shown in the "From:" header (*user@system.subdomain.domain.com*, for example).

By clicking on the **Mail** button on the Internet Services page, you can change the configuration of e-mail forwarding and host hiding (what gets shown on the "From:" header for outgoing mail). If you have a central system that has a full user database for your domain, you can choose to forward "local mail" to that host. In addition, you can specify a system to which all mail outside your domain is delivered. It is intended that this system has good Internet connectivity and is well able to handle large amounts of SMTP traffic.

FTP

By default, your system is configured to allow users who have an account on your system to use the File Transfer Protocol (FTP) to transfer files between your system and other systems. The use of FTP by anonymous users is disabled. (So-called "anonymous FTP" is commonly used to upload and download files from a system by users that are unknown to that system; no authentication is required. If you have ever downloaded a file from the Internet using your Web browser, you probably have used anonymous FTP.)

By clicking on the **FTP** button on the Internet Services page, you can determine whether FTP access is permitted at all, as well as whether anonymous users can download or upload files.

Net

By clicking on the **Net** button on the Internet Services page, you can configure your system's network connections.

By selecting **Network Routing**, you can change which network interface the system uses as your route to the Internet. If you want to make your default route a PPP connection, you must first configure that connection — see “Using a modem to connect to the Internet” (page 18). You can also specify that your system is a gateway. If you configure your system as a gateway, it will forward data packets received on one interface to another interface if appropriate. Otherwise, all received data packets not destined for this system are discarded.

You can configure both inbound and outbound PPP connections by selecting **PPP Connections**. The procedure for adding and configuring PPP connections is described in “Using a modem to connect to the Internet” (page 18).

Security

Because the **Internet Manager** can be used to configure important services on your system, it is important that access to it be restricted to protect your system from unauthorized users. This is accomplished in two ways. First, the **Internet Manager** requires that the user enter a user name and password to gain access. Second, the **Internet Manager** checks that the system from which the user is accessing it is one that you have specifically authorized.

By clicking on the **Security** button on the Internet Services page, you can change the **Internet Manager** password and specify which systems are authorized to use the **Internet Manager**. Initially, the password for the **Internet Manager** is the same as the *root* password. You can change the password by clicking **Set Internet Manager Password** on the Security page.

NOTE Changing the password for the **Internet Manager** does not change the passwords for the Netscape server administration utilities. These must be changed from within those utilities.

The **Internet Manager** uses only the first eight characters of your password.

The system is initially configured to allow access only from the system itself (running the **Internet Manager** on the console display). To allow another system or systems access to the **Internet Manager**, select **Control Access From Remote Sites** on the Security page, then enter the system's IP address.

WARNING By allowing another system to access the **Internet Manager** remotely, system security is decreased and your system is potentially vulnerable to an “IP spoofing attack”. In an IP spoofing attack, a hacker attempts to gain access to your system by making a remote system appear to be one of your trusted systems by using its IP address. It is also possible that someone monitoring data packets on the network could discover your password. The chance of your system actually being attacked in this manner is small, and chances of a successful security breach are even smaller (the attacker must determine both the IP address of one of your trusted systems as well as the **Internet Manager** password). You should weigh the benefits of remote administration against the costs of a potential compromise of system security.

Directory structure before enabling virtual domains

- If you configure anonymous FTP using the **SCO Internet Manager**, the anonymous FTP directory is `/usr/internet/ip/0.0.0.0/sco_ftp`.
- If you configure a Netscape Web server, the Web server document root directory is `/usr/internet/ip/0.0.0.0/publish/htdocs`.
- Mail is received wherever system mail is configured (`/usr/spool/mail/name`).

Managing virtual domains

In its default configuration, your system has exactly one IP address associated with each network interface or PPP connection, and it has exactly one system name. None of the services described in “Configuring Internet services” (page 24) bind to a particular IP address; that is, no matter which network interface or PPP connection is used to access the service, it behaves identically. The system has one set of Web pages, one FTP area, and one set of mail users.

However, it is sometimes useful to have the services on the system behave differently, depending on which network interface is used to access it. For example, if you have two network interfaces on your system, one that connects to your local LAN and one that connects to the Internet, you might want the Web server on your system to provide one set of information to people internal to your organization, and another set of information to everyone else. For your Web server to do this, it must *bind* itself to particular IP addresses so that it can distinguish between accesses from each network interface.

Some system administrators (particularly ISPs) take this concept one step further. By using “IP aliasing”, it is possible to make a single network interface respond to multiple IP addresses. This, in turn, allows a single system to be known by multiple names (such as *abc.com* and *def.com*). If system services

are configured to bind to specific IP addresses, then a single system can serve the Web sites for both *abc.com* and *def.com*, and nobody accessing either Web site could tell that these sites are being served by a single system.

This process of using a single system to respond to multiple IP addresses and system names is called “multihoming”. The multiple distinct environments that the system presents to the outside world are called “virtual domains”. Your SCO Internet FastStart system can support up to 254 virtual domains, each with distinct Web, FTP, and e-mail services.

See also:

- “Enabling virtual domains” (this page)
- “Viewing properties of virtual domains” (page 37)
- “Adding and deleting virtual domains” (page 39)
- “Filesystem layout for virtual domains” (page 39)
- “Remote administration of virtual domains” (page 39)

Enabling virtual domains

To make your system present multiple distinct environments to the outside world, you must enable virtual domains. On the Internet Services page, select **Add** or **Enable Virtual Domains**. Once you enable virtual domains, the Internet services on your system are reconfigured to bind to specific IP addresses. Because of the difficulties involved in reversing this step, the **Internet Manager** will prompt you to verify that this is what you want to do. Once you make your system’s Internet services bind to specific IP addresses, you cannot reverse this step using the **Internet Manager**.

When you enable virtual domains, you must choose which network interface to bind the existing Internet services configuration to. You must choose one of your network cards, a PPP connection, or the *localhost* interface. *localhost* always has an IP address of 127.0.0.1 and can only be accessed from the system itself; it is never routed across any network interfaces.

The behavior of the Internet Services page changes after virtual domains are enabled. In addition to the row of buttons used to configure individual services, the **Internet Manager** presents a list of interfaces to configure, as well as a SYSTEM-WIDE option. *localhost* (127.0.0.1), your physical network interface(s) and PPP connection(s) are identified as “physical” interfaces, while any virtual domains you create (additional IP addresses you add to your system) are identified as “virtual” interfaces.

Configuring services

You must choose one of the interfaces (or SYSTEM-WIDE) before you click on a service button. Depending on which interface you select, a service may or may not be configurable. For example, PPP configuration (under **Net**) and **Internet Manager** access control (under **Security**) affect the entire system, and are only accessible when SYSTEM-WIDE is selected. Other services are only configurable when a specific interface is selected.

See also:

- “Configuring SYSTEM-WIDE” (this page)
- “Configuring interfaces” (this page)

Configuring SYSTEM-WIDE

The following services are configurable SYSTEM-WIDE when virtual domains are enabled:

Web	The Netscape Proxy Server is only configurable SYSTEM-WIDE (it cannot be bound to specific IP addresses), as its function is to handle requests to and from other sites. (The Netscape FastTrack Server is not configurable SYSTEM-WIDE as it is bound to a specific IP address.)
Mail	The system-wide configuration of your mail service is the same as it is when virtual domains are not enabled — see “Configuring e-mail” (page 38) for more information.
FTP	You can only determine whether FTP is enabled or disabled SYSTEM-WIDE. Enabling or disabling FTP will affect the operation of all virtual domains (if FTP is disabled SYSTEM-WIDE, FTP to individual virtual domains is also disabled). Anonymous FTP is configured per interface when virtual domains are enabled — see “Configuring interfaces” (this page) for more information.
Net	Configuration of network routing and PPP connections is the same as it is when virtual domains are not enabled — see “Configuring network connections” (page 17) for more information.
Security	Configuring access to the Internet Manager is the same as it is when virtual domains are not enabled — see “Security” (page 32) for more information.

Configuring interfaces

The following services are configurable for each interface when virtual domains are enabled:

Web Clicking on the **Web** button allows you to configure the Netscape FastTrack Server associated with the selected interface. You can easily use the Netscape server administration utility to configure web service for each interface. To start the FastTrack server for a virtual domain, enter this command as *root*:

```
/usr/internet/ip/ipaddress/ns_httpd/start
```

ipaddress is the IP address of the server to start or 0.0.0.0 for system-wide server(s).

If you have configured a secure server, enter:

```
/usr/internet/ns_https/https-443.ipaddress/start
```

where *ipaddress* is the primary system IP address.

NOTE Do not change the "Bind Address", "Port", "Document Root", or "Server Name" in the Netscape administration utility. Doing so will cause the **Internet Manager** to improperly configure the server. If you need to change IP addresses associated with virtual domains, use the **Add** and **Delete** buttons on the Internet Services page. See "Adding and deleting virtual domains" (page 39) for more information.

Mail Clicking on the **Mail** button allows you to manage mail users associated with the selected interface. Each virtual domain can either use the system-wide set of users, or have a unique set of users associated only with that domain. This means that a single system can have multiple users with the same name that are distinguished by the domain with which they are associated (for example, *joe@abc.com* and *joe@def.com* are distinct users). Alternatively, if the interfaces use */etc/passwd* instead of private user lists, mail to *joe@abc.com* and *joe@def.com* go to the same system mailbox. *joe* is a real system user, with a full account. When using private user lists for each interface, the users only have POP e-mail access to their mail file. They are not regular users on the system. They cannot use **telnet**(TC) to connect to their accounts to read mail. POP mail is automatically set up for users in the private user lists.

FTP Clicking on the FTP button allows you to control anonymous FTP associated with the selected interface.

Net Configuration of network connections affects the system as a whole, so it cannot be performed separately for each interface.

Security Access to the **Internet Manager** can only be configured SYSTEM-WIDE.

Viewing properties of virtual domains

By clicking on the **View** button on the Internet Services page, you can view and modify properties of the selected virtual domain.

See also:

- “Virtual domain name and DNS” (this page)
- “Administrative users” (page 38)
- “Configuring e-mail” (page 38)
- “Locking and unlocking an interface” (page 38)

Virtual domain name and DNS

One of the important properties of a virtual domain is its name (for example, *abc.com* or *mywebserver.def.com*). This is the name by which services associated with a virtual domain know themselves — it is the “virtual system name”.

To allow other systems to access a virtual domain or physical interface by its name, create entries for it on a DNS server. These entries need to be made on the DNS server that is acting as the primary or authoritative server for the domain within which you have defined the virtual domain’s name. Your SCO OpenServer system is configured to run a caching DNS server only because the optimal DNS configuration for many situations is different, and often systems are dedicated to the purpose of running DNS. If you have a small site, your ISP will probably offer you DNS service.

Because of the many installation-dependent issues involved in proper DNS configuration, the **Internet Manager** does not attempt to create the DNS entry for you. You should ask your network administrator or ISP to add a DNS entry corresponding to your system name and IP address. If you are administering DNS yourself, refer to Chapter 6, “Configuring the Domain Name Service” in the *Networking Guide* in your online documentation for more information.

If you are creating a new top-level domain (such as *mycompany.com*), you must also register this domain with the Network Information Center (NIC). The NIC is the worldwide authority responsible for granting the use of top-level domain names. It is necessary for such a centralized authority to grant domain names to guarantee the uniqueness of names throughout the Internet. Information about the NIC and applying for a domain name can be found on the Web at <http://www.nic.org>. The process of registering your domain name can take several weeks due to the number of requests that the NIC receives. If you register a top-level domain (such as *mycompany.com*), either you or your ISP must arrange to provide primary and secondary Domain Name Service for the new domain prior to NIC registration of the new domain.

Administrative users

Each virtual domain has an administrative user associated with it. When a virtual domain is created, the administrative user is given ownership of appropriate files within the virtual domain. This enables the administrative user to update information contained within the virtual domain, such as Web and FTP content. You can have a distinct administrative user for each virtual domain, or one administrative user for several virtual domains. We do not recommend that the administrative user for your virtual domains be the *root* user.

The administrative user is a regular user on the system. If the administrative account does not exist, it is created by the **Internet Manager** using the login name and password supplied. System defaults for shell, authorizations, and the like are used. The home directories for the administrative users are the top of the file hierarchy for the virtual domain administered by that user: (*/usr/internet/ip/ipaddress/publish*).

Use the **Account Manager** to modify the attributes of administrative users. For example, you might want to limit system access of an administrative user by changing that user's shell to *rsh*, *rcsh*, or *rksh*. If a user is administering several virtual domains, you might want to give them a different home directory than the first virtual domain they are assigned. Use the **Account Manager** to remove or retire administrative user accounts.

Configuring e-mail

You can select whether the mail service associated with a virtual domain uses the system-wide password file to determine users within that domain or uses a private user list. If you want user names to be the same throughout your virtual domains, choose "Use system (/etc/passwd) users". If you want users within each virtual domain to be distinct, use a private user list. If you use the system-wide password file to define your user accounts, you must use the **Account Manager** to manage them. See Chapter 1, "Administering user accounts" in the *System Administration Guide* for more information.

If you choose to use a private user list, you can add and delete users as well as change their passwords by clicking on the **Mail** button on the Internet Services page with the appropriate virtual domain selected.

Locking and unlocking an interface

By locking an interface, you can disable access to all services associated with a particular virtual domain. You can re-enable all services by simply unlocking it. When you lock a particular virtual domain, the system will stop responding to the IP address associated with it. This feature might be useful if, for example, you are an ISP and the customer for which you are maintaining the virtual domain stops paying its bill, or if you are trying to resolve possible IP address conflicts with other systems on your network.

NOTE Locking a physical interface has no effect. Only virtual domains can be locked and unlocked.

Adding and deleting virtual domains

You can add a virtual domain to your system once you have enabled virtual domains by clicking on the **Add** button on the Internet Services page. You will be prompted for the name and IP address to be used for this virtual domain, as well as an administrative user name and password. You should use IP addresses for the virtual domains that are on the same subnet as your primary physical interface. If you use a separate subnet for your virtual domains, you will have to make manual routing changes on your network's router to enable access to the new subnet.

NOTE It is important to ensure that both the name and IP address for your virtual domain are unique.

You can delete a virtual domain from your system by selecting the virtual domain to delete, and then clicking on the **Delete** button on the Internet Services page. When you delete a virtual domain, the **Internet Manager** reclaims all resources associated with it; this includes removing any Web or FTP content, as well as any mail spool files.

NOTE If you only want to disable a virtual domain and not have the **Internet Manager** reclaim its resources, you should lock it instead: Click on the **View** button on the Internet Services page and select **LOCKED**. For more information, see "Locking and unlocking an interface" (page 38).

Filesystem layout for virtual domains

- If you configure FTP, the anonymous FTP directory for an interface is `/usr/internet/ip/ipaddress/sco_ftp` (*ipaddress* is the interface's IP address).
- For each interface, e-mail spool files for POP mail users are in `/usr/internet/ip/ipaddress/sco_mail/spool/user_name` (*ipaddress* is the interface's IP address; *user_name* is the e-mail user's name).
- If you configure a Netscape Web server for an interface, the Web server document root directory is `/usr/internet/ip/ipaddress/publish/htdocs`.

Remote administration of virtual domains

One of the advantages of having unique administrative users for each virtual domain is that these administrative users can manage their virtual domain remotely using FTP. When administrative users connect to the system using

FTP and logs in, their home directories are set to be the top of the file hierarchy associated with their virtual domain. This enables them to upload and download Web content and files to be made accessible using anonymous FTP. If you are an ISP or network administrator, this means that you can create a virtual domain for a user and then step aside and let them administer it themselves using popular FTP programs and Web authoring programs.

The only limitation on the remote administration of a virtual domain is the addition or deletion of POP e-mail users. Since this can only be done by using the **Account Manager** or **Internet Manager**, the system administrator (not the virtual domain administrative user) must make these changes. The administrative user can manage changes to e-mail user passwords by logging into the system using **telnet**(TC) and running the **pwfile()** utility on the e-mail user file (*/usr/internet/ip/ipaddress/sco_mail/passwd*).

Chapter 3

Migrating from a previous Internet FastStart system

When you reinstall your Internet FastStart release 1.0 or 1.1 system as an SCO OpenServer system, any specialized configuration of **sendmail**, **ppp**, and Netscape servers is lost. However, if you follow the procedures shown in this chapter **before you install** your SCO OpenServer system, you can bring most of the previous configurations forward without needing to manually re-configure the system.

NOTE You must perform a fresh install of SCO OpenServer Release 5.0.4 using your new license key. Licenses from previous Internet FastStart releases will be rejected by SCO OpenServer as invalid.

This migration from an SCO Internet FastStart system to SCO OpenServer is a multi-step process, described in more detail in:

- “Migrating sendmail configuration” (page 42)
- “Migrating PPP configuration to SCO PPP from Morning Star” (page 45)
- “Migrating server configuration and data” (page 46)

The general multi-step process for migrating from Internet FastStart to SCO OpenServer is:

1. Perform a complete backup of the system to be reinstalled. See “Running unscheduled filesystem backups” in the *System Administration Guide*.
2. From the system to be re-installed, save to floppy disk any **sendmail**, **ppp**, and Netscape configuration files that you want to bring forward to the new system.

3. Install SCO OpenServer on your system, following the instructions described in Chapter 2, "Installing or upgrading an SCO system" in the *SCO OpenServer Handbook*.
4. Use the **Internet Manager** to restore your basic system configuration.
5. Restore the files you saved to floppy disk in step 2.

Migrating sendmail configuration

Two key files control **sendmail** operation:

- /usr/lib/sendmail.cf* Contains **sendmail** configuration information including addressing, channel, and domain information.
- /usr/lib/mail/aliases* Contains aliases of user names to their addresses.

In all cases, you can bring each of these files forward to SCO OpenServer.

Additionally, you might want to bring forward virtual domain configuration files. **sendmail** uses these files to route incoming mail to users whose addresses are in virtual domains on your system.

Saving sendmail data from the IFS system

The following files must be saved before you reinstall:

- */usr/lib/sendmail.cf*
Save in all cases.
- */usr/lib/mail/aliases*
Save in all cases.
- Other *aliases* files.
Save only if you configured them and they are referred to by *sendmail.cf*.
- */usr/internet/lib/sco_mail/domains*
/usr/internet/lib/sco_mail/domains.db
/usr/internet/ip/ipaddress/sco_mail/passwd
/usr/internet/ip/ipaddress/sco_mail/config
*/usr/internet/ip/ipaddress/sco_mail/spool/**
Save only if you use virtual domains.
ipaddress is the IP address for each domain.

Example sendmail backup

A system called *phoebe* uses **sendmail**, does not use additional *aliases* files, and has virtual domains configured. The virtual domains are:

Domain name	IP Address
veggies.com	132.147.118.1
fruits.com	132.147.118.2
nuts.com	132.147.118.3

To save the sendmail configuration for this system:

1. Save the names and IP addresses of each of your domains, either by writing them down or by select **Print** from the **Internet Manager's File** menu.
2. Save the following files to floppy (remember that the IP addresses shown below are examples only):

```

/usr/lib/sendmail.cf
/usr/lib/mail/aliases
/usr/internet/lib/sco_mail/domains
/usr/internet/lib/sco_mail/domains.db
/usr/internet/ip/132.147.118.1/sco_mail/passwd
/usr/internet/ip/132.147.118.1/sco_mail/config
/usr/internet/ip/132.147.118.1/sco_mail/spool/*
/usr/internet/ip/132.147.118.2/sco_mail/passwd
/usr/internet/ip/132.147.118.2/sco_mail/config
/usr/internet/ip/132.147.118.2/sco_mail/spool/*
/usr/internet/ip/132.147.118.3/sco_mail/passwd
/usr/internet/ip/132.147.118.3/sco_mail/config
/usr/internet/ip/132.147.118.3/sco_mail/spool/*

```

A simple way to do this is to use a text editor to create a shell script which uses the **tar(C)** command to save these files. For example, you could create a file called *savemail*, which contains the following:

```

tar cv6 /usr/lib/sendmail.cf \
/usr/lib/mail/aliases \
/usr/internet/lib/sco_mail/domains \
/usr/internet/lib/sco_mail/domains.db \
/usr/internet/ip/132.147.118.1/sco_mail/passwd \
/usr/internet/ip/132.147.118.1/sco_mail/config \
/usr/internet/ip/132.147.118.1/sco_mail/spool/* \
/usr/internet/ip/132.147.118.2/sco_mail/passwd \
/usr/internet/ip/132.147.118.2/sco_mail/config \
/usr/internet/ip/132.147.118.2/sco_mail/spool/* \
/usr/internet/ip/132.147.118.3/sco_mail/passwd \
/usr/internet/ip/132.147.118.3/sco_mail/config \
/usr/internet/ip/132.147.118.3/sco_mail/spool/*

```

- The **tar** command shown accesses the 3.5 inch floppy drive (**tar** key 6). You can substitute another device if desired.
- A trailing backslash is necessary on all but the last line.

To run this program, enter the following at your system prompt:

```
sh savemail
```

To confirm that the files were saved, enter the following at your system prompt:

```
tar tv6
```

The files you saved should be listed.

Configuring sendmail on your SCO OpenServer system

After you install your SCO OpenServer system, you can use the configuration files you saved to restore your previous **sendmail** configuration:

1. If you configured virtual domains, start the **Internet Manager**.
Use it to configure virtual domains (page 34), using the domain name and IP addresses you saved previously. This creates the directory structure to hold the files you want to restore.
2. Insert the floppy containing the sendmail configuration files into the disk drive.
3. From the command line, enter:

```
tar xv6
```

This restores the saved **sendmail** (and virtual domain) configuration data.

No additional configuration is required. **sendmail** should now work as it did on your Internet FastStart system. You can verify that the **sendmail** daemon is running by entering:

```
ps -ef | grep send
```

Migrating PPP configuration to SCO PPP from Morning Star

SCO PPP from Morning Star Technologies is included on your SCO OpenServer Release 5.0.4 CD-ROM. **It must be installed as a layered product after installing SCO OpenServer.** To install SCO PPP from Morning Star Technologies, use the **Software Manager**, following the instructions in “Installing software” in the *SCO OpenServer Handbook*.

NOTE The license for SCO PPP from Morning Star is included with your SCO OpenServer Desktop System or SCO OpenServer Enterprise System license.

After installation, use the **Internet Manager** to configure your dial-in connections. The PPP configuration files of SCO TCP/IP are not directly compatible with SCO PPP from Morning Star but can be used for reference.

If you install SCO PPP from Morning Star, use of the PPP features of SCO TCP/IP is not supported.

Migrating from an SCO PPP configuration

To migrate from an SCO TCP/IP PPP configuration to an SCO PPP from Morning Star Technologies configuration:

- Save these files for reference:

/etc/ppphosts

/etc/pppauth

- Configure an outbound PPP connection for each remote host to which your system will connect, as described in “Using a modem to connect to the Internet” (page 18). You can use the entries in your saved */etc/ppphosts* file when filling in the **Internet Manager** page. The entries are described completed in **ppphosts(SFF)**. Refer to the saved */etc/pppauth* for the PAP/CHAP authentication information, as described in **pppauth(SFF)**.
- Configure an inbound PPP connection as described in “Using a modem to connect to the Internet” (page 18), again using the entries in the saved */etc/ppphosts* and */etc/pppauth* files for reference.

Migrating from an existing PPP from Morning Star configuration

To migrate from an existing PPP from Morning Star Technologies configuration:

- Save these files on a floppy disk before installing SCO OpenServer:

```
/usr/lib/mstppp/Autostart  
/usr/lib/mstppp/Accounts  
/usr/lib/mstppp/Auth  
/usr/lib/mstppp/Systems  
/usr/lib/mstppp/Devices  
/usr/lib/mstppp/Dialers.local  
/usr/lib/mstppp/exec.in/*  
/usr/lib/mstppp/exec.out/*
```

(Some of these files and directories might not be present on your system.)

For an example of creating a simple shell script to save these files to disk, see “Example sendmail backup” (page 43) earlier in this chapter.

- Install SCO OpenServer, then use the **Internet Manager** to restore your basic system configuration.
- Restore the saved configuration files.

Migrating server configuration and data

You can migrate your Netscape FastTrack Server configuration and data files to your SCO OpenServer system.

The following sections describe how to:

- save server configuration for a system that does not use virtual domains (this page)
- save server configuration for a system that uses virtual domains (page 47)
- prepare the SCO OpenServer system for the restored files (page 48)
- restore the server configuration (page 48)

Saving server configuration and data: standard configuration

If your system does not use virtual domains, save the following files and directories to a floppy disk:

```

/usr/internet/ip/0.0.0.0/publish/*
/usr/internet/ip/0.0.0.0/publish/ftp/*
/usr/internet/ip/0.0.0.0/ns_httpd/config/magnus.conf
/usr/internet/ip/0.0.0.0/ns_httpd/config/obj.conf
/usr/internet/ip/0.0.0.0/ns_httpd/config/mime.types
/usr/internet/ip/0.0.0.0/ns_https/config/magnus.conf
/usr/internet/ip/0.0.0.0/ns_https/config/mime.types
/usr/internet/ip/0.0.0.0/ns_https/config/obj.conf
/usr/internet/ns_httpd/docs/*
/usr/internet/ns_https/docs/*

```

Some of these files and directories might not be present on your system (if, for example, you have not configured an **ftp** server or a secure server).

For an example of creating a simple shell script to save these files to disk, see “Example sendmail backup” (page 43) earlier in this chapter.

Saving server configuration and data: virtual domain configuration

If your system uses virtual domains, save the following files and directories to a floppy disk:

```

/usr/internet/ip/ipaddress/ns_httpd/config/magnus.conf
/usr/internet/ip/ipaddress/ns_httpd/config/obj.conf
/usr/internet/ip/ipaddress/ns_httpd/config/mime.types
/usr/internet/ip/ipaddress/ns_https/config/magnus.conf
/usr/internet/ip/ipaddress/ns_https/config/obj.conf
/usr/internet/ip/ipaddress/ns_https/config/mime.types
/usr/internet/ip/ipaddress/publish/htdocs/*
/usr/internet/ip/ipaddress/publish/htdocs-s/*
/usr/internet/ip/ipaddress/publish/ftp/*
/usr/internet/ip/ipaddress/HOSTNAME

```

NOTE *ipaddress* is the IP address of each of your virtual domains.

You **must** save one set of files and directories for every IP address you host. For example, if you host virtual domains at addresses 132.147.118.1 and 132.147.118.2, you must save these files:

```

/usr/internet/ip/132.147.118.1/ns_httpd/config/magnus.conf
/usr/internet/ip/132.147.118.2/ns_httpd/config/magnus.conf

```

Some of these files and directories might not be present on your system (if, for example, you have not configured an **ftp** server or a secure server).

For an example of creating a simple shell script to save these files to disk, see “Example sendmail backup” (page 43) earlier in this chapter.

Post-installation server configuration

After you install SCO OpenServer on your system, you might need to use the **Internet Manager** to prepare the system for the configuration files you saved.

- **If you are restoring virtual domains**, follow the instructions in “Enabling virtual domains” (page 34).
- **If you are restoring anonymous ftp**, follow the instructions in “FTP” (page 31).
- **If you are restoring a secure server**, follow the instructions in “Security” (page 32).

If you are not restoring any of the above, proceed to “Restoring server configuration files” (this page).

Restoring server configuration files

NOTE If you are restoring virtual domains, an ftp server, or a secure server, please read the previous section first.

To restore the saved server configuration files:

1. Insert the floppy containing the server configuration files into the disk drive.
2. From the command line, enter:
tar xv6
This restores the saved server configuration data.
3. Follow the instructions in either “Copying server configuration files - no virtual domains” (this page) or “Copying server configuration files - virtual domains” (page 49).

Copying server configuration files - no virtual domains

Several files you restored must be copied or moved into different locations on the system.

Copy the following files into `/usr/internet/ns_httpd/admserv/httpd-80/`:

```
/usr/internet/ip/0.0.0.0/ns_httpd/config/magnus.conf  
/usr/internet/ip/0.0.0.0/ns_httpd/config/obj.conf  
/usr/internet/ip/0.0.0.0/ns_httpd/config/mime.types
```

If you are running the secure server, copy the following files into `/usr/internet/ns_httpd/admserv/https-443/`:

```
/usr/internet/ip/0.0.0.0/ns_https/config/magnus.conf  
/usr/internet/ip/0.0.0.0/ns_https/config/mime.types  
/usr/internet/ip/0.0.0.0/ns_https/config/obj.conf
```

If you are running a secure server, move any files in `/usr/internet/ns_https/docs` into `/usr/internet/ip/0.0.0.0/ns_httpd/publish/htdocs-s`.

Copying server configuration files - virtual domains

Several files you restored must be copied into additional locations on the system.

Copy the following files into `/usr/internet/ns_httpd/admserv/httpd-80.ipaddress`:

```
/usr/internet/ip/ipaddress/ns_httpd/config/magnus.conf  
/usr/internet/ip/ipaddress/ns_httpd/config/obj.conf  
/usr/internet/ip/ipaddress/ns_httpd/config/mime.types
```

ipaddress is the IP address for each virtual domain. For example, for the virtual domain 132.147.118.3, copy files from:

```
/usr/internet/ip/132.147.118.3/ns_httpd/config/
```

into:

```
/usr/internet/ns_httpd/admserv/httpd-80.132.147.118.3/
```

If you are running the secure server, copy the following files into `/usr/internet/ns_httpd/admserv/https-443.ipaddress`:

```
/usr/internet/ip/ipaddress/ns_https/config/magnus.conf  
/usr/internet/ip/ipaddress/ns_https/config/obj.conf  
/usr/internet/ip/ipaddress/ns_https/config/mime.types
```


Chapter 4

Features, limitations, and updates to Internet FastStart

This chapter contains a list of updated documentation, and known limitations for Internet FastStart (SCO OpenServer Internet Services) in SCO OpenServer Release 5.0.4. These notes supplement the SCO OpenServer Release 5.0.4 *Release Notes*.

Read this before installing Internet FastStart

These notes supplement the installation instructions in the *SCO OpenServer Handbook* and the *Release Notes*. If your system is currently running SCO Internet FastStart release 1.0 or 1.1, some of these notes might be duplicates of those from your original product's *Release Notes*.

Hostname and domain

To properly configure the Netscape web servers, the System Name and Domain Name that you enter during installation must exactly match (including case) the fully qualified domain name returned by your nameserver's PTR record for your IP address.

For example, if your nameserver's PTR record for your IP address returns *mymachine.mycompany.COM*, you must enter exactly that text when prompted for the System Name and Domain Name during the installation. If you enter **mymachine.mycompany.com** (lower case **com**), the Netscape web servers will not be properly configured.

Deferred TCP/IP configuration

If you defer configuration of TCP/IP during installation, and do not configure a network card before running the **Internet Manager** for the first time, the **Internet Manager** will add a line to */etc/hosts* of the form:

```
127.0.0.1 host.full.domain host
```

where *host.full.domain* is the fully qualified domain name of your machine. This entry will work in most cases, but if you configure a PPP link with a fixed IP address (that is, if you do not select “dynamic”), you should edit */etc/hosts* and change the IP address on this line to the local IP address on your PPP link.

If you configure a network card after the **Internet Manager** adds this line, it will add a line to */etc/hosts* with the IP address of that network card, but it will be after the line added by the **Internet Manager**. Edit */etc/hosts* and remove the line added by the **Internet Manager**.

Host name length and obj.conf file corruption

If your fully qualified domain name (host name) is exactly 24-characters long, the Netscape Proxy Server configuration manager might corrupt its *obj.conf*, making the Proxy Server unusable. If this occurs, replace the corrupted *obj.conf* file with a new version:

```
cd /usr/internet/ns_proxy/admin/config
cp obj.orig obj.conf
/usr/internet/ns_proxy/restart-proxy
```

If you want to make Proxy Server configuration changes on a system with a 24-character host name, you must make the modifications to *obj.conf* manually, without using the Proxy Server configuration manager.

Installing from a serial console

To install SCO Internet FastStart from a serial console onto a machine that does not have a video adapter, the required settings are 9600 baud, 8 data bits, one stop bit, direct connect.

NOTE If your system does not have a video adapter, you will not be able to run the SCO **Internet Manager** on the system as it requires a forms- and tables-capable browser. In this case, you will either need to add a video adapter or configure your system to allow remote administration using a forms- and tables-capable browser on another system.

Minimum display requirements

SCO OpenServer with Internet FastStart requires that your display support 256 colors or better and a resolution of 800x600 or better.

On a system with support for only 16 colors, the Netscape Navigator will not support the pseudocolor display visual. In addition, the Internet Configuration and Netscape Navigator Desktop icons will display poorly.

In this case, the Netscape Navigator starts up with **visual** set to **StaticGray** by default. To specify an alternate display visual, use the **-visual** option to the Netscape Navigator.

See your Netscape documentation for more information. See "Internet FastStart documentation" (page 71).

Modem support

SCO OpenServer supports serial lines up to 115K baud. In addition, the **Internet Manager** includes support for the modems listed in Table 23-1, "Dialers file entries" in the *SCO OpenServer Handbook*.

See Chapter 23, "Adding modems" in the *SCO OpenServer Handbook* for general information about installing and configuring modems.

Read this after installing Internet FastStart

After installation, but before proceeding to further configure your system, read these important notes:

- "System notes and limitations" (this page)
- "Configuring Domain Name Service (DNS)" (page 55)
- "SCO OpenServer and MMDF" (page 56)
- "Hardware notes" (page 56)
- "Software configuration" (page 57)
- "SCO Internet Manager notes" (page 59)
- "Netscape FastTrack notes" (page 67)
- "Netscape Navigator and Navigator Gold notes" (page 70)
- "Internet FastStart documentation" (page 71)

To obtain the latest information about SCO Internet FastStart, as well as downloadable versions of updated software and fixes, open this URL:

<http://www2.sco.com/FastStart>

System notes and limitations

This section includes these notes:

- "High Security and root password length" (page 54)
- "Programs which depend on termcap do not run on console Multiscreen displays" (page 54)
- "PPP dial-in connections" (page 55)

- “Remote administration” (page 55)
- “Multiple machine names” (page 55)

High Security and root password length

It is no longer necessary when using C2 security to set your *root* password to exactly 8 characters at installation time (as was indicated in the SCO Internet FastStart 1.0 Release Notes).

Programs which depend on termcap do not run on console Multiscreen displays

Only in systems localized for European use, the default **TERM** value for Multiscreen displays is “ansi-850” and there is no entry for ansi-850 entry in the */etc/termcap* file (although there is one in */usr/lib/terminfo*). As a result, older applications which depend on **termcap** will fail with a Can’t load ansi-850 error message. This does not affect **scoterm** windows, for which **TERM** is set to **ansi**.

Only if you run into this problem, enter one of:

For sh or ksh: **TERM=ansi; export TERM**

For csh: **setenv TERM ansi**

Add that line to your *.profile* (**sh**, **ksh**) or *.login* (**csh**) if you want this change to persist from session to session.

The system administrator can fix this for the entire system by editing */etc/ttytype* to replace “ansi-850” with “ansi” on each of the following lines:

```
ansi-850    tty01
ansi-850    tty02
ansi-850    tty03
ansi-850    tty04
ansi-850    tty05
ansi-850    tty06
ansi-850    tty07
ansi-850    tty08
ansi-850    tty09
ansi-850    tty10
ansi-850    tty11
ansi-850    tty12
```

We recommend changing the **TERM** type in the most limited way that fixes your problem (per-session change preferred over per-user change preferred over system-wide change), and then only when you actually encounter this problem.

PPP dial-in connections

PPP dial-in connections sometimes fail during initialization; this produces the following error message in */usr/adm/pppd.log*:

```
pppd: Fatal system error: Can't ifconfig dul (SIOCSIFADDR): File exists
```

Repeating the dial-in attempt should be successful.

Remote administration

To remotely administer your SCO OpenServer system from a machine whose web browser is configured to use a proxy server, you must put the IP address of that proxy server into the remote access list of the **Internet Manager**.

WARNING This will enable any user who is using the same proxy server to administer your SCO OpenServer system if they have the correct password.

Multiple machine names

If your machine has multiple names, such as when more than one networking interface is configured and each IP address has its own name, **sendmail** must be configured to accept mail for all of those names. To do this, run **mkdev cf** and add all the hostnames to the "Alternate Host Names" section. See "Running mkdev cf" in the *Mail and Messaging Guide* for more information.

Configuring Domain Name Service (DNS)

The **Internet Manager** automatically configures a caching nameserver. This allows you to make use of the root nameservers out on the Internet to resolve domain names. However, if you already have a nameserver for your domain configured on a different machine to resolve names in your own domain as well as those out on the Internet, you might want to configure your SCO OpenServer system to use that nameserver instead.

To do so:

1. Edit the */etc/resolv.conf* file as follows:

```
domain yourdomain.COM
nameserver IP address your nameserver
hostresorder local bind
```

For example, if your domain is *foo.COM*, and the IP address of your nameserver is 199.199.198.1, *resolv.conf* contains:

```
domain foo.COM
nameserver 199.199.198.1
hostresorder local bind
```

2. Set the permissions on */etc/resolv.conf*:
chmod 644 /etc/resolv.conf
3. Rename the */etc/named.boot* file:
mv /etc/named.boot /etc/named.boot-
4. Kill the **named** daemon:
kill 'cat /etc/named.pid'

To configure a primary or secondary nameserver on your SCO OpenServer system, see Chapter 6, “Configuring the Domain Name Service” in the *Networking Guide*.

SCO OpenServer and MMDF

When you install SCO OpenServer, you are given a choice of choosing MMDF or **sendmail** as your Mail Transport Agent (MTA). By default, SCO OpenServer is configured to use MMDF. The **Internet Manager** requires you to choose **sendmail**. If you choose **sendmail**, you will have full access to multihoming and other advanced mail features not available if you choose MMDF.

NOTE If you use MMDF instead of **sendmail** on your SCO OpenServer system, the **Internet Manager** Mail configuration will no longer work. In addition, this means that you cannot have POP email users in the virtual domains.

If you installed MMDF, but now want to use **sendmail** as your MTA, use the **Software Manager** and the instructions in “Removing software” and “Installing software” in the *SCO OpenServer Handbook* to remove the MMDF package, then add the **sendmail** package.

Hardware notes

This section includes these notes:

- “Enhanced serial driver” (this page)
- “Mouse sluggish with Internet FastStart” (page 57)
- “Core dump with Matrox video card” (page 57)

Enhanced serial driver

SCO OpenServer contains an enhanced serial driver for use with your standard COM1 and COM2 and other supported non-intelligent serial boards as listed by the **mkdev serial** command.

The enhanced serial driver supports data speeds up to and including 115200bps. However, this is subject to the following hardware limitations:

- Serial ports without a 16550 UART chip are only supported at data rates up to and including 9600bps. Contact your serial board or system manufacturer to be sure that you are using a serial board with a 16550 UART chip.
- Due to the rate at which interrupts can be handled and the speed at which the UART buffer is overwritten at high speeds, simultaneous data rates of 57600bps or higher are only supported on a single serial port at a time.

Mouse sluggish with Internet FastStart

If this occurs, run `mkdev mouse` to delete, then re-add the mouse.

Core dump with Matrox video card

When running Netscape Navigator in 640x480, 16-color mode on a system with a Matrox video card, we have experienced core dumps. This does not appear to be a problem with other video cards.

Software configuration

This section includes these notes:

- “Software notes and limitations” (this page)
- “Providing access to unlisted packet filter services” (page 58)

Software notes and limitations

SCO Internet FastStart does not use SCO PPP

SCO Internet FastStart is designed to use SCO PPP from Morning Star Technologies in place of SCO PPP. Use the **Internet Manager** (not **netconfig** or the **Network Configuration Manager**) to configure SCO PPP from Morning Star Technologies.

Also note that the online documentation, the *Networking Guide* and *Configuring Network Connections*, contains obsolete configuration information for SCO PPP. To configure PPP, use the Morning Star PPP documentation in the online library “Internet Documentation Set”, accessible using `scohelp(XC)`. See also “Accessing PostScript documentation files” (page 72) for information.

Do not modify Netscape server options

The following options should *not* be modified by the Netscape server configuration managers:

- Server Location

- Server Port
- Bind Address
- Document Root
- Chroot Directory

Document contains no data

Slower machines that are configured to have more than one interface may experience problems on the “Control SYSTEM Data Flow” page of the **Internet Manager**. After clicking on the **OK** button, the browser might time out before the Administration Tool can return any information to it. If this is the case, click on the **Reload** button on your browser to get back to the “Control SYSTEM Data Flow” page.

Use standard serial port for dial-in PPP connections

If you use a device other than a standard serial port for a dial-in PPP connection, the following error message may appear in `/usr/lib/mstppp/Log`:

```
ioctl: Invalid argument
```

This is normal and does not affect PPP functionality.

FTP file permissions

The default file permissions on files transferred to an SCO OpenServer system using FTP are 644 (world readable) so that users can transfer WWW publishing files with FTP.

To change the default file permissions back to the standard UNIX default permissions of 640, edit the `/etc/inetd.conf` file and remove the `-u 022` argument from the following line:

```
ftp      stream  tcp      nowait  root    /etc/ftpd  ftpd -u 022
```

Dynamically assigned IP addresses and web servers

Configuring web servers bound to dynamically assigned local IP addresses (for example, using dynamic PPP) is not recommended and is unsupported.

Providing access to unlisted packet filter services

To provide access to a service not listed in the packet filter, open the TCP ports 1024-5999 and 6006-65535. To do this:

1. Start the **SCO Internet Manager**.
2. Click on the **Security** button.
3. Click on the **Control INTERFACE Data Flow** button.
4. Select the **World Wide Web** subsystem and click on **OK**.
5. For each interface you are opening access to (most people will perform these steps for the **net0** interface only):

- a. Select that interface to configure and click on **OK**.
- b. Set the **Inbound** "nonStandard" option to "true" to allow access to an otherwise unlisted service.
- c. Set the **outbound** "nonStandard" to "true" to allow an otherwise unlisted service access to the Internet.
- d. Click on the **OK** button.

SCO Internet Manager notes

This section includes these notes:

- "WARNING: Internet Manager security" (page 60)
- "admin password" (page 60)
- "Cannot change Netscape administration password" (page 60)
- "Unique IP addresses" (page 60)
- "Testing your Internet connection" (page 60)
- "Removing a dialout PPP connection" (page 60)
- "Forwarding email" (page 61)
- "Internet Manager Advanced Security configuration page problem" (page 61)
- "Remote configuration error and Back button" (page 61)
- "Use unique user name when adding new dial-in PPP connection" (page 61)
- "Assigning IP addresses from a pool" (page 61)
- "Deleting a PPP connection on a High security system" (page 62)
- "Line not dropped when active inbound PPP connection deleted" (page 62)
- "Using PPP to connect to SCO UNIX Release 3.2v4.2 or SCO Open Desktop Release 3.0" (page 62)
- "PPP connections not counted as logins" (page 63)
- "PPP logs in UTC time in /usr/adm/pppd.log" (page 63)
- "Specifying the amount of detail in pppd log" (page 63)
- "Deferring or changing network configuration" (page 63)
- "Changing the hostname or IP address of an SCO OpenServer system" (page 63)
- "Disabling automatic gateway configuration" (page 66)
- "Virtual domain status on Internet Services page" (page 67)

- “Virtual domain admin user password error” (page 67)
- “Document contains no data error” (page 67)
- “Not a mana document: / error” (page 67)

WARNING: Internet Manager security

The **Internet Manager** can configure your system in ways that greatly affect its security. Because of this, access to the **Internet Manager** should be treated the same as access to the *root* account. Do not give the **Internet Manager** password to any user to whom you would not also give the *root* password, and do not enable remote access to the **Internet Manager** from any machine that untrusted users can log into.

admin password

If you defer setting the *root* password during the initial installation procedure, the **Internet Manager** *admin* password and the Netscape Server *admin* passwords are set to (Enter).

Cannot change Netscape administration password

You cannot change the Netscape administration password using the **Internet Manager**. If you change this password in the **Internet Manager**, you should also change it in the Netscape Administration utility.

Unique IP addresses

On SCO OpenServer systems, no two interfaces can share the same IP address. For example, if you assign the same IP address to both the local end of a PPP connection and a network card interface, the **SCO Internet Manager** fails.

Testing your Internet connection

While running the **Internet Manager** for the first time, you have the choice of testing your connection to the Internet. If your Internet connection is through a modem, there is a chance that, although you might have PPP and the modem properly configured, the connection will time out. If this occurs, it is best to try the connection test twice before assuming that there is a problem.

Removing a dialout PPP connection

After removing a dialout PPP connection using the **Internet Manager**, the line in */usr/lib/mstppp/Devices* for this connection is left in the file. This might affect future attempts to add connections, should that *Devices* file entry be incorrect. If you are unsure as to the correctness of the entry, remove the *Devices* file entry with a text editor after removing the dialout PPP connection with the **Internet Configuration Manager**. Multiple PPP lines can use the same *Devices* file entry, so beware of removing this line if you have multiple dialout PPP lines.

Forwarding email

When you set the mailer domain in the “Domain in From: header” section of the **Internet Manager’s** Email Forwarding page, you can only choose the machine’s hostname, or a subset of it. If you want an email domain that is not a subset of the hostname, you must manually edit `/usr/lib/sendmail.cf`. Whenever you change any other system-wide email configuration parameter, the **Internet Manager** replaces your changes with your machine’s fully-qualified domain name, and you must re-edit your `sendmail.cf` file to undo these changes.

Internet Manager Advanced Security configuration page problem

In the **Internet Manager**, on the Advanced Security page, you must click on **OK** each time you remove or add to an attribute’s set of values.

Remote configuration error and Back button

If you attempt to configure an SCO OpenServer system remotely using the **Internet Manager** from a site that does not have access, you see this error:

Use the browser’s Back button to return to the previous page.

In this case, the previous page is the password prompt, so your browser’s **Back** button is stippled.

Use unique user name when adding new dial-in PPP connection

When adding a new dial-in PPP connection, the “Local PPP account login name” might not be a user name that already exists on the system. Enter a new user name. This user will be created for use only with this PPP connection.

Assigning IP addresses from a pool

To configure the system to select an IP address for inbound PPP connections automatically from a pool of addresses, first define the pool, then activate IP address pool selection:

1. Create the file `/usr/lib/mstppp/IPPool` with one line for each IP address to include in the pool of addresses. (This file is used instead of the `/etc/ppppool` file previously used with SCO PPP.)

On each line, include three fields: local IP address, remote IP address that might connect to the local address, and netmask. For example:

```
154.224.87.98      145.127.182.124    255.255.255.0
```

2. On the Internet Services page of the **Internet Manager**, click on the **Network** button (if virtual domains have been enabled, first select SYSTEM-WIDE), then click on **PPP Connections**. Click on **Add New Dial-in PPP Connection** or select an existing dial-in connection to modify.

When the `/usr/lib/mstppp/IPPool` file exists, the inbound PPP connection configuration page displays a "Use IP Address Pool" checkbox. If you check this box, an IP address for the inbound connection will be chosen from available addresses listed in the `IPPool` file.

Make sure dynamic reassignment of IP addresses is enabled on the system dialing in. (If the dialing system is an SCO OpenServer system with Internet FastStart, select the "Dynamic" checkbox when configuring the dial-out connection.)

Deleting a PPP connection on a High security system

Deleting a PPP connection (with the **Internet Manager**) on a system that is configured for High security will display an error message because users cannot be deleted on High security systems. The PPP connection has been deleted, but not the user identified as that connection's "Local PPP account login name."

To prevent the use of the user account that was associated with that PPP connection, use the **Account Manager** to lock out or retire the user.

Line not dropped when active inbound PPP connection deleted

If you delete a PPP connection (with the **Internet Manager**) while that connection is active, the line will not be dropped, the `pppd` daemon will not be killed, and the `/dev/tty*` file will still be owned by the UID of the deleted user.

To correct this, the system administrator should kill the orphaned `pppd` process (or reboot).

Using PPP to connect to SCO UNIX Release 3.2v4.2 or SCO Open Desktop Release 3.0

Before using PPP to connect your SCO OpenServer Release 5.0.4 system to either of the following systems, first install Support Level Supplement (SLS) net382e on that system:

- SCO® UNIX® System V/386 Release 3.2 v4.2.0 system with SCO TCP/IP 1.2.1
- SCO® Open Desktop® Release 3.0

This prevents intersystem PPP option negotiation problems. SLS net382e is available at:

`ftp://ftp.sco.com/SLS/net382e.Z`

Also, download the instructions and notes for the SLS:

`ftp://ftp.sco.com/SLS/net382e.ltr.Z`

If you are using PPP to connect to an SCO system running a release of SCO TCP/IP earlier than 1.2.1, add the PPP option **no!qm** to the end of the line for that the connection in these files on your SCO OpenServer Release 5.0.4 system:

`/usr/lib/mstppp/Autostart` (for outgoing connections)
`/usr/lib/mstppp/Accounts` (for incoming connections)

This will avoid LQM option negotiation problems.

PPP connections not counted as logins

PPP sessions are not counted as user logins. No additional SCO OpenServer Enterprise or SCO Internet FastStart user licenses are required to support multiple simultaneous PPP connections.

PPP logs in UTC time in /usr/adm/pppd.log

The **pppd** daemon writes to the log file `/usr/adm/pppd.log` (not to the `/usr/adm/syslog` file) using UTC (not local) time in entries. UTC (Universal Time Coordinated) is Greenwich Mean Time (GMT).

Specifying the amount of detail in pppd log

The amount of detail for debugging information written to the `/usr/adm/pppd.log` file can now be specified on the Add New Dial-in PPP Connection, Add New Dial-out PPP Connection, and Configure Outbound PPP Connection pages.

Deferring or changing network configuration

During installation, Netscape servers are configured with default settings for the "ServerName", "Hosts", and "Addresses" fields in the server configuration files. If you deferred network configuration during installation or if you reconfigure TCP/IP, your Netscape servers might no longer be properly configured and you might therefore have to edit the configuration files as described in the following note, "Changing the hostname or IP address of an SCO OpenServer system" (this page).

Changing the hostname or IP address of an SCO OpenServer system

1. **To change the hostname** of your SCO OpenServer system, first follow the instructions in "Changing the system name" in the *Mail and Messaging Guide* skipping step 4 unless you have removed **sendmail** and installed **MMDF**. **Do not reboot (step 7) yet.**

2. **To change the IP address** of your SCO OpenServer system, first use the **Network Configuration Manager** (or **netconfig**).
3. **If virtual domains have been enabled**, skip to step 9.
4. Edit these files to replace each old hostname and IP address with the new hostname and IP address:

for the Administration server:

```
/usr/internet/ns_httpd/admserv/ns-admin.conf    /usr/internet/ns_httpd/httpd-80/config/magnus.conf
```

for the Netscape Proxy Server:

```
/usr/internet/ns_proxy/admin/config/magnus.conf  
/usr/internet/ns_proxy/admin/config/obj.conf
```

for the web server on port 80:

```
/usr/internet/ns_httpd/httpd-80/config/magnus.conf  
/usr/internet/ns_httpd/httpd-80/config/obj.conf
```

5. Copy the web server files you just edited:

```
/usr/internet/ns_httpd/httpd-80/config/magnus.conf  
/usr/internet/ns_httpd/httpd-80/config/obj.conf
```

to the administration server directory for the web server on port 80:

```
/usr/internet/ns_httpd/admserv/httpd-80
```

6. **If a secure server is configured**, also edit these files to replace each old hostname and IP address with the new hostname and IP address:

```
/usr/internet/ns_https/https-443/config/magnus.conf  
/usr/internet/ns_https/https-443/config/obj.conf
```

7. Copy those two files to the administration server directory for the web server on port 443:

```
/usr/internet/ns_httpd/admserv/https-443
```

8. **Skip to step 21.** (Steps 9 through 20 are for systems on which virtual domains have been enabled.)
9. **To change a virtual domain's IP number**, use the **Internet Manager** to remove and reinstall the virtual domain. Select the virtual domain, then click on the **Delete** button on the Internet Services page. Click on the **Add** button to recreate the virtual domain with a new IP address.

NOTE In the following steps, substitute the old primary IP address for *OldIPaddress* and the new primary IP address for *NewIPaddress*.

10. **If you changed the system's primary IP address in step 2**, change the IP address of the web server(s) that are bound to the physical network interface by editing these files to replace each occurrence of the old primary

hostname and IP address with the new primary hostname and IP address:

for the administration server:

```
/usr/internet/ns_httpd/admserv/ns-admin.conf
```

for the web server on port 80 of old IP address:

```
/usr/internet/ns_httpd/httpd-80.OldIPAddress/config/magnus.conf
```

```
/usr/internet/ns_httpd/httpd-80.OldIPAddress/config/obj.conf
```

11. Rename these directories:

```
mv /usr/internet/ns_httpd/httpd-80.OldIPAddress \
   /usr/internet/ns_httpd/httpd-80.NewIPAddress
```

```
mv /usr/internet/ns_httpd/admserv/httpd-80.OldIPAddress \
   /usr/internet/ns_httpd/admserv/httpd-80.NewIPAddress
```

12. Copy the two configuration files to the administration server directory for the web server on port 80:

```
cp /usr/internet/ns_httpd/httpd-80.NewIPAddress/magnus.conf \
   /usr/internet/ns_httpd/admserv/httpd-80.NewIPAddress/magnus.conf
```

```
cp /usr/internet/ns_httpd/httpd-80.NewIPAddress/obj.conf \
   /usr/internet/ns_httpd/admserv/httpd-80.NewIPAddress/obj.conf
```

13. Remove the old *admin.conf* file:

```
rm /usr/internet/ns_httpd/admserv/httpd-80.NewIPAddress/admin.conf
```

14. Recreate symbolic links by entering these commands:

```
mv /usr/internet/ip/OldIPAddress /usr/internet/ip/NewIPAddress
```

```
rm /usr/internet/ipNewIPAddress/ns_httpd/
```

```
ln -s /usr/internet/ns_httpd/httpd-80.NewIPAddress \
    /usr/internet/ip/NewIPAddress/ns_httpd
```

```
rm /usr/internet/ip/NewIPAddress/ns_https
```

```
ln -s /usr/internet/ns_https/https-443.NewIPAddress \
    /usr/internet/ip/NewIPAddress/ns_https
```

15. If a secure server is installed on port 443, edit these files to replace each occurrence of the old primary hostname and IP address with the new primary hostname and IP address:

```
/usr/internet/ns_https/https-443.OldIPAddress/config/magnus.conf
```

```
/usr/internet/ns_https/https-80.OldIPAddress/config/obj.conf
```

16. Rename the directory for the primary IP address secure web server with this command:

```
mv /usr/internet/ns_https/https-443.OldIPAddress \
   /usr/internet/ns_https/https-443.NewIPAddress
```

17. Rename the administration server directory associated with the secure web server on port 443:

```
mv /usr/internet/ns_httpd/admserv/https-443.OldIPAddress \
   /usr/internet/ns_httpd/admserv/https-443.NewIPAddress
```

18. Copy the two configuration files to the administration server directory for the web server on port 443:

```
cp /usr/internet/ns_https/https-443.NewIPAddress/magnus.conf \
   /usr/internet/ns_httpd/admserv/https-443.NewIPAddress/magnus.conf
cp /usr/internet/ns_httpd/https-443.NewIPAddress/obj.conf \
   /usr/internet/ns_httpd/admserv/https-443.NewIPAddress/obj.conf
```

19. Remove the old *admin.conf* file:

```
rm /usr/internet/ns_httpd/admserv/https-443.NewIPAddress/admin.conf
```

20. Recreate symbolic links by entering these commands:

```
rm /usr/internet/ns_httpd/https-443.OldIPAddress
ln -s /usr/internet/ns_https/https-443.NewIPAddress \
    /usr/internet/ns_httpd/https-443.NewIPAddress
rm /usr/internet/ip/NewIPAddress/ns_https
ln -s /usr/internet/ns_https/https-443.NewIPAddress \
    /usr/internet/ip/NewIPAddress/ns_https
```

21. Reboot your system.

Disabling automatic gateway configuration

Your system will automatically be configured as a gateway (forwarding IP packets through your system is allowed) if it has more than one network interface—including all LAN adapter cards and PPP connections. If only one network interface remains when a PPP link is disconnected, packet forwarding will be disabled.

To disable this automatic configuration, edit these files:

```
/usr/lib/mstppp/dialout
/usr/lib/mstppp/exec.dialin
```

Locate the line in each file that contains the command:

```
osavtcl -c "ObjectReplace {sco ip} dummy {{gateway auto}}"
```

Place a # at the beginning of that line to disable its execution. You will then be able to use the **Internet Manager** to configure the gateway status of your machine (on the Internet Services page, click on **Net**, then click on **Network Routing**).

Virtual domain status on Internet Services page

When a virtual domain is LOCKED, that word replaces “virtual” in the “Type” column. (Since only virtual domains can be locked, either “virtual” or “LOCKED” in the “Type” column identifies a virtual domain.)

Virtual domain admin user password error

When creating or modifying a virtual domain, you can assign a new password for the virtual domain’s *admin* user. If you enter the *root* password, you will get an error like:

OSA command failed:

```
ObjectAction {sco user} admin setPassword longleft7
General failure occurred in processing the request.
You may not re-use the same password
```

(Use the browser’s Back button to return to the previous page.)

If creating a new virtual domain, click on the browser’s **Back** button, then click on **Internet Services** at the top of the page, and then click on **View**. If modifying an existing virtual domain, just click on the browser’s **Back** button. Enter an *admin* user password that is not the same as that of the user designated as *admin* user. If the user already exists on the system, you can specify the user’s existing password by leaving the password fields blank.

Document contains no data error

Slower systems configured with more than one interface might experience time-out problems. After you click on **OK** on the Set Up Packet Filter Data Flow page, Navigator might time out before the **Internet Manager** can set up packet filtering and respond. If this happens, click on the **Reload** button to return to the Set Up Packet Filter Data Flow page and try again (this might require more than one try).

Not a mana document: / error

You might get this error when remotely accessing the **Internet Manager** if, instead of entering the URL *http://hostname:615/mana/mana/menu.mana* you entered *http://hostname:615/mana/mana* (the browser is appending a final “/”). Try again, using the correct URL:

http://hostname:615/mana/mana/menu.mana

Netscape FastTrack notes

The Netscape FastTrack Server updates and replaces the Netscape Communications Server from SCO Internet FastStart 1.0 and (if installed) the Netscape Commerce Server. This section includes these notes:

- “Editing access control files” (this page)
- “Setting Access Control for nested directories” (this page)
- “Unauthorized host error when opening administration server” (this page)
- “Intermittent scaling cache size error” (page 69)
- “Group creation display does not clearly show subgroups” (page 69)
- “Archiving logs stops FastTrack Server” (page 70)
- “Setting the Java directory stops FastTrack Server” (page 70)
- “Element” (page 70)

Editing access control files

The directories `/usr/internet/ns_httpd/httpacl`, `/usr/internet/ns_httpd/authdb`, and `/usr/internet/ns_httpd/userdb` contain access control and user authentication information. The permissions for these directories are set to 0711 to allow the Netscape administration server to write files in them.

To modify these databases, use the Netscape administration server (accessed through the **Internet Manager**). After making changes to the databases, change the permissions for the directories listed above to 0700 to prevent shell users from gaining access to this information. Then, stop and restart the server so these changes take effect.

To make additional changes to the databases, first change the permission to 0711. After making the changes, return the permissions to 0700.

Setting Access Control for nested directories

Setting access control (ACL) for nested directories does not work. For example, you cannot set access control for `user1` to be able to read `/usr/internet/ns_httpd/docs/user1` and also have `user2` access only the `/usr/internet/ns_httpd/docs/user1/user2` subdirectory. Instead, you must set up parallel directories, such as:

```
/usr/internet/ns_httpd/docs/user1
/usr/internet/ns_httpd/docs/user2
```

Unauthorized host error when opening administration server

The Netscape administration server will sometimes incorrectly refuse access from the system console or from a remote host that is normally allowed access. That might be the problem if you get this error when trying to access the administration server:

Internal Error

The Administration Server was unable to fulfill your request.

Reason: Unauthorized host

If you get this message at the console, go to:

<http://localhost:620/admin-serv/bin/index>

Select **Configure Administration** and then select the **Access Control** link. In the “IP addresses to allow” field, enter a comma-separated list of all the IP addresses that may access the administration server, including the IP address of the system’s primary network interface, the IP address associated with the system’s name (if different than that of the primary network interface), and any other IP addresses by which the system may be referenced. Restart the administration server to implement these access configuration changes. For more information (including instructions for using wildcard characters when specifying IP addresses), see Chapters 3 and 6 of the *Netscape FastTrack Server Administrator’s Guide*.

If you get this message on a remote system, first try clicking on **Reload** (repeat several times, if necessary). If that does not work, edit the following file, to add the IP addresses of the systems that may remotely access the administration server:

`/usr/internet/ns_httpd/admserv/ns-admin.conf`

Use this syntax (for more information, see Appendix B, “Server Configuration Files” in the *Netscape FastTrack Programmer’s Guide*):

`Addresses (IP-ADDR1|IP-ADDR2|ipaddr3|...|IP-ADDRn)`

After editing and saving *ns-admin.conf*, restart the administration server to implement the access configuration changes.

Alternatively, you can go the console of the local system and follow the instructions above for console access, entering the remote system’s IP address instead of the local one.

Intermittent scaling cache size error

Occasionally when starting the administration server, you might see a message about scaling down cache size. This indicates that the administration server is attempting to allocate system resources and is readjusting its allocation attempt to the resources available on the system. The message, which might be displayed either when starting the server by hand and during system boot-up, can be safely ignored.

Group creation display does not clearly show subgroups

If you select **Create Group** from the **Access Control** menu of the administration server, create a new group, then select from “This group is a part of:”, the new group is a subgroup. This is not obvious from the display. When you edit a **group**, subgroups will be shown under “Group members”.

Archiving logs stops FastTrack Server

When trying to archive a log, the FastTrack Server stops. The confirmation dialog says that the server is sent a restart signal, but the server does not restart. If this occurs, restart the server manually by selecting **On** from the **System Settings** menu.

Setting the Java directory stops FastTrack Server

If you select **Java** from the **Programs** menu, then specify the Java directory, the FastTrack Server stops. The confirmation dialog says that the server is sent a restart signal, but the server does not restart. If this occurs, restart the server manually by selecting **On** from the **System Settings** menu.

If you select **Log Preference** from the **Server Status** menu of the administration server, then try to change the name of a log file or other log preferences, this error will be displayed:

```
JavaScript Alert
Form Element Missing:FormatString
You must specify whether to include a format string or not
```

If you get this error, you must edit the *obj.conf* file for the server, and then restart the server. The *obj.conf* file is in the *config* directory, which is a relative path to the *ServerRoot* displayed when you select **View Server Settings** from the **System Settings** menu. In *obj.conf*, edit "AddLog" to configure log preferences. For instructions, see Appendix B of the *Netscape FastTrack Programmer's Guide*.

Netscape Navigator and Navigator Gold notes

Installing additional Netscape Navigator packs

If you install an additional Netscape Navigator pack on a system with an existing Navigator, you do not have to relicense Navigator using the **License Manager**.

Using Netscape Navigator to view online documentation

You can use Netscape Navigator to view Internet Family documents. To do this, open the following URL:

<http://localhost:457/inethome.html>

You can also use Netscape Navigator to view the documentation in the online SCO OpenServer Documentation Library by opening the following URL:

<http://localhost:457/dochome.html>

Difficulty accessing some Java applets

There is a known problem accessing some Java applets such as the Java Interactive Atlas at <http://www.mapquest.com> or the weather maps at <http://cavis.atmos.uiuc.edu>.

These problems have been reported to Netscape and will be fixed in an upcoming release of Navigator. We will make this release available from the SCO Internet Family web site (<http://www2.sco.com/FastStart/>) as soon as it is available.

Internet FastStart documentation

Internet FastStart documentation includes:

- This book, *SCO OpenServer Internet Services*, in hard copy.
- *SCO PPP from Morning Star User's Guide*, available on the SCO OpenServer Enterprise System and SCO OpenServer Desktop System when SCO PPP from Morning Star Technologies is installed

The SCO OpenServer Enterprise System and SCO OpenServer Desktop System include this book:

- *Netscape Navigator Handbook*
(at </usr/lib/scohelp/Internet/Navigator/handbook.html>)

The SCO OpenServer Enterprise System includes this book with Netscape Navigator Gold:

- *Netscape Navigator Gold Authoring Guide*
(at </usr/lib/scohelp/Internet/NavGoldAuthoring/navgold.htm>)

Because they make use of features not available in the **scohelp** browser, the **Netscape books are best viewed with Netscape Navigator** by opening the URL :

<http://localhost:457/inethome.html>

The Netscape Navigator Handbook is also available over the Internet from the Navigator **Help** menu.

SCO OpenServer Enterprise System includes these books with the Netscape FastTrack Server:

- *SCO Internet FastStart Administrator's Guide*
(at </usr/lib/scohelp/FASTSTART/CONTENTS.html>)
- *Netscape FastTrack Server Administrator's Guide*
(at </usr/lib/scohelp/Internet/FastTrack/ag/admin.htm>)

- *Netscape FastTrack Server Programmer's Guide*
(at `/usr/lib/scohelp/Internet/FastTrack/pg/contents.htm`)
- *Netscape Javascript Guide*
(at `/usr/lib/scohelp/Internet/FastTrack/javascript/contents.htm`)

To view these books online, click on the desktop **Help** icon, select the "Internet Documentation Set" book set, then click on the book you want.

Accessing PostScript documentation files

PostScript documentation files are available for printing (or copying) in the following directories on the SCO OpenServer CD-ROM:

- **Netscape Navigator Gold Authoring Guide**
`/info/inetfam/netscape/ps_doc/goldauth`
- **Netscape FastTrack Server Administrator's Guide**
`/info/inetfam/netscape/ps_doc/ftadmin`
- **SCO PPP from Morning Star User's Guide**
`/info/inetfam/ppp`

NOTE The CD-ROM is a mountable filesystem. To access the files, you must have CD-ROM support configured on your system.

To access the Postscript files:

1. Log in as *root* and insert the CD-ROM disk into the drive.
2. Mount the CD-ROM disk:

```
mount /dev/cd0 /mnt
```
3. Change to the appropriate documentation directory. For example:

```
cd /mnt/info/inetfam/netscape/ps_doc/goldauth/  
ls
```
4. Some Postscript files are compressed on the CD. Copy them to a temporary location and uncompress them before printing:

```
cp 01TITLEP.PS.Z /tmp  
cd /tmp  
uncompress 01TITLEP.PS.Z
```

5. Print the file to a Postscript printer. For example:

```
lp -dprinter_name 01TITLEP.ps
```

6. Unmount the CD-ROM filesystem by entering:

```
cd /  
umount /dev/cd0
```


30 May 1997
AU20018P000

19987

CTM

0987654321

