

# MultiNet for OpenVMS Programmer's Reference

Part Number: N-5003-44-NN-A

**December 2001**

This manual documents the programmer's interface to MultiNet, and is intended to guide the programmer in developing applications that use network services.

**Revision/Update:** This manual supersedes the *MultiNet Programmers' Reference*, V4.3

**Operating System/Version:** VAX/VMS V5.5-2 or later, OpenVMS VAX 6.0 or later, and OpenVMS Alpha V6.1 or later

**Software Version:** MultiNet V4.4

**Process Software  
Framingham, Massachusetts  
USA**

The material in this document is for informational purposes only and is subject to change without notice. It should not be construed as a commitment by Process Software. Process Software assumes no responsibility for any errors that may appear in this document.

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

The following third-party software may be included with your product and will be subject to the software license agreement.

Network Time Protocol (NTP). Copyright © 1992 by David L. Mills. The University of Delaware makes no representations about the suitability of this software for any purpose.

Point-to-Point Protocol. Copyright © 1989 by Carnegie-Mellon University. All rights reserved. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

RES\_RANDOM.C. Copyright © 1997 by Niels Provos <provos@physnet.uni-hamburg.de> All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Niels Provos.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

Copyright © 1990 by John Robert LoVerso. All rights reserved. Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by John Robert LoVerso.

Kerberos. Copyright © 1989, DES.C and PCBC\_ENCRYPT.C Copyright © 1985, 1986, 1987, 1988 by Massachusetts Institute of Technology. Export of this software from the United States of America is assumed to require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting. WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

DNSSIGNER (from BIND distribution) Portions Copyright (c) 1995-1998 by Trusted Information Systems, Inc. Portions Copyright (c) 1998-1999 Network Associates, Inc. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE

SOFTWARE IS PROVIDED "AS IS" AND TRUSTED INFORMATION SYSTEMS DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TRUSTED INFORMATION SYSTEMS BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

ERRWARN.C. Copyright © 1995 by RadioMail Corporation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of RadioMail Corporation, the Internet Software Consortium nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY RADIOMAIL CORPORATION, THE INTERNET SOFTWARE CONSORTIUM AND CONTRIBUTORS ``AS IS`` AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RADIOMAIL CORPORATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This software was written for RadioMail Corporation by Ted Lemon under a contract with Vixie Enterprises. Further modifications have been made for the Internet Software Consortium under a contract with Vixie Laboratories.

IMAP4R1.C, MISC.C, RFC822.C, SMTP.C Original version Copyright © 1988 by The Leland Stanford Junior University

ACCPORNAM technology Copyright (c) 1999 by Brian Schenkenberger - TMESIS SOFTWARE

NS\_PARSER.C Copyright © 1984, 1989, 1990 by Bob Corbett and Richard Stallman  
This program is free software. You can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 1, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139 USA

IF\_ACPC Copyright © 1985 and IF\_DDAC Copyright © 1986 by Advanced Computer Communications

IF\_PPPC Copyright © 1993 by Drew D. Perkins

ASCII\_ADDR.C Copyright © 1994 Bell Communications Research, Inc. (Bellcore)

DEBUG.C Copyright © 1998 by Lou Bergandi. All Rights Reserved.

NTP\_FILEGEN.C Copyright © 1992 by Rainer Pruy Friedrich-Alexander Universitaet Erlangen-Nuernberg

RANNY.C Copyright © 1988 by Rayan S. Zachariassen. All Rights Reserved.

MD5.C Copyright © 1990 by RSA Data Security, Inc. All Rights Reserved.

Portions Copyright © 1981, 1982, 1983, 1984, 1985, 1986, 1987, 1988, 1989 by SRI International

Portions Copyright © 1984, 1989 by Free Software Foundation

Portions Copyright © 1993, 1994, 1995, 1996, 1997, 1998 by the University of Washington. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notices appear in all copies and that both the above copyright notices and this permission notice appear in supporting documentation, and that the name of the University of Washington or The Leland Stanford Junior University not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. This software is made available "as is", and THE UNIVERSITY OF WASHINGTON AND THE LELAND STANFORD JUNIOR UNIVERSITY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, WITH REGARD TO THIS SOFTWARE, INCLUDING WITHOUT LIMITATION ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND IN NO EVENT SHALL THE UNIVERSITY OF WASHINGTON OR THE LELAND STANFORD JUNIOR UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR STRICT LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright © 1980, 1982, 1985, 1986, 1988, 1989, 1990, 1993 by The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright © 1993 by Compaq Computer Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Compaq Computer Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission. THE SOFTWARE IS PROVIDED "AS IS" AND COMPAQ COMPUTER CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL COMPAQ COMPUTER CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING

FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright © 1995 by International Business Machines, Inc.

International Business Machines, Inc. (hereinafter called IBM) grants permission under its copyrights to use, copy, modify, and distribute this Software with or without fee, provided that the above copyright notice and all paragraphs of this notice appear in all copies, and that the name of IBM not be used in connection with the marketing of any product incorporating the Software or modifications thereof, without specific, written prior permission. To the extent it has a right to do so, IBM grants an immunity from suit under its patents, if any, for the use, sale or manufacture of products to the extent that such products are used for performing Domain Name System dynamic updates in TCP/IP networks by means of the Software. No immunity is granted for any product per se or for any other function of any product. THE SOFTWARE IS PROVIDED "AS IS", AND IBM DISCLAIMS ALL WARRANTIES, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL IBM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE, EVEN IF IBM IS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

Portions Copyright © 1995, 1996, 1997, 1998, 1999, 2000 by Internet Software Consortium. All Rights Reserved. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 1996-2000 Internet Software Consortium.

Use is subject to license terms which appear in the file named ISC-LICENSE that should have accompanied this file when you received it. If a file named ISC-LICENSE did not accompany this file, or you are not sure the one you have is correct, you may obtain an applicable copy of the license at: <http://www.isc.org/isc-license-1.0.html>. This file is part of the ISC DHCP distribution. The documentation associated with this file is listed in the file DOCUMENTATION, included in the top-level directory of this release. Support and other services are available for ISC products - see <http://www.isc.org> for more information.

ISC LICENSE, Version 1.0

1. This license covers any file containing a statement following its copyright message indicating that it is covered by this license. It also covers any text or binary file, executable, electronic or printed image that is derived from a file that is covered by this license, or is a modified version of a file covered by this license, whether such works exist now or in the future. Hereafter, such works will be referred to as "works covered by this license," or "covered works."
2. Each source file covered by this license contains a sequence of text starting with the copyright message and ending with "Support and other services are available for ISC products - see <http://www.isc.org> for more information." This will hereafter be referred to as the file's Bootstrap License.
3. If you take significant portions of any source file covered by this license and include those portions in some other file, then you must also copy the Bootstrap License into that other file, and that file becomes a covered file. You may make a good-faith judgement as to where in this file the bootstrap license should appear.
4. The acronym "ISC", when used in this license or generally in the context of works covered by this license, is an abbreviation for the words "Internet Software Consortium."
5. A distribution, as referred to hereafter, is any file, collection of printed text, CD ROM, boxed set, or other collection, physical or electronic, which can be distributed as a single object and which contains one or more works covered by this license.
6. You may make distributions containing covered files and provide copies of such distributions to whomever you choose, with or without charge, as long as you obey the other terms of this license. Except as stated in (9), you may include as many or as few covered files as you choose in such distributions.

7. When making copies of covered works to distribute to others, you must not remove or alter the Bootstrap License. You may not place your own copyright message, license, or similar statements in the file prior to the original copyright message or anywhere within the Bootstrap License. Object files and executable files are exempt from the restrictions specified in this clause.
8. If the version of a covered source file as you received it, when compiled, would normally produce executable code that would print a copyright message followed by a message referring to an ISC web page or other ISC documentation, you may not modify the the file in such a way that, when compiled, it no longer produces executable code to print such a message.
9. Any source file covered by this license will specify within the Bootstrap License the name of the ISC distribution from which it came, as well as a list of associated documentation files. The associated documentation for a binary file is the same as the associated documentation for the source file or files from which it was derived. Associated documentation files contain human-readable documentation which the ISC intends to accompany any distribution.

If you produce a distribution, then for every covered file in that distribution, you must include all of the associated documentation files for that file. You need only include one copy of each such documentation file in such distributions.

Absence of required documentation files from a distribution you receive or absence of the list of documentation files from a source file covered by this license does not excuse you from this from this requirement. If the distribution you receive does not contain these files, you must obtain them from the ISC and include them in any redistribution of any work covered by this license. For information on how to obtain required documentation not included with your distribution, see: <http://www.isc.org/getting-documentation.html>.

If the list of documentation files was removed from your copy of a covered work, you must obtain such a list from the ISC. The web page at <http://www.isc.org/getting-documentation.html> contains pointers to lists of files for each ISC distribution covered by this license.

It is permissible in a source or binary distribution containing covered works to include reformatted versions of the documentation files. It is also permissible to add to or modify the documentation files, as long as the formatting is similar in legibility, readability, font, and font size to other documentation in the derived product, as long as any sections labeled CONTRIBUTIONS in these files are unchanged except with respect to formatting, as long as the order in which the CONTRIBUTIONS section appears in these files is not changed, and as long as the manual page which describes how to contribute to the Internet Software Consortium (hereafter referred to as the Contributions Manual Page) is unchanged except with respect to formatting.

Documentation that has been translated into another natural language may be included in place of or in addition to the required documentation, so long as the CONTRIBUTIONS section and the Contributions Manual Page are either left in their original language or translated into the new language with such care and diligence as is required to preserve the original meaning.

10. You must include this license with any distribution that you make, in such a way that it is clearly associated with such covered works as are present in that distribution. In any electronic distribution, the license must be in a file called "ISC-LICENSE".

If you make a distribution that contains works from more than one ISC distribution, you may either include a copy of the ISC-LICENSE file that accompanied each such ISC distribution in such a way that works covered by each license are all clearly grouped with that license, or you may include the single copy of the ISC-LICENSE that has the highest version number of all the ISC-LICENSE files included with such distributions, in which case all covered works will be covered by that single license file. The version number of a license appears at the top of the file containing the text of that license, or if in printed form, at the top of the first page of that license.

11. If the list of associated documentation is in a seperated file, you must include that file with any distribution you make, in such a way that the relationship between that file and the files that refer to it is clear. It is not permissible to merge such files in the event that you make a distribution including files from more than one ISC distribution, unless all the Bootstrap Licenses refer to files for their lists of associated documentation, and those

references all list the same filename.

12. If a distribution that includes covered works includes a mechanism for automatically installing covered works, following that installation process must not cause the person following that process to violate this license, knowingly or unknowingly. In the event that the producer of a distribution containing covered files accidentally or wilfully violates this clause, persons other than the producer of such a distribution shall not be held liable for such violations, but are not otherwise excused from any requirement of this license.

13. COVERED WORKS ARE PROVIDED "AS IS". ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO COVERED WORKS INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

14. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OF COVERED WORKS.

Use of covered works under different terms is prohibited unless you have first obtained a license from ISC granting use pursuant to different terms. Such terms may be negotiated by contacting ISC as follows:

Internet Software Consortium  
950 Charter Street  
Redwood City, CA 94063  
Tel: 1-888-868-1001 (toll free in U.S.)  
Tel: 1-650-779-7091  
Fax: 1-650-779-7055  
Email: info@isc.org  
Email: licensing@isc.org

#### DNSSAFE LICENSE TERMS

This BIND software includes the DNSsafe software from RSA Data Security, Inc., which is copyrighted software that can only be distributed under the terms of this license agreement.

The DNSsafe software cannot be used or distributed separately from the BIND software. You only have the right to use it or distribute it as a bundled, integrated product.

The DNSsafe software can ONLY be used to provide authentication for resource records in the Domain Name System, as specified in RFC 2065 and successors. You cannot modify the BIND software to use the DNSsafe software for other purposes, or to make its cryptographic functions available to end-users for other uses.

If you modify the DNSsafe software itself, you cannot modify its documented API, and you must grant RSA Data Security the right to use, modify, and distribute your modifications, including the right to use any patents or other intellectual property that your modifications depend upon.

You must not remove, alter, or destroy any of RSA's copyright notices or license information. When distributing the software to the Federal Government, it must be licensed to them as "commercial computer software" protected under 48 CFR 12.212 of the FAR, or 48 CFR 227.7202.1 of the DFARS.

You must not violate United States export control laws by distributing the DNSsafe software or information about it, when such distribution is prohibited by law.

THE DNSSAFE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY WARRANTY WHATSOEVER. RSA HAS NO OBLIGATION TO SUPPORT, CORRECT, UPDATE OR MAINTAIN THE RSA SOFTWARE. RSA DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO ANY MATTER WHATSOEVER, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A

PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS.

If you desire to use DNSsafe in ways that these terms do not permit, please contact:

RSA Data Security, Inc.

100 Marine Parkway

Redwood City, California 94065, USA

to discuss alternate licensing arrangements.

Secure Shell (SSH). Copyright © 2000. This License agreement, including the Exhibits (“Agreement”), effective as of the latter date of execution (“Effective Date”), is hereby made by and between Data Fellows, Inc., a California corporation, having principal offices at 675 N. First Street, 8th floor, San Jose, CA 95112170 (“Data Fellows”) and Process Software, Inc., a Massachusetts corporation, having a place of business at 959 Concord Street, Framingham, MA 01701 (“OEM”).

All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective holders.

MultiNet is a registered trademark and Process Software and the Process Software logo are trademarks of Process Software.

Copyright ©1997, 1998, 1999, 2000 Process Software Corporation. All rights reserved. Printed in USA.

Copyright ©2000, 2001 Process Software, LLC. All rights reserved. Printed in USA.

If the examples of URLs, domain names, internet addresses, and web sites we use in this documentation reflect any that actually exist, it is not intentional and should not to be considered an endorsement, approval, or recommendation of the actual site, or any products or services located at any such site by Process Software. Any resemblance or duplication is strictly coincidental.

---

# Contents

## Preface

Purpose of this Guide.....	xv
Document Structure .....	xv
Obtaining Customer Support .....	xvi
Before Contacting Customer Support.....	xvi
Sending Electronic Mail .....	xvii
Calling Customer Support .....	xviii
Contacting Customer Support by Fax.....	xviii
Obtaining Online Help.....	xviii
MultiNet Frequently Asked Questions List .....	xviii
Accessing the MultiNet Public Mailing List .....	xviii
Process Software World Wide Web Server.....	xix
Obtaining Software Patches Over the Internet .....	xix
Typographical Conventions .....	xx
Further Reading .....	xxi
Documentation Comments .....	xxi

## Chapter 1 MultiNet Programming Tutorial

Sockets .....	1-1
TCP Client .....	1-3
TCP Server.....	1-4
UDP .....	1-4
BSD-Specific Tips .....	1-5
BSD Sockets Porting Note.....	1-5
BSD 4.3 TCP/IP Future Compatibility Considerations .....	1-5

## Chapter 2 Socket Library Functions

AST Reentrancy .....	2-1
----------------------	-----

## Chapter 3 \$QIO Interface

## Chapter 4 SNMP Extensible Agent API Routines

Requirements .....	4-2
Linking the Extension Agent Image.....	4-2
Installing the Extension Agent Image .....	4-3
Debugging Code.....	4-3
Subroutine Reference .....	4-3

## Chapter 5 RPC Fundamentals

Introduction .....	5-1
What Are RPC Services? .....	5-1
MultiNet Implementation .....	5-1
Distributed Applications.....	5-1
Components of RPC Services .....	5-2
Run-Time Libraries (RTLs).....	5-2
RPCGEN Compiler .....	5-2
Port Mapper.....	5-2
RPC Information .....	5-3
Client-Server Relationship .....	5-3
External Data Representation (XDR).....	5-3
RPC Processing Flow .....	5-3
Local Calls Versus Remote Calls .....	5-4
Handling System Crashes.....	5-4
Handling Errors .....	5-4
Call Semantics .....	5-5
Programming Interface.....	5-5
High-Level Routines .....	5-5
Mid-Level Routines.....	5-5
Low-Level Routines .....	5-6
Transport Protocols .....	5-6
XID Cache.....	5-7
Cache Entries.....	5-7

Cache Size.....	5-7
Execution Guarantees .....	5-7
Enabling XID Cache .....	5-8
Broadcast RPC.....	5-8
Identifying Remote Programs and Procedures .....	5-8
Remote Program Numbers.....	5-8
Remote Version Numbers .....	5-9
Remote Procedure Numbers .....	5-9
Additional Terms .....	5-9

## **Chapter 6 Building Distributed Applications with RPC**

Introduction.....	6-1
Distributed Application Components .....	6-1
What You Need to Do.....	6-1
Step 1: Design the Application .....	6-2
Step 2: Write and Compile the Interface Definition .....	6-2
Step 3: Write the Necessary Code .....	6-3
Step 4: Compile All Files.....	6-3
Step 5: Link the Object Code.....	6-3
Step 6: Start the Port Mapper.....	6-3
Step 7: Execute the Client and Server Programs .....	6-4
Obtaining RPC Information.....	6-4
Requesting a Program Listing.....	6-4

## **Chapter 7 RPCGEN Compiler**

Introduction.....	7-1
What Is RPCGEN? .....	7-1
Software Requirements.....	7-1
Input Files .....	7-2
Output Files .....	7-3
Preprocessor Directives .....	7-3
Invoking RPCGEN .....	7-4
Creating All Output Files at Once .....	7-4
Creating Specific Output Files.....	7-4
Examples:.....	7-5
Creating Server Stubs for TCP or UDP Transports .....	7-5
Error Handling .....	7-6

Restrictions ..... 7-6

## **Chapter 8 RPC RTL Management Routines**

Introduction ..... 8-1  
Management Routines ..... 8-1  
Routine Name Conventions ..... 8-1  
Header Files ..... 8-1  
Management Routines ..... 8-2

## **Chapter 9 RPC RTL Client Routines**

Introduction ..... 9-1  
Common Arguments ..... 9-1  
Client Routines ..... 9-2

## **Chapter 10 RPC RTL Port Mapper Routines**

Introduction ..... 10-1  
Port Mapper Routines ..... 10-1  
Port Mapper Arguments ..... 10-1

## **Chapter 11 RPC RTL Server Routines**

Introduction ..... 11-1  
Server Routines ..... 11-1

## **Chapter 12 RPC RTL XDR Routines**

Introduction ..... 12-1  
XDR Routines ..... 12-1  
    What XDR Routines Do ..... 12-1  
    When to Call XDR Routines ..... 12-2  
Quick Reference ..... 12-2  
    Diagnostics ..... 12-13

## **Appendix A Example TCP Client Program**

**Appendix B Example TCP Server Programs**

Standalone TCP Server ..... B-1  
 TCP Server as Part of the MULTINET\_SERVER..... B-4

**Appendix C Example UDP Client Program**

**Appendix D Example UDP Server Programs**

Standalone UDP Server ..... D-1  
 UDP Server as Part of the MULTINET\_SERVER ..... D-3  
 Run-Once UDP Server as Part of the MULTINET\_SERVER..... D-7

**Index**

**Reader's Comments**



---

# Preface

## Purpose of this Guide

This guide describes the programming interfaces provided with the MultiNet software: A socket library based on the UNIX 4.3BSD system calls, and an OpenVMS \$QIO interface. All socket functions documented in this guide are available in the shareable image MULTINET:MULTINET\_SOCKET\_LIBRARY.EXE, included in the standard MultiNet distribution. The include files and example programs are part of the optional *MultiNet Programmers' Kit*, and should be installed as described in the *Installation and Administrator's Guide* before using the programming interface.

If you are writing socket programs in C, Process Software recommends that you use the Compaq C include files for the socket definitions. Your program will then use the TCP/IP Services for VMS-emulation interface in TCPware and MultiNet. The MultiNet header files have been updated to work with more current versions of Compaq C. The MultiNet files should be used only if you are planning to use the MultiNet INETDRIVER API explicitly.

## Document Structure

Read this guide to perform the following tasks:

- Chapter 1, *IP Programming Tutorial*, to write clients and servers that access the network.
- Chapter 2, *Socket Library Functions*, to view detailed information about socket library functions.
- Chapter 3, *\$QIO Interface*, to view detailed information about SYSSQIO calls that you can use to access the network.
- Chapter 4, *SNMP Extensible Agent API Routines*.
- Chapter 5, *RPC Fundamentals*, explains RPC.
- Chapter 6, *Building Distributed Applications With RPC*, explains what components a distributed application contains, how to use RPC to develop a distributed application, step-by-step, and how to get RPC information.
- Chapter 7, *RPCGEN Compiler*, explains the RPC compiler.
- Chapter 8, *RPC RTL Management Routines*.
- Chapter 9, *RPC RTL Client Routines*.

- Chapter 10, *RPC RTL Port Mapper Routines*.
- Chapter 11, *RPC RTL Server Routines*.
- Chapter 12, *RPC RTL XDR Routines*.
- Appendix A, *Example TCP Client Routines*.
- Appendix B, *Example TCP Server Routines*.
- Appendix C, *Example UDP Client Routines*.
- Appendix D, *Example UDP Server Routines*.

This Preface also contains more information in the next sections about getting help directly from Process Software Customer Support.

## Obtaining Customer Support

Process Software provides customer support if you have a current Maintenance Service Agreement. If you obtained MultiNet from an authorized distributor or partner, you receive your customer support directly from them.

You can contact Customer Support by:

- Sending electronic mail (see the section *Sending Electronic Mail*).
- Calling the Customer Support Specialist (see the section *Calling Customer Support*).
- Fax a description of your problem to the Customer Support Group (see the section *Contacting Customer Support by Fax*).

## Before Contacting Customer Support

Before you call, or send e-mail or a fax, please:

- 1 Verify that your Maintenance Service Agreement is current.
- 2 Read the online Release Notes, available either in BookReader format or in `SY$HELP:MULTINETnnn.RELEASE_NOTES` (nnn) is the current MultiNet software version installed on your system.
- 3 Have the following information available:
  - Your name
  - Your company name
  - Your e-mail address
  - Your voice and fax telephone numbers
  - Your Maintenance Agreement Number
  - OpenVMS architecture
  - OpenVMS version
  - MultiNet layered products and versions
- 4 Have complete information about your configuration, error messages that appeared, and problem specifics.

- 5 Be prepared to let an engineer connect to your system either with TELNET or by dialing in using a modem. Be prepared to give the engineer access to a privileged account to diagnose your problem.

You can obtain information about your OpenVMS architecture, OpenVMS version, MultiNet version, and layered products with the MULTINET SHOW /LICENSE command. For example:

```
$ MULTINET SHOW /LICENSE
```

```
Process Software MultiNet V4.4, VAXstation 4000-90, OpenVMS VAX V7.1
```

In this example:

- The machine or system architecture is VAX.
- The OpenVMS version is V7.1.
- The MultiNet version is V4.4.

You can use the following table as a template to record the relevant information about your system.

Required Information	Your System Information
Your name Company name Your e-mail address Your voice and fax telephone numbers System architecture OpenVMS version MultiNet version MultiNet optional software components: - MultiNet NFS Client - MultiNet NFS Server - MultiNet Secure/IP Client - MultiNet Secure/IP Server - TCP/IP applications - Online documentation - MultiNet Programmer's Kit	VAX   Alpha           Installed? Yes   No Installed? Yes   No Installed? Yes   No Installed? Yes   No Installed? Yes   No Installed? Yes   No Installed? Yes   No

## Sending Electronic Mail

For many questions, electronic mail is the preferred communication method. Customer support via electronic mail is available to customers with a current support contract. Send electronic mail to support@process.com

At the beginning of your mail message, include the information listed in the section Before Contacting Customer Support. Continue with the description of your situation and problem specifics. Include all relevant information to help your Customer Support Specialist process and track your electronic support request.

Electronic mail is answered Monday through Thursday from 8:30 a.m. to 7:00 p.m., and on Friday

from 8:30 a.m. to 5:00 p.m. United States Eastern Time.

## Calling Customer Support

For regular support issues, call 800-394-8700 or 508-628-5074 for support Monday through Thursday from 8:30 a.m. to 7:00 p.m., and on Friday from 8:30 a.m. to 5:00 p.m. United States Eastern Time.

For our customers in North America with critical problems, an option for support 7 days per week, 24 hours per day is available at an additional charge. Please contact your account representative for further details.

Before calling, have available the information described in *Before Contacting Customer Support*. When you call, you will be connected to a Customer Support Specialist.

Be prepared to discuss problem specifics with your Customer Support Specialist and to let that person connect to your system.

If a Specialist is not available immediately, your call will be returned as soon as possible.

## Contacting Customer Support by Fax

You can send fax transmissions directly to Customer Support at 508-879-0042.

Before faxing comments or questions, complete the steps in *Before Contacting Customer Support* and include all your system information at the beginning of your fax message. Continue with the description of your situation and problem specifics. Include all relevant information to help your Customer Support Specialist process and track your fax support request.

Faxed questions are answered Monday through Thursday from 8:30 a.m. to 7:00 p.m., and on Friday from 8:30 a.m. to 5:00 p.m. United States Eastern Time.

## Obtaining Online Help

Extensive information about MultiNet is provided in the MultiNet help library. For more information, use the following command:

```
$ HELP MULTINET
```

## MultiNet Frequently Asked Questions List

You can obtain an updated list of frequently asked questions (FAQs) and answers about MultiNet products from the Process Software home page located at <http://www.support.process.com/multinet.html>.

## Accessing the MultiNet Public Mailing List

Process Software maintains two public mailing lists for MultiNet customers:

- **Info-MultiNet@process.com**
- **MultiNet-Announce@process.com**

The **Info-MultiNet@process.com** mailing list is a forum for discussion among MultiNet system managers and programmers. Questions and problems regarding MultiNet can be posted for a response by any of the subscribers. To subscribe to Info-MultiNet, send a mail message with the word “SUBSCRIBE” in the body to Info-MultiNet-request@process.com. The information exchanged over Info-MultiNet is also available via the USENET newsgroup vmsnet.networks.tcp-ip.multinet.

You can retrieve the Info-MultiNet archives by anonymous FTP to ftp.multinet.process.com. The archives are located in the directory [INFO-MULTINET].

You can also find the Info-MultiNet archives on the MultiNet consolidated CD-ROM in the [CONTRIBUTED-SOFTWARE.LIST-ARCHIVES.INFO-MULTINET] directory.

The **MultiNet-Announce@process.com** mailing list is a one-way communication (from Process Software to you) used for the posting of announcements relating to MultiNet (patch releases, product releases, etc.). To subscribe to MultiNet-Announce, send a mail message with the word “SUBSCRIBE” in the body to MultiNet-Announce-request@process.com.

## Process Software World Wide Web Server

Electronic support is provided through the Process Software World Wide Web server, which you can access with any World Wide Web browser; the URL is **http://www.process.com** (select Customer Support).

## Obtaining Software Patches Over the Internet

Process Software provides software patches in save set and ZIP format on its anonymous FTP server, ftp.multinet.process.com. For the location of software patches, read the .WELCOME file in the top-level anonymous directory. This file refers you to the directories containing software patches.

To retrieve a software patch, enter the following commands:

```
$ MULTINET FTP /USERNAME=ANONYMOUS/PASSWORD="emailaddress"
FTP . MULTINET . PROCESS . COM
```

A message welcoming you to the Process Software FTP directory appears next followed by the FTP prompt. Enter the following at the prompts:

```
FTP . MULTINET . PROCESS . COM>
CD [CUSTOMER_SUPPORT.SOFTWARE_UPDATES_VMS.Vnn]
FTP.MULTINET.PROCESS.COM>GET update_filename
```

- *emailaddress* is your e-mail address in the standard *user@host* format.
- *nn* is the version of MultiNet you want to transfer.
- *update\_filename* is the name of the file you want to transfer.

To transfer files from Process Software directly to an OpenVMS system, you can use the GET command without any other FTP commands. However, if you need to transfer a software patch through an intermediate non-OpenVMS system, use BINARY mode to transfer the files to and

from that system.

In addition, if you are fetching the software patch in save set format, make sure the save set record size is 2048 bytes when you transfer the file from the intermediate system to your OpenVMS system:

- If you use the GET command to download the file from the intermediate system, use the FTP **RECORD-SIZE 2048** command before transferring the file.
- If you use the PUT command to upload the file to your OpenVMS system, log into the intermediate system and use the FTP quote site **rms recsize 2048** command before transferring the file.

Process Software also supplies UNZIP utilities for OpenVMS VAX and Alpha for decompressing ZIP archives in the [THIRD\_PARTY\_TOOLS.VMS] directory. To use ZIP format kits, you need a copy of the UNZIP utility.

The following example shows how to use the UNZIP utility, assuming you have copied the appropriate version of UNZIP.EXE to your current default directory.

```
$ UNZIP := $SYS$DISK:[ ]UNZIP.EXE
```

```
$ UNZIP filename.ZIP
```

Use VMSINSTAL to upgrade your MultiNet system with the software patch.

## Typographical Conventions

Examples in this guide use the following conventions:

Convention	Example	Meaning
Bold text	<b>YES</b>	Represents user input in instructions or examples.
Bold, uppercase Courier text	<b>RETURN</b>	Represents a key on your keyboard.
Bold Courier text with a slash	<b>Ctrl/A</b>	Indicates that you holddown the key labeled <b>Control</b> or <b>Ctrl</b> while simultaneously pressing another key; in this example, the "A" key.
A vertical bar within braces	{ ON   OFF }	Indicates a list of values permitted in commands. The vertical bar separates alternatives; do not type the vertical bar in the actual command.
Italicized text	<i>file_name</i>	Represents a variable or placeholder; introduces new terminology or concepts; emphasizes something important; represents the title of a book or publication.

Convention	Example	Meaning
Square brackets	[FULL]	Indicates optional choices; you can enter none of the choices, or as many as you like. When shown as part of an example, square brackets are actual characters you should type.
Underscore or hyphen	<i>file_name</i> or <i>file-name</i>	Between words in commands, indicates the item is a single element.

## Further Reading

The following references contain additional information about programming under TCP/IP. They may be useful in learning more about socket programming. Additional titles of recommended books can be displayed using this command:

```
$ HELP MULTINET BOOKS
```

Comer, Douglas. *Internetworking with TCP/IP: Principles, Protocols, and Architecture*, Englewood Cliffs, NJ: Prentice-Hall, 1988.

Curry, Donald A. *Using C on the UNIX System*, O'Reilly and Associates. 1-800-338-NUTS.

Harspool, R. Nigel. *C Programming in the Berkeley Unix Environment*, Toronto, Canada: Prentice-Hall, 1986.

Kochan, Stephen G. and Patrick K. Wood, editors. *UNIX Networking*, Indianapolis, IN: Hatden Books, 1989.

Leffler, Samuel J., Marshall Kirk McKusick, Michael J. Karels, and John S. Quarterman. *The Design and Implementation of the 4.3BSD UNIX Operating System*, Reading, MA: Addison-Wesley, 1989.

*UNIX Programming Manuals*, U. C. Berkeley.

## Documentation Comments

Your comments about the information in this guide can help us improve the documentation. If you have corrections or suggestions for improvement, please let us know.

Be as specific as possible about your comments: include the exact title of the document, version, date, and page references as appropriate.

You can send your comments by e-mail to: [techpubs@process.com](mailto:techpubs@process.com) or mail the completed form to:

Process Software  
 959 Concord Street  
 Framingham, MA 01701-4682  
 Attention: Marketing Manager

You can also fax the form to us at 508-879-0042.

Your comments about our documentation are appreciated.



# **PART I    MultiNet Programmer's Reference**

---

Chapter 1	MultiNet Programming Tutorial
Chapter 2	Socket Library Functions
Chapter 3	\$QIO Interface
Chapter 4	SNMP Extensible Agent API Routines



## MultiNet Programming Tutorial

This chapter contains short tutorials on various aspects of application programming using MultiNet.

Once you have installed the MultiNet Programmers' Kit, you will find a number of example programs in the appendices in this guide and in the directory `MULTINET_ROOT:[MULTINET.EXAMPLES]`. The following tutorials, together with the example programs, are designed to get you started as an application programmer using MultiNet.

### Sockets

A socket is an endpoint for communication. Two cooperating sockets, one on the local host and one on the remote host, form a connection. Each of the two sockets has a unique address that is described generically by the 16-byte **sockaddr** C programming language structure. The **sockaddr** structure is defined as follows:

```
struct sockaddr {
    u_short sa_family; /* address family */
    char    sa_data[14]; /* up to 14 bytes */
};
```

The **sa\_family** field specifies the address family for the communications domain to which the socket belongs. For example, it can be the constant **AF\_INET** for the Internet family or the constant **AF\_CHAOS** for CHAOSnet addresses. The **sa\_data** field contains up to 14 bytes of data, the interpretation of which depends on the value of **sa\_family**.

If the **sa\_family** field is *AF\_INET*, the same 16- byte **sockaddr** structure can also be interpreted as a **sockaddr\_in** structure that describes an Internet address. A **sockaddr\_in** structure is defined as follows:

```
struct sockaddr_in {
    short    sin_family;
    u_short  sin_port;
    struct   in_addr sin_addr;
```

```
    char    sin_zero[8];
};
```

The **sin\_family** field specifies the address family **AF\_INET**. The **sin\_port** field specifies the TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) port number of the address. Whether the communication uses TCP or UDP is not determined here, but rather by the type of socket created with the **socket()** call: **SOCK\_STREAM** for TCP or **SOCK\_DGRAM** for UDP. The **sin\_addr** field specifies the Internet address. The **sin\_zero** field must be zero. Both the **sin\_port** field and the **sin\_addr** field are in network byte order. See the **htons()** and **htonl()** functions in Chapter 3 for further information about network byte ordering.

The **sockaddr** and **sockaddr\_in** structures serve as input and output to a number of library routines. For example, they may be used as input, specifying the address to which to make a connection or send a packet, or as output, reporting the address from which a connection was made or a packet transmitted.

Internet addresses are normally manipulated with the **gethostbyname()**, **gethostbyaddr()**, **inet\_addr()**, and **inet\_ntoa()** functions. **gethostbyname()** and **inet\_addr()** convert a host name or ASCII representation of an address into the binary representation for the **sockaddr\_in** structure. **gethostbyaddr()** and **inet\_ntoa()** are used to convert the binary representation into the host name or ASCII representation for display.

Port numbers are normally manipulated with the **getservbyname()** and **getservbyport()** functions. **getservbyname()** converts the ASCII service name to the numeric value, and **getservbyport()** converts the numeric value to the ASCII name.

The following example shows a typical program that converts the Internet address and the port into binary representations.

```
#include "multinet_root:[multinet.include.sys]types.h"
#include "multinet_root:[multinet.include.sys]socket.h"
#include "multinet_root:[multinet.include]netdb.h"
#include "multinet_root:[multinet.include.netinet]in.h"

main(argc,argv)
int argc;
char *argv[];
{

    struct sockaddr_in sin;
    struct hostent *hp;
    struct servent *sp;

    /* Zero the sin structure to initialize it */

    bzero((char *) &sin, sizeof(sin));
    sin.sin_family = AF_INET;

    /* Lookup the host and initialize sin_addr */

    hp = gethostbyname(argv[1]);
```

```

    if (!hp) {          /* Perhaps it is an ASCII string */
        sin.sin_addr.s_addr = inet_addr(argv[1]);
    if (sin.sin_addr.s_addr == -1) {
        printf("syntax error in IP address\n");
        exit(1);
    }
} else {              /* Extract the IP address */
    bcopy(hp->h_addr, (char *) &sin.sin_addr,
          hp->h_length);
}

/* Lookup up the name of the SMTP service */

sp = getservbyname("smtp","tcp");
if (!sp) {
    printf("unable to find smtp service");
    exit(1);
}

sin.sin_port = sp->s_port;

/* Now we are ready to create a socket and
pass the address of this sockaddr_in
structure to the connect() call to
connect to the remote SMTP port */
}

```

## TCP Client

A TCP client process establishes a connection to a server and uses the **socket\_read()** and **socket\_write()** functions to transfer data. Typically, you use the following sequence of functions to set up the connection:

- 1 Create a TCP socket: `socket(AF_INET, SOCK_STREAM, 0);`
- 2 Set up a **sockaddr\_in** structure with the address you want to connect to by calling **gethostbyname()** and **getservbyname()**.
- 3 Make a connection to the server with the **connect()** function.
- 4 Once **connect()** completes, the TCP connection is established and you can use **socket\_read()** and **socket\_write()** to transfer data.

Refer to the sample program TCPECHOCLIENT.C in Appendix A and in the *MultiNet Programmers' Kit* examples directory. This program sends data to a server and displays what the server sends back.

## TCP Server

A TCP server process binds a socket to a well-known port and listens on that port for connection attempts. When a connection arrives, the server processes it by transferring data using `socket_read()` and `socket_write()`. Typically, you use the following sequence of functions to set up a server:

- 1 Create a TCP socket: `socket(AF_INET, SOCK_STREAM, 0);`
- 2 Use the `getservbyname()` function to get the port number of the service on which you want to listen for connections.
- 3 Set up a `sockaddr_in` structure with the port number and an Internet address of `INADDR_ANY`, and bind this address to the socket with the `bind()` function.
- 4 Use the `listen()` function to inform the MultiNet kernel that you are listening for connections on this socket. Then wait for a connection and accept it with `accept()`.
- 5 Once `accept()` completes, the TCP connection is established and you can use `socket_read()` and `socket_write()` to transfer data. When you are done with the connection, you can close the channel returned by `accept()` and start a new `accept()` call on the original channel to wait for another connection.

**Note!** When writing a TCP server that will run under the control of the `MultiNet_Server` process, you must assign a channel to `SYS$INPUT` before calling any of the VAX C I/O routines.

Refer to the sample program `TCPECHOSERVER-STANDALONE.C` in Appendix B and in the *MultiNet Programmers' Kit* examples directory for an example of a server program that echoes data sent to it.

Another way to write a TCP server is to let the `MULTINET_SERVER` process do the work for you. The `MULTINET_SERVER` can perform all of the above steps, and when a connection request arrives, can use the OpenVMS system service `$CREPRC` to create a process running your program. Refer to the sample program `TCPECHOSERVER.C` in Appendix B and in the *MultiNet Programmers' Kit* examples directory for an example of how this is done.

## UDP

A UDP program sends and receives packets to and from a remote port using the `send()` or `sendto()` and `recv()` or `recvfrom()` functions. UDP is a connectionless transport protocol. It does not incur the overhead of creating and maintaining a connection between two sockets, but rather merely sends and receives datagrams. It is not a reliable transport, and does not provide guaranteed data delivery, packet ordering, or flow control.

Typically, you use the following sequence of functions in a UDP program:

- 1 Create a UDP socket: `socket(AF_INET, SOCK_DGRAM, 0);`

- 2 Bind the socket to a local port number with the **bind()** function. Specify the **sin\_port** field as 0 (zero) if you want MultiNet to choose an unused port number for you automatically (typical of a client), or specify the **sin\_port** field as the UDP port number (typical of a server). The **sin\_addr** field is usually specified as **INADDR\_ANY**, which means that packets addressed to any of the host's Internet addresses are accepted.
- 3 Optionally, use **connect()** to specify the remote port and Internet address. If you do not use **connect()**, you must use **sendto()** to specify the remote address when you send packets, and **recvfrom()** to learn the address when you receive them.
- 4 Read and write packets to transfer data using the **send()** or **sendto()** and **recv()** or **recvfrom()** functions, respectively.

**Note!** When writing a UDP server that will run under the control of the MultiNet\_Server process, you must assign a channel to SYS\$INPUT before calling any of the VAX C I/O routines.

Another way to write a UDP server is to let the MULTINET\_SERVER process handle the work. The MULTINET\_SERVER can perform all the above steps, and when a packet arrives on a UDP port, can use the OpenVMS system service \$CREPRC to create a process running your program. Refer to the sample programs in Appendix C, Appendix D, and in the *MultiNet Programmers' Kit* examples directory for examples of UDP clients and servers.

## BSD-Specific Tips

The following sections contain information specific to working with BSD code.

### ***BSD Sockets Porting Note***

When porting a program written for BSD sockets to MultiNet, observe the following guidelines:

- Change any *#include* statements to reference files with the same names in the MULTINET\_ROOT:[MULTINET.INCLUDE...] directory areas.
- Implement your change in the source code using *#ifdef* statements to enable the use of MultiNet include files; you can then compile your software in a UNIX environment by selecting the other side of the *#ifdef*.

### ***BSD 4.3 TCP/IP Future Compatibility Considerations***

MultiNet is currently based on the 4.3BSD-tahoe TCP/IP code; however, future releases may be based on the 4.3 BSD TCP/IP code from the University of California at Berkeley. This will entail incompatible changes to the formats of the **sockaddr** and **sockaddr\_in** structure definitions, which may affect certain customer applications and third-party software. This change is to support the variable-length *sockaddr* structures necessary for the ISO protocols.

By taking these changes into account now, you can make applications compatible with both prior and new MultiNet releases.

The current format of the **sockaddr\_in** structure is:

```
struct sockaddr_in {
    short    sin_family;
    u_short  sin_port;
    struct   in_addr sin_addr;
    char     sin_zero[8];
};
```

In the future, the **sin\_family** field will be changed to a single byte, with a **sin\_len** field added. The new format will be:

```
struct sockaddr_in {
    u_char   sin_len;
    u_char   sin_family;
    u_short  sin_port;
    struct   in_addr sin_addr;
    char     sin_zero[8];
};
```

Future versions of MultiNet will accept either format from customer applications, but will return only the new format structures. This affects applications that explicitly check the **sin\_family** field for the value **AF\_INET**. Applications can avoid incompatibilities by avoiding explicit references or checks of the **sin\_family** field, or by assuming that it can be in either format.

Support for the BSD 4.3 style **sockaddr** data structure has been added to the BGDRIVER (UCX interface). If the IO\$M\_EXTEND modifier is set on any one of the following QIO operations, the **sockaddr** parameter passed in these operations is assumed to be in BSD 4.3 format.

- IO\$\_SETMODE/IO\$\_SETCHAR (socket, bind)
- IO\$\_ACCESS (connect, listen)
- IO\$\_SENSEMODE/IO\$\_SENSECHAR (getsockname, getpeername)
- IO\$\_READVBLK (recv\_from, when P3 is specified for a UDP or raw IP message)
- IO\$\_WRITEVBLK (send\_to, when P3 is specified for a UDP or raw IP message)

When the IO\$M\_EXTEND modifier is used in the creation of a socket via IO\$\_SETMODE/IO\$\_SETCHAR (socket, bind), the setting is remembered for the lifetime of the socket and all **sockaddr** structures passed in are assumed to be in BSD 4.3 format. Refer to the *Compaq TCP/IP Services for OpenVMS System Services and C Socket Programming* manual for additional information.

Operations that return a **sockaddr** (READVBLK (recv\_from) like accept, getsockname, and getpeername), return that **sockaddr** in BSD 4.3 format. Operations that accept a **sockaddr** (WRITEVBLK (send\_to) like connect and bind) expect the address family value to be in the position it is in for the BSD 4.3 structure. When a CONNECT/BIND/ACCEPT operation is done for a TCP connection with the IO\$V\_EXTEND bit set, the setting is remembered for the duration of the connection and all specified **sockaddr** structures are expected to be in BSD 4.3 format, and operations returning a **sockaddr** will return it in BSD 4.3 format.

For IO\$\_ACCESS (connect) and IO\$\_SETMODE (bind), if the portion of the **sockaddr** structure that is used to specify the address family in BSD 4.3 format is non-zero, then the **sockaddr** structure is assumed to be in BSD 4.3 format.

# Socket Library Functions

This chapter describes the purpose and format of each MultiNet socket library function.

The socket functions described in this chapter are available in the shareable image `MULTINET:MULTINET_SOCKET_LIBRARY.EXE`, included in the standard MultiNet distribution. The include files and example programs are part of the optional MultiNet Programmers' Kit, and should be installed as described in the *Installation and Administrator's Guide* before you use the programming interface.

In addition to supporting the MultiNet socket library, applications developed for the Compaq OpenVMS/ULTRIX Connection (UCX) software using the VAX C socket library (`UCX$IPC.OLB`) will run over MultiNet, using an emulation of `UCX$IPC_SHR.EXE`.

**Note!** To avoid potential conflicts between MultiNet socket library definitions and C compiler definitions, include a reference to the file `MULTINET_ROOT:[MULTINET.INCLUDE.SYS]TYPES.H` before any other header file references.

## AST Reentrancy

The MultiNet socket library is based on the equivalent UNIX programming library, and was therefore not designed with reentrancy in mind. If you call into the socket library with AST delivery disabled, some of the library routines will suspend execution and fail to return control to the caller.

This situation occurs most often when applications try to call those functions from within an AST routine where AST delivery is not possible.

Any routine that relies on the `select()` function is subject to this restriction (including the `select()` call itself, and most of the domain name resolution routines such as `gethostbyname()`, and so on).

Another reentrancy consideration is the socket library's use of static internal data structures, some of which are passed back to the application, as in the case of the `hostent` structure address returned by `gethostbyname()`. Other functions use these data structures internally to maintain context.

In either case, it is dangerous to call into these routines from an AST because it is possible to

interrupt a similar call already in progress, using the same static buffer, thereby corrupting the contents of the buffer.

Another consideration is the use of routines that send and receive data. Every socket in the kernel contains two fixed-size buffers for sending and receiving data. If an application tries to transmit data when there is insufficient buffer space, that call will block (or suspend execution) until buffer space becomes available. This can become an issue if the application blocks while attempting to transmit a large data buffer, and an AST routine tries to transmit a small data buffer. The small data buffer is transmitted before the large one.

The same situation applies to the functions that read data from the network. This situation may also arise if multiple reads and writes are performed on sockets which have been set up to be non-blocking (NBIO).

These considerations might seem overly restrictive; however, the MultiNet socket library is a port of the BSD socket library, which is subject to all of the same restrictions. Applications which need to perform I/O from within AST routines should use the SYS\$QIO system service to talk directly to the MultiNet device driver.

Therefore, *none* of the socket routines should be considered AST reentrant.

## accept()

Extracts the first connection from the queue of pending connections on a socket, creates a new socket with the same properties as the original socket, and assigns a new OpenVMS channel to the new socket. If no pending connections are present on the queue, **accept()** blocks the caller until a new connection is present. The original socket remains open and can be used to accept more connections, but the new socket cannot be used to accept additional connections.

The original socket is created with the **socket()** function, bound to an address with **bind()**, and is listening for connections after a **listen()**.

The **accept()** function is used with connection-based socket types. Currently the only connection-based socket is **SOCK\_STREAM**, which, together with **AF\_INET**, constitutes a TCP socket.

### FORMAT

```
New_VMS_Channel = accept(VMS_Channel, Address, AddrLen);
short New_VMS_Channel, VMS_Channel;
struct sockaddr *Address;
unsigned int *AddrLen;
```

### ARGUMENTS

#### VMS\_Channel

VMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the original socket from which to accept the connection.

#### Address

VMS Usage: **socket\_address**  
 type: **struct sockaddr**  
 access: **write only**  
 mechanism: **by reference**

The optional Address argument is a result parameter. It is filled in with the address of the connecting entity, as known to the communications layer. The exact format of the Address argument is determined by the domain in which the communication is occurring.

#### AddrLen

VMS Usage: **socket\_address\_length**  
 type: **longword (unsigned)**  
 access: **modify**  
 mechanism: **by reference**

On entry, the optional **AddrLen** argument contains the length of the space pointed to by **Address**,

in bytes. On return, it contains the actual length, in bytes, of the address returned.

## RETURNS

If the **accept()** is successful, an OpenVMS channel number is returned. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vmserro**.

An error code of ENETDOWN can indicate that the program has run out of VMS channels to use in creating new sockets. This can be due to either the SYSGEN parameter CHANNELCNT being too low for the number of connections in use by the program, or to a socket leak in the code. Make sure the code closes the socket (using **close()**) when it is done with the socket.

## bcmp()

Compares a range of memory. This function operates on variable-length strings of bytes and does not check for null bytes as **strcmp()** does.

**bcmp()** is part of the 4.3BSD run-time library, but is not provided by Compaq Computer as part of the VAX C run-time library. It is provided here for compatibility with the 4.3BSD library.

### FORMAT

```
Status = bcmp(String1, String2, Length);  
char *String1, *String2;  
unsigned int Length;
```

### ARGUMENTS

#### **String1,String2**

VMS Usage:     **arbitrary**  
type:           **byte buffer**  
access:         **read only**  
mechanism:      **by reference**

Pointers to the two buffers to be compared.

#### **Length**

VMS Usage:     **longword\_unsigned**  
type:           **longword (unsigned)**  
access:         **read only**  
mechanism:      **by value**

The number of bytes to be compared.

### RETURNS

The **bcmp()** function returns zero if the strings are identical. It returns a nonzero value if they are different.

## bcopy()

Copies memory from one location to another. This function operates on variable-length strings of bytes and does not check for null bytes as **strecpy()** does.

**bcopy()** is part of the 4.3BSD run-time library, but is not provided by Compaq Computer as part of the VAX C run-time library. It is provided here for compatibility with the 4.3BSD library.

### FORMAT

```
(void) bcopy(String1, String2, Length);  
char *String1, *String2;  
unsigned int Length;
```

### ARGUMENTS

#### **String1**

VMS Usage	<b>arbitrary</b>
type:	<b>byte buffer</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

The source buffer for the copy operation.

#### **String2**

VMS Usage:	<b>arbitrary</b>
type:	<b>byte buffer</b>
access:	<b>write only</b>
mechanism:	<b>by reference</b>

The destination buffer for the copy operation.

#### **Length**

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The number of bytes to be copied.

## bind()

Assigns an address to an unnamed socket. When a socket is created with **socket()**, it exists in a name space (address family) but has no assigned address. **bind()** requests that the address be assigned to the socket.

If the port number specified in the **sin\_port** field of the **sockaddr** structure is less than 1024, **SYSPRV** is required to use this function.

### FORMAT

```
Status = bind(VMS_Channel, Name, NameLen);
short VMS_Channel;
struct sockaddr *Name;
unsigned int NameLen;
```

### ARGUMENTS

<b>VMS_Channel</b>	
VMS Usage:	<b>channel</b>
type:	<b>word (signed)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

A channel to the socket.

<b>Name</b>	
VMS Usage:	<b>socket_address</b>
type:	<b>struct sockaddr</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

The address to which the socket should be bound. The exact format of the **Address** argument is determined by the domain in which the socket was created.

<b>NameLen</b>	
VMS Usage:	<b>socket_address_length</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The length of the Name argument, in bytes.

### RETURNS

If the **bind()** is successful, a value of 0 is returned. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vmserro**.

## **bzero()**

Fills memory with zeros.

**bzero()** is part of the 4.3BSD run-time library, but is not provided by Compaq Computer as part of the VAX C run-time library. It is provided here for compatibility with the 4.3BSD library.

### **FORMAT**

```
(void) bzero(String, Length);  
char *String;  
unsigned int Length;
```

### **ARGUMENTS**

#### **String**

VMS Usage: **arbitrary**  
type: **byte buffer**  
access: **write only**  
mechanism: **by reference**

The address of the buffer to receive the zeros.

#### **Length**

VMS Usage: **longword\_unsigned**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The number of bytes to be zeroed.

## connect()

When used on a **SOCK\_STREAM** socket, **connect()** attempts to make a connection to another socket. This function, when used on a **SOCK\_DGRAM** socket, permanently specifies the peer to which datagrams are sent to and received from. The peer socket is specified by name, which is an address in the communications domain of the socket. Each communications domain interprets the name parameter in its own way. If the address of the local socket has not yet been specified with **bind()**, the local address is also set to an unused port number when **connect()** is called.

### FORMAT

```
Status = connect(VMS_Channel, Name, NameLen);
short VMS_Channel;
struct sockaddr *Name;
unsigned int NameLen;
```

### ARGUMENTS

#### VMS\_Channel

VMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the socket.

#### Name

VMS Usage: **socket\_address**  
 type: **struct sockaddr**  
 access: **read only**  
 mechanism: **by reference**

The address of the peer to which the socket should be connected. The exact format of the **Address** argument is determined by the domain in which the socket was created.

#### NameLen

VMS Usage: **socket\_address\_length**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by value**

The length of the **Name** argument, in bytes.

### RETURNS

If the **connect()** is successful, a value of 0 is returned. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vmserro**.

## Domain Name Resolver Routines

The following functions exist for compatibility with UNIX 4.3BSD programs that call the DNS Name Resolver directly rather than through **gethostbyname()**. The arguments and calling conventions are compatible with BIND Version 4.8.3. They are subject to change and are not documented here.

The `h_errno` variable in the MultiNet socket library that contains the error status of the resolver routine is accessible to C programs.

<b>dn_comp()</b>	<b>p_rr()</b>
<b>dn_expand()</b>	<b>p_type()</b>
<b>dn_skip()</b>	<b>putlong()</b>
<b>dn_skipname()</b>	<b>putshort()</b>
<b>fp_query()</b>	<b>_res_close()</b>
<b>_getlong()</b>	<b>res_init()</b>
<b>_getshort()</b>	<b>res_mkquery()</b>
<b>herror()</b>	<b>res_query()</b>
<b>p_cdname()</b>	<b>res_querydomain()</b>
<b>p_class()</b>	<b>res_search()</b>
<b>p_query()</b>	<b>res_send()</b>

## **endhostent()**

Tells the DNS Name Resolver to close the TCP connection to the DNS Name Server that may have been opened as the result of calling **sethostent()** with **StayOpen** set to 1.

### **FORMAT**

(void) endhostent();

## **endnetent()**

Tells the DNS Name Resolver to close the TCP connection to the DNS Name Server that may have been opened as the result of using **setnetent()** with **StayOpen** set to 1.

### **FORMAT**

(void) endnetent();

## **endprotoent()**

Tells the host table routines that the scan started by **getprotoent()** is complete. **endprotoent()** is provided only for compatibility with UNIX 4.3BSD, and is ignored by the MultiNet software.

### **FORMAT**

(void) endprotoent();

## **endservent()**

Tells the host table routines that the scan started by **getservent()** is complete. **endservent()** is provided only for compatibility with UNIX 4.3BSD, and is ignored by the MultiNet software.

### **FORMAT**

(void) endservent();

## **getdtablesize()**

Returns the maximum number of channels available to a process. This function is normally used to determine the **Width** argument to the **select()** function.

### **FORMAT**

Width = getdtablesize();

### **RETURNS**

The size of the channel table.

## gethostbyaddr()

Looks up a host by its address in the binary host table or the DNS Name Server and returns information about that host. An alternate entry point **\_gethostbyaddr()**, that looks only in the binary host table, is also available.

**Note!** The MultiNet socket library is not reentrant. If you call into it from an AST (interrupt) routine, the results are unpredictable.

### FORMAT

```
(struct hostent *) gethostbyaddr(Addr, Length, Family);  
(struct hostent *) _gethostbyaddr(Addr, Length, Family);  
char *Addr;  
unsigned int Length;  
unsigned int Family;
```

### ARGUMENTS

#### **Addr**

VMS Usage: **address**  
type: **dependent on Family**  
access: **read only**  
mechanism: **by reference**

A pointer to the address to look up. The type is dependent on the **Family** argument. For Internet (**AF\_INET** family) addresses, **Addr** is a pointer to an **in\_addr** structure.

#### **Length**

VMS Usage: **address\_length**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The size, in bytes, of the buffer pointed to by **Addr**.

#### **Family**

VMS Usage: **address\_family**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The address family, and consequently the interpretation of the **Addr** argument. Normally, this is **AF\_INET**, indicating the Internet family of addresses.

### RETURNS

If **gethostbyaddr()** succeeds, it returns a pointer to a structure of type **hostent**. (See

**gethostbyname()** for more information on the hostent structure.) If this function fails, a value of 0 is returned, and the global variable **h\_errno** is set to one of the DNS Name Server error codes defined in the file **multinet\_root:[multinet.include]netdb.h**.

## gethostbyname()

Looks up a host by name in the binary host table or the DNS Name Server and returns information about that host. An alternate entry point **\_gethostbyname()**, that looks only in the binary host table, is also available.

**Note!** The MultiNet socket library is not reentrant. If you call into it from an AST (interrupt) routine, the results are unpredictable.

### FORMAT

```
(struct hostent *) gethostbyname(Name);
(struct hostent *) _gethostbyname(Name);
char *Name;
```

### ARGUMENTS

<b>Name</b>	
VMS Usage:	<b>host_name</b>
type:	<b>ASCIZ string</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A C-language string containing the name of the host to look up.

### RETURNS

If **gethostbyname()** succeeds, it returns a pointer to a structure of type **hostent**. If this function fails, a value of 0 is returned, and the global variable **h\_errno** is set to one of the DNS Name Server error codes defined in the file **multinet\_root:[multinet.include]netdb.h**.

The **hostent** structure is defined as follows:

```
struct hostent {
    char    *h_name;           /* official name */
    char    **h_aliases;      /* alias list */
    int     h_addrtype;       /* host address type */
    int     h_length;         /* length of address */
    char    **h_addr_list;    /* list of addresses */
#define h_addr h_addr_list[0] /* address, for compat */
    char    *h_cputype;       /* cpu type */
    char    *h_opsys;         /* operating system */
    char    **h_protos;       /* protocols */
    struct  sockaddr *h_addresses; /* sockaddr form */
};
```

## gethostbysockaddr()

Looks up a host by socket address in the binary host table or the DNS Name Server and returns information about that host. An alternate entry point `_gethostbysockaddr()`, that looks only in the binary host table, is also available. `gethostbysockaddr()` is identical in functionality to `gethostbyaddr()`, but takes its arguments in a different form.

**Note!** The MultiNet socket library is not reentrant. If you call into it from an AST (interrupt) routine, the results are unpredictable.

### FORMAT

```
(struct hostent *) gethostbysockaddr(Addr, Length);
struct sockaddr *Addr;
unsigned int Length;
```

### ARGUMENTS

#### Addr

VMS Usage:       **socket\_address**  
 type:            **struct sockaddr**  
 access:          **read only**  
 mechanism:       **by reference**

A pointer to a **sockaddr** structure describing the address to look up.

#### Length

VMS Usage:       **socket\_address\_length**  
 type:            **longword (unsigned)**  
 access:          **read only**  
 mechanism:       **by value**

The size, in bytes, of the **sockaddr** structure pointed to by **Addr**.

### RETURNS

If `gethostbysockaddr()` succeeds, it returns a pointer to a structure of type **hostent**. (See `gethostbyname()` for more information on the **hostent** structure.) If this function fails, a value of 0 is returned, and the global variable **h\_errno** is set to one of the DNS Name Server error codes defined in the file **multinet\_root:[multinet.include]netdb.h**.

## gethostname()

Returns the Internet name of the host it is executed on. This name comes from the logical name MULTINET\_HOST\_NAME and can be set using the SET HOST-NAME command in the MultiNet Network Configuration utility (NET-CONFIG).

### FORMAT

```
Status = gethostname(String, Length);  
char *String;  
unsigned int Length;
```

### ARGUMENTS

**String**

VMS Usage:	<b>hostname</b>
type:	<b>ASCIZ string</b>
access:	<b>write only</b>
mechanism:	<b>by reference</b>

A pointer to a buffer to receive the host name.

**Length**

VMS Usage:	<b>hostname_length</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The length of the buffer, in bytes. The buffer should be at least 33 bytes long to guarantee that the complete host name is returned.

### RETURNS

If the **gethostname()** function is successful, it returns a 0. It returns a -1 if it is unable to translate the logical name.

## getnetbyaddr()

Looks up a network by its network number in the binary host table or the DNS Name Server and returns information about that network. An alternate entry point `_getnetbyaddr()`, that looks only in the binary host table, is also available.

### FORMAT

```
(struct netent *) getnetbyaddr(Net, Protocol);
(struct netent *) _getnetbyaddr(Net, Protocol);
unsigned int Net, Protocol;
```

### ARGUMENTS

#### Net

VMS Usage: **network\_number**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by value**

The network number to look up.

#### Protocol

VMS Usage: **protocol\_number**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by value**

The address family of the network to look up. For Internet networking, this should be specified as `AF_INET`.

### RETURNS

If `getnetbyaddr()` succeeds, it returns a pointer to a structure of type **netent**. (See `getnetbyname()` for more information on the `netent` structure.) If this function fails, a value of 0 is returned, and the global variable `h_errno` is set to one of the DNS Name Server error codes defined in `multinet_root:[multinet.include]netdb.h`.

## getnetbyname()

Looks up a network by name in the binary host table or the DNS Name Server and returns information about that network. An alternate entry point **\_getnetbyname()**, that looks only in the binary host table, is also available.

### FORMAT

```
(struct netent *) getnetbyname(Name);
(struct netent *) _getnetbyname(Name);
char *Name;
```

### ARGUMENTS

<b>Name</b>	
VMS Usage:	<b>network_name</b>
type:	<b>ASCII string</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to a C-language string containing the name of the network.

### RETURNS

If **getnetbyname()** succeeds, it returns a pointer to a structure of type **netent**. If this function fails, a value of 0 is returned, and the global variable **h\_errno** is set to one of the DNS Name Server error codes defined in **multinet\_root:[multinet.include]netdb.h**.

The **netent** structure is defined as follows:

```
struct netent {
    char      *n_name;          /* official name */
    char      **n_aliases;     /* alias list */
    int       n_addrtype;      /* address type */
    unsigned long n_net;       /* network # */
    struct sockaddr *n_addresses; /* sockaddr form */
};
```

## getpeername()

Returns the name of the peer connected to the specified socket.

### FORMAT

```
Status = getpeername(VMS_Channel, Address, AddrLen);
short VMS_Channel;
struct sockaddr *Address;
unsigned int *AddrLen;
```

### ARGUMENTS

#### VMS\_Channel

VMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the socket.

#### Address

VMS Usage: **socket\_address**  
 type: **struct sockaddr**  
 access: **write only**  
 mechanism: **by reference**

A result parameter. This argument is filled in with the address of the peer, as known to the communications layer. The exact format of the **Address** argument is determined by the domain in which the communication is occurring.

#### AddrLen

VMS Usage: **socket\_address\_length**  
 type: **longword (unsigned)**  
 access: **modify**  
 mechanism: **by reference**

On entry, contains the length of the space pointed to by **Address**, in bytes. On return, it contains the actual length, in bytes, of the address returned.

### RETURNS

If the **getpeername()** is successful, a value of 0 is returned. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vm serrno**.

## getprotobyname()

Looks up a protocol by name in the binary host table and returns information about that protocol.

### FORMAT

```
(struct protoent *) getprotobyname(Name);  
char *Name;
```

### ARGUMENTS

<b>Name</b>	
VMS Usage:	<b>protocol_name</b>
type:	<b>ASCIZ string</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to a C-language string containing the name of the protocol.

### RETURNS

If **getprotobyname()** succeeds, it returns a pointer to a structure of type **protoent**. If this function fails, a value of 0 is returned.

The **protoent** structure is defined as follows:

```
struct protoent {  
    char    *p_name;      /* official protocol name */  
    char    **p_aliases; /* alias list */  
    int     p_proto;     /* protocol # */  
};
```

## getprotobynumber()

Looks up a protocol by number in the binary host table and returns information about that protocol.

### FORMAT

```
(struct protoent *) getprotobynumber(Number);
unsigned int Number;
```

### ARGUMENTS

<b>Number</b>	
VMS Usage:	<b>protocol_number</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The numeric value of the protocol.

### RETURNS

If **getprotobynumber()** succeeds, it returns a pointer to a structure of type **protoent**. If this function fails, a value of 0 is returned.

The **protoent** structure is defined as follows:

```
struct protoent {
    char    *p_name;        /* official protocol name */
    char    **p_aliases;   /* alias list */
    int     p_proto;       /* protocol # */
};
```

## getprotoent()

Returns the next protocol entry from the binary host table. It is used with **setprotoent()** and **endprotoent()** to scan through the protocol table. The scan is initialized with **setprotoent()**, run by calling **getprotoent()** until it returns a 0, and terminated by calling **endprotoent()**.

### FORMAT

```
(struct protoent *) getprotoent();
```

### RETURNS

The **getprotoent()** function returns either a 0, indicating that there are no more entries, or a pointer to a structure of type **protoent**.

The **protoent** structure is defined as follows:

```
struct protoent {
    char    *p_name;      /* official protocol name */
    char    **p_aliases; /* alias list */
    int     p_proto;     /* protocol # */
};
```

## getservbyname()

Looks up a service by name in the binary host table and returns information about that service.

The service must be present in the HOSTS.SERVICES or HOSTS.LOCAL file, and the host table must be compiled into binary form using the host table compiler. See the *MultiNet for OpenVMS Administrator's Guide* for more information about editing and compiling the host table files.

### FORMAT

```
(struct servent *) getservbyname(Name, Protocol);
char *Name, *Protocol;
```

### ARGUMENTS

#### Name

VMS Usage: **service\_name**  
 type: **ASCIZ string**  
 access: **read only**  
 mechanism: **by reference**

A pointer to a C-language string containing the name of the service.

#### Protocol

VMS Usage: **protocol\_name**  
 type: **ASCIZ string**  
 access: **read only**  
 mechanism: **by reference**

A pointer to a C-language string containing the name of the protocol associated with the service, such as "TCP".

### RETURNS

If **getservbyname()** succeeds, it returns a pointer to a structure of type **servent**. If this function fails, a value of 0 is returned.

The **servent** structure is defined as follows:

```
struct servent {
    char    *s_name;           /* official service name */
    char    **s_aliases;      /* alias list */
    int     s_port;           /* port # */
    char    *s_proto;         /* protocol to use */
};
```

## getservbyport()

Looks up a service by protocol port in the binary host table and returns information about that service.

The service must be present in the HOSTS.SERVICES or HOSTS.LOCAL file, and the host table must be compiled into binary form using the host table compiler. See the *MultiNet for OpenVMS Administrator's Guide* for more information about editing and compiling the host table files.

### FORMAT

```
(struct servent *) getservbyport(Number, Protocol);  
unsigned int Number;  
char *Protocol;
```

### ARGUMENTS

#### Number

VMS Usage:	<b>service_number</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The numeric value of the service port.

#### Protocol

VMS Usage:	<b>protocol_name</b>
type:	<b>ASCIZ string</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to a C-language string containing the name of the protocol associated with the service, such as "TCP".

### RETURNS

If **getservbyport()** succeeds, it returns a pointer to a structure of type **servent**. (See **getservbyname()** for the format of the **servent** structure.) If this function fails, a value of 0 is returned.

## getservent()

Returns the next server entry from the binary host table. This function is used with **setservent()** and **endservent()** to scan through the service table. The scan is initialized with **setservent()**, run by calling **getservent()** until it returns a 0, and terminated by calling **endservent()**.

### FORMAT

(struct servent \*) getservent();

### RETURNS

If **getservbyport()** succeeds, it returns a pointer to a structure of type **servent**. (See **getservbyname()** for the format of the **servent** structure.) If this function fails, a value of 0 is returned.

## getsockname()

Returns the current name of the specified socket.

### FORMAT

```
Status = getsockname(VMS_Channel, Address, AddrLen);
short VMS_Channel;
struct sockaddr *Address;
unsigned int *AddrLen;
```

### ARGUMENTS

#### **VMS\_Channel**

VMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

#### **Address**

VMS Usage: **socket\_address**  
type: **struct sockaddr**  
access: **write only**  
mechanism: **by reference**

A result parameter. It is filled in with the address of the local socket, as known to the communications layer. The exact format of the **Address** argument is determined by the domain in which the communication is occurring.

#### **AddrLen**

VMS Usage: **socket\_address\_length**  
type: **longword (unsigned)**  
access: **modify**  
mechanism: **by reference**

On entry, contains the length of the space pointed to by **Address**, in bytes. On return, it contains the actual length, in bytes, of the address returned.

### RETURNS

If **getsockname()** is successful, a value of 0 is returned. If an error occurs, a value of -1 is returned and a more specific message is returned in the global variables **socket\_errno** and **vm serrno**.

## getsockopt()

Retrieves the options associated with a socket. Options can exist at multiple protocol levels; however, they are always present at the uppermost socket level.

When manipulating socket options, you must specify the level at which the option resides and the name of the option. To manipulate options at the socket level, specify **Level** as **SOL\_SOCKET**. To manipulate options at any other level, specify the protocol number of the appropriate protocol controlling the option. For example, to indicate that an option will be interpreted by the TCP protocol, set **Level** to the protocol number of TCP, which can be determined by calling **getprotobyname()**.

**OptName** and any specified options are passed without modification to the appropriate protocol module for interpretation. The include file **multinet\_root:[multinet.include.sys]socket.h** contains definitions for socket-level options. Options at other protocol levels vary in format and name.

For more information on what socket options may be retrieved with **getsockopt()**, see **socket options**.

### FORMAT

```
Status = getsockopt(VMS_Channel, Level, OptName, OptVal, OptLen);
short VMS_Channel;
unsigned int Level, OptName, *OptLen;
char *OptVal;
```

### ARGUMENTS

**VMS\_Channel**  
VMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

**Level**  
VMS Usage: **option\_level**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The protocol level at which the option will be manipulated. Specify **Level** as **SOL\_SOCKET**, or as a protocol number as returned by **getprotobyname()**.

**OptName**  
VMS Usage: **option\_name**  
type: **longword (unsigned)**

access: **read only**  
mechanism: **by value**

The option to be manipulated.

**OptVal**  
VMS Usage: **dependent on OptName**  
type: **byte buffer**  
access: **write only**  
mechanism: **by reference**

A pointer to a buffer that will receive the current value of the option. The format of this buffer is dependent on the option requested.

**OptLen**  
VMS Usage: **option\_length**  
type: **longword (unsigned)**  
access: **modify**  
mechanism: **by reference**

On entry, contains the length of the space pointed to by **OptVal**, in bytes. On return, it contains the actual length, in bytes, of the option returned.

## RETURNS

If the **getsockopt()** is successful, a value of 0 is returned. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vm serrno**.

## gettimeofday()

Returns the current time of day in UNIX format. This is the number of seconds and microseconds elapsed since January 1, 1970.

**gettimeofday()** is part of the 4.3BSD run-time library, but is not provided by Compaq Computer as part of the VAX C run-time library. It is provided here for compatibility with the 4.3BSD library.

### FORMAT

```
Status = gettimeofday(TimeVal);
struct timeval *TimeVal;
```

### ARGUMENTS

<b>TimeVal</b>	
VMS Usage:	<b>UNIX_time</b>
type:	<b>struct timeval</b>
access:	<b>write only</b>
mechanism:	<b>by reference</b>

A pointer to a structure that receives the current time. The timeval structure is defined as follows:

```
struct timeval {
    long    tv_sec;        /* seconds */
    long    tv_usec;      /* and microseconds */
};
```

### RETURNS

The **gettimeofday()** function always returns a value of 0, which indicates it was successful.

## hostalias()

Examines the user-specific host alias table (if the user has set one by defining the `MULTINET_HOSTALIASES` logical name) to see if the specified host name is a valid alias for another host name. This is normally called by `gethostbyname()` and `res_search()` automatically.

### FORMAT

```
(char *) hostalias(Name);  
char *Name;
```

### ARGUMENTS

<b>Name</b>	
VMS Usage:	<b>host_name</b>
type:	<b>ASCIZ string</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A C-language string containing the name of the host to look up in the host alias table.

### RETURNS

If successful, the `hostalias()` function returns a pointer to the character string of the canonical name of the host. Otherwise, it returns a 0 to indicate that no alias exists.

## htonl()

Swaps the byte order of a four-byte integer from OpenVMS byte order to network byte order. This allows you to develop programs that are independent of the hardware architecture on which they are running.

### FORMAT

```
RetVal = htonl(Val);  
unsigned long Val;
```

### ARGUMENTS

<b>Val</b>	
VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The four-byte integer to convert to network byte order.

### RETURNS

The **htonl()** function returns the byte-swapped integer that corresponds to **Val**. For example, if **Val** is 0xc029e401, the returned value is 0x01e429c0.

## htons()

Swaps the byte order of a two-byte integer from OpenVMS byte order to network byte order. This allows you to develop programs that are independent of the hardware architecture on which they are running.

### FORMAT

```
RetVal = htons(Val);  
unsigned short Val;
```

### ARGUMENTS

<b>Val</b>	
VMS Usage:	<b>word_unsigned</b>
type:	<b>word (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The two-byte integer to convert to network byte order.

### RETURNS

The **htons()** function returns the byte-swapped integer that corresponds to **Val**. For example, if **Val** is 0x0017, the returned value is 0x1700.

## inet\_addr()

Converts Internet addresses represented in the ASCII form "xx.yy.zz.ww" to a binary representation in network byte order.

### FORMAT

```
RetVal = inet_addr(Address);  
char *Address;
```

### ARGUMENTS

<b>Address</b>	
VMS Usage:	<b>internet_address_string</b>
type:	<b>ASCIZ string</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to a C-language string containing an ASCII representation of the Internet address to convert.

### RETURNS

If successful, the **inet\_addr()** function returns an integer corresponding to the binary representation of the Internet address in network byte order. It returns a -1 to indicate that it could not parse the specified **Address** string.

## inet\_inaof()

Returns the local network address portion of the specified Internet address. For example, the class A address 0x0a050010 (10.5.0.16) is returned as 0x00050010 (5.0.16).

### FORMAT

```
RetVal = inet_inaof(Address);  
struct in_addr Address;
```

### ARGUMENTS

<b>Address</b>	
VMS Usage:	<b>internet_address</b>
type:	<b>struct in_addr</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The Internet address from which to extract the local network address portion. The Internet address is specified in network byte order.

### RETURNS

The **inet\_inaof()** function returns the local network address portion of the Internet address in OpenVMS byte order.

## inet\_makeaddr()

Builds a complete Internet address from the separate host and network portions.

### FORMAT

```
RetVal = inet_makeaddr(Network, Host);  
unsigned int Network, Host;
```

### ARGUMENTS

#### Network

VMS Usage:	<b>network_number</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The network portion of the Internet address to be constructed. The network portion is specified in OpenVMS byte order.

#### Host

VMS Usage:	<b>host_number</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The host portion of the Internet address to be constructed. The host portion is specified in OpenVMS byte order.

### RETURNS

The **inet\_makeaddr()** function returns the complete Internet address in network byte order.

## **inet\_netof()**

Returns the network number portion of the specified Internet address. For example, the class A address 0x0a050010 (10.5.0.16) is returned as 0x0a (10).

### **FORMAT**

```
RetVal = inet_netof(Address);  
struct in_addr Address;
```

### **ARGUMENTS**

**Address**

VMS Usage:	<b>internet_address</b>
type:	<b>struct in_addr</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The Internet address from which to extract the network number portion. The Internet address is specified in network byte order.

### **RETURNS**

The **inet\_netof()** routine returns the network portion of the Internet address in OpenVMS byte order.

## inet\_network()

Interprets Internet network numbers represented in the ASCII form "xx", "xx.yy", or "xx.yy.zz", and converts them into a binary representation in OpenVMS byte order.

### FORMAT

```
RetVal = inet_network(Address);  
char *Address;
```

### ARGUMENTS

**Address**

VMS Usage:	<b>network_address_string</b>
type:	<b>ASCIZ string</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to a C-language string containing an ASCII representation of the Internet network number to convert.

### RETURNS

If successful, the **inet\_network()** function returns an integer corresponding to the binary representation of the Internet network in OpenVMS byte order. It returns a -1 to indicate that it could not parse the specified string.

## **inet\_ntoa()**

Converts an Internet address represented in binary form into an ASCII string suitable for printing.

### **FORMAT**

```
(char *) inet_ntoa(Address);  
struct in_addr Address;
```

### **ARGUMENTS**

<b>Address</b>	
VMS Usage:	<b>internet_address</b>
type:	<b>struct in_addr</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The Internet address in binary form. The Internet address is specified in network byte order.

### **RETURNS**

The **inet\_ntoa()** function returns a pointer to a C- language string corresponding to the Internet address.

## klread()

Used with **klseek()** and **multinet\_kernel\_nlist()** to emulate the UNIX 4.3BSD **nlist()** function and the reading of the **/dev/kmem** device. **klread()** and **klseek()** read OpenVMS kernel memory through an interface that is similar to using **read()** and **lseek()** on the **/dev/kmem** device.

The OpenVMS CMKRNL privilege is required to use **klread()**.

Before calling **klread()**, specify the address to read from using **klseek()**.

### FORMAT

```
Status = klread(Buffer, Size);
char *Buffer;
unsigned int Size;
```

### ARGUMENTS

#### **Buffer**

VMS Usage:     **arbitrary**  
type:           **byte buffer**  
access:         **write only**  
mechanism:      **by reference**

The address to which to return the kernel memory.

#### **Size**

VMS Usage:     **longword\_unsigned**  
type:           **longword (unsigned)**  
access:         **read only**  
mechanism:      **by value**

The number of bytes to read.

### RETURNS

If successful, the **klread()** function returns the number of bytes read. It returns a -1 to indicate that it failed because the kernel memory was not readable. This usually indicates that the current position, as set by **klseek()**, is invalid.

## klseek()

Used with **klread()** and **multinet\_kernel\_nlist()** to emulate the UNIX 4.3BSD **nlist()** function and reading the **/dev/kmem** device. **klread()** and **klseek()** read OpenVMS kernel memory through an interface that is similar to using **read()** and **lseek()** on the **/dev/kmem** device.

Use **klseek()** to set the current position in the network kernel. This position will be used by **klread()** and **klwrite()** in the next attempt to read or write data.

### FORMAT

```
Status = klseek(Position);  
unsigned int Position;
```

### ARGUMENTS

<b>Position</b>	
VMS Usage:	<b>kernel_address</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The address in the network kernel to make the current position for the next **klread()** or **klwrite()** call.

### RETURNS

The **klseek()** routine returns the current position as a success status.

## klwrite()

Used with **klseek()** and **multinet\_kernel\_nlist()** to emulate the UNIX 4.3BSD **nlist()** and writing the **/dev/kmem** device. **klwrite()** and **klseek()** write OpenVMS kernel memory through an interface that is similar to using **write()** and **lseek()** on the **/dev/kmem** device.

The OpenVMS CMKRNL privilege is required to use **klwrite()**.

Before calling **klwrite()**, specify the address to write using **klseek()**.

### FORMAT

```
Status = klwrite(Buffer, Size);
char *Buffer;
unsigned int Size;
```

### ARGUMENTS

#### Buffer

VMS Usage:	<b>arbitrary</b>
type:	<b>byte buffer</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

The address of the data to write into kernel memory.

#### Size

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The number of bytes to write.

### RETURNS

If successful, the **klwrite()** function returns the number of bytes written. It returns a -1 to indicate that it failed because the kernel memory was not writeable. This usually indicates that the current position, as set by **klseek()**, is invalid.

## listen()

Specifies the number of incoming connections that may be queued waiting to be accepted. This backlog must be specified before accepting a connection on a socket. The **listen()** function applies only to sockets of type **SOCK\_STREAM**.

### FORMAT

```
Status = listen(VMS_Channel, Backlog);  
short VMS_Channel;  
unsigned int Backlog;
```

### ARGUMENTS

#### **VMS\_Channel**

VMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

#### **Backlog**

VMS Usage: **connection\_backlog**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The maximum length of the queue of pending connections. If a connection request arrives when the queue is full, the request is ignored. The backlog queue length is limited to 5.

### RETURNS

If **listen()** is successful, a value of 0 is returned. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vmserrno**.

## multinet\_kernel\_nliith

A special version of the UNIX 4.3BSD **nlist()** function that reads the symbol table to the MultiNet kernel. Unlike the UNIX 4.3BSD kernel, the MultiNet kernel's symbol table must be relocated before you can use **klseek()**, **klread()**, or **klwrite()** to examine the networking kernel.

Many of the same kernel symbols available under 4.3BSD are also available under the MultiNet software. Use of this interface is unsupported, as the symbol names and data types may change in future releases of the Berkeley TCP/IP networking code and in future releases of the MultiNet software.

To access the symbol table to the MultiNet image that is currently running, read from the file indicated by the logical name `MULTINET_NETWORK_IMAGE`:

For more information about how to use **multinet\_kernel\_nlist()**, see **nlist()**.

## **nlist()**

Examines the symbol table in an executable image or symbol table file.

### **FORMAT**

```
Status = nlist(Filename, nl);  
char *Filename;  
struct nlist nl[];
```

### **ARGUMENTS**

#### **Filename**

VMS Usage:	<b>filename</b>
type:	<b>ASCIZ string</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

The file name of the executable image or symbol table file to read.

#### **nl**

VMS Usage:	<b>symbol_table_info</b>
type:	<b>array of struct nlist</b>
access:	<b>modify</b>
mechanism:	<b>by reference</b>

An array of **nlist** structures. The **n\_name** field of each element specifies the name of the symbol to look up; the array is terminated by a null name. Each symbol is looked up in the file. If the symbol is found, the **n\_type** and **n\_value** fields are filled in with the type and value of the symbol. Otherwise, they are set to 0.

### **RETURNS**

If successful, the **nlist()** function returns a 0. Otherwise, it returns a -1.

## ntohl()

Swaps the byte order of a four-byte integer from network byte order to OpenVMS byte order. This allows you to develop programs that are independent of the hardware architecture on which they are running.

### FORMAT

```
RetVal = ntohl(Val);  
unsigned long Val;
```

### ARGUMENTS

<b>Val</b>	
VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The four-byte integer to convert to OpenVMS byte order.

### RETURNS

The **ntohl()** function returns the byte-swapped integer that corresponds to **Val**. For example, if **Val** is 0x01e429c0, the returned value is 0xc029e401.

## ntohs()

Swaps the byte order of a two-byte integer from network byte order to OpenVMS byte order. This allows you to develop programs that are independent of the hardware architecture on which they are running.

### FORMAT

```
RetVal = ntohs(Val);  
unsigned short Val;
```

### ARGUMENTS

<b>Val</b>	
VMS Usage:	<b>word_unsigned</b>
type:	<b>word (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The two-byte integer to convert to OpenVMS byte order.

### RETURNS

The **ntohs()** function returns the byte-swapped integer that corresponds to **Val**. For example, if **Val** is 0x1700, the returned value is 0x0017.

## recv()

Receives messages from a socket. This function is equivalent to a **recvfrom()** function called with the **From** and **FromLen** arguments specified as zero. The **socket\_read()** function is equivalent to a **recv()** function called with the **Flags** argument specified as zero.

The length of the message received is returned as the status. If a message is too long to fit in the supplied buffer and the socket is type **SOCK\_DGRAM**, excess bytes are discarded.

If no messages are at the socket, the receive function waits for a message to arrive, unless the socket is non-blocking (see **socket ioctl FIONBIO**). In this case, a status of -1 is returned and the global variable **socket\_errno** is set to **EWOULDBLOCK**.

## FORMAT

Status = int recv (short VMS\_Channel, char \*Buffer, int Size, int Flags);

## ARGUMENTS

### VMS\_Channel

VMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the socket.

### Buffer

VMS Usage: **arbitrary**  
 type: **byte buffer**  
 access: **write only**  
 mechanism: **by reference**

The address of a buffer in which to place the data read.

### Size

VMS Usage: **longword\_signed**  
 type: **longword (signed)**  
 access: **read only**  
 mechanism: **by value**

The length of the buffer specified by **Buffer**. The actual number of bytes read is returned in the **Status**.

### Flags

VMS Usage: **mask\_word**  
 type: **word (unsigned)**  
 access: **read only**

mechanism: **by value**

Control information that affects the **recv()** function. The **Flags** argument is formed by ORing one or more of the following values:

```
#define MSG_OOB    0x1    /* process out-of-band data */
#define MSG_PEEK  0x2    /* peek at incoming message */
```

The **MSG\_OOB** flag causes **recv()** to read any out-of-band data that has arrived on the socket.

The **MSG\_PEEK** flag causes **recv()** to read the data present in the socket without removing the data. This allows the caller to view the data, but leaves it in the socket for future **recv()** calls.

## RETURNS

If **recv()** is successful, a count of the number of characters received is returned. A return value of 0 indicates an end-of-file; that is, the connection has been closed. A return value of -1 indicates an error occurred. A more specific message is returned in the global variables **socket\_errno** and **vmerrno**.

## recvfrom()

Receives messages from a socket. This function is equivalent to the **recv()** function, but takes two additional arguments that allow the caller to determine the remote address from which the message was received.

The length of the message received is returned as the status. If a message is too long to fit in the supplied buffer and the socket is type **SOCK\_DGRAM**, excess bytes are discarded.

If no messages are available at the socket, the receive call waits for a message to arrive, unless the socket is non-blocking (see **socket ioctl FIONBIO**). In this case, a status of -1 is returned and the global variable **socket\_errno** is set to **EWOULDBLOCK**.

### FORMAT

```
Status = int recvfrom (short VMS_Channel, char *Buffer, int Size, int Flags, struct sockaddr
*From, unsigned int *FromLen);
```

### ARGUMENTS

#### VMS\_Channel

VMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

#### Buffer

VMS Usage: **arbitrary**  
type: **byte buffer**  
access: **write only**  
mechanism: **by reference**

The address of a buffer in which to place the data read.

#### Size

VMS Usage: **longword\_signed**  
type: **longword (signed)**  
access: **read only**  
mechanism: **by value**

The length of the buffer specified by **Buffer**. The actual number of bytes read is returned in the **Status**.

**Flags**

VMS Usage: **mask\_word**  
type: **word (unsigned)**  
access: **read only**  
mechanism: **by value**

Control information that affects the **recvfrom()** function. The **Flags** argument is formed by ORing one or more of the following values:

```
#define MSG_OOB 0x1 /* process out-of-band data */  
#define MSG_PEEK 0x2 /* peek at incoming message */
```

The **MSG\_OOB** flag causes **recvfrom()** to read any out-of-band data that has arrived on the socket.

The **MSG\_PEEK** flag causes **recvfrom()** to read the data present in the socket without removing the data. This allows the caller to view the data, but leaves it in the socket for future **recvfrom()** calls.

**From**

VMS Usage: **socket\_address**  
type: **struct sockaddr**  
access: **write only**  
mechanism: **by reference**

On return, this optional argument is filled in with the address of the host that transmitted the packet, as known to the communications layer. The exact format of the **Address** argument is determined by the domain in which the communication is occurring.

**FromLen**

VMS Usage: **socket\_address\_length**  
type: **longword (unsigned)**  
access: **modify**  
mechanism: **by reference**

On entry, this optional argument contains the length of the space pointed to by **From**, in bytes. On return, it contains the actual length, in bytes, of the address returned.

**RETURNS**

If **recvfrom()** is successful, a count of the number of characters received is returned. A return value of 0 indicates an end-of-file condition; that is, the connection has been closed. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vmserno**.

## recvmsg()

Receives messages from a socket. This function is equivalent to the **recvfrom()** function, but takes its arguments in a different fashion and can receive into noncontiguous buffers.

The length of the message received is returned as the status. If a message is too long to fit in the supplied buffer and the socket is type **SOCK\_DGRAM**, excess bytes are discarded.

If no messages are available at the socket, the receive call waits for a message to arrive, unless the socket is non-blocking (see **socket ioctl FIONBIO**). In this case, a status of -1 is returned and the global variable **socket\_errno** is set to **EWOULDBLOCK**.

### FORMAT

```
Status = recvmsg(VMS_Channel, Message, Flags);
short VMS_Channel;
struct msghdr *Message;
unsigned int Flags;
```

### ARGUMENTS

#### VMS\_Channel

VMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the socket.

#### Message

VMS Usage: **message header**  
 type: **struct msghdr**  
 access: **read only**  
 mechanism: **by reference**

A pointer to a "msghdr" structure that describes the buffer to be received into. The access rights portion of the structure is unused.

#### Flags

VMS Usage: **mask\_longword**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by value**

Control information that affects the **recvmsg()** function. The **Flags** argument is formed by ORing one or more of the following values:

```
#define MSG_OOB 0x1 /* process out-of-band data */  
#define MSG_PEEK 0x2 /* peek at incoming message */
```

The **MSG\_OOB** flag causes **recvmsg()** to read any out-of-band data that has arrived on the socket.

The **MSG\_PEEK** flag causes **recvmsg()** to read the data present in the socket without removing the data. This allows the caller to view the data, but leaves it in the socket for future **recvmsg()** calls.

## RETURNS

If **recvmsg()** is successful, a count of the number of characters received is returned. A return value of 0 indicates an end-of-file condition; that is, the connection has been closed. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vmserro**.

## select()

Examines the OpenVMS Channel sets whose addresses are passed in **ReadFds**, **WriteFds**, and **ExceptFds** to see if some of their Channels are ready for reading, ready for writing, or have an exceptional condition pending. On return, **select()** replaces the given Channel sets with subsets consisting of the Channels that are ready for the requested operation. The total number of ready Channels in all the sets is returned.

The **select()** function is only useful for NETWORK file descriptors and cannot be used for any other OpenVMS I/O device.

The Channel sets are stored as bit fields in arrays of integers. The following macros are provided for manipulating such Channel sets: **FD\_ZERO(&fdset)** initializes a Channel set **fdset** to the null set; **FD\_SET(VMS\_Channel, &fdset)** includes a particular Channel **VMS\_Channel** in **fdset**; **FD\_CLR(VMS\_Channel, &fdset)** removes **VMS\_Channel** from **fdset**; **FD\_ISSET(VMS\_Channel, &fdset)** is nonzero if **VMS\_Channel** is a member of **fdset**, otherwise it is zero. The behavior of these macros is undefined if a Channel value is less than zero or greater than or equal to **FD\_SETSIZE \* CHANNELSIZE**, which is normally at least equal to the maximum number of Channels supported by the system. Make sure that the definition of these macros comes from the MultiNet types.h file, as the definitions differ from the UNIX definitions.

**Caution!** Process Software recommends that you do not change the value of **FD\_SETSIZE**. However, if you must change it, make sure its value is equal to the maximum number of channels your system can handle.

**Note!** The MultiNet socket library is not reentrant. If you call into it from an AST (interrupt) routine, the results are unpredictable. The **select()** call must not be used while ASTs have been disabled. If the **select()** call is performed with ASTs disabled, the **select()** call will never return and will hang the program from which it was called. Instances when this improper call to **select()** can occur are as follows:

- A call to **select()** is performed within an AST routine (that is, executing an AST routine disables the delivery of other ASTs at the same (user-mode) priority).
- You have explicitly disabled AST delivery in normal (non-AST) code using the **\$SETAST** system service.

## FORMAT

```
Status = int select(int Width, fd_set, *ReadFds, fd_set, *WriteFds, fd_set, *ExceptFds,
struct timeval, *Timeout);
FD_SET (VMS_Channel, &fdset)
FD_CLR (VMS_Channel, &fdset)
FD_ISSET (VMS_Channel, &fdset)
FD_ZERO (&fdset)
fd_set fdset;
```

## ARGUMENTS

### Width

VMS Usage: **channel count**  
type: **long (unsigned)**  
access: **read only**  
mechanism: **by value**

The number of bits to be checked in each bit mask that represents a Channel; the Channels from 0 through **Width**-1 in the Channel sets are examined. Typically, **width** has the value returned by **getdtablesize** for the maximum number of Channels.

### ReadFds

VMS Usage: **channel bitmask**  
type: **struct fd\_set**  
access: **modify**  
mechanism: **by reference**

A bit-mask of the Channels that **select()** should test for the ready for reading status. May be specified as a NULL pointer if no Channels are of interest. Selecting true for reading on a Channel on which a **listen()** call has been performed indicates that a subsequent **accept()** call on that Channel will not block.

### WriteFds

VMS Usage: **channel bitmask**  
type: **struct fd\_set**  
access: **modify**  
mechanism: **by reference**

A bit-mask of the Channels that **select()** should test for the ready for writing status. May be specified as a NULL pointer if no Channels are of interest.

### ExceptFds

VMS Usage: **channel bitmask**  
type: **struct fd\_set**  
access: **modify**  
mechanism: **by reference**

A bit-mask of the Channels that **select()** should test for exceptional conditions pending. May be specified as a NULL pointer if no Channels are of interest. Selecting true for exception conditions indicates that out-of-band data is present in the Channel's input buffers.

### Timeout

VMS Usage: **timeout**  
type: **struct timeval**  
access: **read only**  
mechanism: **by reference**

A maximum interval to wait for the selection to complete. If **Timeout** is a NULL pointer, the select blocks indefinitely. To effect a poll, the **Timeout** argument should be a non-NULL pointer, pointing to a zero-valued timeval structure.

## **RETURNS**

**select()** returns the number of ready Channels that are contained in the Channel sets, or -1 if an error occurred. If the time limit expires, **select()** returns 0. If **select()** returns with an error, the Channel sets are unmodified.

## **select\_wake()**

Wakes a process waiting in a **select()** call, aborting the **select()** operation. This function may be called from an AST (interrupt) routine, in which case the **select()** call will be aborted when the AST routine completes.

### **FORMAT**

```
select_wake();
```

## send()

Transmits a message to another socket. This function is equivalent to a **sendto()** called with the **To** and **ToLen** arguments specified as zero. The **socket\_write()** function is equivalent to a **send()** function called with **Flags** specified as zero. Use the **send()** function only when a socket has been connected with **connect()**; however, you can use **sendto()** at any time.

If no message space is available at the socket to hold the message to be transmitted, **send()** blocks unless the socket has been placed in non-blocking I/O mode via the **socket ioctl FIONBIO**. If the socket is type **SOCK\_DGRAM** and the message is too long to pass through the underlying protocol in a single unit, the error **EMSGSIZE** is returned and the message is not transmitted.

### FORMAT

```
Status = int send (short VMS_Channel, char *Buffer, int Size);
```

### ARGUMENTS

#### VMS\_Channel

VMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the socket.

#### Buffer

VMS Usage: **arbitrary**  
 type: **byte buffer**  
 access: **read only**  
 mechanism: **by reference**

The address of a buffer containing the data to send.

#### Size

VMS Usage: **longword\_signed**  
 type: **longword (signed)**  
 access: **read only**  
 mechanism: **by value**

The length of the buffer specified by **Buffer**.

### RETURNS

If the **send()** function is successful, the count of the number of characters sent is returned. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vmserrno**.

## sendmsg()

Transmits a message to another socket. It is equivalent to **sendto()**, but takes its arguments in a different fashion and can send noncontiguous data.

If no message space is available at the socket to hold the message to be transmitted, **sendmsg()** blocks unless the socket has been placed in non-blocking I/O mode via the **socket ioctl FIONBIO**. If the socket is type **SOCK\_DGRAM** and the message is too long to pass through the underlying protocol in a single unit, the error **EMSGSIZE** is returned and the message is not transmitted.

### FORMAT

```
Status = sendmsg(VMS_Channel, Message, Flags);
short VMS_Channel;
struct msghdr *Message;
unsigned int Flags;
```

### ARGUMENTS

<b>VMS_Channel</b>	
VMS Usage:	<b>channel</b>
type:	<b>word (signed)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

A channel to the socket.

<b>Message</b>	
VMS Usage:	<b>message header</b>
type:	<b>struct msghdr</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to a "msghdr" structure that describes the data to be sent and the address to send it to. The access rights portion of the structure is unused.

<b>Flags</b>	
VMS Usage:	<b>mask_longword</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

Control information that affects the **sendto()** function. The Flags argument can be zero or the following:

```
#define MSG_OOB 0x1 /* process out-of-band data */
```

The **MSG\_OOB** flag causes **sendto()** to send out-of-band data on sockets that support this

operation (such as **SOCK\_STREAM**).

## **RETURNS**

If the **sendmsg()** function is successful, the count of the number of characters sent is returned. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vmserro**.

## sendto()

Transmits a message to another socket. It is equivalent to **send()**, but also allows the caller to specify the address to which to send the message. The **sendto()** function can be used on unconnected sockets, while **send()** and **socket\_write()** cannot.

If no message space is available at the socket to hold the message to be transmitted, **sendto()** blocks unless the socket has been placed in non-blocking I/O mode via the **socket ioctl FIONBIO**. If the socket is type **SOCK\_DGRAM** and the message is too long to pass through the underlying protocol in a single unit, the error **EMSGSIZE** is returned and the message is not transmitted.

## FORMAT

```
Status = sendto(VMS_Channel, Buffer, Size, Flags, To, ToLen);
short VMS_Channel;
char *Buffer;
int Size;
unsigned short Flags;
struct sockaddr *To;
unsigned int ToLen;
```

## ARGUMENTS

<b>VMS_Channel</b>	
VMS Usage:	<b>channel</b>
type:	<b>word (signed)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

A channel to the socket.

<b>Buffer</b>	
VMS Usage:	<b>arbitrary</b>
type:	<b>byte buffer</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

The address of a buffer containing the data to send.

<b>Size</b>	
VMS Usage:	<b>longword_signed</b>
type:	<b>longword (signed)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The length of the buffer specified by **Buffer**.

**Flags**

VMS Usage: **mask\_word**  
 type: **word (unsigned)**  
 access: **read only**  
 mechanism: **by value**

Control information that affects the **sendto()** function. The **Flags** argument can be zero or the following:

```
#define MSG_OOB 0x1 /* process out-of-band data */
```

The **MSG\_OOB** flag causes **sendto()** to send out-of-band data on sockets that support this operation (such as **SOCK\_STREAM**).

**To**

VMS Usage: **socket\_address**  
 type: **struct sockaddr**  
 access: **read only**  
 mechanism: **by reference**

This optional argument is a pointer to the address to which the packet should be transmitted. The exact format of the **Address** argument is determined by the domain in which the communication is occurring.

**ToLen**

VMS Usage: **socket\_address\_length**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by value**

This optional argument contains the length of the address pointed to by the **To** argument.

**RETURNS**

If the **sendto()** function is successful, the count of the number of characters sent is returned. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vmserrno**.

## sethostent()

Initializes the host table and DNS Name Server routines. It is usually unnecessary to call this function because the host table and Name Server routines are initialized automatically when any of the other host table routines are called.

### FORMAT

```
(void) sethostent(StayOpen);  
unsigned int StayOpen;
```

### ARGUMENTS

**StayOpen**

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

Specifies whether the DNS Name Resolver should use TCP or UDP to communicate with the DNS Name Server. A nonzero value indicates TCP, and a value of 0 (the default if **sethostent()** is not called) indicates UDP.

## setnetent()

Initializes the host table and DNS Name Server routines. It is usually unnecessary to call this function because the host table and Name Server routines are initialized automatically when any of the other host table routines are called.

### FORMAT

```
(void) setnetent(StayOpen);  
unsigned int StayOpen;
```

### ARGUMENTS

**StayOpen**

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

Specifies whether the DNS Name Resolver should use TCP or UDP to communicate with the DNS Name Server. A nonzero value indicates TCP, and a value of 0 (the default if **setnetent()** is not called) indicates UDP.

## **setprotoent()**

Initializes the host table routines and sets the next protocol entry returned by **getprotoent()** to be the first entry.

### **FORMAT**

```
(void) setprotoent(StayOpen);  
unsigned int StayOpen;
```

### **ARGUMENTS**

**StayOpen**

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

Provided only for compatibility with UNIX 4.3BSD, and is ignored by the MultiNet software.

## setservent()

Initializes the host table routines and sets the next service entry returned by **getservent()** to be the first entry.

### FORMAT

```
(void) setservent(StayOpen);  
unsigned int StayOpen;
```

### ARGUMENTS

**StayOpen**

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

Provided only for compatibility with UNIX 4.3BSD, and is ignored by the MultiNet software.

## setsockopt()

Manipulates options associated with a socket. Options may exist at multiple protocol levels; however, they are always present at the uppermost socket level.

When manipulating socket options, you must specify the level at which the option resides and the name of the option. To manipulate options at the socket level, specify **Level** as **SOL\_SOCKET**. To manipulate options at any other level, specify the protocol number of the appropriate protocol controlling the option. For example, to indicate that an option is to be interpreted by the TCP protocol, set **Level** to the protocol number of TCP; see **getprotobyname()**.

**OptName** and any specified options are passed without modification to the appropriate protocol module for interpretation. The include file **multinet\_root:[multinet.include.sys]socket.h** contains definitions for socket-level options. Options at other protocol levels vary in format and name.

### FORMAT

```
Status = setsockopt(VMS_Channel, Level, OptName, OptVal, OptLen);
short VMS_Channel;
unsigned int Level, OptName, OptLen;
char *OptVal;
```

### ARGUMENTS

<b>VMS_Channel</b>	
VMS Usage:	<b>channel</b>
type:	<b>word (signed)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

A channel to the socket.

<b>Level</b>	
VMS Usage:	<b>option_level</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The protocol level at which the option is to be manipulated. **Level** can be specified as **SOL\_SOCKET**, or a protocol number as returned by **getprotobyname()**.

<b>OptName</b>	
VMS Usage:	<b>option_name</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The option that is to be manipulated.

**OptVal**

VMS Usage:       **dependent on OptName**  
type:             **byte buffer**  
access:           **read only**  
mechanism:       **by reference**

A pointer to a buffer that contains the new value of the option. The format of this buffer depends on the option requested.

**OptLen**

VMS Usage:       **option\_length**  
type:             **longword (unsigned)**  
access:           **read only**  
mechanism:       **by value**

The length of the buffer pointed to by **OptVal**.

**RETURNS**

If the **setsockopt()** is successful, a value of 0 is returned. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vmserrno**.

## shutdown()

Shuts down all or part of a full-duplex connection on the socket associated with **VMS\_Channel**. This function is usually used to signal an end-of-file to the peer without closing the socket, which would prevent further data from being received.

### FORMAT

```
Status = shutdown(VMS_Channel, How);  
short VMS_Channel;  
unsigned int How;
```

### ARGUMENTS

#### **VMS\_Channel**

VMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

#### **How**

VMS Usage: **longword\_unsigned**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

Controls which part of the full-duplex connection to shut down. If **How** is 0, further receive operations are disallowed. If **How** is 1, further send operations are disallowed. If **How** is 2, further send and receive operations are disallowed.

### RETURNS

If **shutdown()** is successful, a value of 0 is returned. If an error occurs, a value of -1 is returned, and a more specific error message is returned in the global variables **socket\_errno** and **vmserro**.

## socket()

Creates an end point for communication and returns an OpenVMS channel that describes the end point.

### FORMAT

```
VMS_Channel = socket(Address_Family, Type, Protocol);
short VMS_Channel;
unsigned int Address_Family, Type, Protocol;
```

### ARGUMENTS

#### Address\_Family

VMS Usage: **address\_family**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by value**

An address family with which addresses specified in later operations using the socket should be interpreted. The following formats are currently supported; they are defined in the include file **multinet\_root:[multinet.include.sys]socket.h**:

AF_INET	Internet (TCP/IP) addresses
AF_PUP	Xerox PUP addresses
AF_CHAOS	CHAOSnet addresses
AF_NS	Xerox XN addresses

#### Type

VMS Usage: **socket\_type**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by value**

The semantics of communication using the created socket. The following types are currently defined:

SOCK_STREAM	SOCK_DGRAM	SOCK_RAW
-------------	------------	----------

A **SOCK\_STREAM** socket provides a sequenced, reliable, two-way connection-oriented byte stream with an out- of-band data transmission mechanism. A **SOCK\_DGRAM** socket supports communication by connectionless, unreliable messages of a fixed (typically small) maximum length. **SOCK\_RAW** sockets provide access to internal network interfaces. The type

**SOCK\_RAW** is available only to users with SYSPRV privilege.

The **Type** argument, together with the **Address Family** argument, specifies the protocol to be used. For example, a socket created with **AF\_INET** and **SOCK\_STREAM** is a TCP socket, and a socket created with **AF\_INET** and **SOCK\_DGRAM** is a UDP socket.

**Protocol**

VMS Usage:	<b>protocol_number</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

A particular protocol to be used with the socket. Normally, only a single protocol exists to support a particular socket type using a given address format. However, it is possible that many protocols may exist, in which case a particular protocol must be specified by **Protocol**. The protocol number to use depends on the communication domain in which communication will take place.

For TCP and UDP sockets, the protocol number **MUST** be specified as 0. For **SOCK\_RAW** sockets, the protocol number should be the value returned by **getprotobyname()**.

## RETURNS

If the **socket()** is successful, an OpenVMS channel is returned. If an error occurs, a value of -1 is returned, and a more specific error message is returned in the global variables **socket\_errno** and **vmserro**.

## socket\_close()

Deassigns the OpenVMS channel from the MultiNet INET: device. When the last channel assigned to the device is deassigned, the device and attached socket are deleted.

If the **SO\_LINGER** socket option is set and data remains in the socket's output queue, **socket\_close()** deletes only the device. The attached socket remains in the system until the data is sent, after which it is deleted. Once **socket\_close()** is called, there is no way to reference this socket.

Normally, channels are automatically deassigned at image exit. However, because there is a limit on the number of open channels per process, the **socket\_close()** function is necessary for programs that deal with many connections.

### FORMAT

```
Status = socket_close(VMS_Channel);
short VMS_Channel;
```

### ARGUMENTS

<b>VMS_Channel</b>	
VMS Usage:	<b>channel</b>
type:	<b>word (signed)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

A channel to the socket to close.

### RETURNS

If the **socket\_close()** is successful, a value of 0 is returned. If an error occurs, a value of -1 is returned, and a more specific error message is returned in the global variables **socket\_errno** and **vm serrno**.

## socket\_ioctl()

Performs a variety of functions on the network. In particular, it manipulates socket characteristics, routing tables, ARP tables, and interface characteristics. A **socket\_ioctl()** request has encoded in it whether the argument is an input or output parameter, and the size of the argument, in bytes. Macro and define statements used in specifying a **socket\_ioctl()** request are located in the file **multinet\_root:[multinet.include.sys]ioctl.h**.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, Request, ArgP);
short VMS_Channel;
unsigned int Request;
char *ArgP;
```

### ARGUMENTS

#### **VMS\_Channel**

VMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

#### **Request**

VMS Usage: **ioctl\_request**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

Which **socket\_ioctl()** function to perform.

#### **ArgP**

VMS Usage: **arbitrary**  
type: **byte buffer**  
access: **read, write, or modify depending on Request**  
mechanism: **by reference**

A pointer to a buffer whose format and function depend on the **Request** specified.

### RETURNS

If the **socket\_ioctl()** is successful, a value of 0 is returned. If an error occurs, a value of -1 is returned, and a more specific error message is returned in the global variables **socket\_errno** and **vmserro**.

For a list of the **socket\_ioctl()** functions supported by MultiNet, see the following pages.

## socket ioctl FIONBIO

Controls nonblocking I/O on a socket. If nonblocking I/O is enabled and another function is called that would have to wait for a connection, for data to arrive, or for data to be transmitted, the function completes with a -1 error return, and the global variable **socket\_errno** is set to **EWOULDBLOCK**.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, FIONBIO, Enable);  
unsigned int *Enable;
```

### ARGUMENTS

**Enable**

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to an integer that specifies whether nonblocking I/O is enabled or disabled. A value of 1 enables nonblocking I/O, and a value of 0 disables nonblocking I/O. By default, nonblocking I/O is disabled when a socket is created.

## socket ioctl FIONREAD

Retrieves the number of bytes waiting to be read. A return of 0 indicates that no data is buffered.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, FIONREAD, Count);  
unsigned int *Count;
```

### ARGUMENTS

**Count**

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>write only</b>
mechanism:	<b>by reference</b>

A pointer to an integer buffer that will receive a count of the number of characters waiting to be read.

## socket ioctl SIOCADDRT

Adds routing information to the network routing tables. This function does not modify the socket itself, but rather modifies the operation of the network in general. It does not matter what the state of the socket is. Normally, to modify Internet routing tables, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCADDRT, Route);
struct rtenry *Route;
```

### ARGUMENTS

<b>Route</b>	
VMS Usage:	<b>routing_entry</b>
type:	<b>struct rtenry</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to the address of a **rtenry** structure that describes the route to be added. The **rtenry** structure is defined in **multinet\_root:[multinet.include.net]route.h** as follows:

```
struct rtenry {
    u_long  rt_hash;
    struct  sockaddr rt_dst;
    struct  sockaddr rt_gateway;
    short   rt_flags;
    short   rt_refcnt;
    u_long  rt_use;
    struct  ifnet *rt_ifp;
};
```

Field	Description
<b>rt_hash</b> , <b>rt_refcnt</b> , <b>rt_use</b> , and <b>rt_ifp</b>	Are ignored by <b>SIOCADDRT</b> and should be set to zero.
<b>rt_dst</b>	Specifies the address of the destination host or network.
<b>rt_gateway</b>	Specifies the address of the local gateway to this host or network.

<b>Field</b>	<b>Description</b>
<b>rt_flags</b>	<p>Specifies one or more of the following flags that affect a routing entry:</p> <pre data-bbox="270 288 1076 371">#define RTF_UP      0x1  /* route useable */ #define RTF_GATEWAY 0x2  /* destination is a gateway */ #define RTF_HOST    0x4  /* host entry (net otherwise)*/</pre> <p><b>RTF_UP</b>—Indicates that the route is usable. It should always be specified.</p> <p><b>RTF_GATEWAY</b>—Indicates that the next hop to the destination is a gateway, so that the output routines know to address the gateway rather than the destination directly.</p> <p><b>RTF_HOST</b>—Indicates that the address specified in <code>rt_dst</code> is an Internet host, rather than an Internet network (the default).</p>

## socket ioctl SIOCDELRT

Deletes routing information from the network routing tables. This function does not modify the socket itself, but rather modifies the operation of the network in general. It does not matter what the state of the socket is. Normally, to modify Internet routing tables, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

It is impossible to obtain a list of the routes installed via **socket\_ioctl()**. To delete a route, you must either know it already exists or use **multinet\_kernel\_nlist()** to read the routing tables directly from the networking kernel.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCDELRT, Route);
struct rentry *Route;
```

### ARGUMENTS

<b>Route</b>	
VMS Usage:	<b>routing_entry</b>
type:	<b>struct rentry</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to the address of a **rtentry** structure that describes the route to be deleted. The **rtentry** structure is defined in **multinet\_root:[multinet.include.net]route.h** as follows:

```
struct rentry {
    u_long   rt_hash;
    struct   sockaddr rt_dst;
    struct   sockaddr rt_gateway;
    short    rt_flags;
    short    rt_refcnt;
    u_long   rt_use;
    struct   ifnet *rt_ifp;
};
```

Field	Description
<b>rt_hash</b> , <b>rt_refcnt</b> , <b>rt_use</b> , and <b>rt_ifp</b>	Are ignored by <b>SIOCDELRT</b> and should be set to zero.
<b>rt_dst</b>	Specifies the address of the destination host or network.
<b>rt_gateway</b>	Specifies the address of the local gateway to this host or network.

<b>Field</b>	<b>Description</b>
<b>rt_flags</b>	<p>Specifies one or more of the following flags that affect a routing entry:</p> <pre>#define RTF_UP      0x1  /* route useable */ #define RTF_GATEWAY 0x2  /* destination is a gateway */ #define RTF_HOST    0x4  /* host entry (net otherwise) */</pre> <p><b>RTF_UP</b>—Indicates that the route is usable. It should always be specified.</p> <p><b>RTF_GATEWAY</b>—Indicates that the next hop to the destination is a gateway, so that the output routines know to address the gateway rather than the destination directly.</p> <p><b>RTF_HOST</b>—Indicates that the address specified in <b>rt_dst</b> is an Internet host, rather than an Internet network (the default).</p>

## socket ioctl SIOCATMARK

Retrieves an indication as to whether the next byte in the stream coincides with an out-of-band or **URGENT** data mark.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCATMARK, AtMark);  
unsigned int *AtMark;
```

### ARGUMENTS

**AtMark**

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>write only</b>
mechanism:	<b>by reference</b>

A pointer to an integer buffer that will receive the indication. The buffer is set to 0 if the socket is not at the out-of-band mark. It is set to nonzero if the socket is at the out-of-band mark.

## socket ioctl SIOCDARP

Deletes an entry from the ARP table. This format is compatible with the UNIX 4.3BSD function of the same name.

### FORMAT

```
Status = socket_ioctl (VMS_Channel, SIOCDARP, ARP_Req);
struct arpreq *ARP_Req;
```

### ARGUMENTS

<b>ARP_Req</b>	
VMS Usage:	<b>arp_request</b>
type:	<b>struct arpreq</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

The address of an **arpreq** structure that contains the protocol address and the hardware address. The **arpreq** structure is defined in **multinet\_root:[multinet.include.net]if\_arp.h** as follows:

```
struct arpreq {
    struct sockaddr arp_pa;           /* protocol address */
    struct sockaddr arp_ha;          /* hardware address */
    int arp_flags;                   /* flags */
};
/* arp_flags and at_flags field values */
#define ATF_INUSE      0x01  /* entry in use */
#define ATF_COM       0x02  /* completed entry (enaddr valid) */
#define ATF_PERM      0x04  /* permanent entry */
#define ATF_PUBL      0x08  /* publish entry (respond for other host)
*/

#define ATF_USETRAILERS 0x10  /* has requested trailers */
#define ATF_PROXY      0x20  /* Do PROXY arp */
```

The **arp\_pa** field is a sockaddr field that is set to the ip address the remote interface uses.

The **arp\_ha.sa\_data** field is 6 bytes of binary data that represents the Ethernet address of the remote interface.

## socket ioctl SIOCGARP

Displays an entry in the ARP table. This function is compatible with the UNIX 4.3BSD function of the same name.

### FORMAT

```
Status = socket_ioctl (VMS_Channel, SIOCGARP, ARP_Req);
struct arpreq *ARP_Req;
```

### ARGUMENTS

<b>ARP_Req</b>	
VMS Usage:	<b>arp_request</b>
type:	<b>struct arpreq</b>
access:	<b>modify</b>
mechanism:	<b>by reference</b>

The address of an **arpreq** structure that contains the protocol address and the hardware address. The **arpreq** structure is defined in **multinet\_root:[multinet.include.net]if\_arp.h** as follows:

```
struct arpreq {
    struct sockaddr arp_pa;           /* protocol address */
    struct sockaddr arp_ha;         /* hardware address */
    int arp_flags;                  /* flags */
};
/* arp_flags and at_flags field values */
#define ATF_INUSE      0x01 /* entry in use */
#define ATF_COM       0x02 /* completed entry (enaddr valid) */
#define ATF_PERM      0x04 /* permanent entry */
#define ATF_PUBL      0x08 /* publish entry (respond for other host)
*/

#define ATF_USETRAILERS 0x10 /* has requested trailers */
#define ATF_PROXY      0x20 /* Do PROXY arp */
```

The **arp\_pa** field is a sockaddr field that is set to the ip address the remote interface uses.

The **arp\_ha.sa\_data** field is 6 bytes of binary data that represents the Ethernet address of the remote interface.

## socket ioctl SIOCSARP

Adds an entry to the ARP table. This function is compatible with the UNIX 4.3BSD function of the same name.

### FORMAT

```
Status = socket_ioctl (VMS_Channel, SIOCSARP, ARP_Req);
struct arpreq *ARP_Req;
```

### ARGUMENTS

<b>ARP_Req</b>	
VMS Usage:	<b>arp_request</b>
type:	<b>struct arpreq</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

The address of an **arpreq** structure that contains the protocol address and the hardware address. The **arpreq** structure is defined in **multinet\_root:[multinet.include.net]if\_arp.h** as follows:

```
struct arpreq {
    struct sockaddr arp_pa;           /* protocol address */
    struct sockaddr arp_ha;          /* hardware address */
    int arp_flags;                   /* flags */
};
/* arp_flags and at_flags field values */
#define ATF_INUSE      0x01 /* entry in use */
#define ATF_COM       0x02 /* completed entry (enaddr valid) */
#define ATF_PERM      0x04 /* permanent entry */
#define ATF_PUBL      0x08 /* publish entry (respond for other host)
*/

#define ATF_USETRAILERS 0x10 /* has requested trailers */
#define ATF_PROXY      0x20 /* Do PROXY arp */
```

The **arp\_pa** field is a sockaddr field that is set to the ip address the remote interface uses.

The **arp\_ha.sa\_data** field is 6 bytes of binary data that represents the Ethernet address of the remote interface.

## socket ioctl SIOCGIFADDR

Retrieves the Internet address of a network interface. This function does not modify the socket itself, but rather examines the operation of the network in general. It does not matter what the state of the socket is. Normally, to examine Internet addresses, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCGIFADDR, Interface_Req);
struct ifreq *Interface_Req;
```

### ARGUMENTS

#### Interface\_Req

VMS Usage:	<b>interface_request</b>
type:	<b>struct ifreq</b>
access:	<b>modify</b>
mechanism:	<b>by reference</b>

The address of an **ifreq** structure that describes the interface from which to retrieve the address. The **ifreq** structure is defined in **multinet\_root:[multinet.include.net]if.h** as follows:

```
struct ifreq {
    char ifr_name[16];
    struct sockaddr ifr_addr;
};
```

The **ifr\_name** field is a null-terminated string specifying the name of the interface to be examined, such as "se0".

The **ifr\_addr** field is a **sockaddr** structure that is set to the address of the interface.

## socket ioctl SIOCSIFADDR

Sets the Internet address of a network interface. Normally, this is done using the MULTINET SET/INTERFACE command. This function does not modify the socket itself, but rather modifies the operation of the network in general. It does not matter what the state of the socket is. Normally, to modify Internet addresses, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCSIFADDR, Interface_Req);
struct ifreq *Interface_Req;
```

### ARGUMENTS

<b>Interface_Req</b>	
VMS Usage:	<b>interface_request</b>
type:	<b>struct ifreq</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

The address of an **ifreq** structure that describes the address to be set. The **ifreq** structure is defined in **multinet\_root:[multinet.include.net]if.h** as follows:

```
struct ifreq {
    char ifr_name[16];
    struct sockaddr ifr_addr;
};
```

The **ifr\_name** field is a null-terminated string specifying the name of the interface to be modified, such as "se0".

The **ifr\_addr** field is a **sockaddr** structure specifying the address to be set.

## socket ioctl SIOCGIFBRDADDR

Retrieves the Internet broadcast address of a network interface. This function does not modify the socket itself, but rather examines the operation of the network in general. It does not matter what the state of the socket is. Normally, to examine Internet broadcast addresses, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCGIFBRDADDR, Interface_Req);
struct ifreq *Interface_Req;
```

### ARGUMENTS

#### Interface\_Req

VMS Usage:	<b>interface_request</b>
type:	<b>struct ifreq</b>
access:	<b>modify</b>
mechanism:	<b>by reference</b>

The address of an **ifreq** structure that describes the interface from which to retrieve the broadcast address. The **ifreq** structure is defined in **multinet\_root:[multinet.include.net]if.h** as follows:

```
struct ifreq {
    char ifr_name[16];
    struct sockaddr ifr_broadaddr;
};
```

The **ifr\_name** field is a null-terminated string specifying the name of the interface to be examined, such as "se0".

The **ifr\_broadaddr** field is a **sockaddr** structure that is set to the broadcast address of the interface.

## socket ioctl SIOCSIFBRDADDR

Sets the Internet broadcast address of a network interface. Normally, this is done using the MULTINET SET/INTERFACE command. This function does not modify the socket itself, but rather modifies the operation of the network in general. It does not matter what the state of the socket is. Normally, to modify Internet broadcast addresses, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCSIFBRDADDR, Interface_Req);  
struct ifreq *Interface_Req;
```

### ARGUMENTS

<b>Interface_Req</b>	
VMS Usage:	<b>interface_request</b>
type:	<b>struct ifreq</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

The address of an **ifreq** structure that describes the interface on which to set the broadcast address. The **ifreq** structure is defined in **multinet\_root:[multinet.include.net]if.h** as follows:

```
struct ifreq {  
    char ifr_name[16];  
    struct sockaddr ifr_broadaddr;  
};
```

The **ifr\_name** field is a null-terminated string specifying the name of the interface to be modified, such as "se0".

The **ifr\_broadaddr** field is a **sockaddr** structure specifying the broadcast address to be set.

## socket ioctl SIOCGIFCONF

Retrieves the list of network interfaces from the networking kernel for further examination by the other **SIOCGxxxx** functions. This function does not modify the socket itself, but rather examines the operation of the network in general. It does not matter what the state of the socket is. Normally, to examine the network configuration, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCGIFCONF, Interface_Config);
struct ifconf *Interface_Config;
```

### ARGUMENTS

#### Interface\_Config

VMS Usage: **interface\_configuration\_request**  
 type: **struct ifconf**  
 access: **modify**  
 mechanism: **by reference**

The address of an **ifconf** structure describing a buffer in which to return the interface configuration. The **ifconf** structure is defined in **multinet\_root:[multinet.include.net]if.h** as follows:

```
struct ifconf {
    int ifc_len; /* size of buffer */
    union {
        caddr_t ifcu_buf;
        struct ifreq *ifcu_req;
    } ifc_ifcu;
#define ifc_buf ifc_ifcu.ifcu_buf /* buffer address */
#define ifc_req ifc_ifcu.ifcu_req /* array of structures */
};
```

The **ifc\_len** field should be set to the length of the buffer specified by **ifc\_buf**. Upon return, the **ifc\_len** field contains the actual number of bytes written into the buffer.

The **ifc\_buf** field should be set to a buffer large enough to hold the entire network configuration. Upon return, the **ifc\_req** buffer contains an array of **ifreq** structures, one for each interface and address.

The following short fragment of C-language code prints all Internet family interfaces and shows how to decode the **ifconf** structure:

```
n = ifc.ifc_len/sizeof(struct ifreq);
for (ifr = ifc.ifc_req; n > 0; n--, ifr++) {
    if (ifr->ifr_addr.sa_family != AF_INET) continue;
    printf("%s\n", ifr->ifr_name);
}
```

## socket ioctl SIOCGIFDSTADDR

Retrieves the destination Internet address of a point-to-point network interface. This function does not modify the socket itself, but rather examines the operation of the network in general. It does not matter what the state of the socket is. Normally, to examine Internet addresses, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCGIFDSTADDR, Interface_Req);  
struct ifreq *Interface_Req;
```

### ARGUMENTS

<b>Interface_Req</b>	
VMS Usage:	<b>interface_request</b>
type:	<b>struct ifreq</b>
access:	<b>modify</b>
mechanism:	<b>by reference</b>

The address of an **ifreq** structure that describes the interface from which to retrieve the destination address. The **ifreq** structure is defined in **multinet\_root:[multinet.include.net]if.h** as follows:

```
struct ifreq {  
    char ifr_name[16];  
    struct sockaddr ifr_dstaddr;  
};
```

The **ifr\_name** field is a null-terminated string specifying the name of the interface to be examined, such as "se0".

The **ifr\_dstaddr** field is a **sockaddr** structure that is set to the destination address of the interface.

## socket ioctl SIOCSIFDSTADDR

Sets the destination Internet address of a point-to-point network interface. Normally, this is done using the MULTINET SET/INTERFACE command. This function does not modify the socket itself, but rather modifies the operation of the network in general. It does not matter what the state of the socket is. Normally, to modify Internet addresses, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCSIFDSTADDR, Interface_Req);
struct ifreq *Interface_Req;
```

### ARGUMENTS

<b>Interface_Req</b>	
VMS Usage:	<b>interface_request</b>
type:	<b>struct ifreq</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

The address of an **ifreq** structure that describes the interface on which to set the destination address. The **ifreq** structure is defined in **multinet\_root:[multinet.include.net]if.h** as follows:

```
struct ifreq {
    char ifr_name[16];
    struct sockaddr ifr_dstaddr;
};
```

The **ifr\_name** field is a null-terminated string specifying the name of the interface to be modified, such as "se0".

The **ifr\_dstaddr** field is a **sockaddr** structure specifying the destination address to be set.

## socket ioctl SIOCGIFFLAGS

Retrieves various control flags from a network interface. This function does not modify the socket itself, but rather examines the operation of the network in general. It does not matter what the state of the socket is. Normally, to examine interface flags, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCSIFFLAGS, Interface_Req);  
struct ifreq *Interface_Req;
```

### ARGUMENTS

<b>Interface_Req</b>	
VMS Usage:	<b>interface_request</b>
type:	<b>struct ifreq</b>
access:	<b>modify</b>
mechanism:	<b>by reference</b>

The address of an **ifreq** structure that describes the state of the flags. The **ifreq** structure is defined in **multinet\_root:[multinet.include.net]if.h** as follows:

```
struct ifreq {  
    char ifr_name[16];  
    short ifr_flags;  
    char xfill[14];  
};
```

The **ifr\_name** field is a null-terminated string specifying the name of the interface to be examined, such as "se0".

The **ifr\_flags** field receives the state of the interface flags. The following flag bits are valid:

```
#define IFF_UP          0x1    /* interface is up */  
#define IFF_BROADCAST  0x2    /* broadcast address valid */  
#define IFF_DEBUG      0x4    /* turn on debugging */  
#define IFF_LOOPBACK   0x8    /* is a loopback net */  
#define IFF_POINTOPOINT 0x10   /* interface is ptp link */  
#define IFF_NOTRAILERS  0x20   /* avoid use of trailers */  
#define IFF_RUNNING    0x40   /* resources allocated */  
#define IFF_NOARP      0x80   /* no ARP protocol */
```

## socket ioctl SIOCSIFFLAGS

Sets various control flags on a network interface. Normally this is done using the MULTINET SET/INTERFACE command.

To modify the state of a flag, first call the SIOCGIFFLAGS `socket_ioctl()` function, change whichever bits are necessary, and then reset the flags by calling **SIOCSIFFLAGS** `socket_ioctl()`.

This function does not modify the socket itself, but rather modifies the operation of the network in general. It does not matter what the state of the socket is. Normally, to modify interface flags, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCSIFFLAGS, Interface_Req);
struct ifreq *Interface_Req;
```

### ARGUMENTS

#### Interface\_Req

VMS Usage:	<b>interface_request</b>
type:	<b>struct ifreq</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

The address of an **ifreq** structure that describes the new state of the flags. The **ifreq** structure is defined in **multinet\_root:[multinet.include.net]if.h** as follows:

```
struct ifreq {
    char ifr_name[16];
    short ifr_flags;
    char xfill[14];
};
```

The **ifr\_name** field is a null-terminated string specifying the name of the interface to be modified, such as "se0".

The **ifr\_flags** field specifies the new state of the interface flags. The following flags can be set or cleared:

```
#define IFF_UP          0x1    /* interface is up */
#define IFF_DEBUG      0x4    /* turn on debugging */
#define IFF_NOTRAILERS 0x20   /* avoid use of trailers */
#define IFF_NOARP      0x80   /* no ARP protocol */
```

## **socket ioctl SIOCGIFMETRIC**

Retrieves the network interface metric, or cost. The interface metric is ignored by the MultiNet software, and is not documented further here.

## socket ioctl SIOCSIFMETRIC

Sets the network interface metric, or cost. The interface metric is ignored by the MultiNet software, and is not documented further here.

## socket ioctl SIOCGIFNETMASK

Retrieves the Internet address mask of a network interface. This function does not modify the socket itself, but rather examines the operation of the network in general. It does not matter what the state of the socket is. Normally, to examine Internet address masks, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCGIFNETMASK, Interface_Req);
struct ifreq *Interface_Req;
```

### ARGUMENTS

<b>Interface_Req</b>	
VMS Usage:	<b>interface_request</b>
type:	<b>struct ifreq</b>
access:	<b>modify</b>
mechanism:	<b>by reference</b>

The address of an **ifreq** structure that describes the interface from which to retrieve the address mask. The **ifreq** structure is defined in **multinet\_root:[multinet.include.net]if.h** as follows:

```
struct ifreq {
    char ifr_name[16];
    struct sockaddr ifr_addr;
};
```

The **ifr\_name** field is a null-terminated string specifying the name of the interface to be examined, such as "se0".

The **ifr\_addr** field is a **sockaddr** structure that is set to the address mask of the interface.

## socket ioctl SIOCSIFNETMASK

Sets the Internet address mask of a network interface. Normally, this is done using the MULTINET SET/INTERFACE command. This function does not modify the socket itself, but rather modifies the operation of the network in general. It does not matter what the state of the socket is. Normally, to modify Internet address masks, you use a socket created with the **AF\_INET** and **SOCK\_DGRAM** arguments.

### FORMAT

```
Status = socket_ioctl(VMS_Channel, SIOCSIFNETMASK, Interface_Req);
struct ifreq *Interface_Req;
```

### ARGUMENTS

<b>Interface_Req</b>	
VMS Usage:	<b>interface_request</b>
type:	<b>struct ifreq</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

The address of an **ifreq** structure that describes the interface on which to set the address mask. The **ifreq** structure is defined in **multinet\_root:[multinet.include.net]if.h** as follows:

```
struct ifreq {
    char ifr_name[16];
    struct sockaddr ifr_addr;
};
```

The **ifr\_name** field is a null-terminated string specifying the name of the interface to be modified, such as "se0".

The **ifr\_addr** field is a **sockaddr** structure specifying the address mask to be set.

## socket option SO\_BROADCAST

Enables transmission of broadcast messages on the specified socket.

### FORMAT

```
Status = setsockopt(VMS_Channel, SOL_SOCKET, SO_BROADCAST, On, sizeof(*On));  
unsigned int *On;
```

### ARGUMENTS

<b>On</b>	
VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to an integer buffer that specifies whether the transmission of broadcast messages is enabled or disabled. A nonzero value enables the transmission of broadcast messages, a value of 0 disables the transmission.

## socket option **SO\_DEBUG**

Controls the recording of debugging information by the MultiNet networking kernel.

### FORMAT

```
Status = setsockopt(VMS_Channel, SOL_SOCKET, SO_DEBUG, On, sizeof(*On));  
unsigned int *On;
```

### ARGUMENTS

**On**

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to an integer buffer that specifies whether debugging is enabled or disabled. A nonzero value enables debugging. A value of 0 disables debugging.

## socket option SO\_DONTRROUTE

Indicates that outgoing messages bypass the standard routing facilities. Instead, messages are directed to the appropriate network interface, as determined by the network portion of the destination address.

### FORMAT

```
Status = setsockopt(VMS_Channel, SOL_SOCKET, SO_DONTRROUTE, On, sizeof(*On));  
unsigned int *On;
```

### ARGUMENTS

<b>On</b>	
VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to an integer buffer that specifies whether **SO\_DONTRROUTE** is enabled or disabled. A nonzero value enables **SO\_DONTRROUTE**. A value of 0 disables **SO\_DONTRROUTE**.

## socket option **SO\_ERROR**

Retrieves and clears any error status pending on the socket. This function is only valid with the **getsockopt()** function.

### FORMAT

```
Status = getsockopt(VMS_Channel, SOL_SOCKET, SO_ERROR, Value, Length);  
unsigned int *Value;  
unsigned int *Length;
```

### ARGUMENTS

#### **Value**

VMS Usage:     **longword\_unsigned**  
type:           **longword (unsigned)**  
access:         **write only**  
mechanism:      **by reference**

A pointer to an integer buffer that receives the value of **errno** (the error number) that is pending on the socket.

#### **Length**

VMS Usage:     **longword\_unsigned**  
type:           **longword (unsigned)**  
access:         **modify**  
mechanism:      **by reference**

On entry, contains the length of the space pointed to by **Value**, in bytes. On return, it contains the actual length, in bytes, of the **Value** returned.

## socket option SO\_KEEPALIVE

Enables periodic transmission of messages on an idle connected socket. If the connected party fails to respond to these messages, the connection is considered broken and processes using the socket are notified via an error returned by a read.

Keepalives are a questionable use of the network in that they cause idle connections to add network traffic by constantly probing their peer. Avoid keepalives if another mechanism is available to detect the loss of a peer, such as timeouts.

### FORMAT

```
Status = setsockopt(VMS_Channel, SOL_SOCKET, SO_KEEPA
```

LIVE, On, sizeof(\*On));  
unsigned int \*On;

### ARGUMENTS

<b>On</b>	
VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to an integer buffer that specifies whether keepalives are enabled or disabled. A nonzero value enables keepalives. A value of 0 disables keepalives.

## socket option **SO\_LINGER**

Controls the action taken when unsent messages are queued on a socket and a **socket\_close()** function call is issued. If the socket promises reliable delivery of data and **SO\_LINGER** is set, **socket\_close()** deletes only the device. The attached socket remains in the system until this data is sent or until it determines that it cannot deliver the information (a timeout period, termed the linger interval, is specified in the **setsockopt()** function). Only then is the attached socket deleted.

### FORMAT

```
Status = setsockopt(VMS_Channel, SOL_SOCKET, SO_LINGER, Linger, sizeof(*Linger));
struct linger *Linger;
```

### ARGUMENTS

#### **Linger**

VMS Usage:	<b>linger_structure</b>
type:	<b>struct linger</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to a structure describing whether the **SO\_LINGER** option is enabled or disabled.

```
struct linger {
    int    l_onoff;        /* option on/off */
    int    l_linger;      /* linger time */
};
```

When the **l\_onoff** field is nonzero, **SO\_LINGER** is enabled. When it is 0, **SO\_LINGER** is disabled. If **SO\_LINGER** is being enabled, the **l\_linger** field specifies the timeout period, in seconds.

## socket option SO\_OOBINLINE

Enables receipt of out-of-band data along with the regular data stream. You can use this option instead of specifying the **MSG\_OOB** flag to the **recv()** or **recvfrom()** functions.

### FORMAT

```
Status = setsockopt(VMS_Channel, SOL_SOCKET, SO_OOBINLINE, On, sizeof(*On));  
unsigned int *On;
```

### ARGUMENTS

<b>On</b>	
VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to an integer buffer that specifies whether the **SO\_OOBINLINE** option is enabled or disabled. A nonzero value enables **SO\_OOBINLINE**. A value of 0 disables **SO\_OOBINLINE**.

## socket option **SO\_RCVBUF**

Specifies the amount of buffer space that can be used to buffer received data on the socket. The default value is 6144. You can specify this option to raise the TCP window size, increase the maximum size of UDP datagrams that can be received, or increase buffer space in general.

### FORMAT

```
Status = setsockopt(VMS_Channel, SOL_SOCKET, SO_RCVBUF, Value, sizeof(*Value));  
unsigned int *Value;
```

### ARGUMENTS

**Value**

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to an integer buffer that specifies the new size of the receive buffer, in bytes.

## **socket option SO\_RCVLOWAT**

This option exists only for compatibility with UNIX 4.3BSD and has no effect on MultiNet sockets.

## socket option **SO\_RCVTIMEO**

This option exists only for compatibility with UNIX 4.3BSD and has no effect on MultiNet sockets.

## socket option SO\_REUSEADDR

Specifies how to reuse local addresses.

When **SO\_REUSEADDR** is enabled, **bind()** allows a local port number to be used even if sockets using the same local port number already exist, provided that these sockets are connected to a unique remote port. This option allows a server to **bind()** to a socket to listen for new connections, even if connections are already in progress on this port.

### FORMAT

```
Status = setsockopt(VMS_Channel, SOL_SOCKET, SO_REUSEADDR, On, sizeof(*On));  
unsigned int *On;
```

### ARGUMENTS

<b>On</b>	
VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to an integer buffer that specifies whether **SO\_REUSEADDR** is enabled or disabled. A nonzero value enables **SO\_REUSEADDR**. A value of 0 disables **SO\_REUSEADDR**.

## socket option **SO\_SNDBUF**

Specifies the amount of buffer space that can be used to buffer transmitted data on the socket. The default value is 6144 for TCP and 2048 for UDP. You can specify this option to raise the TCP window size, increase the maximum size of UDP datagrams that can be transmitted, or increase buffer space in general.

### FORMAT

```
Status = setsockopt(VMS_Channel, SOL_SOCKET, SO_SNDBUF, Value, sizeof(*Value));  
unsigned int *Value;
```

### ARGUMENTS

**Value**

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to an integer buffer that specifies the new size of the transmit buffer, in bytes.

## **socket option SO\_SNDLOWAT**

This option exists only for compatibility with UNIX 4.3BSD and has no effect on MultiNet sockets.

## socket option **SO\_SNDTIMEO**

This option exists only for compatibility with UNIX 4.3BSD and has no effect on MultiNet sockets.

## socket option SO\_TYPE

Retrieves the socket type (such as **SOCK\_DGRAM** or **SOCK\_STREAM**). This function is only valid with the **getsockopt()** function.

### FORMAT

```
Status = getsockopt(VMS_Channel, SOL_SOCKET, SO_TYPE, sizeof(*Value));  
unsigned int *Value;
```

### ARGUMENTS

**Value**

VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>write only</b>
mechanism:	<b>by reference</b>

A pointer to an integer buffer that receives the socket type.

## socket option TCP\_KEEPAIVE

Lets you specify how long an idle socket remains open if the **SO\_KEEPAIVE** option is enabled.

If **SO\_KEEPAIVE** is enabled, **TCP\_KEEPAIVE** lets you specify:

Idle time	The amount of time a TCP socket should remain idle before sending the first keepalive packet.
Probe interval	The amount of time between keepalive packets.
Probe count	The number of keepalive packets to be sent before the connection is closed.

This feature is available to both the INETDRIVER and the UCXDRIVER, although it is usually accessed through the UCXDRIVER.

### FORMAT

```
Status = setsockopt(VMS_Channel, IPPROTO_TCP, TCP_KEEPAIVE, keepalive), sizeof(struct tcp_keepalive));
```

```
struct tcp_keepalive *Keepalive
```

### ARGUMENTS

#### Keepalive

VMS Usage:       **keepalive\_structure**  
 type:             **struct tcp\_keepalive**  
 access:           **read only**  
 mechanism:       **by reference**

A pointer to a structure specifying the keepalive parameter values **idle\_time**, **probe\_intvl**, and **probe\_count**.

The structure **TCP\_KEEPAIVE** definition can be found in the include file TCP.H, as follows:

```
struct tcp_keepalive {
    int idle_time;     /*Time before first probe */
    int probe_intvl;  /*Time between probes */
    int probe_count;  /*Number of probes before closing connection */
};
```

The **idle\_time** and **probe\_intvl** values are specified in seconds; **probe\_count** is the number of probes to send before closing the connection.

The minimum value for **idle\_time** is 75 seconds. If a value less than 75 is specified, 75 is used.

If a value of 0 (zero) is specified for any of the entries in the structure, the current value is retained.

**Note!** The system default values are an **idle\_time** value of 120 minutes, a **probe\_intvl** value of 75 seconds, and a **probe\_count** value of 8.

## socket option TCP\_NODELAY

Disables the Nagle algorithm (RFC 896) which causes TCP to have, at most, one outstanding unacknowledged small segment. By default, the Nagle algorithm is enabled, delaying small segments of output data up to 200 ms so that they can be packaged into larger segments. If you enable **TCP\_NODELAY**, TCP sends small segments as soon as possible, without waiting for acknowledgments from the receiver or for the 200 ms TCP fast timer to expire.

### FORMAT

```
Status = setsockopt(VMS_Channel, IPPROTO_TCP, TCP_NODELAY, On, sizeof(*On));  
unsigned int *On;
```

### ARGUMENTS

<b>On</b>	
VMS Usage:	<b>longword_unsigned</b>
type:	<b>longword (unsigned)</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A pointer to an integer buffer that specifies whether the **TCP\_NODELAY** option is enabled or disabled. A value of 0 disables **TCP\_NODELAY**.

## socket\_perror()

Formats and prints the error code that is placed in the global variables **socket\_errno** and **vmserro** when an error occurs in one of the other socket functions. The error message is printed on the OpenVMS equivalent to the UNIX "stdout" device (normally SYS\$OUTPUT), and is prefixed by the specified string.

A typical use of **socket\_perror()** might be the following:

```
if (connect(s, &sin, sizeof(sin)) < 0) {
    socket_perror("connect failed");
    exit(1);
}
```

### FORMAT

```
(void) socket_perror(String);
char *String;
```

### ARGUMENTS

<b>String</b>	
VMS Usage:	<b>arbitrary_string</b>
type:	<b>ASCIZ string</b>
access:	<b>read only</b>
mechanism:	<b>by reference</b>

A C-language string with information about the last call to fail. This is printed as a prefix to the error message.

## socket\_read()

Reads messages from a socket. See also **recv()** and **recvfrom()**. This function is equivalent to a **recv()** function called with **Flags** specified as zero. The length of the message received is returned as the status. If a message is too long to fit in the supplied buffer and the socket is type **SOCK\_DGRAM**, excess bytes are discarded.

If no messages are available at the socket, the receive call waits for a message to arrive, unless the socket is non-blocking (see **socket\_ioctl()**). In this case, a status of -1 is returned, and the global variable **socket\_errno** is set to **EWOULDBLOCK**.

### FORMAT

```
int socket_read (short VMS_Channel, char *Buffer, int Size);
```

### ARGUMENTS

<b>VMS_Channel</b>	
VMS Usage:	<b>channel</b>
type:	<b>word (signed)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

A channel to the socket.

<b>Buffer</b>	
VMS Usage:	<b>arbitrary</b>
type:	<b>byte buffer</b>
access:	<b>write only</b>
mechanism:	<b>by reference</b>

The address of a buffer into which to place the data read.

<b>Size</b>	
VMS Usage:	<b>longword_signed</b>
type:	<b>longword (signed)</b>
access:	<b>read only</b>
mechanism:	<b>by value</b>

The length of the buffer specified by **Buffer**. The actual number of bytes read is returned in the **Status**.

### RETURNS

If the **socket\_read()** routine is successful, the count of the number of characters received is returned. A return value of 0 indicates an end-of-file condition; that is, the connection has been closed. If an error occurs, a value of -1 is returned, and a more specific message is returned in the global variables **socket\_errno** and **vmserro**.

## socket\_write()

Writes a message to another socket. This function is equivalent to a **send()** function called with **Flags** specified as zero.

This function can be used only when a socket has been connected with **connect()**.

If no message space is available at the socket to hold the message to be transmitted, **socket\_write()** blocks unless the socket has been placed in non-blocking I/O mode via the **socket ioctl FIONBIO**. If the socket is type **SOCK\_DGRAM** and the message is too long to pass through the underlying protocol in a single unit, the error **EMSGSIZE** is returned and the message is not transmitted.

### FORMAT

```
int socket_write ( short VMS_Channel, char *Buffer, int Size);
```

### ARGUMENTS

#### VMS\_Channel

VMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the socket.

#### Buffer

VMS Usage: **arbitrary**  
 type: **byte buffer**  
 access: **read only**  
 mechanism: **by reference**

The address of a buffer containing the data to send.

#### Size

VMS Usage: **longword\_signed**  
 type: **longword (signed)**  
 access: **read only**  
 mechanism: **by value**

The length of the buffer specified by **Buffer**.

### RETURNS

If the **socket\_write()** routine is successful, the count of the number of characters sent is returned. If an error occurs, a value of -1 is returned, and a more specific error message is returned in the global variables **socket\_errno** and **vmserrno**.

## **vms\_errno\_string()**

Formats a string corresponding to the error code that is placed in **socket\_errno** and **vmserro** when an error occurs in one of the other socket functions.

### **FORMAT**

(char \*) vms\_errno\_string();

### **RETURNS**

The **vms\_errno\_string()** function returns a pointer to the string.

## Chapter 3

---

### \$QIO Interface

The \$QIO interface allows programmers to use more sophisticated programming techniques than available with the socket library. Using the \$QIO interface, you can perform fully asynchronous I/O to the network and receive Asynchronous System Traps (ASTs) when out-of-band data arrives (similar to the UNIX **SIGURG** signal). In general, there is a one-to-one mapping between the socket library functions and \$QIO calls.

The \$QIO interface returns an OpenVMS error code in the first word of the Input/Output Status Block (**IOSB**). If the low bit of the OpenVMS error code is clear, an error has been returned by the network. The OpenVMS error code is generated from the UNIX **errno** code by multiplying the UNIX code by 8 (eight) and logical ORing it with 0x8000.

You can mix and match the socket library function and the \$QIO calls. For example, you can use **socket()** and **connect()** to establish a connection, then use **IO\$\_SEND** and **IO\$\_RECEIVE** to send and receive data on it.

**Note!** If more than one \$QIO operation is pending on a socket at any one time, there is no guarantee that the \$QIO calls will complete in the order they are queued. In particular, if more than one read or write operation is pending at any one time, the data may be interleaved. You do not need to use multiple read or write operations concurrently on the same socket to increase performance because of the network buffering.

The function codes for the MultiNet-specific \$QIO functions are defined in the include file **multinet\_root:[multinet.include.vms]inetio.def.h**.

## **IO\$\_ACCEPT**

Extracts the first connection from the queue of pending connections on a socket, creates a new socket with the same properties as the original socket, and associates an OpenVMS channel to the new socket. **IO\$\_ACCEPT** is equivalent to the **accept()** socket library function.

Normally, instead of calling **IO\$\_ACCEPT** to wait for a connection to become available, **IO\$\_ACCEPT\_WAIT** is used. This allows your process to wait for the connection without holding the extra network channel and tying up system resources. When the **IO\$\_ACCEPT\_WAIT** completes, it indicates that a connection is available. **IO\$\_ACCEPT** is then called to accept it.

### **FORMAT**

Status = SY\$QIOW(Efn, New\_VMS\_Channel, IO\$\_ACCEPT, IOSB, AstAdr, AstPrm, Address, AddrLen, VMS\_Channel, 0, 0, 0);

### **ARGUMENTS**

#### **New\_VMS\_Channel**

OpenVMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

An OpenVMS channel to a newly-created INET device. Create this channel by using **SY\$ASSIGN** to assign a fresh channel to INET0: before issuing the **IO\$\_ACCEPT** call. The accepted connection is accessed using this channel.

#### **VMS\_Channel**

OpenVMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

The OpenVMS channel to the INET: device on which the **IO\$\_LISTEN** call was performed. After accepting the connection, this device remains available to accept new connections.

#### **Address**

OpenVMS Usage: **special\_structure**  
type: **structure defined below**  
access: **write only**  
mechanism: **by reference**

An optional pointer to a structure that, following the completion of the **IO\$\_ACCEPT** call, contains the address of the socket that made the connection. This structure is defined as follows:

```
struct {  
    unsigned long Length;  
    struct sockaddr Address;  
};
```

**AddrLen**

OpenVMS Usage: **word\_unsigned**  
type: **word (unsigned)**  
access: **read only**  
mechanism: **by value**

The length of the buffer pointed to by the **Address** argument, in bytes. It must be at least 20 bytes.

## **IO\$\_ACCEPT\_WAIT**

Used to wait for an incoming connection without accepting it. This allows your process to wait for the connection without holding the extra network channel and tying up system resources. When the **IO\$\_ACCEPT\_WAIT** call completes, it indicates that a connection is available. **IO\$\_ACCEPT** is then called to accept it.

The **IO\$\_ACCEPT\_WAIT** call takes no function-specific parameters.

### **FORMAT**

Status = SYS\$QIOW(Efn, VMS\_Channel, IO\$\_ACCEPT\_WAIT, IOSB, AstAdr, AstPrm, 0, 0, 0, 0, 0, 0);

### **ARGUMENTS**

**VMS\_Channel**  
OpenVMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

The OpenVMS channel to the INET: device on which the **IO\$\_LISTEN** call was performed.

## IO\$\_BIND

Assigns an address to an unnamed socket. When a socket is created with **IO\$\_SOCKET**, it exists in a name space (address family) but has no assigned address. **IO\$\_BIND** requests that the address be assigned to the socket. **IO\$\_BIND** is equivalent to the **bind()** socket library function.

### FORMAT

```
Status = SYS$QIOW(Efn, VMS_Channel, IO$_BIND, IOSB, AstAdr, AstPrm, Name, NameLen,
0, 0, 0, 0);
```

### ARGUMENTS

#### VMS\_Channel

OpenVMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

#### Name

OpenVMS Usage: **socket\_address**  
type: **struct sockaddr**  
access: **read only**  
mechanism: **by reference**

The address to which the socket should be bound. The exact format of the **Address** argument is determined by the domain in which the socket was created.

#### NameLen

OpenVMS Usage: **socket\_address\_length**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The length of the **Name** argument, in bytes.

## **IO\$\_CONNECT**

When used on a **SOCK\_STREAM** socket, this function attempts to make a connection to another socket. When used on a **SOCK\_DGRAM** socket, this function permanently specifies the peer to which datagrams are sent to and received from. The peer socket is specified by name, which is an address in the communications domain of the socket. Each communications domain interprets the name parameter in its own way. **IO\$\_CONNECT** is equivalent to the **connect()** socket library function.

If the address of the local socket has not yet been specified with **IO\$\_BIND**, the local address is also set to an unused port number when **IO\$\_CONNECT** is called.

### **FORMAT**

Status = SYS\$QIOW(Efn, VMS\_Channel, IO\$\_CONNECT, IOSB, AstAdr, AstPrm, Name, NameLen, 0, 0, 0, 0);

### **ARGUMENTS**

#### **VMS\_Channel**

OpenVMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

#### **Name**

OpenVMS Usage: **socket\_address**  
type: **struct sockaddr**  
access: **read only**  
mechanism: **by reference**

The address of the peer to which the socket should be connected. The exact format of the **Address** argument is determined by the domain in which the socket was created.

#### **NameLen**

OpenVMS Usage: **socket\_address\_length**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The length of the Name argument, in bytes.

## IO\$\_GETPEERNAME

Returns the name of the peer connected to the specified socket. It is equivalent to the `getpeername()` socket library function.

### FORMAT

```
Status = SYS$QIOW(Efn, VMS_Channel, IO$_GETPEERNAME, IOSB, AstAdr, AstPrm,
Address, AddrLen, 0, 0, 0, 0);
```

### ARGUMENTS

#### VMS\_Channel

OpenVMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

#### Address

OpenVMS Usage: **socket\_address**  
type: **struct sockaddr**  
access: **write only**  
mechanism: **by reference**

A result parameter filled in with the address of the peer, as known to the communications layer. The exact format of the Address argument is determined by the domain in which the communication is occurring.

#### AddrLen

OpenVMS Usage: **socket\_address\_length**  
type: **longword (unsigned)**  
access: **modify**  
mechanism: **by reference**

On entry, contains the length of the space pointed to by **Address**, in bytes. On return, it contains the actual length, in bytes, of the address returned.

## **IO\$\_GETSOCKNAME**

Returns the current name of the specified socket. Equivalent to the **getsockname()** socket library function.

### **FORMAT**

Status = SYS\$QIOW(Efn, VMS\_Channel, IO\$\_GETSOCKNAME, IOSB, AstAdr, AstPrm, Address, AddrLen, 0, 0, 0, 0);

### **ARGUMENTS**

#### **VMS\_Channel**

OpenVMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

#### **Address**

OpenVMS Usage: **socket\_address**  
type: **struct sockaddr**  
access: **write only**  
mechanism: **by reference**

A result parameter filled in with the address of the local socket, as known to the communications layer. The exact format of the **Address** argument is determined by the domain in which the communication is occurring.

#### **AddrLen**

OpenVMS Usage: **socket\_address\_length**  
type: **longword (unsigned)**  
access: **modify**  
mechanism: **by reference**

On entry, contains the length of the space pointed to by **Address**, in bytes. On return, it contains the actual length, in bytes, of the address returned.

## IO\$\_GETSOCKOPT

Retrieves options associated with a socket. It is equivalent to the **getsockopt()** library routine. Options can exist at multiple protocol levels; however, they are always present at the uppermost socket level.

When manipulating socket options, you must specify the level at which the option resides and the name of the option. To manipulate options at the socket level, specify level as **SOL\_SOCKET**. To manipulate options at any other level, specify the protocol number of the appropriate protocol controlling the option. For example, to indicate that an option is to be interpreted by the TCP protocol, set **Level** to the protocol number of TCP, as determined by calling **getprotobyname()**.

**OptName** and any specified options are passed without modification to the appropriate protocol module for interpretation. The include file **multinet\_root:[multinet.include.sys]socket.h** contains definitions for socket-level options. Options at other protocol levels vary in format and name.

For more information on what socket options may be retrieved with **IO\$\_GETSOCKOPT**, see the **socket option** sections.

### FORMAT

```
Status = SYS$QIOW(Efn, VMS_Channel, IO$_GETSOCKOPT, IO$B, AstAdr, AstPrm, Level,
OptName, OptVal, OptLen, 0, 0);
```

### ARGUMENTS

#### VMS\_Channel

OpenVMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

#### Level

OpenVMS Usage: **option\_level**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The protocol level at which the option will be manipulated. Specify **Level** as **SOL\_SOCKET** or a protocol number as returned by **getprotoent()**.

#### OptName

OpenVMS Usage: **option\_name**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The option that is to be manipulated.

**OptVal**

OpenVMS Usage: **dependent on OptName**

type: **byte buffer**

access: **write only**

mechanism: **by reference**

A pointer to a buffer that is to receive the current value of the option. The format of this buffer is dependent on the option requested.

**OptLen**

OpenVMS Usage: **option\_length**

type: **longword (unsigned)**

access: **modify**

mechanism: **by reference**

On entry, contains the length of the space pointed to by **OptVal**, in bytes. On return, it contains the actual length, in bytes, of the option returned.

## IO\$\_IOCTL

Performs a variety of functions on the network; in particular, it manipulates socket characteristics, routing tables, ARP tables, and interface characteristics. The **IO\$\_IOCTL** call is equivalent to the **socket\_ioctl()** library routine.

A **IO\$\_IOCTL** request has encoded in it whether the argument is an input or output parameter, and the size of the argument, in bytes. Macro and define statements used in specifying an **IO\$\_IOCTL** request are located in the file **multinet\_root:[multinet.include.sys]ioctl.h**.

### FORMAT

Status = SYSS\$QIOW(Efn, VMS\_Channel, IO\$\_IOCTL, IOSB, AstAdr, AstPrm, Request, ArgP, 0, 0, 0, 0);

### ARGUMENTS

#### VMS\_Channel

OpenVMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the socket.

#### Request

OpenVMS Usage: **ioctl\_request**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by value**

Which **IO\$\_IOCTL** function to perform. The available **IO\$\_IOCTL** functions are documented in the **socket ioctl** sections.

#### ArgP

OpenVMS Usage: **arbitrary**  
 type: **byte buffer**  
 access: **read, write, or modify depending on Request**  
 mechanism: **by reference**

A pointer to a buffer whose format and function is dependent on the **Request** specified.

## **IO\$\_LISTEN**

Specifies the number of incoming connections that may be queued while waiting to be accepted. This backlog must be specified before accepting a connection on a socket. The **IO\$\_LISTEN** function applies only to sockets of type **SOCK\_STREAM**. The **IO\$\_LISTEN** call is equivalent to the **listen()** socket library function.

### **FORMAT**

Status = SYS\$QIOW(Efn, VMS\_Channel, IO\$\_LISTEN, IOSB, AstAdr, AstPrm, BackLog, 0, 0, 0, 0, 0);

### **ARGUMENTS**

#### **VMS\_Channel**

OpenVMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

#### **Backlog**

OpenVMS Usage: **connection\_backlog**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

Defines the maximum length of the queue of pending connections. If a connection request arrives when the queue is full, the request is ignored. The backlog queue length is limited to 5.

## IO\$\_RECEIVE (IO\$\_READVBLK)

Receives messages from a socket. This call is equivalent to the `recvfrom()`, `recv()`, and `socket_read()` socket library functions.

The length of the message received is returned in the second and third word of the I/O Status Block (**IOSB**). A count of 0 indicates an end-of-file condition; that is, the connection has been closed. If a message is too long to fit in the supplied buffer and the socket is type **SOCK\_DGRAM**, excess bytes are discarded.

If no messages are available at the socket, the **IO\$\_RECEIVE** call waits for a message to arrive, unless the socket is nonblocking (see `socket_ioctl()`).

### FORMAT

Status = SY\$QIOW(Efn, VMS\_Channel, IO\$\_RECEIVE, IOSB, AstAdr, AstPrm, Buffer, Size, Flags, From, FromLen, 0);

### ARGUMENTS

#### VMS\_Channel

OpenVMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the socket.

#### Buffer

OpenVMS Usage: **arbitrary**  
 type: **byte buffer**  
 access: **write only**  
 mechanism: **by reference**

The address of a buffer in which to place the data read.

#### Size

OpenVMS Usage: **longword\_unsigned**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by value**

The length of the buffer specified by **Buffer**. The actual number of bytes read is returned in the **Status**.

**Flags**

OpenVMS Usage: **mask\_longword**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

Control information that affects the **IO\$\_RECEIVE** call. The **Flags** argument is formed by ORing one or more of the following values:

```
#define MSG_OOB 0x1 /* process out-of-band data */  
#define MSG_PEEK 0x2 /* peek at incoming message */
```

The **MSG\_OOB** flag causes **IO\$\_RECEIVE** to read any out-of-band data that has arrived on the socket.

The **MSG\_PEEK** flag causes **IO\$\_RECEIVE** to read the data present in the socket without removing the data. This allows the caller to view the data, but leaves it in the socket for future **IO\$\_RECEIVE** calls.

**From**

OpenVMS Usage: **special\_structure**  
type: **structure defined below**  
access: **write only**  
mechanism: **by reference**

An optional pointer to a structure that, following the completion of the **IO\$\_RECEIVE**, contains the address of the socket that sent the packet. This structure is defined as follows:

```
struct {  
    unsigned short Length;  
    struct sockaddr Address;  
};
```

**FromLen**

OpenVMS Usage: **word\_unsigned**  
type: **word (unsigned)**  
access: **read only**  
mechanism: **by value**

The length of the buffer pointed to by the **From** argument, in bytes. It must be at least 18 bytes.

## IO\$\_SELECT

Examines the specified channel to see if it is ready for reading, ready for writing, or has an exception condition pending (the presence of out-of-band data is an exception condition).

The UNIX `select()` system call can be emulated by posting multiple **IO\$\_SELECT** calls on different channels.

**Note!** IO\$\_SELECT is only useful for channels assigned to the INET: device. It cannot be used for any other VMS I/O device.

### FORMAT

```
Status = SYSS$QIOW(Efn, VMS_Channel, IO$_SELECT, IOSB, AstAdr, AstPrm, Modes, 0, 0, 0, 0, 0);
```

### ARGUMENTS

#### VMS\_Channel

OpenVMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the socket.

#### Modes

OpenVMS Usage: **mask\_longword**  
 type: **longword (unsigned)**  
 access: **modify**  
 mechanism: **by reference**

On input, the **Modes** argument is a bit mask of one or more of the following values:

```
#define SELECT_DONTWAIT      (1<<0)
#define SELECT_READABLE     (1<<1)
#define SELECT_WRITEABLE    (1<<2)
#define SELECT_EXCEPTION     (1<<3)
```

If the **SELECT\_DONTWAIT** bit is set, the **IO\$\_SELECT** call will complete immediately, whether or not the socket is ready for any I/O operations. If this bit is not set, the **IO\$\_SELECT** call will wait until the socket is ready to perform one of the requested operations.

If the **SELECT\_READABLE** bit is set, the **IO\$\_SELECT** call will check if the socket is ready for reading or a connecting has been received and is ready to be accepted.

If the **SELECT\_WRITEABLE** bit is set, the **IO\$\_SELECT** call will check if the socket is ready for writing or a connect request has been completed.

If the **SELECT\_EXCEPTION** bit is set, the **IO\$\_SELECT** call will check if the socket has out-of-band data ready to read.

On output, the **Modes** argument is a bit mask that indicates which operations the socket is ready to perform. If the **SELECT\_DONTWAIT** operation was specified, the **Modes** value may be zero; if **SELECT\_DONTWAIT** is not specified, then one or more of the **SELECT\_READABLE**, **SELECT\_WRITABLE**, or **SELECT\_EXCEPTION** bits will be set.

## IO\$\_SEND

Transmits a message to another socket. It is equivalent to the **sendto()**, **send()**, and **socket\_write()** socket library functions.

If no message space is available at the socket to hold the message to be transmitted, **IO\$\_SEND** blocks unless the socket has been placed in non-blocking I/O mode via **IO\$\_IOCTL**. If the message is too long to pass through the underlying protocol in a single unit, the error **EMSGSIZE** is returned and the message is not transmitted.

### FORMAT

Status = SYSS\$QIOW(Efn, VMS\_Channel, IO\$\_SEND, IOSB, AstAdr, AstPrm, Buffer, Size, Flags, To, ToLen, 0);

### ARGUMENTS

#### VMS\_Channel

OpenVMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the socket.

#### Buffer

OpenVMS Usage: **arbitrary**  
 type: **byte buffer**  
 access: **read only**  
 mechanism: **by reference**

The address of a buffer containing the data to send.

#### Size

OpenVMS Usage: **longword\_unsigned**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by value**

The length of the buffer specified by **Buffer**.

#### Flags

OpenVMS Usage: **mask\_longword**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by value**

Control information that affects the **IO\$\_SEND** call. The **Flags** argument can be zero or the following:

```
#define MSG_OOB 0x1 /* process out-of-band data */
```

The **MSG\_OOB** flag causes **IO\$\_SEND** to send out-of-band data on sockets that support this operation (such as **SOCK\_STREAM**).

**To**

OpenVMS Usage: **socket\_address**  
type: **struct sockaddr**  
access: **read only**  
mechanism: **by reference**

An optional pointer to the address to which the packet should be transmitted. The exact format of the **Address** argument is determined by the domain in which the communication is occurring.

**ToLen**

OpenVMS Usage: **socket\_address\_length**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

An optional argument that contains the length of the address pointed to by the **To** argument.

## IO\$\_SENSEMODE

Reads the active connections status and returns status information for all of the active and listening connections.

### FORMAT

Status = SYS\$QIO(efn, chan, IO\$\_SENSEMODE, iosb, astadr, astprm, buffer, address, conn\_type, 0, 0, 0)

### ARGUMENTS

#### **p1=buffer**

OpenVMS Usage: **vector\_byte\_unsigned**

type: **byte (unsigned)**

access: **write only**

mechanism: **by reference**

Optional address of the 8-byte device characteristics buffer. Data returned is: the device class (DC\$\_SCOM) in the first byte, the device type (0) in the second byte, and the default buffer size, which is the maximum datagram size, in the high-order word of the first longword.

IO\$\_SENSEMODE returns the second longword as 0.

#### **p2=address**

OpenVMS Usage: **vector\_word\_unsigned**

type: **word (unsigned)**

access: **write only**

mechanism: **by descriptor**

Address of the descriptor for the buffer to receive the status information on the active connections.

#### **P3=value**

OpenVMS Usage: **Longword\_unsigned**

type: **Longword (unsigned)**

access: **Read only**

mechanism: **by value**

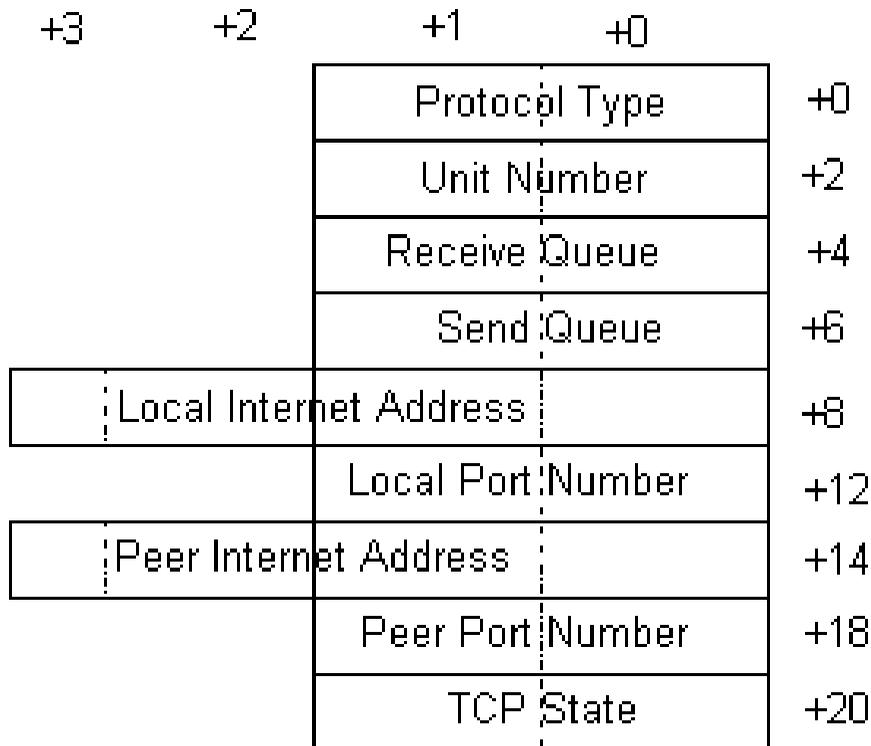
0 to get information about TCP connections, non-zero to get information about UDP connections.

Figure 3-1 shows the 22 bytes of information returned for each connection.

Protocol type	Word value is 4 for INETDRIVER stream sockets, and 5 for BGDRIVER stream sockets.
Unit number	Word value is the INETDRIVER, or BGDRIVER device unit number for the connection.

Receive queue	Word value is the number of bytes received from the peer waiting to be delivered to the user through the IO\$_READVBLK function.
Send queue	Word value is the number of bytes waiting to be transmitted to or to be acknowledged by the peer.
Local internet address	Longword value is the local internet address (or 0 if the connection is not open and no local internet address was specified for the connection).
Local port number	Word value is the local port number.
Peer internet address	Longword value is the peer's internet address (or 0 if the connection is not open and no peer internet address was specified for the connection).
Peer port number	Word value is the peer's port number, or 0 if the connection is not open and you did not specify a peer port number for the connection.
TCP state	Word value is the Transmission Control Protocol connection state mask. See the Table 3-3 description for the mask value definitions.

**Figure 3-1 Connection Status Information**



## Status

SS\$_BUFFEROVF	Buffer too small for all connections Truncated buffer returned
SS\$_DEVINACT	Device not active Contact system manager why MultiNet (or INETDRIVER) not started
SS\$_NORMAL	Success Status information returned

The byte count for the status information buffer is returned in the high-order word of the first longword of the I/O status block. This may be less than the bytes requested. See Figure 3-2 for more information.

The size in bytes of each connection's record (22 bytes) is returned in the low order word of the second longword of the I/O status block.

The total number of active connections is returned in the high-order word of the second longword of the I/O status block. This can be greater than the number of reported connections if the buffer is full.

**Figure 3-2 I/O Status Block**

Byte Count	Status Code
Number of Connections	Bytes/Record=22

**Table 3-3 TCP State Mask Values**

Mask Value	State	Mask Value	State	Mask Value	State
1	LISTEN	16	FIN-WAIT-1	256	LAST-ACK
2	SYN-SENT	32	FIN-WAIT-2	512	TIME-WAIT
4	SYN-RECEIVED	64	CLOSE-WAIT	1024	CLOSED

**Table 3-3 TCP State Mask Values**

<b>Mask Value</b>	<b>State</b>	<b>Mask Value</b>	<b>State</b>	<b>Mask Value</b>	<b>State</b>
8	ESTABLISHED	128	CLOSING		

## IO\$\_SENSEMODE | IO\$\_M\_CTRL

SS\$_BUFFEROVF	Buffer too small for all characteristics Truncated characteristics buffer is returned
SS\$_DEVINACT	Device not active Contact system manager why MultiNet (or TCPDRIVER) not started
SS\$_NORMAL	Success Characteristics returned

The byte count for the characteristics buffer is returned in the high-order word of the first longword of the I/O status block. This may be less than the bytes requested. The number of bytes in the receive queue is returned in the low order word of the second longword in the I/O status block. The number of bytes in the read queue is returned in the high-order word of the second longword in the I/O status block. Figure Figure 3-4 shows the I/O Status Block.

**Figure 3-4 I/O Status Block**

Byte Count	Status Code
Bytes in Send Queue	Bytes in Receive Queue

**Note!** You can use the SYS\$GETDVI system service to obtain the local port number, peer port number, and peer internet address. The DEVDEPEND field stores the local port number (low order word) and peer port number (high-order word). The DEVDEPEND2 field stores the peer internet address.

Performs the following functions:

- Reads network device information
- Reads the routing table
- Reads the ARP information
- Reads the IP SNMP information
- Reads the ICMP SNMP information
- Reads the TCP SNMP information
- Reads the UDP SNMP information

## FORMAT

Status = SY\$QIO(efn, chan, IO\$\_SENSEMODE | IO\$\_M\_CTRL, iosb, astadr, astprm, buffer, address, function, line-id, 0, 0)

## ARGUMENTS

### **p1=buffer**

OpenVMS Usage: **vector\_byte\_unsigned**

type: **byte (unsigned)**

access: **write only**

mechanism: **by reference**

Optional address of the 8-byte device characteristics buffer. The data returned is the device class (DC\$\_SCOM) in the first byte, the device type (0) in the second byte, and the default buffer size (0) in the high-order word of the first longword. The second longword is returned as 0.

### **p2=address**

OpenVMS Usage: **vector\_word\_unsigned**

type: **Word (unsigned)**

access: **write only**

mechanism: **by descriptor**

Address of the descriptor for the buffer to receive the information. The format of the buffer depends on the information requested. Each buffer format is described separately in the section that follows.

If bit 12 (mask 4096) is set in the parameter identifier (PID), the PID is followed by a counted string. If bit 12 is clear, the PID is followed by a longword value. While MultiNet currently never returns a counted string for a parameter, this may change in the future.

### **p3=function**

OpenVMS Usage: **Longword-unsigned**

type: **Longword (unsigned)**

access: **read only**

mechanism: **by value**

Code that designates the function.

The function codes are shown in Table 3-5.

**Table 3-5 P3 Function Codes**

<b>Code</b>	<b>Function</b>
1	P1 of the QIO is not used
2	VMS descriptor of the space to put the return information
3	10

**Table 3-5 P3 Function Codes (Continued)**

<b>Code</b>	<b>Function</b>
4	Not used
5	Not used
6	Not used
7	Read UDP SNMP counters
8	Read routing table
10	Read interface throughput information

**p4=line-id**

OpenVMS Usage: **Longword-unsigned**  
type: **Longword (unsigned)**  
access: **read only**  
mechanism: **by value**

Specify this argument only if you are reading a network device's ARP table function.

**Reading Network Device Information**

Use IO\$\_SENSEMODE | IO\$\_M\_CTRL with p3=1 to read network device information. The information returned in the buffer (specified by p2=address) can consist of multiple records. Each record consists of nine longwords, and one record is returned for each device.

When you read network device information, the data in each record is returned in the order presented below. All are longword values.

1	Line id (see the description of the line-id argument)
2	Line's local internet address
3	Line's internet address network mask
4	Line's maximum transmission unit (MTU) in the low-order word, and the line flags in the high-order word
5	Number of packets transmitted (includes ARP packets for Ethernet lines)
6	Number of transmit errors
7	Number of packets received (includes ARP and trailer packets for Ethernet lines)
8	Number of receive errors
9	Number of received packets discarded due to insufficient buffer space

## Reading the Routing Table

Use IO\$\_SENSEMODE | IO\$\_M\_CTRL with  $p3=8$  to read the routing table. The information returned in the buffer (specified by  $p2=address$ ) can consist of multiple records. Each record consists of five longwords, and one record is returned for each table entry.

The  $p3=8$  function returns full routing information and is a superset of  $p3=2$ , which was retained for backwards compatibility with existing programs.  $p3=2$  and  $p3=8$  return the same table of routing entries, in the following order, except that  $p3=2$  does not return items 7 and 8 (address mask and Path MTU):

1	Destination internet address.	Destination host or network to which the datagram is bound. Returned as a longword value.
2	Gateway internet address.	Internet address to which the datagram for this route is transmitted. Returned as a longword value.
3	Flags.	<p>Routing table entry's flag bits. Returned as a word value:</p> <p>Mask 1, name GATEWAY, if set, the route is to a gateway (the datagram is sent to the gateway internet address). If clear, the route is a direct route.</p> <p>Mask 2, name HOST, if set, the route is for a host. If clear, the route is for a network.</p> <p>Mask 4, name DYNAMIC, if set, the route was created by a received ICMP redirect message.</p> <p>Mask 8, name AUTOMATIC, if set, this route was added by MULTINET_RAPD process and will be modified or removed by that process as appropriate.</p> <p>Mask 16, name LOCKED, if set, the route cannot be changed by an ICMP redirect message.</p> <p>Mask 32, name INTERFACE, if set, the route is for a network interface.</p> <p>Mask 64, name DELETED, if set, the route is marked for deletion (it is deleted when the reference count reaches 0).</p> <p>Mask 128, name POSSDOWN, if set, the route is marked as possibly down.</p>
4	Reference count.	Number of connections currently using the route. Returned as a word value.
5	Use count.	Number of times the route has been used for outgoing traffic. Returned as a longword value.

6	Line ID.	Line identification for the network device used to transmit the datagram to the destination. See the description of the line-id argument later in this section for the line ID codes. Table 3-6 shows the line identification values.
7	Address mask.	Address mask for the destination address. Returned as a longword value.
8	Path MTU.	Path maximum transmission unit. Returned as a longword value.

**Table 3-6 Line ID Values**

Line ID	Line ID Value	Line ID	Line ID Value	Line ID	Line ID Value
LO-0	^X00000001	DN- <i>n</i>	^X00 <i>nn</i> 0241	PD- <i>n</i>	^X00 <i>nn</i> 0042
PSI- <i>n</i>	^X00 <i>nn</i> 0006	PPP- <i>n</i>	^X00 <i>nn</i> 0341		
SL- <i>n</i>	^X00 <i>nn</i> 0141	SE- <i>n</i>	^X00 <i>nn</i> 0402		

**Note!** The I/O status block (iosb) returns routing table entry size information for the p3=8 function to assist in diagnosing buffer overflow situations. See the Status section for details.

## Reading Interface Throughput Information

Use IO\$\_SENSEMODE | IO\$\_M\_CTRL with p3=10 to read network device information. The information returned in the buffer (specified by p2=descriptor) can consist of multiple records. Each record consists of nine longwords, and one record is returned for each device.

When you read network device information, the data in each record is returned in the order presented below. All are longword values.

**Table 3-7 QIO Parameters**

Code	Function
1	P1 of the QIO is not used
2	is a VMS descriptor of the space to put the return information
3	10
4	Not used
5	Not used
6	Not used

The returned data is in the following format (all values are integers):

1	Line ID
2	Average Out Bytes (for the last 6 seconds)
3	Average In Bytes
4	Average Out Packets
5	Average In Packets

### Reading the ARP Table Function

Use IO\$\_SENSEMODE | IO\$\_M\_CTRL with function=3 to read a network device's ARP table function. The information returned in the buffer (specified by p2=address) depends on the line id specified in line-id.

The line-id argument is the line id and is a longword value. The least significant byte of the line id is the major device type code. The next byte is the device type subcode. The next byte is the controller unit number. The most significant byte is ignored.

The information returned in the buffer can consist of multiple records. Each record consists of 12 bytes, and one record is returned for each ARP table entry.

When reading a table function, the data in each record is returned in the following order:

1	Internet address.	Returned as a longword value.
2	Physical address.	Returned as a 6 byte value.
3	Flags.	Returned as a word value. The ARP table entry's flag bits are shown in Table 3-8.

**Table 3-8 ARP Table Entry Flag Bits**

Mask	Name	Description
1	PERMANENT	If set, the entry can only be removed by a NETCU REMOVE ARP command and if RARP is enabled, the local host responds if a RARP request is received for this address. If clear, the entry can be removed if not used within a short period.
2	PUBLISH	If set, the local host responds to ARP requests for the internet address (this bit is usually only set for the local hosts's entry). If clear, the local host does not respond to received ARP requests for this address.

**Table 3-8 ARP Table Entry Flag Bits**

Mask	Name	Description
4	LOCKED	If set, the physical address cannot be changed by received ARP requests/replies.
4096	LASTUSED	If set, last reference to entry was a use rather than an update.
8192	CONFNEED	If set, confirmation needed on next use.
16384	CONFPEND	If set, confirmation pending.
32768	RESOLVED	If set, the physical address is valid.

**Status**

SS\$_BADPARAM	Code specified in <i>function argument invalid</i> .
SS\$_BUFFEROVF	Buffer too small for all information Truncated buffer returned.
SS\$_DEVINACT	Device not active Contact your system manager to determine why MultiNet was not started.
SS\$_NORMAL	Success Requested information returned.
SS\$_NOSUCHDEV	Line identification specified in <i>arp argument does not exist</i> .

The byte count for the information or counters buffer is returned in the high-order word of the first longword of the I/O status block. This can be less than the bytes requested.

- For the p3=2 routing table function, in the second longword of the I/O status block, bit 0 is always set, bit 1 is set if the forwarding capability is enabled, and bit 2 is set if ARP replies for non-local internet addresses are enabled.
- For the p3=8 routing table function, the IOSB contains the following:

Status Code	SS\$_NORMAL or SS\$_BUFFEROVF
Transfer Byte Count	Number of bytes of returned information
Entry Size	Number of bytes in each entry
Number of Entries	Number of entries in the routing table

If the status is SS\$\_BUFFEROVF, you can determine the number of routing entries actually

returned by calculating (Transfer Byte Count) DIV (Entry Size) and comparing that with the Number of Entries value. Be sure to check the Entry Size in the IO status block. Later versions of MultiNet may return more information for each entry, which will return a larger Entry Size. Any additional information to be returned in the future will be added to the end of the returned entry.

## Reading the IP SNMP Counters Function

Use `IO$_SENSEMODE | IO$_M_CTRL` with `function=4` to read the IP SNMP counters.

The data returned is an array of longwords in the following format:

- Indicates whether or not this entity is acting as an IP router.
- The default value inserted in the IP header's time-to-live field.
- The total number of input datagrams received.
- The number of input datagrams discarded due to errors in their IP headers.
- The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity.
- The number of IP datagrams for which this entity was not their final destination, and for which forwarding to another entity was required.
- The number of datagrams received but discarded because of an unknown or unsupported protocol.
- The number of input datagrams received but discarded for reasons other than errors.
- The total number of input datagrams successfully delivered to IP user protocols, including ICMP.
- The total number of IP datagrams that local IP user protocols (including ICMP) supplied to IP in request for transmission.
- The number of output IP datagrams that were discarded for reasons other than errors.
- The number of IP datagrams discarded because no route could be found to transmit them to their destination.
- The maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
- The number of IP fragments received that needed to be reassembled at this entity.
- The number of IP datagrams successfully reassembled.
- The number of failures detected by the IP reassembly algorithm.
- The number of IP datagrams that have been successfully fragmented at this entity.
- The number of IP datagrams that have been discarded at this entity because they could not be fragmented.
- The number of IP datagrams that have been created as a result of fragmentation at this entity.

## Reading the ICMP SNMP Counters Function

Use `IO$_SENSEMODE | IO$_M_CTRL` with `function=5` to read the ICMP SNMP counters.

The data returned is an array of longwords in the following format:

- The total number of ICMP messages received.

- The number of ICMP messages received but determined as having ICMP-specific errors.
- The number of ICMP Destination Unreachable messages received.
- The number of ICMP Time Exceeded messages received.
- The number of ICMP Parameter Problem messages received.
- The number of ICMP Source Quench messages received.
- The number of ICMP Redirect messages received.
- The number of ICMP Echo (request) messages received.
- The number of ICMP Echo reply messages received.
- The number of ICMP Timestamp (request) messages received.
- The number of ICMP Timestamp Reply messages received.
- The number of ICMP Address Mask Request messages received.
- The number of ICMP Address Mask Reply messages received.
- The total number of ICMP messages that this entity attempted to send.
- The number of ICMP messages that this entity did not send because of ICMP-related problems.
- The number of ICMP Destination Unreachable messages sent.
- The number of ICMP Time Exceeded messages sent.
- The number of ICMP Parameter Problem messages sent.
- The number of ICMP Source Quench messages sent.
- The number of ICMP Redirect messages sent.
- The number of ICMP Echo (request) messages sent.
- The number of ICMP Echo reply messages sent.
- The number of ICMP Timestamp (request) messages sent.
- The number of ICMP Timestamp Reply messages sent.
- The number of ICMP Address Mask Request messages sent.
- The number of ICMP Address Mask Reply messages sent.

## Reading the TCP SNMP Counters Function

Use `IO$_SENSEMODE | IO$_M_CTRL` with `function=6` to read TCP SNMP counters.

The data returned is an array of longwords in the following format:

- The algorithm used to determine the timeout value for retransmitting unacknowledged octets.
- The minimum value (measured in milliseconds) permitted by a TCP implementation for the retransmission timeout.
- The maximum value (measured in milliseconds) permitted by a TCP implementation for the retransmission timeout.
- The limit on the total number of TCP connections supported.
- The number of times TCP connections have made a transition to the SYN-SENT state from the CLOSED state.
- The number of times TCP connections have made a direct transition to the SYN-REVD state from the LISTEN state.
- The number of failed connection attempts.
- The number of resets that have occurred.
- The number of TCP connections having a current state of either ESTABLISHED or CLOSE-WAIT.
- The total number of segments received.
- The total number of segments sent.
- The total number of segments retransmitted.

## Reading the UDP SNMP Counters Function

Use `IO$_SENSEMODE | IO$_M_CTRL` with `function=7` to read the UDP SNMP counters.

The data returned is an array of longwords in the following format:

- The total number of IDP datagrams delivered to UDP users.
- The total number of received UDP datagrams for which there was not an application at the destination port.
- The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
- The total number of UDP datagrams sent from this entity.

## IO\$\_SETCHAR

Sets special characteristics that control the operation of the INET: device, rather than the socket attached to it. These operations are normally used by only the MULTINET\_SERVER process to hand off a connection to a process that it creates to handle the connection.

### FORMAT

```
Status = SYSS$QIOW(Efn, VMS_Channel, IO$_SETCHAR, IOSB, AstAdr, AstPrm, Flags, 0, 0, 0, 0, 0);
```

### ARGUMENTS

#### VMS\_Channel

OpenVMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the socket.

#### Flags

OpenVMS Usage: **mask\_longword**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by reference**

A bit mask of one or more of the following values. If **IO\$\_SETCHAR** is not called, all options are set to **OFF**.

```
#define SETCHAR_PERMANENT (1<<0)
#define SETCHAR_SHAREABLE (1<<1)
#define SETCHAR_HANDOFF (1<<2)
```

If the **SETCHAR\_PERMANENT** bit is set when the last channel to the socket device is deassigned using the **SYSS\$DASSGN** system service, the socket is not closed and the socket device is not deleted. Normally, the last deassign closes the socket. If this bit has been set, it must be explicitly cleared before the socket can be deleted.

If the **SETCHAR\_SHAREABLE** bit is set, the socket becomes a shareable device and any process can assign a channel to it.

If the **SETCHAR\_HANDOFF** bit is set, the socket is not closed and the socket device is not deleted when the last channel to the socket device is deassigned. After this occurs, the socket reverts to a normal socket, and if a new channel is assigned and deassigned, the socket is closed. The **SETCHAR\_HANDOFF** bit is a safer version of the **SETCHAR\_PERMANENT** bit because it allows a single hand-off to another process without the risk of a socket getting permanently stuck on your system.

## **IO\$\_SETMODE|IO\$\_M\_ATTNAST**

Enables an AST to be delivered to your process when out-of-band data arrives on a socket. This is similar to the UNIX 4.3BSD **SIGURG** signal being delivered. You cannot enable the delivery of the AST through the socket library functions.

After the AST is delivered, you must explicitly reenable it using this call if you want the AST to be delivered when future out-of-band data arrives.

### **FORMAT**

Status = SYS\$QIOW(Efn, VMS\_Channel, IO\$\_SETMODE|IO\$\_M\_ATTNAST, IOSB, AstAdr, AstPrm, Routine, Parameter, 0, 0, 0, 0);

### **ARGUMENTS**

#### **Routine**

OpenVMS Usage: **ast\_procedure**  
type: **procedure entry mask**  
access: **call without stack unwinding**  
mechanism: **by reference**

The address of the AST routine to call when out-of-band data arrives on the socket. To disable AST delivery, set **Routine** to 0.

#### **Parameter**

OpenVMS Usage: **user\_arg**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The argument with which to call the AST routine.

## IO\$\_SETSOCKOPT

Manipulates options associated with a socket. It is equivalent to the **setsockopt()** socket library function. Options may exist at multiple protocol levels; however, they are always present at the uppermost socket level.

When manipulating socket options, you must specify the level at which the option resides and the name of the option. To manipulate options at the socket level, specify **Level** as **SOL\_SOCKET**. To manipulate options at any other level, specify the protocol number of the appropriate protocol controlling the option. For example, to indicate that an option is to be interpreted by the TCP protocol, set **Level** to the protocol number of TCP; see **getprotobyname()**.

**OptName** and any specified options are passed without modification to the appropriate protocol module for interpretation. The include file **multinet\_root:[multinet.include.sys]socket.h** contains definitions for socket-level options. Options at other protocol levels vary in format and name.

### FORMAT

```
Status = SYS$QIOW(Efn, VMS_Channel, IO$_SETSOCKOPT, IOSB, AstAdr, AstPrm, Level,
OptName, OptVal, OptLen, 0, 0);
```

### ARGUMENTS

#### VMS\_Channel

OpenVMS Usage: **channel**  
type: **word (signed)**  
access: **read only**  
mechanism: **by value**

A channel to the socket.

#### Level

OpenVMS Usage: **option\_level**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The protocol level at which the option will be manipulated. Specify **Level** as **SOL\_SOCKET**, or a protocol number as returned by **getprotobyname()**.

#### OptName

OpenVMS Usage: **option\_name**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The option that is to be manipulated. For a description of each of the valid options for **IO\$\_SETSOCKOPT**, see the **socket option** sections.

**OptVal**

OpenVMS Usage: **dependent on OptName**

type: **byte buffer**

access: **read only**

mechanism: **by reference**

A pointer to a buffer that contains the new value of the option. The format of this buffer depends on the option requested.

**OptLen**

OpenVMS Usage: **option\_length**

type: **longword (unsigned)**

access: **read only**

mechanism: **by value**

The length of the buffer pointed to by **OptVal**.

## IO\$\_SHUTDOWN

Shuts down all or part of a full-duplex connection on the socket associated with **VMS\_Channel**. This function is usually used to signal an end-of-file to the peer without closing the socket itself, which would prevent further data from being received. It is equivalent to the **shutdown()** socket library function.

### FORMAT

```
Status = SYS$QIOW(Efn, VMS_Channel, IO$_SHUTDOWN, IOSB, AstAdr, AstPrm, How, 0, 0, 0, 0, 0);
```

### ARGUMENTS

#### **VMS\_Channel**

OpenVMS Usage: **channel**  
 type: **word (signed)**  
 access: **read only**  
 mechanism: **by value**

A channel to the socket.

#### **How**

OpenVMS Usage: **longword\_unsigned**  
 type: **longword (unsigned)**  
 access: **read only**  
 mechanism: **by value**

Controls which part of the full-duplex connection to shut down, as follows: if **How** is 0, further receive operations are disallowed; if **How** is 1, further send operations are disallowed; if **How** is 2, further send and receive operations are disallowed.

## IO\$\_SOCKET

Creates an end point for communication and returns an OpenVMS channel that describes the end point. It is equivalent to the **socket()** socket library function.

Before issuing the **IO\$\_SOCKET** call, an OpenVMS channel must first be assigned to the INET0: device to get a new channel to the network.

### FORMAT

```
Status = SYS$QIOW(Efn, VMS_Channel, IO$_SOCKET, IOSB, AstAdr, AstPrm,
Address_Family, Type, Protocol, 0, 0, 0);
```

### ARGUMENTS

#### Address\_Family

OpenVMS Usage: **address\_family**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

An address family with which addresses specified in later operations using the socket will be interpreted. The following formats are currently supported; they are defined in the include file **multinet\_root:[multinet.include.sys]socket.h**:

AF_INET	Internet (TCP/IP) addresses
AF_PUP	Xerox PUP addresses
AF_CHAOS	CHAOSnet addresses

#### Type

OpenVMS Usage: **socket\_type**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

The semantics of communication using the created socket. The following types are currently defined:

SOCK_STREAM	SOCK_DGRAM	SOCK_RAW
-------------	------------	----------

A **SOCK\_STREAM** socket provides a sequenced, reliable, two-way connection-oriented byte stream with an out-of-band data transmission mechanism. A **SOCK\_DGRAM** socket supports communication by connectionless, unreliable messages of a fixed (typically small) maximum length. **SOCK\_RAW** sockets provide access to internal network interfaces. The type **SOCK\_RAW** is available only to users with SYSPRV privilege.

The **Type** argument, together with the **Address\_Family** argument, specifies the protocol to be used. For example, a socket created with **AF\_INET** and **SOCK\_STREAM** is a TCP socket, and a socket created with **AF\_INET** and **SOCK\_DGRAM** is a UDP socket.

**Protocol**

OpenVMS Usage: **protocol\_number**  
type: **longword (unsigned)**  
access: **read only**  
mechanism: **by value**

A protocol to be used with the socket. Normally, only a single protocol exists to support a particular socket type using a given address format. However, many protocols may exist, in which case a particular protocol must be specified by **Protocol**. The protocol number to use depends on the communication domain in which communication will take place.

For TCP and UDP sockets, the protocol number **MUST** be specified as 0. For **SOCK\_RAW** sockets, the protocol number should be the value returned by **getprotobyname()**.

## **SY\$CANCEL**

Cancels any I/O **IOSB** status of **SS\$\_CANCEL**.

Outstanding I/O operations are automatically cancelled at image exit.

For more information on **SY\$CANCEL**, see the *OpenVMS System Services Reference Manual*.

### **FORMAT**

Status = SY\$CANCEL(VMS\_Channel);

## SYS\$DASSGN

Equivalent to the `socket_close()` function. When you deassign a channel, any outstanding I/O is completed with an **IOSB** status of `SS$_CANCEL`. Deassigning a channel closes the network connection.

I/O channels are automatically deassigned at image exit.

For more information on **SYS\$DASSGN**, see the *OpenVMS System Services Reference Manual*.

### FORMAT

Status = SYS\$DASSGN(VMS\_Channel);



## Chapter 4

# SNMP Extensible Agent API Routines

This chapter is for application programmers. It describes the Application Programming Interface (API) routines required for an application program to export private Management Information Bases (MIBs) using the MultiNet SNMP agent.

To be able to use your private Management Information Base (MIB) with MultiNet's SNMP agent, develop a shareable image that exports the following application programming interface routines, in addition to routines you may need to access the MIB variables:

<b>SnmpExtensionInit</b>	Called by the SNMPD agent after startup to initialize the MIB subagent
<b>SnmpExtensionInitEx</b>	Registers multiple subtrees with the subagent (called by the SNMPD agent at startup only implemented)
<b>SnmpExtensionQuery</b>	Completes the MIB subagent query (called by the SNMPD agent to handle a <code>get</code> , <code>getnext</code> , or <code>set</code> request)
<b>SnmpExtensionTrap</b>	Sends an enterprise-specific trap (called by the SNMPD agent when the subagent alerts the agent that a trap needs to be set)

**Note!** The routine names used in this API are taken from the Microsoft SNMP Extension Agent for Windows NT.

The SNMP shareable images need to be configured for the SNMP agent to interact with them.

See the *Configuring MultiNet SNMP Agents* chapter of the *MultiNet for OpenVMS Installation and Administrator's Guide* for details on configuring the SNMP agent.

SNMP subagent developers should use the include file `SNMP_COMMON.H` found in the `MULTINET_COMMON_ROOT:[MULTINET.INCLUDE]` directory. This file defines the data structures the API uses.

For details on MultiNet's SNMP agent, see *Configuring MultiNet SNMP Agents* in the *MultiNet for OpenVMS Installation and Administrator's Guide*.

## Requirements

You require the following before using the SNMP extensible agent API routines:

- Working knowledge of SNMP; specifically the following RFCs:
  - RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*
  - RFC 1157, *A Simple Network Management Protocol (SNMP)*
  - RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*
- Working knowledge of OpenVMS shareable images

## Linking the Extension Agent Image

To link the Extension Agent Image you need to create an option file. The two examples below are for VAX systems and Alpha Systems, respectively.

### VAX

```
!Note: Exclude SnmpExtensionInitEx if it is not needed.
!See the definition of this routine.
!
UNIVERSAL=SnmpExtensionInit, -
SnmpExtensionQuery, -
SnmpExtensionTrap, -
SnmpExtensionInitEx
SYS$SHARE:VAXCRTL/SHARE
!
!List your object/library files here
```

### Alpha

```
!Note: Exclude SnmpExtensionInitEx if it is not needed.
!See the definition of this routine.
!
SYMBOL_VECTOR=( SnmpExtensionInit=PROCEDURE, -
SnmpExtensionQuery=PROCEDURE, -
SnmpExtensionTrap=PROCEDURE, -
SnmpExtensionInitEx=PROCEDURE)
!
!List your object/library files here
```

Your link statement should then look like this:

```
$ LINK /SHARE= image-name option-file/OPT
```

*image-name* is the name of the shareable image you want to build, and *option-file* is the option file mentioned above.

## Installing the Extension Agent Image

You should copy the shareable image you build for your SNMP subagent to the SYSSHARE.

**CAUTION!** Since the shareable image is loaded into the same process address space as the SNMPD server, an access violation by the subagent shareable image can crash the server application. Ensure the integrity of your shareable image by testing it thoroughly. Shareable image errors can also corrupt the server's memory space or may result in memory or resource leaks.

## Debugging Code

SNMP subagent developers can use a debug logical, MULTINET\_SNMP\_DEBUG, to set certain debug masks. Define the logical as follows and use the *mask* values in Table 4-1:

```
$ DEFINE MULTINET_SNMP_DEBUG mask
```

**Table 4-1** Debugging Mask Values

Mask Value	Description
0010	Raw SNMP input
0020	Raw SNMP output
0040	ASN.1 encoded message input
0080	ASN.1 encoded message output
1000	SNMP Subagent Developer debug mask (prints events and statuses)

## Subroutine Reference

The following pages include the subroutine descriptions.

## SnmExtensionInit

Initializes the SNMP subagent and registers the subagent in the SNMPD agent. The subagent calls this routine at startup.

### Format

status = SmnpExtensionInit (*trap-alert-routine, time-zero-reference, trap-event, supported-view*)

### Return Values

TRUE	Subagent initialized successfully
FALSE	Subagent initialization failed

### Arguments

#### **trap-alert-routine**

OpenVMS usage:	address
type:	integer
access:	read only
mechanism:	by value

Address of the routine the subagent should call when it is ready to send a trap.

#### **trap-event**

OpenVMS usage:	unsigned long
type:	longword (unsigned)
access:	write only
mechanism:	by reference

Currently unused.

**time-zero-reference**

OpenVMS usage:	unsigned long
type:	longword (unsigned)
access:	read only
mechanism:	by value

Time reference the SNMP agent provides, in hundredths of a second. Use C routines `time()` and `difftime()` to calculate MIB uptime (in hundredths of a second).

**supported-view**

OpenVMS usage:	object identifier
type:	AsnOBJID (see the SNMP_COMMON.H file)
access:	write only
mechanism:	by reference

Prefix of the MIB tree the subagent supports.

## SnmExtensionInitEx

Registers multiple MIB subtrees with agent.

This routine is called multiple times, once for each MIB subtree that needs to be registered. If the routine passes back the first or next MIB subtree, return with TRUE. If all the MIB subtrees were passed back, return with FALSE.

**Note!** Only implement this routine if you have multiple MIB subtrees in your extendible agent. The MultiNet SNMP agent executes this routine if it exists and overwrites MIB information set by `SnmExtensionInit`.

### Format

status = SmnExtensionInitEx (*supported-view*)

### Return Values

TRUE	Returning first or next MIB subtree
FALSE	All MIB subtrees were passed back

### Arguments

#### **supported-view**

OpenVMS usage:	object identifier
type:	AsnOBJID (see the SNMP_COMMON.H file)
access:	write only
mechanism:	by reference

Prefix of the MIB tree the subagent supports.

### Example

```
int SmnExtensionInitEx (AsnOBJID *supportedView)
{
    int view1[] = {1, 3, 6, 1, 4, 1, 12, 2, 1 };
    int view2[] = {1, 3, 6, 1, 4, 1, 12, 2, 2 };
    int view3[] = {1, 3, 6, 1, 4, 1, 12, 2, 5 };
    static int whichView = 0;
    switch ( whichView++ ) {
    case 0:
        supportedView->idLength = 9;
```

```
    memcpy (supportedView->ids, view1, 9* sizeof (int));
    break;
case 1:
    supportedView->idLength = 9;
    memcpy (supportedView->ids, view2, 9* sizeof (int));
    break;
case 2:
    supportedView->idLength = 9;
    memcpy (supportedView->ids, view3, 9* sizeof (int));
    break;
default:
    return (0);
}
return (1);
}
```

## SnmExtensionQuery

Queries the SNMP subagent to get or set a variable in the MIB tree served by the subagent. This routine is called by the SNMPD agent to handle a `get`, `getnext`, or `set` request.

### Format

status = SnmExtensionQuery (*request-type*, *var-bind-list*, *error-status*, *error-index*)

### Return Values

TRUE	Operation successfully completed
FALSE	Operation could not be carried out by the subagent; use <i>error-status</i> and <i>error-index</i> to provide more information

### Arguments

#### **request-type**

OpenVMS usage:	byte
type:	unsigned char
access:	read only
mechanism:	by value

Identifies the type of request GET, SET, or GET NEXT.

#### **var-bind-list**

OpenVMS usage:	user defined
type:	RFC1157VarBindList (see the SNMP_COMMON.H file)
access:	read-write
mechanism:	by value

The list of name-value pairs used in the request. For a GET request the value is filled by the subagent and for a SET request, the value is be used to change the current variable value in the subagent.

**error-status**

OpenVMS usage:	integer
type:	integer
access:	write only
mechanism:	by reference

Status of a failed operation.

**error-index**

OpenVMS usage:	integer
type:	integer
access:	write only
mechanism:	by reference

The index of the variable in the variable binding list for which the operation failed.

## SnmExtensionTrap

Sends a trap from the subagent. If the subagent wants to send a trap, it must first call the `trap-alert-routine` (see the `SnmExtensionInit` routine). The `trap-alert-routine` should be called with two parameters (`objids`, `idlength`). For example:

If the Process Software's DNS process wants to send trap information to all the communities that are interested then the DNS server must be running and the objectids passed are 1, 3, 6, 1, 4, 1, 105, 1, 2, 1, 1, 1, 3, 1, and the length of 14.

- 1,3,6,1,4,1 is the default prefix
- 105 is the enterprise id for Process Software
- 1,2,1,1,1 are the Mib object ids for the DNS process
- 3,1 are the objectids for DNSUpTrap

The SNMP agent `trap-alert-routine` creates a table of all received trap mibs. For each of these entries, the agent then calls the subagent's `SnmExtensionTrap` routine when it is ready to send the trap.

**Note!** The SNMP agent calls the subagent from inside the `trap-alert-routine`.

### Format

status = `SnmExtensionTrap` (*enterprise*, *generic-trap*, *specific-trap*, *time-stamp*, *var-bind-list*)

### Return Values

TRUE	More traps to be generated
FALSE	No more traps to be generated

### Arguments

#### **enterprise**

OpenVMS usage:	array of object identifiers
type:	AsnOBJID (see the <code>SNMP_COMMON.H</code> file)
access:	write only
mechanism:	by reference

The prefix of the MIB for the enterprise sending the trap.

**generic-trap**

OpenVMS usage:	integer
type:	integer
access:	write only
mechanism:	by reference

The generic enterprise trap id(6).

**specific-trap**

OpenVMS usage:	integer
type:	integer
access:	write only
mechanism:	by reference

The enterprise-specific trap number.

**Note!** Since an enterprise can have many traps, the combination of enterprise id, generic trap, and specific trap should give a unique identification for a trap.

**time-stamp**

OpenVMS usage:	integer
type:	integer (timeticks)
access:	write only
mechanism:	by reference

The time at which the trap was generated.

**var-bind-list**

OpenVMS usage:	user defined
type:	RFC1157VarBindList (see the SNMP_COMMON.H file)
access:	read-write
mechanism:	by value

The list of name-value pairs. This list contains name and value of the MIB variable for which the trap is generated.

---

## **PART II    RPC Programming**

Chapter 5	RPC Fundamentals
Chapter 6	Building Distributed Applications with RPC
Chapter 7	RPCGEN Compiler
Chapter 8	RPC RTL Management Routines
Chapter 9	RPC RTL Client Routines
Chapter 10	RPC RTL Port Mapper Routines
Chapter 11	RPC RTL Server Routines
Chapter 12	RPC RTL XDR Routines



# Chapter 5

---

## RPC Fundamentals

### Introduction

MultiNet RPC Services must be used with the Compaq C Socket Library

This chapter is for RPC programmers. It provides basic information you need to know before using RPC Services to write distributed applications, including:

- What RPC Services are
- What components are in RPC Services
- How RPC clients and servers communicate
- Important RPC concepts and terms

### What Are RPC Services?

RPC Services are a set of software development tools that allow you to build distributed applications on OpenVMS systems.

### MultiNet Implementation

RPC Services are based on the Open Network Computing Remote Procedure Call (RPC) protocols developed by Sun Microsystems, Inc. These protocols are defined in the following Requests for Comments (RFCs):

- *RPC: Remote Procedure Call Protocol Specification, Version 2* (RFC 1057)
- *XDR: External Data Representation Standard* (RFC 1014)

### Distributed Applications

A distributed application executes different parts of its programs on different hosts in a network. Computers on the network share the processing workload, with each computer performing the tasks for which it is best equipped.

For example, a distributed database application might consist of a central database running on a VAX server and numerous client workstations. The workstations send requests to the server. The server carries out the requests and sends the results back to the workstations. The workstations use the results in other modules of the application.

RPCs allow programs to invoke procedures on remote hosts as if the procedures were local. RPC Services hides the networking details from the application.

RPC Services facilitates distributed processing because it relieves the application programmer of performing low-level network tasks such as establishing connections, addressing sockets, and converting data from one machine's format to another.

## Components of RPC Services

RPC Services comprises the following components:

Run-time libraries (RTLs)	RPCGEN compiler	Port Mapper	RPC Information
---------------------------	-----------------	-------------	-----------------

### Run-Time Libraries (RTLs)

RPC Services provides a single shareable RTL. The library contains:

- RPC client and server routines
- XDR routines

The *RPC RTL Management Routines*, Chapter 10, and the chapters that follow it describe the RTLs in detail.

### RPCGEN Compiler

RPCGEN is a compiler that creates the network interface portion of a distributed application. It effectively hides from the programmer the details of writing and debugging low-level network interface code. The *RPCGEN Compiler*, Chapter 8, describes how to use RPCGEN.

### Port Mapper

The Port Mapper helps RPC client programs connect to ports that are being used by RPC servers. A Port Mapper runs on each host that implements RPC Services. These steps summarize how the Port Mapper works:

- 1 RPC servers register with the Port Mapper by telling it which ports they are using.
- 2 When an RPC client needs to reach a particular server, it supplies the Port Mapper with the numbers of the remote program and program version it wants to reach. The client also specifies a transport protocol (UDP or TCP). (*Identifying Remote Programs and Procedures* provides details on these numbers.)
- 3 The Port Mapper provides the correct port number for the requested service. This process is called binding.

Once binding has taken place, the client does not have to call the Port Mapper for subsequent calls to the same server. A service can register for different ports on different hosts. For example, a server can register for port 800 on Host A and port 1000 on Host B. The Port Mapper is itself an RPC server and uses the RPC RTL. The Port Mapper plays an important role in disseminating messages for broadcast RPC. The Port Mapper is part of the Master Server Process. See the *Broadcast RPC* section for details.

## RPC Information

Use the RPC information command to:

- Request a listing of all programs that are registered with the Port Mapper

You enter this command at the DCL prompt. (See *RPC Information* in Chapter 12, *Building Distributed Applications*, for details.)

## Client-Server Relationship

In RPC, the terms client and server do not describe particular hosts or software entities. Rather, they describe the roles of particular programs in a given transaction. Every RPC transaction has a client and a server. The client is the program that calls a remote procedure; the server is the program that executes the procedure on behalf of the caller.

A program can be a client or a server at different times. The program's role merely depends on whether it is making the call or servicing the call.

## External Data Representation (XDR)

External Data Representation (XDR) is a standard that solves the problem of converting data from one machine's format to another.

RPC Services uses the XDR data description language to describe and encode data. Although similar to C language, XDR is not a programming language. It merely describes the format of data, using implicit typing. *XDR: External Data Representation Standard* (RFC 1014) defines the XDR language.

## RPC Processing Flow

Remote and local procedure calls share some similarities. In both cases, a calling process makes arguments available to a procedure. The procedure uses the arguments to compute a result, then returns the result to the caller. The caller uses the results of the procedure and resumes execution.

Figure 5-1 shows the underlying processing that makes a remote procedure call different from a local call.

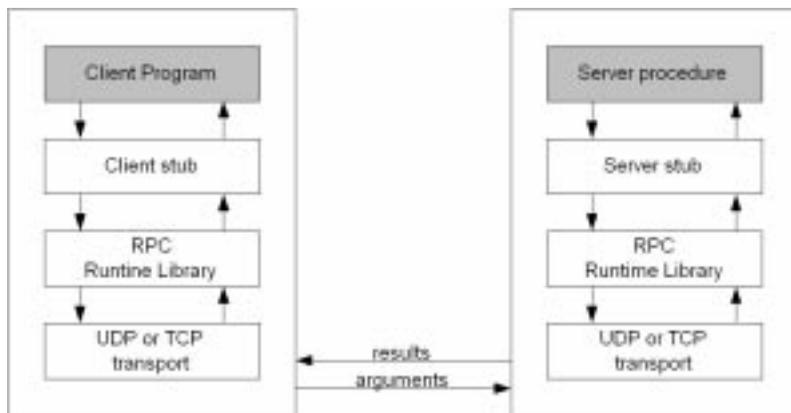
The following steps describe the processing flow during a remote procedure call:

- 1 The client program passes arguments to the client stub procedure. (See Chapter 7, *RPCGEN Compiler*, for details on how to create stubs.)
- 2 The client stub marshals the data by:
  - Calling the XDR routines to convert the arguments from the local representation to XDR
  - Placing the results in a packet

Using RPC RTL calls, the client stub sends the packet to the UDP or TCP layer for transmission to the server.

- 3 The packet travels on the network to the server, up through the layers to the server stub.
- 4 The server stub un-marshals the packet by converting the arguments from XDR to the local representation. Then it passes the arguments to the server procedure.

**Figure 5-1 RPC Processing Flow**



## Local Calls Versus Remote Calls

This section describes some of the ways in which local and remote procedure calls handle system crashes, errors, and call semantics.

### Handling System Crashes

Local procedure calls involve programs that reside on the same host. Therefore, the called procedure cannot crash independently of the calling program.

Remote procedure calls involve programs that reside on different hosts. Therefore, the client program does not necessarily know when the remote host has crashed.

### Handling Errors

If a local procedure call encounters a condition that prevents the call from executing, the local operating system usually tells the calling procedure what happened.

If a remote procedure call cannot be executed for some reason (e.g., errors occur on the network or remote host), the client might not be informed of what happened. You may want to build a signaling or condition-handling mechanism into the application to inform the client of such errors.

RPC returns certain types of errors to the client, such as those that occur when it cannot decode arguments. The RPC server must be able to return processing-related errors, such as those that occur when arguments are invalid, to the client. However, the RPC server may not return errors during batch processing or broadcast RPC.

## Call Semantics

Call semantics determine how many times a procedure executes.

Local procedures are guaranteed to execute once and only once.

Remote procedures have different guarantees, depending on which transport protocol is used.

The TCP transport guarantees execution once and only once as long as the server does not crash. The UDP transport guarantees execution at least once. It relies on the XID cache to prevent a remote procedure from executing multiple times.

See *XID Cache* for details on the XID cache.

## Programming Interface

The RPC RTL is the programming interface to RPC. You may think of this interface as containing multiple levels.

The RPC RTL reference chapters describe each routine.

## High-Level Routines

The higher-level RPC routines provide the simplest RPC programming interface. These routines call lower-level RPC routines using default arguments, effectively hiding the networking details from the application programmer.

When you use high-level routines, you sacrifice control over such tasks as client authentication, port registration, and socket manipulation, but you gain the benefits of using a simpler programming interface. Programmers using high-level routines can usually develop applications faster than they can using low-level RPC routines.

You can use the RPCGEN compiler only when you use the highest-level RPC programming interface.

## Mid-Level Routines

The mid-level routines provide the most commonly used RPC interface. They give the programmer some control over networking tasks, but not as much control as the low-level routines permit.

For example, you can control memory allocation, authentication, ports, and sockets using mid-level routines.

The mid-level routines require you to know procedure, program, and version numbers, as well as input and output types. Output data is available for future use. You can use the `registerrpc` and `callrpc` routines.

## Low-Level Routines

The low-level routines provide the most complicated RPC interface, but they also give you the most control over networking tasks such as client authentication, port registration, and socket manipulation. These routines are used for the most sophisticated distributed applications.

## Transport Protocols

RPC Services uses the transport protocols listed in Table 5-1. The RPC client and server must use the same transport protocol for a given transaction.

**Table 5-1** RPC Transport Protocols

Protocols	Characteristics
UDP	Unreliable datagram service
	Connectionless
	Used for broadcast RPC
	Maximum broadcast message size in either direction on an Ethernet line: 1500
	Execution is guaranteed at least once (see <i>XID Cache</i> )
	Calls cannot be processed in batch
TCP	Reliable
	Connection-oriented
	Can send an unlimited number of bytes per RPC call
	Execution is guaranteed once and only once
	Calls can be processed in batch
No broadcasting	

**Note!** You must use the Compaq C Socket Library with RPC Services.

## XID Cache

The XID cache stores responses the server has sent. When the XID cache is enabled, the server does not have to recreate every response to every request. Instead, the server can use the responses in the cache. Thus, the XID cache saves computing resources and improves the performance of the server.

Only the UDP transports can use the XID cache. The reliability of the TCP transport generally makes the XID cache unnecessary. UDP is inherently unreliable.

Table 5-2 shows how the XID caches differ for the UDP and UDPA/TCPA transports.

**Table 5-2 XID Cache Differences**

UDP Transport	UDPA/TCPA Transports
Places every response in the XID cache	Allows the server to specify which responses are to be cached, using the <code>sv cudpa_enablecache</code> and <code>sv tcpa_enablecache</code> routines
XID cache cannot be disabled	Requires you to disable the XID cache after use

## Cache Entries

Each entry in the XID cache contains:

- The encoded response that was sent over the network
- The internet address of the client that sent the request
- The transaction ID that the client assigned to the request

## Cache Size

You determine the size of the XID cache. Consider these factors:

- How many clients are using the server.
- Approximately how long the cache should save the responses.
- How much memory you can allocate. Each entry requires about 8Kbytes.

The more active the server is, the less time the responses remain in the cache.

## Execution Guarantees

As explained earlier in *Local Calls Versus Remote Calls*, remote procedures have different execution guarantees, depending on which transport protocol is used. The XID cache affects the execution guarantee.

The TCP transport guarantees execution once and only once as long as the server does not crash. The UDP transport guarantees execution at least once. If the XID cache is enabled, a UDP procedure is unlikely to execute more than once.

## Enabling XID Cache

Use the `svcadp_enablecache` routine to enable the XID cache. This routine is described in the RPC RTL reference chapters.

Not enabling the XID cache saves memory.

## Broadcast RPC

Broadcast RPC allows the client to send a broadcast call to all Port Mappers on the network and wait for multiple replies from RPC servers.

For example, a host might use a broadcast RPC message to inform all hosts on a network of a system shutdown.

Table 5-3 shows the differences between normal RPC and broadcast RPC.

**Table 5-3 Normal RPC vs Broadcast RPC**

<b>Normal RPC</b>	<b>Broadcast RPC</b>
Client expects one answer	Client expects many answers
Can use TCP or UDP	Requires UDP
Server always responds to errors	Server does not respond to errors; Client does not know when errors occur
Port Mapper is desirable, but not required if you use fixed port numbers	Requires Port Mapper services

Broadcast RPC sends messages to only one port—the Port Mapper port—on every host in the network. On each host, the Port Mappers pass the messages to the target RPC server. The servers compute the results and send them back to the client.

## Identifying Remote Programs and Procedures

The RPC client must uniquely identify the remote procedure it wants to reach. Therefore, all remote procedure calls must contain these three fields:

- A remote program number
- The version number of the remote program
- A remote procedure number

## Remote Program Numbers

A remote program is a program that implements at least one remote procedure. Remote programs

are identified by numbers that you assign during application development. Use Table 5-4 to determine which program numbers are available. The numbers are in groups of hexadecimal 20000000.

**Table 5-4 Remote Program Numbers**

Range	Purpose
0 to 1FFFFFFF	Defined and administered by Sun Microsystems. Should be identical for all sites. Use only for applications of general interest to the Internet community.
20000000 to 3FFFFFFF	Defined by the client application program. Site-specific. Use primarily for new programs.
40000000 to 5FFFFFFF	Use for applications that generate program numbers dynamically.
60000000 to FFFFFFFF	Reserved for the future. Do not use.

## Remote Version Numbers

Multiple versions of the same program may exist on a host or network. Version numbers distinguish one version of a program from another. Each time you alter a program, remember to increment its version number.

## Remote Procedure Numbers

A remote program may contain many remote procedures. Remote procedures are identified by numbers that you assign during application development. Follow these guidelines when assigning procedure numbers:

- Use 1 for the first procedure in a program. (Procedure 0 should do nothing and require no authentication to the server.)
- For each additional procedure in a program, increment the procedure number by one.

## Additional Terms

Before writing RPC applications, you should be familiar with the terms in Table 5-5.

**Table 5-5 Additional Terms**

Term	Definition
Channel	An OpenVMS term referring to a logical path that connects a process to a physical device, allowing the process to communicate with that device. A process requests OpenVMS to assign a channel to a device. Refer to Compaq documentation for more information on channels.

**Table 5-5 Additional Terms (Continued)**

Term	Definition									
Client handle	<p>Information that uniquely identifies the server to which the client is sending the request. Consists of the server's host name, program number, program version number, and transport protocol.</p> <p>See the following routines in the <i>RPC RTL Client Routines</i>:</p> <table data-bbox="286 423 991 517"> <tr> <td>authnone_create</td> <td>clnt_create</td> <td>clnt_perror</td> </tr> <tr> <td>authunix_create</td> <td>clnttcp_create</td> <td></td> </tr> <tr> <td>authunix_create_default</td> <td>clntudp_create</td> <td></td> </tr> </table>	authnone_create	clnt_create	clnt_perror	authunix_create	clnttcp_create		authunix_create_default	clntudp_create	
authnone_create	clnt_create	clnt_perror								
authunix_create	clnttcp_create									
authunix_create_default	clntudp_create									
Port	<p>An abstract point through which a datagram passes from the host layer to the application layer protocols.</p>									
Server handle	<p>Information that uniquely identifies the server. Content varies according to the transport being used. See the following routines in <i>RPC RTL Server Routines</i>:</p> <table data-bbox="286 708 940 802"> <tr> <td>svcudp_create</td> <td>svctcp_create</td> <td>svc_destroy</td> </tr> <tr> <td>svc_freeargs</td> <td>svc_getargs</td> <td>svc_getcaller</td> </tr> <tr> <td>svc_register</td> <td>svc_sendreply</td> <td>svcerr_routines</td> </tr> </table>	svcudp_create	svctcp_create	svc_destroy	svc_freeargs	svc_getargs	svc_getcaller	svc_register	svc_sendreply	svcerr_routines
svcudp_create	svctcp_create	svc_destroy								
svc_freeargs	svc_getargs	svc_getcaller								
svc_register	svc_sendreply	svcerr_routines								
Socket	<p>An abstract point through which a process gains access to the Internet. A process must open a socket and bind it to a specific destination. Note: The Compaq C Socket Library must be used with RPC Services.</p>									

---

# Building Distributed Applications with RPC

## Introduction

This chapter is for RPC programmers. It explains:

- What components a distributed application contains
- How to use RPC to develop a distributed application, step by step
- How to get RPC information

## Distributed Application Components

Table 6-1 lists the components of a distributed application.

**Table 6-1 Application Components**

<b>Component</b>	<b>Description</b>
Main program (client)	An ordinary main program that calls a remote procedure as if local
Network interface	Client and server stubs, header files, XDR routines for input arguments and results
Server procedure	Carries out the client's request (at least one is required)

These components may be written in any high-level language. The RPC Run-Time Library (RTL) routines are written in the C language.

## What You Need to Do

The following steps summarize what you need to do to build a distributed application:

- 1 Design the application.
- 2 Write an RPC interface definition. Compile it using RPCGEN, then edit the output files as necessary. (This step is optional. An RPC interface definition is not required. If you do not write one, proceed to step 3.)
- 3 Write any necessary code that RPCGEN did not generate.
- 4 Compile the RPCGEN output files, server procedures, and main program using the appropriate language compiler(s). RPCGEN output files must be compiled using Compaq C.
- 5 Link the object code, making sure you link in the RPC RTL.
- 6 Start the Port Mapper on the server host.
- 7 Execute the client and server programs.

## Step 1: Design the Application

You must write a main (client) program and at least one server procedure. The network interface, however, may be hand-written or created by RPCGEN. The network interface files contain client and server stubs, header files, and XDR routines. You may edit any files that RPCGEN creates.

When deciding whether to write the network interface yourself, consider these factors:

<b>Is execution time critical?</b>	Your hand-written code may execute faster than code that RPCGEN creates.
<b>Which RPC interface layer do you want to use?</b>	RPCGEN permits you to use only the highest layer interface. If you want to use the lower layers, you must write original code. The <i>RPC Fundamentals</i> , Chapter 6, describes the characteristics of each RPC interface layer.
<b>Which transport protocol do you want to use?</b>	

You may write your own XDR programs, but it is usually best to let RPCGEN handle these.

## Step 2: Write and Compile the Interface Definition

An interface definition is a program the RPCGEN compiler accepts as input. The *RPCGEN Compiler*, Chapter 8, explains exactly what interface definitions must contain.

Interface definitions are optional. If you write the all of the network interface code yourself, you do not need an interface definition.

You must write an interface definition if you want RPCGEN to generate network interface code.

After compiling the interface definition, edit the output file(s).

If you are not writing an interface definition, skip this step and proceed to step3.

## Step 3: Write the Necessary Code

Write any necessary code that RPCGEN did not create for you. Table 6-2 lists the texts you may use as references.

**Table 6-2 Coding References**

Reference	Purpose
RFC 1057	Defines the RPC language. Use for writing interface definitions.
RFC 1014	Defines the XDR language. Use for writing XDR filter routines.
The <i>RPC RTL Client Routines</i> chapter and those that follow	Defines each routine in the RPC RTL. Use for writing stub procedures and XDR filter routines.

## Step 4: Compile All Files

Compile the RPCGEN output files, server procedures, and main program separately.

Compaq C (VAX and Alpha):

```
$ CC /STANDARD=RELAXED /WARNING=DISABLE=(IMPLICITFUNC) filename.C
```

## Step 5: Link the Object Code

Link the object code files. Make sure you link in the RPC RTL. Use the following command.

Compaq C (VAX and Alpha):

```
$ LINK filenames, SYS$INPUT /OPTIONS
TCPIPC$RPCXDR_SHR /SHARE
SYS$SHARE:DECC$SHR /SHARE
Ctrl/Z
```

After entering the command, press **Ctrl/Z**.

To avoid repetitive data entry, you may create an OpenVMS command procedure to execute these commands.

## Step 6: Start the Port Mapper

The Port Mapper must be running on the server host. If it is not running, use the MULTINET CONFIGURE/SERVER command to start it. If you want to generate your own screen shot, you can use CRASH. Then all you have to do is change the user-entered items to **bold**, and change the v4.4(

42) to v4.4 (nnn) in the banner line.

## Step 7: Execute the Client and Server Programs

Perform these steps:

- 1 Run the server program interactively to debug it, or using the /DETACHED qualifier. Refer to Compaq documentation for details.
- 2 Run the client main program.

## Obtaining RPC Information

You can:

- Request a listing of all programs registered with a Port Mapper.

### Requesting a Program Listing

To request a listing of all programs that are registered with the Port Mapper, enter the MULTINET SHOW /RPC\_PORTMAP command in the following format at the DCL prompt:

```
$ MULTINET SHOW /RPC_PORTMAP
```

If you add /REMOTE\_HOST=*hostname* to this command:

```
$ MULTINET SHOW /RPC_PORTMAP /REMOTE_HOST=[host-name]
```

Specify the domain name of the host on which the Port Mapper resides. If you omit this parameter, RPC uses the name of the local host. Example 7-1 shows an example.

#### Example 7-1 Sample RPC Information Output

---

```
$ MULTINET SHOW/RPC_PORTMAP
MultiNet registered RPC programs:
Program  Version  Protocol  Port
-----  -
NLOCKMGR  3         TCP       2049
NLOCKMGR  1         TCP       2049
NLOCKMGR  3         UDP       2049
NLOCKMGR  1         UDP       2049
NFS       2         TCP       2049
NFS       2         UDP       2049
MOUNT    1         TCP       1024
MOUNT    1         UDP       1028
STATUS   1         TCP       1024
STATUS   1         UDP       1024
```

## RPCGEN Compiler

### Introduction

This chapter is for RPC programmers.

### What Is RPCGEN?

RPCGEN is the RPC Protocol Compiler. This compiler creates the network interface portion of a distributed application, effectively hiding from the programmer the details of writing and debugging low-level network interface code.

You are not required to use RPCGEN when developing a distributed application. If speed and flexibility are critical to your application, you can write the network interface code yourself, using RPC Run-Time Library (RTL) calls where they are needed.

Compiling with RPCGEN is one step in developing distributed applications. See Chapter 7, *Building Distributed Applications*, for a complete description of the application development process.

RPCGEN allows you to use the highest layer of the RPC programming interface. The *RPC Fundamentals*, Chapter 6, provides details on these layers.

### Software Requirements

The following software must be installed on your system before you can use RPCGEN:

VMS Version 5.0 or later	Compaq C compiler Version 3.2 or later
--------------------------	--

## Input Files

The RPCGEN compiler accepts as input programs called *interface definitions*, written in RPC Language (RPCL), an extension of XDR language. RFC 1057 and RFC 1014 describe these languages in detail.

An interface definition must always contain the following information:

- Remote program number
- Version number of the remote program
- Remote procedure number(s)
- Input and output arguments

Table 7-1 shows a sample interface definition.

---

### Example 7-1 Interface Definition

---

```
/*
** RPCGEN input file for the print file RPC batching example.
**
** This file is used by RPCGEN to create the files PRINT.H and PRINT_XDR.C
** The client and server files were developed from scratch.
*/

const MAX_STRING_LEN = 1024;    /* maximum string length */

/*
** This is the information that the client sends to the server
*/
struct a_record
{
    string  ar_buffer< MAX_STRING_LEN>;
};

program PRINT_FILE_PROG
{
    version PRINT_FILE_VERS_1
    {
        void  PRINT_RECORD( a_record) = 1;
        u_long SHOW_COUNT( void) = 2;
    } = 1;
} = 0x20000003;

/* end file PRINT.X */
```

The default extension for RPCGEN input files is `.X`.

You do not need to call the RPC RTL directly when writing an interface definition. RPCGEN inserts the necessary library calls in the output file.

## Output Files

RPCGEN output files contain code in C language. Table 7-1 lists the RPCGEN output files and summarizes their purpose. You can edit RPCGEN output files during application development.

**Table 7-1 RPCGEN Output Files**

File	Purpose
Client and server stub calls	Interface between the network and the client and server programs. Stubs use RPC RTL to communicate with the network.
XDR routines	Convert data from a machine's local data format to XDR for mat, and vice versa.
Header	Contains common definitions, such as those needed for any structures being passed.

*Invoking RPC* explains how to request specific output files.

Table 7-2 shows the conventions you should use to name output files.

**Table 7-2 RPCGEN File Naming Conventions**

File	Output Filename
Client stub	<i>inputname</i> _CLNT.C
Server stub	<i>inputname</i> _SVC.C
Header file	<i>inputname</i> .H
XDR filter routines	<i>inputname</i> _XDR.C

- *inputname* is the name of the input file. For example, if the input file is TEST.X, the server stub is TEST\_SVC.C.

When you use the RPCGEN command to create all output files at once, RPCGEN creates the output filenames listed in Table 7-2 by default. When you want to create specific kinds of output files, you must specify the names of the output files in the command line.

## Preprocessor Directives

RPCGEN runs the input files through the C preprocessor before compiling. You can use the macros listed in Table 7-3 with the `#ifdef` preprocessor directive to indicate that specific lines of code in

the input file are to be used only for specific RPCGEN output files.

**Table 7-3 Macros**

File	Macro
Client stub	RPC_CLNT
Server stub	RPC_SVC
Header file	RPC_HDR
XDR filter routines	RPC_XDR

## Invoking RPCGEN

This section explains how to invoke RPCGEN to create:

- All output files at once
- Specific output files
- Server stubs for either the TCP or UDP transport

### Creating All Output Files at Once

This command creates all four RPCGEN output files at once:

```
RPCGEN input
```

where *input* is the name of the file containing the interface definition.

In the following example, RPCGEN creates the output files PROGRAM.H, PROGRAM\_CLNT.C, PROGRAM\_SVC.C, and PROGRAM\_XDR.C:

```
RPCGEN PROGRAM.X
```

### Creating Specific Output Files

This command creates only the RPCGEN output file that you specify:

```
RPCGEN {-c | -h | -l | -m} [-o output] input
```

-c	Creates an XDR filter file (_XDR.C)
-h	Creates a header file (.H)
-l	Creates a client stub (_CLNT.C)
-m	Creates a server stub (_SVC.C) that uses both the UDP and TCP transports

-o	Specifies an output file (or the terminal if no output file is given)
output	Name of the output file
input	Name of an interface definition file with a .X extension

Follow these guidelines:

- Specify just one output file (-c, -h, -l, or -m) in a command line
- If you omit the output file, RPCGEN sends output to the terminal screen

### Examples:

#### 1 RPCGEN -h PROGRAM

RPCGEN accepts the file PROGRAM.X as input and sends the header file output to the screen, because no output file is specified.

#### 2 RPCGEN -l -o PROGRAM\_CLNT.C PROGRAM.X

RPCGEN accepts the PROGRAM.X file as input and creates the PROGRAM\_CLNT.C client stub file.

#### 3 RPCGEN -m -o PROGRAM\_SVC.C PROGRAM.X

RPCGEN accepts the PROGRAM.X file as input and creates the PROGRAM\_SVC.C server stub file. The server can use both the UDP and TCP transports.

### Creating Server Stubs for TCP or UDP Transports

This command creates a server stub file for either the TCP or UDP transport:

```
RPCGEN -s {udp | tcp} [-o output] input
```

-s	Creates a server (_SVC.C) that uses either the UDP or TCP transport (with -s, you must specify either <b>udp</b> or <b>tcp</b> ; do not also use -m)
udp	Creates a UDP server
tcp	Creates a TCP server
-o	Specifies an output file (or the terminal if no output file is given)
output	Name of the output file
input	Name of an interface definition file with a .X extension

If you omit the output file, RPCGEN sends output to the terminal screen.

In this example, RPCGEN accepts the PROGRAM.X file as input and creates the PROGRAM\_SVC.C output file, containing a TCP server stub:

```
RPCGEN -s tcp -o PROGRAM_SVC.C PROGRAM.X
```

## Error Handling

RPCGEN stops processing when it encounters an error. It indicates which line the error is on.

## Restrictions

RPCGEN does not support the following:

- The syntax `int x, y;`. You must write this as `int x; int y;`

# RPC RTL Management Routines

## Introduction

This chapter is for RPC programmers. It introduces RPC Run-Time Library (RTL) conventions and documents the management routines in the RPC RTL. These routines are the programming interface to RPC.

## Management Routines

The RPC RTL contains:

- RPC management routines
- RPC client and server routines for the UDP and TCP transport layers
- On VAX and Alpha systems, RPC provides a single shareable image accessed via the TCPIP\$RPCXDR\_SHR logical. This shareable image contains routines for all of the Compaq C floating-point types. The correct routines will automatically be called based on the compiler options used to compile the RPC application. See the Compaq C documentation for how to use the floating-point compiler options.

Chapter 7, *Building Distributed Applications with RPC*, explains how to link in the RPC RTL.

## Routine Name Conventions

In this chapter, all routines are documented according to their standard UNIX names.

## Header Files

All RPC programs include the file named RPC.H. Locations for this file are:

- TCPIP\$RPC:RPC.H

The RPC.H file includes the files listed in Table 8-1.

**Table 8-1 Header Files Included In RPC.H**

Filename	Purpose
AUTH.H	Used for authentication.
AUTH_UNIX.H	Contains XDR definitions for UNIX-style authentication.
CLNT.H	Contains various RPC client definitions.
IN.H	Defines structures for the internet and socket addresses ( <i>in_addr</i> and <i>sockaddr_in</i> ). This file is part of the C Socket Library.
RPC_MSG.H	Defines the RPC message format.
SVC.H	Contains various RPC server definitions.
SVC_AUTH.H	Used for server authentication.
TYPES.H	Defines UNIX C data types.
XDR.H	Contains various XDR definitions.
NETDB.H	Defines structures and routines to parse <i>/etc/rpc</i> .

There is an additional header file not included by RPC.H that is used by *xdr\_pmap* and *xdr\_pmaplist* routines. The file name is *pmap\_prot.h*, and the location is:

```
TCPIP$RPC:PMAP_PROT.H
```

## Management Routines

RPC management routines retrieve and maintain information that describes how a process is using RPC. This section describes each management routine and function in detail. The following information is provided for each routine:

- Format
- Arguments
- Description
- Diagnostics, or status codes returned, if any

## get\_myaddress

Returns the internet address of the local host.

### Format

```
#include  
void get_myaddress (struct sockaddr_in *addr);
```

### Argument

*addr*

Address of a `sockaddr_in` structure that will be loaded with the host internet address. The port number is always set to `htons(PMAPPORT)`.

### Description

The `get_myaddress` routine returns the internet address of the local host without doing any name translation or DNS lookups.

## getrpcbynumber

Gets an RPC entry.

### Format

```
#include
struct rpcent *getrpcbynumber(number)
int number;
```

### Argument

*number*

Program name or number.

### Description

The `getrpcbynumber` routine returns a pointer to an object with the following structure containing the broken-out fields of a line in the RPC program number database, `/etc/rpc`.

```
struct rpcent {
    char *r_name;           /* name of server for this RPC program */
    char **r_aliases;      /* alias list */
    long r_number;         /* RPC program number */
};
```

The members of this structure are:

<code>r_name</code>	Name of the server for this RPC program
<code>r_aliases</code>	Zero-terminated list of alternate names for the RPC program
<code>r_number</code>	RPC program number for this service

The `getrpcbynumber` routine sequentially searches from the beginning of the file until a matching RPC program name or program number is found, or until an EOF is encountered.

### Diagnostics

A NULL pointer is returned on EOF or error.

## getrpcport

Gets an RPC port number.

### Format

```
int getrpcport(host, prognum, versnum, proto)
```

```
char *host;
```

```
int prognum, versnum, proto;
```

### Arguments

*host*

Host running the RPC program.

*prognum*

Program number.

*proto*

Protocol name. Must be IPPROTO\_TCP or IPPROTO\_UDP.

### Description

The `getrpcport` routine returns the port number for version *versnum* of the RPC program *prognum* running on *host* and using protocol *proto*.

It returns 0 if it cannot contact the portmapper, or if *prognum* is not registered. If *prognum* is registered but not with *versnum*, it still returns a port number (for some version of the program), indicating that the program is indeed registered. The version mismatch is detected on the first call to the service.



## RPC RTL Client Routines

### Introduction

This chapter is for RPC programmers. It documents the client routines in the RPC Run-Time Library (RTL). These routines are the programming interface to RPC.

### Common Arguments

Many client, Port Mapper, and server routines use the same arguments.

Table 9-1 lists these arguments and defines their purpose. Arguments that are unique to each routine are documented together with their respective routines in this and the following chapters

**Table 9-1 Common Arguments**

<b>Argument</b>	<b>Purpose</b>
args_ptr	Address of the buffer to contain the decoded RPC arguments.
auth	RPC authentication client handle created by the <code>authnone_create</code> , <code>authunix_create</code> , or <code>authunix_create_default</code> routine.
clnt	Client handle returned by any of the client create routines.
in	Input arguments for the service procedure.
inproc	XDR routine that encodes input arguments.
out	Results of the remote procedure call.
outproc	XDR routine that decodes output arguments.
procnum	Number of the service procedure.

**Table 9-1 Common Arguments (Continued)**

<b>Argument</b>	<b>Purpose</b>
prognum	Program number of the service program.
protocol	Transport protocol for the service. Must be IPPROTO_UDP or IPPROTO_TCP.
s	String containing the message of your choice. The routines append an error message to this string.
sockp	Socket to be used for this remote procedure call. If <i>sockp</i> is RPC_ANYSOCK, the routine creates a new socket and defines <i>sockp</i> . The <i>clnt_destroy</i> routine closes the socket.  If <i>sockp</i> is a value other than RPC_ANYSOCK, the routine uses this socket and ignores the internet address of the server.
versnum	Version number of the service program.
xdr_args	XDR procedure that describes the RPC arguments.
xdrs	Structure containing XDR encoding and decoding information.
xprt	RPC server handle.

## Client Routines

The client routines are called by the client main program or the client stub procedures.

The following sections describe each client routine in detail.

## auth\_destroy

A macro that destroys authentication information associated with an authentication handle.

### Format

```
void auth_destroy (AUTH *auth)
```

### Argument

*auth*

RPC authentication client handle created by the `authnone_create`, `authunix_create`, or `authunix_create_default` routine.

### Description

Use `auth_destroy` to free memory that was allocated for authentication handles. This routine undefines the value of *auth* by deallocating private data structures.

Do not use this memory space after `auth_destroy` has completed. You no longer own it.

### See Also

`authnone_create`, `authunix_create`, `authunix_create_default`

## **authnone\_create**

Creates and returns a null RPC authentication handle for the client process.

### **Format**

```
#include
```

```
AUTH *authnone_create();
```

### **Arguments**

None.

### **Description**

This routine is for client processes that require no authentication. RPC uses it as a default when it creates a client handle.

### **See Also**

```
authnone_create, authunix_create_default,  
clnt_create, clntraw_create, clnttcp_create,  
clntudp_create / clntudp_bufcreate
```

## authunix\_create

Creates and returns an RPC authentication handle for the client process. Use this routine when the server requires UNIX-style authentication.

### Format

```
#include  
  
AUTH *authunix_create (char *host, int uid, int gid, int len, int gids);
```

### Arguments

*host*

Address of the name of the host that created the authentication information. This is usually the local host running the client process.

*uid*

User ID of the person who is executing this process.

*gid*

User's group ID.

*len*

Number of elements in the *\*gids* array.

*gids*

Address of the array of groups to which the user belongs.

### Description

Since the client does not validate the *uid* and *gid*, it is easy to impersonate an unauthorized user. Choose values the server expects to receive. The application must provide OpenVMS-to-UNIX authorization mapping.

You can use a Socket Library lookup routine to get the host name.

### See Also

authnone\_create, authunix\_create\_default

## authunix\_create\_default

Calls the `authunix_create` routine and provides default values as arguments.

### Format

```
#include
AUTH *authunix_create_default()
```

### Arguments

See below.

### Description

Like the `authunix_create` routine, `authunix_create_default` provides UNIX-style authentication for the client process. However, `authunix_create_default` does not require you to enter any arguments. Instead, this routine provides default values for the arguments used by `authunix_create`, listed in Table 9-2.

**Table 9-2 Default Arguments**

Argument	Default Value
host	local host domain name
uid	<code>getuid()</code>
gid	<code>getgid()</code>
len	0
gids	0

You can replace this call with `authunix_create` and provide appropriate values.

### Example

```
auth_destroy(client->cl_auth);
client->cl_auth = authunix_create_default();
```

This example overrides the `authnone_create` routine, where `client` is the value returned by the `clnt_create`, `clntraw_create`, `clnttcp_create`, or `clntudp_create` routine.

### See Also

`callrpc`

Calls the remote procedure identified by the routine's arguments.

# callrpc

## Format

```
#include

int callrpc (char *host, u_long prognum, u_long versnum, u_long procnum,
xdrproc_t inproc, u_char *in,
xdrproc_t outproc, u_char *out);
```

## Arguments

*host*

Host where the procedure resides.

*prognum, versnum, procnum, inproc, in, outproc, out*

See Table 9-1 for a description of the above arguments.

## Description

The `callrpc` routine performs the same functions as the `clnt_create`, and `clnt_destroy` routines.

Since the `callrpc` routine uses the UDP transport protocol, messages can be no larger than 8Kbytes. This routine does not allow you to control timeouts or authentication.

If you want to use the TCP transport, use the `clnt_create` or `clnttcp_create` routine.

## Diagnostics

The `callrpc` routine returns zero if it succeeds, and the value of enum `clnt_stat` cast to an integer if it fails.

You can use the `clnt_perrno` routine to translate failure status codes into messages.

## See Also

```
clnt_broadcast, clnt_call, clnt_create, clnt_destroy,
clnt_perrno / clnt_sperrno, clnttcp_create
```

## clnt\_broadcast

Broadcasts a remote procedure call to all local networks, using the broadcast address.

### Format

```
#include

enum clnt_stat clnt_broadcast (u_long prognum, u_long versnum, u_long
procnum, xdrproc_t inproc, u_char *in,
xdrproc_t outproc, u_char *out, resultproc_t eachresult);
```

### Arguments

*prognum, versnum, procnum, inproc, in, outproc, out*

See Table 9-1 for a description of the above arguments.

*eachresult*

Each time `clnt_broadcast` receives a response, it calls the *eachresult* routine. If *eachresult* returns zero, `clnt_broadcast` waits for more replies. If *eachresult* returns a nonzero value, `clnt_broadcast` stops waiting for replies. The *eachresult* routine uses this form:

**int eachresult(out, addr)**

**u\_char \*out;**

**struct sockaddr\_in \*addr;**

out	Contains the results of the remote procedure call, in the local data format.
*addr	Is the address of the host that sent the results.

### Description

The `clnt_broadcast` routine performs the same functions as the `callrpc` routine. However, `clnt_broadcast` sends a message to all local networks, using the broadcast address. The `clnt_broadcast` routine uses the UDP protocol.

Table 9-3 indicates how large a broadcast message can be.

**Table 9-3 Maximum Message Size**

Line	Maximum Size
Ethernet	1500 bytes
proNet	2044 bytes

## **Diagnostics**

This routine returns diagnostic values defined in the CLNT.H file for `enumclnt_stat`.

## **See Also**

`callrpc`, `clnt_perrno` / `clnt_sperrno`

## clnt\_call

A macro that calls a remote procedure.

### Format

```
enum clnt_stat clnt_call (CLIENT *clnt, u_long procnum,  
xdrproc_t inproc, u_char *in, xdrproc_t outproc, u_char *out,  
struct timeval tout);
```

### Arguments

*clnt*, *procnum*, *inproc*, *in*, *outproc*, *out*

See Table 9-1 for a description of the above arguments.

*tout*

Time allowed for the results to return to the client, in seconds and microseconds. If you use the `clnt_control` routine to change the `CLSET_TIMEOUT` code, this argument is ignored.

### Description

Use the `clnt_call` routine after using `clnt_create`. After you have finished with the client handle, use the `clnt_destroy` routine. You can use the `clnt_perror` routine to print messages for any errors that occurred.

### Diagnostics

This routine returns diagnostic values defined in the `CLNT.H` file for `enumclnt_stat`.

### See Also

`clnt_control`, `clnt_create`, `clnt_destroy`,  
`clnt_perrno` / `clnt_sperrno`

## clnt\_control

A macro that changes or retrieves information about an RPC client process.

### Format

```
bool_t clnt_control (CLIENT *clnt, u_long code, void *info);
```

### Arguments

*clnt*

Client handle returned by any of the client create routines.

*code*

Code listed in Table 9-4.

**Table 9-4 Valid Codes**

Code	Type	Purpose
CLSET_TIMEOUT	struct timeval	Set total timeout
CLGET_TIMEOUT	struct timeval	Get total timeout
CLSET_RETRY_TIMEOUT*	struct timeval	Set retry timeout
CLGET_RETRY_TIMEOUT*	struct timeval	Get retry timeout
CLGET_SERVER_ADDR	struct sockaddr_in	Get server address
* Valid only for the UDP transport protocol.		

The `timeval` is specified in seconds and microseconds. The total timeout is the length of time that the client waits for a reply. The default total timeout is 25 seconds.

The retry time is the length of time that UDP waits for the server to reply before transmitting the request. The default retry timeout is 5 seconds. You might want to increase the retry time if your network is slow.

For example, suppose the total timeout is 10 seconds and the retry time is five seconds. The client sends the request and waits five seconds. If the client does not receive a reply, it sends the request again. If the client does not receive a reply within five seconds, it does not send the request again.

If you use `CLSET_TIMEOUT` to set the timeout, the `clnt_call` routine ignores the timeout parameter it receives for all future calls.

*info*

Address of the information being changed or retrieved.

## **Diagnostics**

This routine returns TRUE if it succeeds, and FALSE if it fails.

## **See Also**

`clnt_call`, `clnt_create`, `clnt_destroy`, `clntraw_create`,  
`clnttcp_create`, `clntudp_create` / `clntudp_bufcreate`

## clnt\_create

Creates an RPC client handle.

### Format

```
#include
```

```
CLIENT *clnt_create (char *host, u_long prognum, u_long versnum, char  
*proto);
```

### Arguments

*host*

Address of the string containing the name of the remote host where the server is located.

*prognum, versnum*

See Table 9-1 for a description of the above arguments.

*proto*

Address of a string containing the name of the transport protocol. Valid values are **UDP** and **TCP**.

### Description

The `clnt_create` routine creates an RPC client handle for *prognum*. An RPC client handle is a structure containing information about the RPC client. The client can use the UDP or TCP transport protocol.

This routine uses the Port Mapper. You cannot control the local port.

The default sizes of the send and receive buffers are 8800 bytes for the UDP transport, and 4000 bytes for the TCP transport.

The retry time for the UDP transport is five seconds.

Use the `clnt_create` routine instead of the `callrpc` or `clnt_broadcast` routines if you want to use one of the following:

- The TCP transport
- An authentication other than null
- More than one active client at the same time

You can also use `clntraw_create` to use the IP protocol, `clnttcp_create` to use the TCP protocol, or `clntudp_create` to use the UDP protocol.

The `clnt_create` routine uses the global variable `rpc_createerr`. `rpc_createerr` is a structure that contains the most recent service creation error. Use `rpc_createerr` if you want the client program to handle the error. The value of `rpc_createerr` is set by any RPC client creation routine that does not succeed.

The `rpc_createerr` variable is defined in the `CLNT.H` file.

## Diagnostics

The `clnt_create` routine returns the address of the client handle, or zero (if it could not create the client handle).

If the `clnt_create` routine fails, you can use the `clnt_pcreateerror` or `clnt_spcreateerror` routines to obtain diagnostic information.

## See Also

`clnt_call`, `clnt_control`, `clnt_destroy`,  
`clnt_pcreateerror` / `clnt_spcreateerror`, `clntraw_create`,  
`clnttcp_create`, `clntudp_create` / `clntudp_bufcreate`

## clnt\_destroy

A macro that destroys an RPC client handle.

### Format

```
void clnt_destroy (CLIENT *clnt);
```

### Argument

*clnt*

Client handle returned by any of the client create routines.

### Description

The `clnt_destroy` routine destroys the client's RPC handle by deallocating all memory related to the handle. The client is undefined after the `clnt_destroy` call.

If the `clnt_create` routine had previously opened a socket, this routine closes the socket. Otherwise, the socket remains open.

### See Also

`clnt_create`, `clntraw_create`, `clnttcp_create`,  
`clntudp_create` / `clntudp_bufcreate`

## clnt\_geterr

A macro that returns an error code indicating why an RPC call failed.

### Format

```
void clnt_geterr (CLIENT *clnt, struct rpc_err *errp);
```

### Arguments

*clnt*

Client handle returned by any of the client create routines.

*errp*

Address of the structure containing information that indicates why an RPC call failed. This information is the same as `clnt_stat` contains, plus one of the following: the C error number, the range of server versions supported, or authentication errors.

### Description

This routine is primarily for internal diagnostic use.

### Example

```
#define PROGRAM          1
#define VERSION          1

CLIENT          *clnt;
struct rpc_err  err;

clnt = clnt_create( "server name", PROGRAM, VERSION, "udp");

/* calls to RPC library */

clnt_geterr( clnt, &err);
```

This example creates a UDP client handle and performs some additional RPC processing. If an RPC call fails, `clnt_geterr` returns the error code.

### See Also

`clnt_perror` / `clnt_sperror`

## clnt\_pcreateerror / clnt\_spcreateerror

Return a message indicating why RPC could not create a client handle.

### Format

```
#include

void clnt_pcreateerror (char *s);
char *clnt_spcreateerror (char *s);
```

### Argument

*s*

String containing the message of your choice. The routines append an error message to this string.

### Description

The `clnt_pcreateerror` routine prints a message to `SYSS$OUTPUT`.

The `clnt_spcreateerror` routine returns the address of a string. Use this routine if:

- You want to save the string.
- You do not want to use `printf` to print the message.
- The message format is different from the one that `clnt_perrno` supports.

The `clnt_spcreateerror` routine overwrites the string it returns, unless you save the results.

Use these routines when the `clnt_create`, `clntraw_create`, `clnttcp_create`, or `clntudp_create` routine fails.

### See Also

```
clnt_create,    clntraw_create,    clnttcp_create,
clntudp_create / clntudp_bufcreate
```

## `clnt_perrno / clnt_sperrno`

Return a message indicating why the `callrpc` or `clnt_broadcast` routine failed to create a client handle.

### Format

```
#include

void clnt_perrno (enum clnt_stat stat);
char *clnt_sperrno (enum clnt_stat stat);
```

### Argument

*stat*

Appropriate error condition. Values for *stat* are defined in the CLNT.H file.

### Description

The `clnt_perrno` routine prints a message to SYSS\$OUTPUT.

The `clnt_sperrno` routine returns the address of a string. Use this routine instead if:

- You want to save the string.
- You do not want to use `printf` to print the message.
- The message format is different from the one that `clnt_perrno` supports.

To save the string, copy it into your own memory space.

### See Also

`callrpc`, `clnt_broadcast`

## clnt\_perror / clnt\_sperror

Return a message if the `clnt_call` routine fails.

### Format

```
#include

void clnt_perror (CLIENT *clnt, char *s);
char *clnt_sperror (CLIENT *clnt, char *s);
```

### Arguments

*clnt*

See Table 9-1 for a description of the above argument. String containing the message to output.

### Description

Use these routines after `clnt_call`.

The `clnt_perror` routine prints an error message to `SYSS$OUTPUT`.

The `clnt_sperror` routine returns a string. Use this routine if:

- You want to save the string.
- You do not want to use `printf` to print the message.
- The message format is different from the one that `clnt_perror` supports.

The `clnt_sperror` routine overwrites the string with each call. Copy the string into your own memory space if you want to save it.

### See Also

```
clnt_call, clnt_create, clntraw_create, clnttcp_create,
clntudp_create / clntudp_bufcreate
```

## clntraw\_create

Returns an RPC client handle. The remote procedure call uses the IP transport.

### Format

```
#include
```

```
CLIENT *clntraw_create (struct sockaddr_in *addr,  
u_long prognum, u_long versnum, int *sockp, u_long sendsize,  
u_long recvsize);
```

### Arguments

*addr, prognum, versnum*

See Table 9-1 for a description of the above arguments.

*sockp*

Socket to be used for this remote procedure call. *sockp* can specify the local address and port number. If *sockp* is `RPC_ANYSOCK`, then a port number is assigned. The example shown for the `clntudp_create` routine shows how to set up *sockp* to specify a port. See Table 9-1 for a description of *sockp* and `RPC_ANYSOCK`.

*addr*

Internet address of the host on which the server resides.

*sendsize*

Size of the send buffer. If you enter a value less than 100, then 4000 is used as the default.

*recvsize*

Size of the receive buffer. If you enter a value less than 100, then 4000 is used as the default.

### Description

The `clntraw_create` routine creates an RPC client handle for *addr*, *prognum*, and *versnum*. The client uses the IP transport. The routine is similar to the `clnt_create` routine, except `clnttcp_create` allows you to specify a socket and buffer sizes. If you specify the port number as zero by using `addr->sin_port`, the Port Mapper provides the number of the port on which the remote program is listening.

The transport used to pass messages to the service is actually a buffer within the process's address space, so the corresponding RPC server should live in the same address space (see also `svcrw_create`). This allows simulation of RPC and getting RPC overheads, such as round trip times, without kernel interference.

The `clnttcp_create` routine uses the global variable `rpc_createerr`, which is a structure that contains the most recent service creation error. Use `rpc_createerr` if you want the client

program to handle the error. The value of `rpc_createerr` is set by any RPC client creation routine that does not succeed. The `rpc_createerr` variable is defined in the `CLNT.H` file.

## Diagnostics

The `clntraw_create` routine returns the address of the client handle, or zero (if it could not create the client handle). If the routine fails, use the `clnt_pcreateerror` or `clnt_spcreateerror` routine to obtain additional diagnostic information.

## See Also

`clnt_call`, `clnt_control`, `clnt_create`, `clnt_destroy`,  
`clnt_pcreateerror` / `clnt_spcreateerror`, `clnttcp_create`,  
`clntudp_create` / `clntudp_bufcreate`

## clnttcp\_create

Returns an RPC client handle. The remote procedure call uses the TCP transport.

### Format

```
#include
```

```
CLIENT *clnttcp_create (struct sockaddr_in *addr,  
u_long prognum, u_long versnum, int *sockp, u_long sendsize,  
u_long recvsize);
```

### Arguments

*addr, prognum, versnum*

See Table 9-1 for a description of the above arguments.

*sockp*

Socket to be used for this remote procedure call. *sockp* can specify the local address and port number. If *sockp* is `RPC_ANYSOCK`, then a port number is assigned. The example shown for the `clntudp_create` routine shows how to set up *sockp* to specify a port. See Table 9-1 for a description of *sockp* and `RPC_ANYSOCK`.

*addr*

Internet address of the host on which the server resides.

*sendsize*

Size of the send buffer. If you enter a value less than 100, then 4000 is used as the default.

*recvsize*

Size of the receive buffer. If you enter a value less than 100, then 4000 is used as the default.

### Description

The `clnttcp_create` routine creates an RPC client handle for *addr*, *prognum*, and *versnum*. The client uses the TCP transport. The routine is similar to the `clnt_create` routine, except `clnttcp_create` allows you to specify a socket and buffer sizes. If you specify the port number as zero by using `addr->sin_port`, the Port Mapper provides the number of the port on which the remote program is listening.

The `clnttcp_create` routine uses the global variable `rpc_createerr`. `rpc_createerr` is a structure that contains the most recent service creation error. Use `rpc_createerr` if you want the client program to handle the error. The value of `rpc_createerr` is set by any RPC client creation routine that does not succeed. The `rpc_createerr` variable is defined in the `CLNT.H` file.

## Diagnostics

The `clnttcp_create` routine returns the address of the client handle, or zero (if it could not create the client handle). If the routine fails, use the `clnt_pcreateerror` or `clnt_screateerror` routine to obtain additional diagnostic information.

## See Also

`clnt_call`, `clnt_control`, `clnt_create`, `clnt_destroy`,  
`clnt_pcreateerror` / `clnt_screateerror`,  
`clntudp_create` / `clntudp_bufcreate`

## `clntudp_create / clntudp_bufcreate`

Returns an RPC client handle. The remote procedure call uses the UDP transport.

### Format

```
#include

CLIENT *clntudp_create (struct sockaddr_in *addr,
u_long prognum, u_long versnum, struct timeval wait,
int *sockp);

CLIENT *clntudp_bufcreate (struct sockaddr_in *addr,
u_long prognum, u_long versnum, struct timeval wait,
int *sockp, u_long sendsize, u_long recvsize);
```

### Arguments

#### *addr*

Internet address of the host on which the server resides.

#### *prognum, versnum, sockp*

See Table 9-1 for a description of the above arguments.

#### *wait*

Time interval the client waits before resending the call message. This value changes the CLSET\_RETRY\_TIMEOUT code. The `clnt_call` routine uses this value.

#### *sendsize*

Size of the send buffer. If you enter a value less than 100, then 4000 is used as the default.

#### *recvsize*

Size of the receive buffer. If you enter a value less than 100, then 4000 is used as the default.

### Description

These routines create an RPC client handle for *addr*, *prognum*, and *versnum*. The client uses the UDP transport protocol.

If you specify the port number as zero by using `addr->sin_port`, the Port Mapper provides the number of the port on which the remote program is listening.

**Note!** Use the `clntudp_create` routine only for procedures that handle messages shorter than 8K bytes. Use the `clntudp_bufcreate` routine for procedures that handle messages longer than 8K bytes.

The `clntudp_create` routine uses the global variable `rpc_createerr`. `rpc_createerr` is a

structure that contains the most recent service creation error. Use `rpc_createerr` if you want the client program to handle the error. The value of `rpc_createerr` is set by any RPC client creation routine that does not succeed.

The `rpc_createerr` variable is defined in the `CLNT.H` file.

## Example

```
main()
{
    int      sock;
    u_long   prog = PROGRAM, vers = VERSION;
    CLIENT   *clnt;
    struct sockaddr_in  local_addr, remote_addr;
    struct timeval      timeout = { 35, 0},
                      retry = { 5, 0};

    remote_addr.sin_family = AF_INET;
    remote_addr.sin_port = 0; /* consult the remote port mapper */
    remote_addr.sin_addr.s_addr = 0x04030201; /* internet
    addr 1.2.3.4 */

    local_addr.sin_family = AF_INET;
    local_addr.sin_port = 12345; /* use port 12345 */
    local_addr.sin_addr.s_addr = 0x05030201; /* internet addr
    1.2.3.5 */

    sock = socket( AF_INET, SOCK_DGRAM, 0);

    /* bind the socket to the local addr */
    bind( sock, &local_addr, sizeof( local_addr));

    /* create a client that uses the local IA and port given above */
    clnt = clntudp_create( &remote_addr, prog, vers, retry, &sock);

    /* use a connection timeout of 35 seconds, not the default */
    clnt_control( clnt, CLSET_TIMEOUT, &timeout);
    /*call the server here*/
}

```

This example defines a socket structure, binds the socket, and creates a UDP client handle.

## **Diagnostics**

These routines return the address of the client handle, or zero (if they cannot create the client handle).

If these routines fail, you can obtain additional diagnostic information by using the `clnt_pcreateerror` or `clnt_screateerror` routine.

## **See Also**

`clnt_call`, `clnt_control`, `clnt_create`, `clnt_destroy`,  
`clnt_pcreateerror` / `clnt_screateerror`, `clnttcp_create`

# RPC RTL Port Mapper Routines

## Introduction

This chapter is for RPC programmers. It documents the port mapper routines in the RPC Run-Time Library (RTL). These routines are the programming interface to RPC.

## Port Mapper Routines

Port Mapper routines provide a simple callable interface to the Port Mapper. They allow you to request Port Mapper services and information about port mappings. Table 10-1 summarizes the purpose of each Port Mapper routine.

**Table 10-1 Port Mapper Routines**

<b>Routine</b>	<b>Purpose</b>
pmap_getmaps	Returns a list of Port Mappings for the specified host.
pmap_getport	Returns the port number on which a specified service is waiting.
pmap_rmtcall	Requests the Port Mapper on a remote host to call a procedure on that host.
pmap_set	Registers a remote service with a remote port.
pmap_unset	Unregisters a service so it is no longer mapped to a port.

## Port Mapper Arguments

Port Mapper routines use many of the same arguments as client routines. See Table 10-1 in the *RPC RTL Client Routines* chapter for a list of these arguments.

The following sections describe each Port Mapper routine in detail.

## **pmap\_getmaps**

Returns a list of Port Mappings for the specified host.

### **Format**

```
struct pmaplist *pmap_getmaps (struct sockaddr_in *addr);
```

### **Argument**

*addr*

Address of a structure containing the internet address of the host whose Port Mapper is being called.

### **Description**

The `pmap_getmaps` routine returns a list of current RPC server-to-Port Mappings on the host at *addr*. The list structure is defined in the `PMAP_PROT.H` file.

The `MULTINET SHOW /RPC_PORTMAP` command uses this routine.

### **Diagnostics**

If an error occurs (for example, `pmap_getmaps` cannot get a list of Port Mappings, the internet address is invalid, or the remote Port Mapper does not exist), the routine returns either `NULL` or the address of the list.

### **See Also**

`pmap_getport`, `pmap_set`, `pmap_unset`

## pmap\_getport

Returns the port number on which a specified service is waiting.

### Format

```
u_short pmap_getport (struct sockaddr_in *addr,  
u_long prognum, u_long versnum, u_long protocol);
```

### Arguments

#### *addr*

Address of a structure containing the internet address of the remote host on which the server resides.

#### *prognum, versnum, protocol*

See Table 10-1 in the *RPC RTL Client Routines* chapter for a list of these arguments.

### Diagnostics

If the requested mapping does not exist or the routine fails to contact the remote Port Mapper, the routine returns either the port number or zero.

The `pmap_getport` routine uses the global variable `rpc_createerr`. `rpc_createerr` is a structure that contains the most recent service creation error. Use `rpc_createerr` if you want the service program to handle the error. The value of `rpc_createerr` is set by any RPC server creation routine that does not succeed.

The `rpc_createerr` variable is defined in the `CLNT.H` file.

### See Also

`pmap_getmaps`, `pmap_set`, `pmap_unset`

## pmap\_rmtcall

Requests the Port Mapper on a remote host to call a procedure on that host.

### Format

```
enum clnt_stat pmap_rmtcall (struct sockaddr_in *addr,  
u_long prognum, u_long versnum, u_long procnum,  
xdrproc_t inproc, u_char *in, xdrproc_t outproc, u_char *out, struct  
timeval tout, u_long *portp);
```

### Arguments

*addr*

Address of a structure containing the internet address of the remote host on which the server resides.

*prognum, versnum, procnum, inproc, in, outproc, out*

See Table 10-1 in the *RPC RTL Client Routines* chapter for a list of these arguments.

*tout*

Time allowed for the results to return to the client, in seconds and microseconds.

*portp*

Address where `pmap_rmtcall` will write the port number of the remote service.

### Description

The `pmap_rmtcall` routine allows you to get a port number and call a remote procedure in one call. The routine requests a remote Port Mapper to call a *prognum*, *versnum*, and *procnum* on the Port Mapper's host. The remote procedure call uses the UDP transport.

If `pmap_rmtcall` succeeds, it changes *portp* to contain the port number of the remote service.

After calling the `pmap_rmtcall` routine, you may call the `clnt_perrno` routine.

### Diagnostics

This routine returns diagnostic values defined in the `CLNT.H` file for `enumclnt_stat`.

### See Also

`clnt_broadcast`, `clnt_perrno`

## pmap\_set

Registers a remote service with a remote port.

### Format

```
bool_t pmap_set (u_long prognum, u_long versnum,  
                u_long protocol, u_short port);
```

### Arguments

*prognum, versnum, protocol*

See Table 10-1 in the *RPC RTL Client Routines* chapter for a list of these arguments.

*port*

Remote port number.

### Description

The `pmap_set` routine calls the local Port Mapper to tell it which *port* and *protocol* the *prognum*, *versnum* is using.

You are not likely to use `pmap_set`, because `svc_register` calls it.

### Diagnostics

The `pmap_set` routine returns TRUE if it succeeds, and FALSE if it fails.

### See Also

`pmap_getport`, `pmap_getmaps`, `pmap_unset`, `svc_register`

## **pmap\_unset**

Unregisters a service so it is no longer mapped to a port.

### **Format**

```
bool_t pmap_unset (u_long prognum, u_long versnum);
```

### **Arguments**

*prognum*, *versnum*

See Table 10-1 in the *RPC RTL Client Routines* chapter for a list of these arguments.

### **Description**

The `pmap_unset` routine calls the local Port Mapper and, for all protocols, removes the *prognum* and *versnum* from the list that maps servers to ports.

You are not likely to use `pmap_unset`, because `svc_unregister` calls it.

### **Diagnostics**

The `pmap_unset` routine returns `TRUE` if it succeeds, `FALSE` if it fails.

### **See Also**

`pmap_getport`, `pmap_getmaps`, `pmap_set`, `svc_unregister`

## RPC RTL Server Routines

### Introduction

This chapter is for RPC programmers. It documents the server routines in the RPC Run-Time Library (RTL). These routines are the programming interface to RPC.

### Server Routines

The server routines are called by the server program or the server stub procedures. Table 11-1 lists each server routine and summarizes its purpose.

**Table 11-1 Server Routines**

<b>Routine</b>	<b>Purpose</b>
registerrpc	Performs creation and registration tasks for server.
svc_destroy	Macro that destroys RPC server handle.
svc_freeargs	Macro that frees memory allocated when RPC arguments were decoded.
svc_getargs	Macro that decodes RPC arguments.
svc_getcaller	Macro that returns address of client that called server.
svc_getchan	Macro that returns channel of server handle.
svc_getport	Macro that returns port associated with server handle.
svc_getreqset	Reads data for each server connection.
svc_register	Adds specified server to list of active servers, and registers service program with Port Mapper.

**Table 11-1 Server Routines (Continued)**

<b>Routine</b>	<b>Purpose</b>
svc_run	Waits for RPC requests and calls <code>svc_getreqset</code> routine to dispatch to appropriate RPC service program.
svc_sendreply	Sends results of remote procedure call to client.
svc_unregister	Calls Port Mapper to unregister specified program and version for all protocols.
svcerr_auth	Sends error code when server cannot authenticate client.
svcerr_decode	Sends error code to client if server cannot decode arguments.
svcerr_noproc	Sends error code to client if server cannot implement requested procedure.
svcerr_noprogram	Sends error code to client when requested program is not registered with Port Mapper.
svcerr_progvers	Sends error code to client when requested program is registered with Port Mapper, but requested version is not registered.
svcerr_systemerr	Sends error code to client when server encounters error not handled by particular protocol.
svcerr_weakauth	Sends error code to client when server cannot perform remote procedure call because it received insufficient (but correct) authentication parameters.
svctcp_create	Returns address of structure containing server handle for specified TCP socket.
svctcp_create	Returns address of server handle that uses TCP transport.
svcupd_bufcreate	Returns address of server handle that uses UDP transport. For procedures that pass messages longer than 8Kbytes.
svcupd_create	Returns address of server handle that uses UDP transport. For procedures that pass messages shorter than 8Kbytes.
svcupd_enablecache	Enables XID cache for specified UDP transport server.
xprt_register	Adds UDP or TCP server socket to list of sockets.
xprt_unregister	Removes UDP or TCP server socket from list of sockets.

The following sections describe each server routine in detail.

## registerrpc

Performs creation and registration tasks for the server.

### Format

```
#include
int registerrpc (u_long prognum, u_long versnum, u_long procnum,
u_char *(*procname) (), xdrproc_t inproc, xdrproc_t outproc);
```

### Arguments

*prognum*, *versnum*, *procnum*, *inproc*, *outproc*

See Table 10-1 in the *RPC RTL Client Routines* chapter for a list of these arguments.

*procname*

Address of the routine that implements the service procedure. The routine uses the following format:

```
u_char *procname(out);
u_char *out;
```

where *out* is the address of the data decoded by *outproc*.

### Description

The `registerrpc` routine performs the following tasks for a server:

- Creates a UDP server handle.
- Calls the `svc_register` routine to register the program with the Port Mapper.
- Adds *prognum*, *versnum*, and *procnum* to an internal list of registered procedures. When the server receives a request, it uses this list to determine which routine to call.

A server should call `registerrpc` for every procedure it implements, except for the NULL procedure.

### Diagnostics

The `registerrpc` routine returns zero if it succeeds, and -1 if it fails.

### See Also

`svc_register`

## svc\_destroy

Macro that destroys the RPC server handle.

### Format

```
void svc_destroy (SVCXPRT *xprt);
```

### Argument

*xprt*

RPC server handle.

### Description

The `svc_destroy` routine destroys *xprt* by deallocating private data structures. After this call, *xprt* is undefined.

If the server creation routine received `RPC_ANYSOCK` as the socket, `svc_destroy` closes the socket. Otherwise, you must close the socket.

### See Also

`svcfld_create`, `svctcp_create`, `svcudp_create`

## svc\_freeargs

Macro that frees the memory that was allocated when the RPC arguments were decoded.

### Format

```
bool_t svc_freeargs (SVCXPRT *xpvt, xdrproc_t xdr_args,  
char *args_ptr);
```

### Arguments

*xpvt, xdr\_args, args\_ptr*

See Table 10-1 in the *RPC RTL Client Routines* chapter for a list of these arguments.

### Description

The `svc_freeargs` routine calls the `xdr_free` routine.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

`svc_getargs`, `xdr_free`

## svc\_getargs

Macro that decodes the RPC arguments.

### Format

```
bool_t svc_getargs (SVCXPRT *xpvt, xdrproc_t xdr_args,  
u_char *args_ptr);
```

### Arguments

*xpvt, xdr\_args, args\_ptr*

See Table 10-1 in the *RPC RTL Client Routines* chapter for a list of these arguments.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

svc\_freeargs

## svc\_getreqset

Reads data for each server connection.

### Format

```
#include  
  
void svc_getreqset (int rdfds);
```

### Argument

*rdfds*

Address of the read socket descriptor array. This array is returned by the `select` routine.

### Description

The server calls `svc_getreqset` when it receives an RPC request. The `svc_getreqset` routine reads in data for each server connection, then calls the server program to handle the data.

The `svc_getreqset` routine does not return a value. It finishes executing after all *rdfds* sockets have been serviced.

You are unlikely to call this routine directly, because the `svc_run` routine calls it. However, there are times when you cannot call `svc_run`. For example, suppose a program services RPC requests and reads or writes to another socket at the same time. The program cannot call `svc_run`. It must call `select` and `svc_getreqset`.

The `svc_getreqset` routine is for servers that implement custom asynchronous event processing, do not use the `svc_run` routine.

You may use the global variable `svc_fdset` with `svc_getreqset`. The `svc_fdset` variable lists all sockets the server is using. It contains an array of structures, where each element is a socket pointer and a service handle. It uses the following format:

```
struct sockarr svc_fdset [MAXSOCK +1];
```

This is how to use `svc_fdset`: first, copy the socket handles from `svc_fdset` into a temporary array that ends with a zero. Pass the array to the `select` routine. The `select` routine overwrites the array and returns it. Pass this array to the `svc_getreqset` routine.

You may use `svc_fdset` when the server does not use `svc_run`.

The `svc_fdset` variable is not compatible with UNIX.

## Example

```
#define MAXSOCK          10

int      readfds[ MAXSOCK+1],    /* sockets to select from */
        i, j;

for( i = 0, j = 0; i < MAXSOCK; i++)
    if( (svc_fdset[i].sockname != 0) && (svc_fdset[i].sockname !=
1))
        readfds[j++] = svc_fdset[i].sockname;
readfds[j] = 0;                /* list of sockets ends w/ a zero */
switch( select( 0, readfds, 0, 0, 0))
{
    case -1:                    /* an error happened */
    case 0:                      /* time out */
        break;
    default:                    /* 1 or more sockets ready for reading */
        errno = 0;
        ONCRPC_SVC_GET_REQSET( readfds);
        if( errno == ENETDOWN || errno == ENOTCONN)
            sys$exit( SS$_THIRDPARTY);
}
```

## See Also

`svc_run`

## svc\_register

Adds the specified server to a list of active servers, and registers the service program with the Port Mapper.

### Format

```
#include  
  
bool_t svc_register (SVCXPRT *xprt, u_long prognum,  
u_long versnum, void (*dispatch) (), u_long protocol);
```

### Arguments

*xprt, prognum, versnum*

See Table 10-1 in the *RPC RTL Client Routines* chapter for a list of these arguments.

*dispatch*

Routine that `svc_register` calls when the server receives a request for *prognum, versnum*. This routine determines which routine to call for each server procedure. This routine uses the following form:

```
void dispatch(request, xprt)
```

```
struct svc_req *request;
```

```
SVCXPRT *xprt;
```

The `svc_getreqset` and `svc_run` routines call *dispatch*.

*protocol*

Must be `IPPROTO_UDP`, `IPPROTO_TCP`, or zero. Zero indicates that you do not want to register the server with the Port Mapper.

### Diagnostics

The `svc_register` routine returns `TRUE` if it succeeds and `FALSE` if it fails.

### See Also

`pmap_set`, `svc_getreqset`, `svc_unregister`

## **svc\_run**

Waits for RPC requests and calls the `svc_getreqset` routine to dispatch to the appropriate RPC service program.

### **Format**

```
#include
```

```
void svc_run()
```

### **Arguments**

None.

### **Description**

The `svc_run` routine calls the `select` routine to wait for RPC requests. When a request arrives, `svc_run` calls the `svc_getreqset` routine. Then `svc_run` calls `select` again.

The `svc_run` routine never returns.

You may use the global variable `svc_fdset` with `svc_run`. See the `svc_getreqset` routine for more information on `svc_fdset`.

### **See Also**

`svc_getreqset`

## svc\_sendreply

Sends the results of a remote procedure call to the client.

### Format

```
#include  
bool_t svc_sendreply (SVCXPRT *xprt, xdrproc_t outproc, caddr_t *out);
```

### Arguments

*xprt, outproc, out*

See Table 10-1 in the *RPC RTL Client Routines* chapter for a list of these arguments.

### Description

The routine sends the results of a remote procedure call to the client.

### Diagnostics

These routines returns TRUE if they succeed and FALSE if they fail.

## svc\_unregister

Calls the Port Mapper to unregister the specified program and version for all protocols. The program and version are removed from the list of active servers.

### Format

```
#include
```

```
void svc_unregister (u_long prognum, u_long versnum);
```

### Arguments

*prognum*, *versnum*

See Table 10-1 in the *RPC RTL Client Routines* chapter for a list of these arguments.

### See Also

`pmap_unset`, `svc_register`

**svcerr\_auth**  
**svcerr\_decode**  
**svcerr\_noproc**  
**svcerr\_noprog**  
**svcerr\_progvers**  
**svcerr\_systemerr**  
**svcerr\_weakauth**

Sends various error codes to the client process.

**Format**

```
#include

void svcerr_auth (SVCXPRT *xprt, enum auth_stat why);
void svcerr_decode (SVCXPRT *xprt);
void svcerr_noproc (SVCXPRT *xprt);
void svcerr_noprog (SVCXPRT *xprt);
void svcerr_progvers (SVCXPRT *xprt, u_long low-vers, u_long high-vers);
void svcerr_systemerr (SVCXPRT *xprt);
void svcerr_weakauth (SVCXPRT *xprt);
```

**Arguments**

*xprt*

RPC server handle.

*why*

Error code defined in the AUTH.H file.

*low-vers*

Lowest version number in the range of versions that the server supports.

*high-vers*

Highest version in the range of versions that the server supports.

**Description**

**svcerr\_auth**

See `svc_getreqset`. Calls `svcerr_auth` when it cannot authenticate a client. The `svcerr_auth` routine returns an error code (*why*) to the caller.

### **svcerr\_decode**

Sends an error code to the client if the server cannot decode the arguments.

### **svcerr\_noproc**

Sends an error code to the client if the server does not implement the requested procedure.

### **svcerr\_noprog**

Sends an error code to the client when the requested program is not registered with the Port Mapper. Generally, the Port Mapper informs the client when a server is not registered. Therefore, the server is unlikely to use this routine.

### **svcerr\_progvers**

Sends an error code to the client when the requested program is registered with the Port Mapper, but the requested version is not registered.

### **svcerr\_systemerr**

Sends an error code to the client when the server encounters an error that is not handled by a particular protocol.

### **svcerr\_weakauth**

Sends an error code to the client when the server cannot perform a remote procedure call because it received insufficient (but correct) authentication parameters. This routine calls the `svcerr_auth` routine. The value of *why* is `AUTH_TOOWEAK`, which means "access permission denied."

## svctcp\_create

Returns the address of a structure containing a server handle for the specified TCP socket.

### Format

```
#include  
  
SVCTCP_CREATE *svctcp_create (int sock, u_long sendsize, u_long recvsize);
```

### Arguments

***sock***

Socket number. Do not specify a file descriptor.

***sendsize***

Size of the send buffer. If you enter a value less than 100, then 4000 is used as the default.

***recvsize***

Size of the receive buffer. If you enter a value less than 100, then 4000 is used as the default.

### Description

The `svctcp_create` routine returns the address of a server handle for the specified TCP socket. This handle cannot use a file. The server calls the `svctcp_create` routine after it accepts a TCP connection.

### Diagnostics

This routine returns zero if it fails.

### See Also

`svctcp_create`

## **svcrow\_create**

Creates a server handle for memory-based Sun RPC for simple testing and timing.

### **Format**

```
#include  
  
SVCXPRT scrow_create ();
```

### **Argument**

None.

### **Description**

The `svcrow_create` routine creates a toy Sun RPC service transport, to which it returns a pointer. The transport is really a buffer within the process's address space, so the corresponding client should live in the same address space.

This routine allows simulation of and acquisition of Sun RPC overheads (such as round trip times) without any kernel interference.

### **Diagnostics**

This routine returns `NULL` if it fails.

### **See Also**

`clntraw_create`

## svctcp\_create

Returns the address of a server handle that uses the TCP transport.

### Format

```
#include
```

```
SVCXPRT *svctcp_create (int sock, u_long sendsize, u_long recvsize);
```

### Arguments

#### *sock*

Socket for this service. The `svctcp_create` routine creates a new socket if you enter `RPC_ANYSOCK`. If the socket is not bound to a TCP port, `svctcp_create` binds it to an arbitrary port.

#### *sendsize*

Size of the send buffer. If you enter a value less than 100, then 4000 bytes is used as the default.

#### *recvsize*

Size of the receive buffer. If you enter a value less than 100, then 4000 bytes is used as the default.

### Diagnostics

The `svctcp_create` routine returns either the address of the server handle, or zero (if it could not create the server handle).

### See Also

`svcfid_create`, `svc_destroy`

## `svcadp_create / svcadp_bufcreate`

Returns the address of a server handle that uses the UDP transport.

### Format

```
#include  
  
SVCPRT *svcadp_create (int sock);  
  
SVCPRT *svcadp_bufcreate (int sock, u_long sendsize,  
u_long recvsize);
```

### Arguments

#### *sock*

Socket for this service. The `svcadp_create` routine creates a new socket if you enter `RPC_ANYSOCK`. If the socket is not bound to a UDP port, the `svcadp_create` routine binds it to an arbitrary port.

#### *sendsize*

Size of the send buffer. The minimum size is 100 bytes. The maximum size is 65468, the maximum UDP packet size. If you enter a value less than 100, then 4000 is used as the default.

#### *recvsize*

Size of the receive buffer. The minimum size is 100 bytes. The maximum size is 65000, the maximum UDP packet size. If you enter a value less than 100, then 4000 is used as the default.

### Description

Use the `svc_create` routine only for procedures that pass messages shorter than 8Kbytes long. Use the `svcadp_bufcreate` routine for procedures that pass messages longer than 8Kbytes.

### Diagnostics

These routines return either a server handle, or zero (if they could not create the server handle).

### See Also

`svc_destroy`, `svcadp_enablecache`

## svcadp\_enablecache

Enables the XID cache for the specified UDP transport server.

### Format

```
bool_t svcudp_enablecache (SVCXPRT *xprt, u_long size);
```

### Arguments

*xprt*

RPC server handle.

*size*

Number of entries permitted in the XID cache. You may estimate this number based on how active the server is, and on how long you want to retain old replies.

### Description

Use the `svcadp_enablecache` routine after a UDP server handle is created. The server places all outgoing responses in the XID cache. The cache can be used to improve the performance of the server, for example, by preventing the server from recalculating the results or sending incorrect results.

You cannot disable the XID cache for UDP servers.

The *RPC Fundamentals*, Chapter 6, provides more information on the XID cache.

### Example

```
#define FALSE    0
#define UDP_CACHE_SIZE  10

SVCXPRT *udp_xprt;

udp_xprt = svcudp_create( RPC_ANYSOCK);
if( svcudp_enablecache( udp_xprts, UDP_CACHE_SIZE) == FALSE)
    printf( "XID cache was not enabled");
else
    printf( "XID cache was enabled");
```

### Diagnostics

This routine returns TRUE if it enables the XID cache, and FALSE if the cache was previously enabled or an error occurs.

## xprt\_register

Adds a TCP or UDP server socket to a list of sockets.

### Format

```
#include  
  
void xprt_register (SVCXPRT *xprt);
```

### Argument

*xprt*  
RPC server handle.

### Description

The `xprt_register` and `xprt_unregister` routines maintain a list of sockets. This list ensures that the correct server is called to process the request. The `xprt_register` routine adds the server socket to the `svc_fdset` variable, which also stores the server handle that is associated with the socket. The `svc_run` routine passes the list of sockets to the `select` routine. The `select` routine returns to `svc_run` a list of sockets that have outstanding requests.

You are unlikely to call this routine directly because `svc_register` calls it.

### See Also

`svc_register`, `xprt_unregister`

## xprt\_unregister

Removes a TCP or UDP server socket from a list of sockets.

### Format

```
#include  
  
void xprt_unregister (SVCXPRT *xprt);
```

### Argument

*xprt*  
RPC server handle.

### Description

This list of sockets ensures that the correct server is called to process the request. See the `xprt_register` routine for a description of how this list is maintained.

You are unlikely to call this routine directly because `svc_unregister` calls it.

### See Also

`svc_unregister`, `xprt_register`



# RPC RTL XDR Routines

## Introduction

This chapter is for RPC programmers. It documents the XDR routines in the RPC Run-Time Library (RTL). These routines are the programming interface to RPC.

## XDR Routines

This section explains what XDR routines do and when you would call them. It also provides quick reference and detailed reference sections describing each XDR routine.

## What XDR Routines Do

Most XDR routines share these characteristics:

- They convert data in two directions: from the host's local data format to XDR format (called encoding or marshalling), or the other way around (called decoding or unmarshalling).
- They use `xdrs`, a structure containing instructions for encoding, decoding, and deallocating memory.
- They return a boolean value to indicate success or failure.

Some XDR routines allocate memory while decoding an argument. To free this memory, call the `xdr_free` routine after the program is done with the decoded value.

Table 12-1 shows the order in which XDR routines perform encoding and decoding.

**Table 12-1 XDR Actions**

Client	Server
1. Encodes arguments 2. Decodes results 3. Frees results from memory	1. Decodes arguments 2. Encodes results 3. Frees arguments from memory

## When to Call XDR Routines

Under most circumstances, you are not likely to call any XDR routines directly. The `clnt_call` and `svc_sendreply` routines call the XDR routines.

You would call the XDR routines directly only when you write your own routines to convert data to or from XDR format.

## Quick Reference

Table 12-2 lists the XDR routines that encode and decode data.

**Table 12-2 XDR Encoding and Decoding Routines**

This routine...	Encodes and decodes...
<code>xdr_array</code>	Variable-length array
<code>xdr_bool</code>	Boolean value
<code>xdr_bytes</code>	Bytes
<code>xdr_char</code>	Character
<code>xdr_double</code>	Double-precision floating point number
<code>xdr_enum</code>	Enumerated type
<code>xdr_float</code>	Floating point value
<code>xdr_hyper</code>	VAX quad word to an XDR hyper-integer, or the other way
<code>xdr_int</code>	Four-byte integer
<code>xdr_long</code>	Longword
<code>xdr_opaque</code>	Contents of a buffer (treats the data as a fixed length of bytes and does not attempt to interpret them)

**Table 12-2 XDR Encoding and Decoding Routines (Continued)**

<b>This routine...</b>	<b>Encodes and decodes...</b>
xdr_pointer	Pointer to a data structure
xdr_reference	Pointer to a data structure (the address must be non-zero)
xdr_short	Two-byte unsigned integer
xdr_string	Null-terminated string
xdr_u_char	Unsigned character
xdr_u_hyper	VAX quad word to an XDR unsigned hyper-integer
xdr_u_int	Four-byte unsigned integer
xdr_u_long	Unsigned longword
xdr_u_short	Two-byte unsigned integer
xdr_union	Union
xdr_vector	Vector (fixed length array)
xdr_void	Nothing
xdr_wrapstring	Null-terminated string

Table 12-3 lists the XDR routines that perform various support functions.

**Table 12-3 XDR Support Routines**

<b>This routine...</b>	<b>Does this...</b>
xdr_free	Deallocates a data structure from memory
xdrmem_create	Creates a memory buffer XDR stream
xdrrec_create	Creates a record-oriented XDR stream
xdrrec_endofrecord	Marks the end of a record
xdrrec_eof	Goes to the end of the current record, then verifies whether any more data can be read
xdrrec_skiprecord	Goes to the end of the current record
xdrstdio_create	Initializes an <code>stdio</code> stream

Table 12-4 lists the upper layer XDR routines that support RPC.

**Table 12-4 Upper Layer XDR Routines**

<b>This routine...</b>	<b>Encodes and decodes...</b>
xdr_accepted_reply	Part of an RPC reply message after the reply is accepted
xdr_authunix_parms	UNIX-style authentication information
xdr_callhdr	Static part of an RPC request message header (encoding only)
xdr_callmsg	RPC request message
xdr_netobj	Data in the <code>netobj</code> structure
xdr_opaque_auth	Authentication information
xdr_pmap	Port Mapper parameters
xdr_pmaplist	List of Port Mapping data
xdr_rejected_reply	Part of an RPC reply message after the reply is rejected
xdr_replymsg	RPC reply header; it then calls the appropriate routine to convert the rest of the message

The following sections describe each XDR routine in detail.

## xdr\_accepted\_reply

Converts an RPC reply message from local format to XDR format, or the other way around.

### Format

```
#include
```

```
bool_t xdr_accepted_reply (XDR *xdrs, struct accepted_reply *ar);
```

### Arguments

*xdrs*

Address of a structure containing XDR encoding and decoding information.

*ar*

Address of the structure containing the RPC reply message.

### Description

The `xdr_replymsg` routine calls the `xdr_accepted_reply` routine.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

`xdr_replymsg`

## xdr\_array

Converts a variable-length array from local format to XDR format, or the other way around.

### Format

```
#include
```

```
bool_t xdr_array (XDR *xdrs, u_char **addrp, u_long *sizep, u_long  
maxsize, u_long elsize, xdrproc_t elproc);
```

### Arguments

*xdrs*

Address of a structure containing XDR encoding and decoding information.

*addrp*

Address of the address containing the array being converted. If *addrp* is zero, then `xdr_array` allocates  $(( *sizep) * elsize)$  number of bytes when it decodes.

*sizep*

Address of the number of elements in the array.

*maxsize*

Maximum number of elements the array can hold.

*elsize*

Size of each element, in bytes.

*elproc*

XDR routine that handles each array element.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

## xdr\_authunix\_parms

Converts UNIX-style authentication information from local format to XDR format, or the other way around.

### Format

```
#include
```

```
bool_t xdr_authunix_parms (XDR *xdrs, struct authunix_parms *aupp);
```

### Arguments

*xdrs*

Address of a structure containing XDR encoding and decoding information.

*aupp*

UNIX-style authentication information being converted.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

## **xdr\_bool**

Converts a boolean value from local format to XDR format, or the other way around.

### **Format**

```
#include
```

```
bool_t xdr_bool (XDR *xdrs, bool_t *bp);
```

### **Arguments**

*xdrs*

Address of a structure containing XDR encoding and decoding information.

*bp*

Address of the boolean value.

### **Diagnostics**

This routine returns TRUE if it succeeds and FALSE if it fails.

## xdr\_bytes

Converts bytes from local format to XDR format, or the other way around.

### Format

```
#include
```

```
bool_t xdr_bytes (XDR *xdrs, u_char **cpp, u_long *sizep, u_long maxsize);
```

### Arguments

*xdrs*

Address of a structure containing XDR encoding and decoding information.

*cpp*

Address of the address of the buffer containing the bytes being converted. If *\*cpp* is zero, `xdr_bytes` allocates *maxsize* bytes when it decodes.

*sizep*

Address of the actual number of bytes being converted.

*maxsize*

Maximum number of bytes that can be used. The server protocol determines this number.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

## **xdr\_callhdr**

Encodes the static part of an RPC request message header.

### **Format**

```
#include
```

```
bool_t xdr_callhdr (XDR *xdrs, struct rpc_msg *chdr);
```

### **Arguments**

*xdrs*

Address of a structure containing XDR encoding and decoding information.

*chdr*

Address of the data being converted.

### **Description**

The `xdr_callhdr` routine converts the following fields: transaction ID, direction, RPC version, server program number, and server version. It converts the last four fields once, when the client handle is created.

The `clnttcp_create` and `clntudp_create` routines call the `xdr_callhdr` routine.

### **Diagnostics**

This routine always returns TRUE.

### **See Also**

`clnt_call`, `clnttcp_create`, `clntudp_create`, `xdr_callmsg`

## xdr\_callmsg

Converts an RPC request message from local format to XDR format, or the other way around.

### Format

```
#include  
  
bool_t xdr_callmsg (XDR *xdrs, struct rpc_msg *cmsg);
```

### Arguments

*xdrs*

Address of a structure containing XDR encoding and decoding information.

*cmsg*

Address of the message being converted.

### Description

The `xdr_callmsg` routine converts the following fields: transaction ID, RPC direction, RPC version, program number, version number, procedure number, client authentication.

The `pmap_rmtcall`, `svc_sendreply`, and `svc_sendreply_dq` routines call `xdr_callmsg`.

### Diagnostics

This routine returns `TRUE` if it succeeds and `FALSE` if it fails.

### See Also

`xdr_callhdr`

## **xdr\_char**

Converts a character from local format to XDR format, or the other way around.

### **Format**

```
#include
```

```
bool_t xdr_char (XDR *xdrs, char *cp);
```

### **Arguments**

*xdrs*

Address of a structure containing XDR encoding and decoding information.

*cp*

Address of the character being converted.

### **Description**

This routine provides the same functionality as the `xdr_u_char` routine.

### **Diagnostics**

This routine returns TRUE if it succeeds and FALSE if it fails.

### **See Also**

`xdr_u_char`

## xdr\_double

Converts a double-precision floating point number between local and XDR format.

### Format

```
#include

bool_t xdr_double (XDR *xdrs, double *dp);
```

### Arguments

*xdrs*

Pointer to an XDR stream handle created by one of the XDR stream handle creation routines.

*dp*

Pointer to the double-precision floating point number.

### Description

This routine provides a filter primitive that translates between double-precision numbers and their external representations. It is actually implemented by four XDR routines:

<code>xdr_double_D</code>	Converts VAX D format floating point numbers
<code>xdr_double_G</code>	Converts VAX G format floating point numbers
<code>xdr_double_T</code>	Converts IEEE T format floating point numbers
<code>xdr_double_X</code>	Converts IEEE X format floating point numbers

You can reference these routines explicitly or you can use compiler settings to control which routine is used when you reference the `xdr_double` routine.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

## **xdr\_enum**

Converts an enumerated type from local format to XDR format, or the other way around.

### **Format**

```
#include
```

```
bool_t xdr_enum (XDR *xdrs, enum_t *ep);
```

### **Arguments**

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*ep*

Address containing the enumerated type.

### **Diagnostics**

This routine returns TRUE if it succeeds and FALSE if it fails.

## xdr\_float

Converts a floating point value from local format to XDR format, or the other way around.

### Format

```
#include

bool_t xdr_float (XDR *xdrs, float *fp);
```

### Arguments

*xdrs*

Pointer to an XDR stream handle created by one of the XDR stream handle creation routines.

*fp*

Pointer to a single-precision floating point number.

### Description

This routine provides a filter primitive that translates between double-precision numbers and their external representations. It is actually implemented by four XDR routines:

<code>xdr_float_F</code>	Converts VAX F format floating point numbers
<code>xdr_float_S</code>	Converts IEEE T format floating point numbers

You can reference these routines explicitly or you can use compiler settings to control which routine is used when you reference the `xdr_float` routine.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

## **xdr\_free**

Deallocates a data structure from memory.

### **Format**

```
#include  
  
void xdr_free (xdrproc_t proc, u_char *objp);
```

### **Arguments**

*proc*  
XDR routine that describes the data structure.

*objp*  
Address of the data structure.

### **Description**

Call this routine after decoded data is no longer needed. Do not call it for encoded data.

### **Diagnostics**

This routine returns TRUE if it succeeds and FALSE if it fails.

## xdr\_hyper

Converts a VAX quad word to an XDR hyper-integer, or the other way around.

### Format

```
bool_t xdr_hyper (XDR *xdrs, quad *ptr);
```

### Arguments

*xdrs*

Address of a structure containing XDR encoding and decoding information.

*ptr*

Address of the structure containing the quad word. The quad word is stored in standard VAX quad word format, with the low-order longword first in memory.

### Description

This routine provided the same functionality as the `xdr_u_hyper` routine.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

`xdr_u_hyper`

## **xdr\_int**

Converts one four-byte integer from local format to XDR format, or the other way around.

### **Format**

```
#include  
  
bool_t xdr_int (XDR *xdrs, int *ip);
```

### **Arguments**

*xdrs*

Address of a structure containing XDR encoding and decoding information.

*ip*

Address containing the integer.

### **Description**

This routine provides the same functionality as the `xdr_u_int`, `xdr_long`, and `xdr_u_long` routines.

### **Diagnostics**

This routine returns TRUE if it succeeds and FALSE if it fails.

### **See Also**

`xdr_u_int`, `xdr_long`, `xdr_u_long`

## xdr\_long

Converts one longword from local format to XDR format, or the other way around.

### Format

```
#include  
  
bool_t xdr_long (XDR *xdrs, u_long *lp);
```

### Arguments

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*lp*

Address containing the longword.

### Description

This routine provides the same functionality as the `xdr_u_long`, `xdr_int`, and `xdr_u_int` routines.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

`xdr_u_long`, `xdr_int`, `xdr_u_int`

## **xdr\_netobj**

Converts data in the `netobj` structure from the local data format to XDR format, or the other way around.

### **Format**

```
bool_t xdr_netobj (XDR *xdrs, netobj *ptr);
```

### **Arguments**

***xdrs***

Address of the structure containing XDR encoding and decoding information.

***ptr***

Address of the following structure:

```
typedef struct
{
    u_long n_len;
    byte *n_bytes;
} netobj;
```

This structure defines the data being converted.

### **Description**

The `netobj` structure is an aggregate data structure that is opaque and contains a counted array of 1024 bytes.

### **Diagnostics**

This routine returns `TRUE` if it succeeds and `FALSE` if it fails.

## xdr\_opaque

Converts the contents of a buffer from the local data format to XDR format, or the other way around. This routine treats the data as a fixed length of bytes and does not attempt to interpret them.

### Format

```
#include  
  
bool_t xdr_opaque (XDR *xdrs, char *cp, u_long cnt);
```

### Arguments

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*cp*

Address of the buffer containing opaque data.

*cnt*

Byte length.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

## **xdr\_opaque\_auth**

Converts authentication information from the local data format to XDR format, or the other way around.

### **Format**

```
#include
```

```
bool_t xdr_opaque_auth (XDR *xdrs, struct opaque_auth *ap);
```

### **Arguments**

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*ap*

Address of the authentication information. This data was created by the `authnone_create`, `authunix_create`, or `authunix_create_default` routine.

### **Diagnostics**

This routine returns TRUE if it succeeds and FALSE if it fails.

## xdr\_pmap

Converts Port Mapper parameters from the local data format to XDR format, or the other way around.

### Format

```
#include "MULTINET_INCLUDE:PMAP_PROT.H"

bool_t xdr_pmap (XDR *xdrs, struct pmap *regs);
```

### Arguments

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*regs*

Address of a structure containing the program number, version number, protocol number, and port number. This is the data being converted.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

## **xdr\_pmaplist**

Converts a list of Port Mapping data from the local data format to XDR format, or the other way around.

### **Format**

```
#include "TCPIP$RPC:PMAP_PROT.H"

bool_t xdr_pmaplist (XDR *xdrs, struct pmaplist **rpp);
```

### **Arguments**

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*rpp*

Address of the address of the structure containing Port Mapper data. If this routine is used to decode a Port Mapper listing, *rpp* is set to the address of the newly allocated linked list of structures.

### **Diagnostics**

This routine returns TRUE if it succeeds and FALSE if it fails.

## xdr\_pointer

Converts a recursive data structure from the local data format to XDR format, or the other way around.

### Format

```
#include tcpip$rpc:xdr.h

bool_t xdr_pointer (XDR *xdrs, u_char **objpp, u_long obj_size,
xdrproc_t xdr_obj);
```

### Arguments

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*objpp*

Address of the address containing the data being converted. May be zero.

*obj\_size*

Size of the data structure in bytes.

*xdr\_obj*

XDR routine that describes the object being pointed to. This routine can describe complex data structures, and these structures may contain pointers.

### Description

An XDR routine for a data structure that contains pointers to other structures, such as a linked list, would call the `xdr_pointer` routine. The `xdr_pointer` routine encodes a pointer from an address into a boolean. If the boolean is TRUE, the data follows the boolean.

### Example

```
bool_t xdr_pointer( xdrs, objpp, obj_size, xdr_obj)
    XDR          *xdrs;
    char          **objpp;
    longw        obj_size;
    xdrproc_t     xdr_obj;
{
    bool_t more_data;

    /*
    ** determine if the pointer is a valid address (0 is invalid)
    */
    if( *objpp != NULL)
```

```
        more_data = TRUE;
    else
        more_data = FALSE;
/*
** XDR the flag

** If we are decoding, then more_data is overwritten.
*/
        if( !xdr_bool( xdrs, &more_data))
            return( FALSE);
/*
** If there is no more data, set the pointer to 0 (No effect if we
** were encoding) and return TRUE
*/
        if( !more_data)
        {
            *objpp = NULL;
            return( TRUE);
        }
/*
** Otherwise, call xdr_reference.  The result is that xdr_pointer is
** the same as xdr_reference, except that xdr_pointer adds a Boolean
** to the encoded data and will properly handle NULL pointers.
*/
        return( xdr_reference( xdrs, objpp, obj_size, xdr_obj));
} /* end function xdr_pointer() */
```

## Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

## xdr\_reference

This routine recursively converts a structure that is referenced by a pointer inside the structure.

### Format

```
#include tcpip$rpc:xdr.h

bool_t xdr_reference (XDR *xdrs, u_char **objpp, u_long obj_size,
xdrproc_t xdr_obj);
```

### Arguments

#### *xdrs*

Address of the structure containing XDR encoding and decoding information.

#### *objpp*

Address of the address of a structure containing the data being converted. If *objpp* is zero, the `xdr_reference` routine allocates the necessary storage when decoding. This argument must be non-zero when encoding.

When `xdr_reference` encodes data, it passes *objpp* to *xdr\_obj*. When decoding, `xdr_reference` allocates memory if *objpp* equals zero.

#### *obj\_size*

Size of the referenced structure.

#### *xdr\_obj*

XDR routine that describes the object being pointed to. This routine can describe complex data structures, and these structures may contain pointers.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

## **xdr\_rejected\_reply**

Converts the remainder of an RPC reply message after the header indicates that the reply is rejected.

### **Format**

```
#include tcpip$rpc:xdr.h

bool_t xdr_rejected_reply (XDR *xdrs, struct rejected_reply *rr);
```

### **Arguments**

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*rr*

Address of the structure containing the reply message.

### **Diagnostics**

This routine returns TRUE if it succeeds and FALSE if it fails.

## xdr\_replymsg

Converts the RPC reply header, then calls the appropriate routine to convert the rest of the message.

### Format

```
#include tcpip$rpc:xdr.h

bool_t xdr_replymsg (XDR *xdrs, struct rpc_msg *rmsg);
```

### Arguments

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*rmsg*

Address of the structure containing the reply message.

### Description

The `xdr_replymsg` routine calls the `xdr_rejected_reply` or `xdr_accepted_reply` routine to convert the body of the RPC reply message from the local data format to XDR format, or the other way around.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

`xdr_accepted_reply`, `xdr_rejected_reply`

## **xdr\_short**

Converts a two-byte integer from the local data format to XDR format, or the other way around.

### **Format**

```
#include tcpip$rpc:xdr.h

bool_t xdr_short (XDR *xdrs, short *sp);
```

### **Arguments**

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*sp*

Address of the integer being converted.

### **Description**

This routine provides the same functionality as `xdr_u_short`.

### **Diagnostics**

This routine returns TRUE if it succeeds and FALSE if it fails.

### **See Also**

`xdr_u_short`

## xdr\_string

Converts a null-terminated string from the local data format to XDR format, or the other way around.

### Format

```
#include tcpip$rpc:xdr.h

bool_t xdr_string (XDR *xdrs, char **cpp, u_long maxsize);
```

### Arguments

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*cpp*

Address of the address of the first byte in the string.

*maxsize*

Maximum length of the string. The service protocol determines this value.

### Description

The `xdr_string` routine is the same as the `xdr_wrapstring` routine, except `xdr_string` allows you to specify the *maxsize*.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

`xdr_wrapstring`

## `xdr_u_char`

Converts an unsigned character from local format to XDR format, or the other way around.

### Format

```
#include tcpip$rpc:xdr.h

bool_t xdr_u_char (XDR *xdrs, u_char bp);
```

### Arguments

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*bp*

Address of the character being converted.

### Description

This routine provides the same functionality as `xdr_char`.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

`xdr_char`

## xdr\_u\_hyper

Converts a VAX quad word to an XDR unsigned hyper-integer, or the other way around.

### Format

```
bool_t xdr_u_hyper (XDR *xdrs, quad *ptr);
```

### Arguments

*xdrs*

Address of a structure containing XDR encoding and decoding information.

*ptr*

Address of the structure containing the quad word. The quad word is stored in standard VAX format, with the low-order longword first in memory.

### Description

This routine provides the same functionality as the `xdr_hyper` routine.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

`xdr_hyper`

## `xdr_u_int`

Converts a four-byte unsigned integer from local format to XDR format, or the other way around.

### Format

```
#include tcpip$rpc:xdr.h

bool_t xdr_u_int (XDR *xdrs, int *ip);
```

### Arguments

*xdrs*

Address of a structure containing XDR encoding and decoding information.

*ip*

Address of the integer.

### Description

This routine provides the same functionality as `xdr_int`, `xdr_long`, and `xdr_u_long`.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

`xdr_int`

## xdr\_u\_long

Converts an unsigned longword from local format to XDR format, or the other way around.

### Format

```
#include tcpip$rpc:xdr.h

bool_t xdr_u_long (XDR *xdrs, u_long *lp);
```

### Arguments

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*lp*

Address of the longword.

### Description

This routine provides the same functionality as `xdr_long`, `xdr_int`, and `xdr_u_int`.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

`xdr_long`, `xdr_int`, `xdr_u_int`

## **xdr\_u\_short**

Converts a two-byte unsigned integer from the local data format to XDR format, or the other way around.

### **Format**

```
#include tcpip$rpc:xdr.h

bool_t xdr_u_short (XDR *xdrs, u_short *sp);
```

### **Arguments**

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*sp*

Address of the integer being converted.

### **Description**

This routine provides the same functionality as `xdr_short`.

### **Diagnostics**

This routine returns TRUE if it succeeds and FALSE if it fails.

### **See Also**

`xdr_short`

## xdr\_union

Converts a union from the local data format to XDR format, or the other way around.

### Format

```
#include tcpip$rpc:xdr.h

bool_t xdr_union (XDR *xdrs, enum_t *dscmp, u_char *unp, xdr_discrim
*choices, xdrproc_t dfault);
```

### Arguments

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*dscmp*

Integer from the *choices* array.

*unp*

Address of the union.

*choices*

Address of an array. This array maps integers to XDR routines.

*dfault*

XDR routine that is called if the *dscmp* integer is not in the *choices* array.

### Description

The `xdr_union` routine searches the array `choices` for the value of `dscmp`. If it finds the value, it calls the corresponding XDR routine to process the remaining data. If `xdr_union` doesn't find the value, it calls the `dfault` routine.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

## **xdr\_vector**

Converts a vector (fixed length array) from the local data format to XDR format, or the other way around.

### **Format**

```
#include tcpip$rpc:xdr.h
```

```
bool_t xdr_vector (XDR *xdrs, u_char *basep, u_long nelem, u_long elmsize,  
xdrproc_t xdr_elem);
```

### **Arguments**

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*basep*

Address of the array.

*nelem*

Number of elements in the array.

*elmsize*

Size of each element.

*xdr\_elem*

Converts each element from the local data format to XDR format, or the other way around.

### **Diagnostics**

This routine returns TRUE if it succeeds and FALSE if it fails.

## xdr\_void

Converts nothing.

### Format

```
#include tcpip$rpc:xdr.h

bool_t xdr_void (XDR *xdrs, u_char *ptr);
```

### Arguments

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*ptr*

Ignored.

### Description

Use this routine as a place-holder for a program that passes no data. The server and client expect an XDR routine to be called, even when there is no data to pass.

### Diagnostics

This routine always returns TRUE.

## xdr\_wrapstring

Converts a null-terminated string from the local data format to XDR format, or the other way around.

### Format

```
#include tcpip$rpc:xdr.h

bool_t xdr_wrapstring (XDR *xdrs, char **cpp);
```

### Arguments

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*cpp*

Address of the address of the first byte in the string.

### Description

The `xdr_wrapstring` routine calls the `xdr_string` routine. The `xdr_wrapstring` routine hides the *maxsize* argument from the programmer. Instead, the maximum size of the string is assumed to be  $2^{32} - 1$ .

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

`xdr_string`

## xdrmem\_create

Creates a memory buffer XDR stream.

### Format

```
#include tcpip$rpc:xdr.h
```

```
void xdrmem_create (XDR *xdrs, u_char *addr, u_long size, enum xdr_op op);
```

### Arguments

***xdrs***

Address of the structure containing XDR encoding and decoding information.

***addr***

Address of the buffer containing the encoded data.

***size***

Size of the *addr* buffer.

***op***

Operations you will perform on the buffer. Valid values are XDR\_ENCODE, XDR\_DECODE, and XDR\_FREE. You may change this value.

### Description

The `xdrmem_create` routine initializes a structure so that other XDR routines can write to a buffer.

## xdrrec\_create

Creates a record-oriented XDR stream.

### Format

```
#include tcpip$rpc:xdr.h
```

```
void xdrrec_create (XDR *xdrs, u_long sendsize, u_long recvsize,  
u_char *tcp_handle, int (*readit)(), int (*writeit)());
```

### Arguments

#### *xdrs*

Address of the structure being created. The `xdrrec_create` routine will write XDR encoding and decoding information to this structure.

#### *sendsize*

Size of the send buffer in bytes. The minimum size is 100 bytes. If you specify fewer than 100 bytes, 4000 bytes is used as the default.

#### *recvsize*

Size of the receive buffer in bytes. The minimum size is 100 bytes. If you specify fewer than 100 bytes, 4000 bytes is used as the default.

#### *tcp\_handle*

Address of the client or server handle.

#### *readit*

Address of a user-written routine that reads data from the stream transport. This routine must use the following format:

```
int readit(tcp_handle, buffer, len)
```

```
u_char *tcp_handle;
```

```
u_char *buffer;
```

```
u_long len;
```

where *\*tcp\_handle* is the client or server handle, *\*buffer* is the buffer to fill, and *len* is the number of bytes to read. The *readit* routine returns either the number of bytes read, or -1 if an error occurs.

***writeit***

Address of a user-written routine that writes data to the stream transport. This routine must use the following format:

```
int writeit(tcp_handle, buffer, len)  
u_char *tcp_handle;  
u_char *buffer;  
u_long len;
```

- *tcp\_handle* is the client or server handle.
- *buffer* is the address of the buffer being written.
- *len* is the number of bytes to write.

The *writeit* routine returns either the number of bytes written, or -1 if an error occurs.

**Description**

The *xdrrec\_create* routine requires one of the following:

- The TCP transport
- A stream-oriented interface (such as file I/O) not supported by MultiNet. The stream consists of data organized into records. Each record is either an RPC request or reply.

The *clnttcp\_create* and *svcfcreate* routines call the *xdrrec\_create* routine.

**See Also**

*clnttcp\_create*, *svcfcreate*, *xdrrec\_endofrecord*, *xdrrec\_eof*,  
*xdrrec\_skiprecord*

## xdrrec\_endofrecord

Marks the end of a record.

### Format

```
#include tcpip$rpc:xdr.h

bool_t xdrrec_endofrecord (XDR *xdrs, bool_t sendnow);
```

### Arguments

#### *xdrs*

Address of the structure containing XDR encoding and decoding information.

#### *sendnow*

Indicates when the calling program will send the record to the *writelit* routine (see *xdrrec\_create*).

If *sendnow* is TRUE, *xdrrec\_endofrecord* sends the record now. If *sendnow* is FALSE, *xdrrec\_endofrecord* writes the record to a buffer and sends the buffer when it runs out of buffer space.

### Description

A client or server program calls the *xdrrec\_endofrecord* routine when it reaches the end of a record it is writing. The program must call the *xdrrec\_create* routine before calling *xdrrec\_endofrecord*.

### Diagnostics

This routine returns TRUE if it succeeds and FALSE if it fails.

### See Also

*xdrrec\_create*, *xdrrec\_eof*, *xdrrec\_skiprecord*

## xdrrec\_eof

Goes to the end of the current record, then verifies whether any more data can be read.

### Format

```
#include tcpip$rpc:xdr.h

bool_t xdrrec_eof (XDR *xdrs);
```

### Argument

*xdrs*

Address of the structure containing XDR encoding and decoding information.

### Description

The client or server program must call the `xdrrec_create` routine before calling `xdrrec_eof`.

### Diagnostics

This routine returns TRUE if it reaches the end of the data stream, and FALSE if it finds more data to read.

### See Also

`xdrrec_create`, `xdrrec_endofrecord`, `xdrrec_skiprecord`

## **xdrrec\_skiprecord**

Goes to the end of the current record.

### **Format**

```
#include tcpip$rpc:xdr.h

bool_t xdrrec_skiprecord (XDR *xdrs);
```

### **Argument**

*xdrs*

Address of the structure containing XDR encoding and decoding information.

### **Description**

A client or server program calls the `xdrrec_skiprecord` routine before it reads data from a stream. This routine ensures that the program starts reading a record from the beginning.

The `xdrrec_skiprecord` routine is similar to the `xdrrec_eof` routine, except that `xdrrec_skiprecord` does not verify whether any more data can be read.

The client or server program must call the `xdrrec_create` routine before calling `xdrrec_skiprecord`.

### **Diagnostics**

This routine returns TRUE if it has skipped to the start of a record. Otherwise, it returns FALSE.

### **See Also**

`xdrrec_create`, `xdrrec_endofrecord`, `xdrrec_eof`

## xdrstdio\_create

Initializes a `stdio` XDR stream.

### Format

```
#include tcpip$rpc:xdr.h

void xdrstdio_create (XDR *xdrs, FILE *file, enum xdr_op op);
```

### Arguments

*xdrs*

Address of the structure containing XDR encoding and decoding information.

*file*

File pointer `FILE *`, which is to be associated with the stream.

*op*

An XDR operation, one of: `XDR_ENCODE`, `XDR_DECODE`, or `XDR_FREE`.

### Description

The `xdrstdio_create` routine initializes an `stdio` stream for the specified file.



---

## **PART III Appendices**

- Appendix A Example TCP Client Program
- Appendix B Example TCP Server Programs
- Appendix C Example UDP Client Program
- Appendix D Example UDP Server Programs



### Example TCP Client Program

The following is an example of a TCP client that connects to the TCP ECHO port on the local machine, and echos what the user types through it.

If you have installed the library and include files, the following program is provided as `MULTINET_ROOT:[MULTINET.EXAMPLES]TCPECHOCIENT.C`.

```
#include "multinet_root:[multinet.include.sys]types.h"
#include "multinet_root:[multinet.include.sys]socket.h"
#include "multinet_root:[multinet.include.netinet]in.h"
#include <stdio.h>
#include "multinet_root:[multinet.include]netdb.h"

main()
{
    int s, n;
    char buf[256];
    struct sockaddr_in sin;
    struct hostent *hp;
    struct servent *sp;

    /*
     * Get the IP address of the host named "LOCALHOST".
     * This is the loopback address for ourselves
     */

    hp = gethostbyname("localhost");
    if (hp == NULL) {
        fprintf(stderr, "tcpechoclient: localhost unknown\n");
        exit(0x10000000);
    }
    /*
     * Create an IP-family socket on which to make
     * the connection
     */
    s = socket(hp->h_addrtype, SOCK_STREAM, 0);
    if (s < 0) {
```

## Example TCP Client Program

---

```
        socket_perror("tcpechoclient: socket");
        exit(0x10000000);
    }

    /*
     * Get the TCP port number of the "echo" server.
     *
     * This is commented out, but left as an example. We
     * hardwire port 500 to talk to the TCPECHOSERVER
     * programs.
     */

#ifdef notdef
    sp = getservbyname("echo", "tcp");
    if (sp == NULL) {
        fprintf(stderr,
            "tcpechoclient: echo/tcp: unknown service\n");
        exit(0x10000000);
    }
#endif notdef
    /*
     * Create a "sockaddr_in" structure which describes
     * the remote IP address we want to connect to (from
     * gethostbyname()) and the remote TCP port number
     * (from getservbyname()).
     */

    sin.sin_family = hp->h_addrtype;
    bcopy(hp->h_addr, &sin.sin_addr, hp->h_length);
#ifdef notdef
    sin.sin_port = sp->s_port;
#else
    sin.sin_port = htons(500);
#endif notdef
    /*
     * Connect to that address...
     */

    if (connect(s, &sin, sizeof (sin)) < 0) {
        socket_perror("tcpechoclient: connect");
        exit(0x10000000);
    }

    /*
     * Now go into a loop, reading data from
     * the network, writing it to the terminal
     * and reading data from the terminal,
     * writing it to the network...
     */
}
```

```
while ((n = socket_read(s, buf, sizeof(buf))) > 0) {
    write(1, buf, n);
    if (!fgets(buf, sizeof(buf), stdin)) break;
    socket_write(s, buf, strlen(buf));
}
if (n < 0) {
    socket_perror("tcpechoclient: socket_read");
    exit(0x10000000);
}
exit(1);
}
```



# Example TCP Server Programs

## Standalone TCP Server

The following is an example of a TCP server that listens on the TCP ECHO port for connections to the local machine, reads data from the connection and sends it back out.

If you have installed the MultiNet Programmers' Kit, you will find the following program on-line as `MULTINET_ROOT:[MULTINET.EXAMPLES]TCPECHOSERVER-STANDALONE.C`.

```
#include "multinet_root:[multinet.include.sys]types.h"
#include "multinet_root:[multinet.include.sys]socket.h"
#include "multinet_root:[multinet.include.netinet]in.h"
#include <stdio.h>
#include "multinet_root:[multinet.include]netdb.h"

main()
{
    short s, vs;
    int n, on=1;
    char buf[256];
    struct sockaddr_in sin, sin2;
    struct hostent *hp;
    struct servent *sp;
    /*
     * Create an IP-family socket on which to
     * listen for connections
     */

    s = socket(AF_INET, SOCK_STREAM, 0);
    if (s < 0) {
        socket_perror("tcpechoserver: socket");
        exit(0x10000000);
    }

    /*
```

## Example TCP Server Programs

---

```
* Get the TCP port number of the "echo" server.
*
* This is commented out, but left as an
* example. We hardwire port 500 so we
* don't have to stop the MultiNet echo
* server before running this.
*/

#ifdef notdef
    sp = getservbyname("echo", "tcp");
    if (sp == NULL) {
        fprintf(stderr,
            "tcpechoserver: echo/tcp: unknown service\n");
        exit(0x10000000);
    }
#endif notdef

/*
 * Set the "REUSEADDR" option on this socket.
 * This will allow us to bind() to it EVEN if
 * there already connections in progress on
 * this port number. Otherwise, we would get an
 * "Address already in use" error.
 */

if (setsockopt(s, SOL_SOCKET, SO_REUSEADDR,
    &on, sizeof(on)) < 0) {
    socket_perror("tcpechoserver: setsockopt");
    exit(0x10000000);
}

/*
 * Create a "sockaddr_in" structure which describes
 * the port we want to listen to. Address INADDR_ANY
 * means we will accept connections to any of our
 * local IP addresses.
 */

sin.sin_family = AF_INET;
sin.sin_addr.s_addr = INADDR_ANY;
#ifdef notdef
    sin.sin_port = sp->s_port;
#else
    sin.sin_port = htons(500);
#endif notdef

/*
 * Bind to that address...
 */

if (bind(s, &sin, sizeof (sin)) < 0) {
```

```

        socket_perror("tcpechoserver: bind");
        exit(0x10000000);
    }

    /*
     * Declare to the kernel that we want to listen for
     * connections on this port, and that the kernel may
     * queue up to five such connections for us.
     */

    if (listen(s, 5) < 0) {
        socket_perror("tcpechoserver: listen");
        exit(0x10000000);
    }

    /*
     * Now go into a loop, waiting for a connection and
     * processing it.
     */
    for (;;) {
        /*
         * Call accept to accept a new connection. This
         * 'peels' a connection off of the original socket
         * and returns to us a new channel to the connection.
         * We could now close down the original socket if we
         * didn't want to handle more connections.
         */
        n = sizeof(sin2);          /* Pass in the length */
        vs = accept(s, &sin2, &n);
        if (vs < 0) {
            socket_perror("tcpechoserver: accept");
            exit(0x10000000);
        }

        /*
         * 'sin2' will be a sockaddr_in structure describing
         * the remote IP address (and port #) which the
         * connection was made from. Before we start to echo
         * data, write a string into the network describing
         * this port.
         */

        hp = gethostbyaddr(&sin2.sin_addr,
                           sizeof(sin2.sin_addr), AF_INET);
        if (hp) {
            /*
             * We found a corresponding hostname,
             * format the string one way...
             */
            sprintf(buf, "Connection received from %s [%s]\r\n",

```

```
                hp->h_name, inet_ntoa(sin2.sin_addr));
    } else {
        /*
         * This host not in the host tables or Domain
         * Name Server.
         */
        sprintf(buf, "Connection received from [%s]\r\n",
                inet_ntoa(sin2.sin_addr));
    }
    socket_write(vs, buf, strlen(buf));
    /*
     * Now go into a loop, reading data from the network
     * and sending it right back...
     */

    while ((n = socket_read(vs, buf, sizeof(buf))) > 0) {
        socket_write(vs, buf, n);
    }

    /*
     * socket_read() will return 0 on end-of-file, or -1
     * on error...
     */

    if (n < 0) {
        socket_perror("tcpechoserver: read");
    }

    /*
     * Now close down the connection we accepted before
     * going back to get another...
     */

    socket_close(vs);
}
}
```

## TCP Server as Part of the MULTINET\_SERVER

The following is another example of a TCP server program that uses the MULTINET\_SERVER to listen for connections on the TCP ECHO port, read data from the connection and sends it back out.

To configure the MULTINET\_SERVER process to automatically create a process running this image when a connection arrives:

```
$ MULTINET CONFIGURE/SERVER
MultiNet Server Configuration Utility 4.4(nnn)
[Reading in symbols from SERVER image MULTINET:SERVER.EXE]
[Reading in configuration from MULTINET:SERVICES.MASTER_SERVER]
SERVER-CONFIG>ADD TEST
[Adding new configuration entry for service "TEST"]
```

```

Protocol: [TCP] TCP
TCP Port number: 500
Program to run: USERS:[ADELMAN]TCPECHOSERVER.EXE
[Added service TEST to configuration]
[Selected service is now TEST]
SERVER-CONFIG>RESTART

```

If you have installed the MultiNet Programmers' Kit, you will find the following program on-line as MULTINET\_ROOT:[MULTINET.EXAMPLES]TCPECHOSERVER.C.

```

#include "multinet_root:[multinet.include.sys]types.h"
#include "multinet_root:[multinet.include.sys]socket.h"
#include "multinet_root:[multinet.include.netinet]in.h"
#include <stdio.h>
#include "multinet_root:[multinet.include]netdb.h"

main()
{
    short s;
    int n, Status;
    char buf[256];
    struct sockaddr_in sin;
    struct hostent *hp;
    static struct {int Size; char *Ptr;} Descr={9 , "SYS$INPUT"};

    /*
     * $ASSIGN a channel to SYS$INPUT. This channel is the
     * channel to the network connection. This call must
     * be performed prior to any calls to VAX C I/O routines.
     */

    Status = SYS$ASSIGN(&Descr, &s, 0, 0);
    if (!(Status&1)) {
        exit(Status);
    }
    /*
     * Use getpeername() to find out who made the
     * connection to us, so we can act exactly like the
     * example tcpechoserver-standalone.
     */

    n = sizeof(sin);          /* Pass in the length */
    if (getpeername(s, &sin, &n) < 0) {
        socket_perror("tcpechoserver: getpeername");
        exit(0x10000000);
    }

    /*
     * 'sin' will be a sockaddr_in structure describing the
     * remote IP address (and port #) which the connection
     * was made from. Before we start to echo data, write a

```

```

* string into the network describing this port.
*/

hp = gethostbyaddr(&sin.sin_addr,
                  sizeof(sin.sin_addr), AF_INET);
if (hp) {
    /*
     * We found a corresponding hostname, format the string
     * one way...
     */
    sprintf(buf, "Connection received from %s [%s]\r\n",
            hp->h_name, inet_ntoa(sin.sin_addr));
} else {
    /*
     * This host not in the host tables or
     * Domain Name Server.
     */
    sprintf(buf, "Connection received from [%s]\r\n",
            inet_ntoa(sin.sin_addr));
}
socket_write(s, buf, strlen(buf));

/*
 * Now go into a loop, reading data from the network
 * and sending it right back...
 */
while ((n = socket_read(s, buf, sizeof(buf))) > 0) {
    socket_write(s, buf, n);
}

/*
 * socket_read() will return 0 on end-of-file, or -1
 * on error...
 */

if (n < 0) {
    socket_perror("tcpechoserver: read");
}

/*
 * Now close down the connection...
 */

socket_close(s);

/*
 * Exit successfully.
 */
exit(1);
}

```

### Example UDP Client Program

The following is an example of a UDP client that sends a packet to the UDP ECHO port on the local machine and prints what comes back.

**Note!** It uses `SYSQIO` to read the packet so that it can timeout and retransmit the packet.

If you have installed the MultiNet Programmers' Kit, you will find the following program on-line as `MULTINET_ROOT:[MULTINET.EXAMPLES]UDPECHOCIENT.C`.

```
#include "multinet_root:[multinet.include.sys]types.h"
#include "multinet_root:[multinet.include.sys]socket.h"
#include "multinet_root:[multinet.include.netinet]in.h"
#include <stdio.h>
#include "multinet_root:[multinet.include]netdb.h"
#include "multinet_root:[multinet.include]errno.h"
#include "multinet_root:[multinet.include.vms]inetiodef.h"

main()
{
    int s, n;
    char buf[256];
    struct sockaddr_in sin;
    struct hostent *hp;
    struct servent *sp;

    /*
     * Get the IP address of the host named "LOCALHOST".
     * This is the loopback address for ourselves
     */
    hp = gethostbyname("localhost");
    if (hp == NULL) {
        fprintf(stderr, "udpechoclient: localhost unknown\n");
        exit(0x10000000);
    }
}
```

## Example UDP Client Program

---

```
/*
 * Create an IP-family socket on which to
 * make the connection
 */

s = socket(hp->h_addrtype, SOCK_DGRAM, 0);
if (s < 0) {
    socket_perror("udpechoclient: socket");
    exit(0x10000000);
}

/*
 * Get the UDP port number of the "echo" server.
 *
 * This is commented out, but left as an example. We
 * hardwire port 500 to talk to the UDPECHOSERVER
 * programs.
 */

#ifdef notdef
    sp = getservbyname("echo", "udp");
    if (sp == NULL) {
        fprintf(stderr,
            "udpechoclient: echo/udp: unknown service\n");
        exit(0x10000000);
    }
#endif notdef
/*
 * Create a "sockaddr_in" structure which
 * describes the remote IP address we want
 * to send to (from gethostbyname()) and
 * the remote UDP port number (from
 * getservbyname()).
 */
sin.sin_family = hp->h_addrtype;
bcopy(hp->h_addr, &sin.sin_addr, hp->h_length);
#ifdef notdef
    sin.sin_port = sp->s_port;
#else
    sin.sin_port = htons(500);
#endif notdef

/*
 * Do a pseudo-connect to that address. This tells
 * the kernel that anything written on this socket
 * gets sent to this destination. It also binds us
 * to a local port number (random, but that is ok).
 */
```

```

n = connect(s, &sin, sizeof(sin));
if (n < 0) {
    socket_perror("udpechoclient: connect");
    exit(0x10000004);
}

/*
 * Now go into a loop, reading data from the network,
 * writing it to the terminal and reading data from
 * the terminal, writing it to the network...
 */
while (fgets(buf, sizeof(buf), stdin)) {
again: socket_write(s, buf, strlen(buf));
    n = socket_read_with_timeout(s, buf, sizeof(buf), 10);
    if (n < 0) {
        /*
         * If the read times out, assume that the
         * packet is lost and retransmit it. UDP is
         * not a reliable transport.
         */
        if (socket_errno == ETIMEDOUT) goto again;
        socket_perror("udpechoclient: socket_read");
        exit(0x10000000);
    } else {
        write(1, buf, n);
    }
}
exit(1);
}

/*
 * This routine does a normal read using $QIO and
 * also sets a timer. If no data arrives within the
 * specified time, the read is aborted.
 */

int socket_read_with_timeout(fd, buf, len, timeout)
int fd, len, timeout;
char *buf;
{
    unsigned short IOSB[4];
    int Status, TIME[2]={-10000000 * timeout, -1};

    /*
     * Start the read on the socket.
     */
    Status = SYS$QIO(1,
                    fd,
                    IO$_RECEIVE,
                    IOSB,

```

```

                                0, 0,
                                buf,
    len,
    0, 0, 0, 0);

    if (!(Status&1)) {
        vmserrno = Status;
        if (vmserrno & 0x8000) {
            vmserrno |= 0x4;
            socket_errno = (Status & 0x7fff) >> 3;
        } else {
            socket_errno = EIO;
        }
        return(-1);
    }

/*
 * Start the timer
 */

Status = SYS$SETIMR(2, TIME, 0, 0, 0);
if (!(Status&1)) {
    vmserrno = Status;
    if (vmserrno & 0x8000) {
        vmserrno |= 0x4;
        socket_errno = (Status & 0x7fff) >> 3;
    } else {
        socket_errno = EIO;
    }
    return(-1);
}

SYS$WFLOR(1, (1<<1)|(1<<2));

/*
 * Check if timer went off, or packet was received
 */
if (IOSB[0] == 0) {
/*
 * Timer went off. Cancel the I/O
 */
SYS$CANCEL(fd);
socket_errno = ETIMEDOUT;
vmserrno = 0x8004 | (ETIMEDOUT << 3);
return(-1);
} else {
/*
 * I/O completed, cancel the timer.
 */
SYS$CANTIM(0,0);

```

```
        /*
        *      Check for errors
        */
    if (!(IOSB[0] & 1)) {
        vmserrno = IOSB[0];
        if (vmserrno & 0x8000) {
            vmserrno |= 0x4;
            socket_errno = (IOSB[0] & 0x7fff) >> 3;
        } else {
            socket_errno = EIO;
        }
        return(-1);
    }
}
/*
 *      And the character count
 */
return(IOSB[1]);
}
```



# Example UDP Server Programs

## Standalone UDP Server

The following program is an example of a UDP server that listens for packets on the UDP ECHO port and sends them back to the port that transmitted them.

If you have installed the MultiNet Programmers' Kit, you will find the following program on-line as `MULTINET_ROOT:[MULTINET.EXAMPLES] UDPECHOSERVER-STANDALONE.C`.

```
#include "multinet_root:[multinet.include.sys]types.h"
#include "multinet_root:[multinet.include.sys]socket.h"
#include "multinet_root:[multinet.include.netinet]in.h"
#include <stdio.h>
#include "multinet_root:[multinet.include]netdb.h"

main()
{
    short s;
    int n, len;
    char buf[256];
    static int on=1;
    struct sockaddr_in sin;

    /*
     * Create an IP-family socket on which to
     * listen for packets
     */

    s = socket(AF_INET, SOCK_DGRAM, 0);
    if (s < 0) {
        socket_perror("udpechoserver: socket");
        exit(0x10000000);
    }
    /*
     * Get the UDP port number of the "echo" server.
```

```
*
* This is commented out, but left as an
* example. We hardwire port 500 so we
* don't have to stop the MultiNet echo
* server before running this.
*/

#ifdef notdef
    sp = getservbyname("echo", "udp");
    if (sp == NULL) {
        fprintf(stderr,
            "udpechoserver: echo/tcp: unknown service\n");
        exit(0x10000000);
    }
#endif notdef

/*
 * Set the "REUSEADDR" option on this socket. This
 * will allow us to bind() to it EVEN if there
 * already connections in progress on this port
 * number. Otherwise, we would get an "Address
 * already in use" error.
 */

if (setsockopt(s, SOL_SOCKET, SO_REUSEADDR,
    &on, sizeof(on)) < 0) {
    socket_perror("udpechoserver: setsockopt");
    exit(0x10000000);
}

/*
 * Create a "sockaddr_in" structure which describes
 * the port we want to listen to. Address INADDR_ANY
 * means we will accept connections to any of our
 * local IP addresses.
 */
sin.sin_family = AF_INET;
sin.sin_addr.s_addr = INADDR_ANY;
#ifdef notdef
    sin.sin_port = sp->s_port;
#else
    sin.sin_port = htons(500);
#endif notdef

/*
 * Bind to that address...
 */

if (bind(s, &sin, sizeof (sin)) < 0) {
    socket_perror("udpechoserver: bind");
}
```

```

        exit(0x10000000);
    }

    /*
     * Now go into a loop, reading data from the network
     * and sending it right back...
     */

while ((n = recvfrom(s, buf, sizeof(buf),
                    0, &sin, &len)) > 0) {
    sendto(s, buf, n, 0, &sin, len);
}

if (n < 0) {
    socket_perror("udpechoserver: recvfrom");
    exit(0x10000004);
}

/*
 * Now close down the connection...
 */

socket_close(s);

/*
 * Exit successfully.
 */

    exit(1);
}

```

## UDP Server as Part of the MULTINET\_SERVER

The following is an example of a UDP server that lets the MULTINET\_SERVER process listen for it. When a packet arrives for the UDP ECHO port the MULTINET\_SERVER will create a process running this image with SY\$\$INPUT being a socket on which a pseudo-connect() has been done.

To configure the MULTINET\_SERVER process to automatically create a process running this image when a packet arrives:

```

$ MULTINET CONFIGURE/SERVER
MultiNet Server Configuration Utility 4.4(nnn)
[Reading in symbols from SERVER image MULTINET:SERVER.EXE]
[Reading in configuration from MULTINET:SERVICES.MASTER_SERVER]SERVER-
CONFIG>ADD TEST
[Adding new configuration entry for service "TEST"]
Protocol: [TCP] UDP
TCP Port number: 500
Program to run: USERS: [ADELMAN]UDPECHOSERVER.EXE
[Added service TEST to configuration]

```

```
[Selected service is now TEST]
```

```
SERVER-CONFIG>RESTART
```

If you have installed the MultiNet Programmers' Kit, you will find the following program on-line as MULTINET\_ROOT:[MULTINET.EXAMPLES] UDPECHOSERVER.C.

```
#include "multinet_root:[multinet.include.sys]types.h"
#include "multinet_root:[multinet.include.sys]socket.h"
#include <stdio.h>
#include "multinet_root:[multinet.include]errno.h"
#include "multinet_root:[multinet.include.vms]inetiodef.h"

main()
{
    short s;
    int n, Status;
    char buf[256];
    static struct {int Size; char *Ptr;} Descr={9 , "SYS$INPUT"};

    /*
     * $ASSIGN a channel to SYS$INPUT. This
     * channel is the channel to the network
     * connection. This call must
     * be performed prior to any calls to
     * VAX C I/O routines.
     */

    Status = SYS$ASSIGN(&Descr, &s, 0, 0);
    if (!(Status&1)) {
        exit(Status);
    }

    /*
     * Now go into a loop, reading data from
     * the network and sending it right back...
     *
     * If we don't receive any packets in 30
     * seconds, assume that we are no longer
     * needed and exit. If we were needed,
     * when a new packet arrives the
     * MULTINET_SERVER will just create a new
     * process to handle it.
     */

    while ((n = socket_read_with_timeout(s, buf,
        sizeof(buf), 30)) > 0) {
        socket_write(s, buf, n);
    }

    /*
     * Now close down the connection...
     */
}
```

```

    */

    socket_close(s);
    /*
    * Exit successfully.
    */

    exit(1);
}

/*
* This routine does a normal read using $QIO and
* also sets a timer.  If no data arrives within the
* specified time, the read is aborted.
*/

int socket_read_with_timeout(fd, buf, len, timeout)
int fd, len, timeout;
char *buf;
{

    unsigned short IOSB[4];
    int Status, TIME[2]={-1000000 * timeout, -1};

    /*
    * Start the read on the socket.
    */

    Status = SYS$QIO(1,
                    fd,
                    IO$RECEIVE,
                    IOSB,
                    0, 0,
                    buf,
                    len,
                    0, 0, 0, 0);

    if (!(Status&1)) {
        vmserrno = Status;
        if (vmserrno & 0x8000) {
            vmserrno |= 0x4;
            socket_errno = (Status & 0x7fff) >> 3;
        } else {
            socket_errno = EIO;
        }
        return(-1);
    }

    /*
    * Start the timer

```

```

        */

Status = SYS$SETIMR(2, TIME, 0, 0, 0);
if (!(Status&1)) {
    vmserrno = Status;
    if (vmserrno & 0x8000) {
        vmserrno |= 0x4;
        socket_errno = (Status & 0x7fff) >> 3;
    } else {
        socket_errno = EIO;
    }
    return(-1);
}

SYS$WFLOR(1, (1<<1)|(1<<2));

/*
 * Check if timer went off, or packet was received
 */

if (IOSB[0] == 0) {
    /*
     * Timer went off. Cancel the I/O
     */
    SYS$CANCEL(fd);
    socket_errno = ETIMEDOUT;
    vmserrno = 0x8004 | (ETIMEDOUT << 3);
    return(-1);
} else {
    /*
     * I/O completed, cancel the timer.
     */
    SYS$CANTIM(0,0);
    /*
     * Check for errors
     */
    if (!(IOSB[0] & 1)) {
        vmserrno = IOSB[0];
        if (vmserrno & 0x8000) {
            vmserrno |= 0x4;
            socket_errno = (IOSB[0] & 0x7fff) >> 3;
        } else {
            socket_errno = EIO;
        }
        return(-1);
    }
}
/*
 * And the character count
 */

```

```

    return( IOSB[1] );
}

```

## Run-Once UDP Server as Part of the MULTINET\_SERVER

The following program is an example of alternative UDP ECHO server that lets the MULTINET\_SERVER process listen for it. When a packet arrives for the UDP ECHO port, the MULTINET\_SERVER will create a process running this image, with SYSS\$INPUT being the socket on which the original packet arrives. This process can handle as many packets as it would like; when it exits the MULTINET\_SERVER will go back to listening for new packets.

To configure the MULTINET\_SERVER process to automatically create a process running this image when a connection arrives:

```

$ MULTINET CONFIGURE/SERVER
MultiNet Server Configuration Utility 4.4(nnn)
[Reading in symbols from SERVER image MULTINET:SERVER.EXE]
[Reading in configuration from MULTINET:SERVICES.MASTER_SERVER]
SERVER-CONFIG>ADD TEST
[Adding new configuration entry for service "TEST"]
Protocol: [TCP] UDP
TCP Port number: 500
Program to run: USERS: [ADELMAN]UDPECHOSERVER.EXE
[Added service TEST to configuration]
[Selected service is now TEST]
SERVER-CONFIG>SET CONNECTED UDP_CONNECTED_SINGLE
[Connected action of TEST set to UDP_Connected_Single]
SERVER-CONFIG>RESTART

```

If you have installed the MultiNet Programmers' Kit, you will find the following program on-line as MULTINET\_ROOT:[MULTINET.EXAMPLES]UDPECHOSERVER-ONE.C.

```

#include "multinet_root:[multinet.include.sys]types.h"
#include "multinet_root:[multinet.include.sys]socket.h"
#include <stdio.h>
#include "multinet_root:[multinet.include]errno.h"
#include "multinet_root:[multinet.include.vms]inetiodef.h"

main()
{
    short s;
    int n, Status, len;
    char buf[256];
    static struct {int Size; char *Ptr;} Descr={9 , "SYSS$INPUT"};
    struct sockaddr sa;

    /*
     * $ASSIGN a channel to SYSS$INPUT. This
     * channel is the channel to the network
     * connection.
     */
}

```

```

Status = SYS$ASSIGN(&Descr, &s, 0, 0);
if (!(Status&1)) {
    exit(Status);
}
/*
 * Now go into a loop, reading data from the network
 * and sending it right back...
 *
 * If we don't receive any packets in 30
 * seconds, assume that we are no longer
 * needed and exit.  If we were needed,
 * when a new packet arrives the
 * MULTINET_SERVER will just create a new
 * process to handle it.
 */

while ((n = recvfrom_with_timeout(s, buf,
    sizeof(buf), 0, &sa, &len, 60)) > 0) {
    sendto(s, buf, n, 0, &sa, len);
}

/*
 * Now close down the connection...
 */

socket_close(s);

/*
 * Exit successfully.
 */

exit(1);
}

/*
 * This routine does a normal read using $QIO and
 * also sets a timer.  If no data arrives within the
 * specified time, the read is aborted.
 */

int recvfrom_with_timeout(fd, buf, len, flags,
from, fromlen, timeout)
int fd, len, timeout, flags, *fromlen;
struct sockaddr *from;
char *buf;
{
    unsigned short IOSB[4];
    int Status, TIME[2]={-10000000 * timeout, -1};
    struct {short int Length;

```

```

        char Sockaddr[sizeof(struct sockaddr)];
        Local_Buffer;

/*
 * Start the read on the socket.
 */

Status = SYS$QIO(1,
                fd,
                IO$_RECEIVE,
                IOSB,
                0, 0,
                buf,
                len,
                flags,
                fromlen ? &Local_Buffer : 0,
                fromlen ? sizeof(Local_Buffer) : 0, 0);

if (!(Status&1)) {
    vmserrno = Status;
    if (vmserrno & 0x8000) {
        vmserrno |= 0x4;
        socket_errno = (Status & 0x7fff) >> 3;
    } else {
        socket_errno = EIO;
    }
    return(-1);
}

/*
 * Start the timer
 */

Status = SYS$SETIMR(2, TIME, 0, 0, 0);
if (!(Status&1)) {
    vmserrno = Status;
    if (vmserrno & 0x8000) {
        vmserrno |= 0x4;
        socket_errno = (Status & 0x7fff) >> 3;
    } else {
        socket_errno = EIO;
    }
    return(-1);
}

SYS$WFLOR(1, (1<<1)|(1<<2));

/*
 * Check if timer went off, or packet was received
 */

```

```

    if (IOSB[0] == 0) {
        /*
         * Timer went off. Cancel the I/O
         */
        SYS$CANCEL(fd);
        socket_errno = ETIMEDOUT;
        vmserrno = 0x8004 | (ETIMEDOUT << 3);
        return(-1);
    } else {
        /*
         * I/O completed, cancel the timer.
         */
        SYS$CANTIM(0,0);
        /*
         * Check for errors
         */
        if (!(IOSB[0] & 1)) {
            vmserrno = IOSB[0];
            if (vmserrno & 0x8000) {
                vmserrno |= 0x4;
                socket_errno = (IOSB[0] & 0x7fff) >> 3;
            } else {
                socket_errno = EIO;
            }
            return(-1);
        }
    }
}
/*
 * Return the sockaddr to the user
 */
if (fromlen) {
    *fromlen = Local_Buffer.Length;
    bcopy(Local_Buffer.Sockaddr,
          from,
          sizeof(Local_Buffer.Sockaddr));
}
/*
 * And the character count
 */
return(IOSB[1]);
}

```

# Index

---

## A

accept() 1-4  
AF\_CHAOS 1-1  
AF\_INET 1-1, 1-2, 1-6  
Application Programming Interface (API) routines 4-1  
AST reentrancy 2-1  
auth\_destroy, RPC RTL 9-3  
authnone\_create, RPC RTL 9-4  
authunix\_create, RPC RTL 9-5  
authunix\_create\_default, RPC RTL 9-6

---

## B

bind() 1-4, 1-5  
BSD 1-5

---

## C

callrpc, RPC RTL 9-6  
clnt\_broadcast, RPC RTL 9-8  
clnt\_call, RPC RTL 9-10  
clnt\_control, RPC RTL 9-11  
clnt\_create, RPC RTL 9-13  
clnt\_destroy, RPC RTL 9-15  
clnt\_geterr, RPC RTL 9-16  
clnt\_pcreateerror, RPC RTL 9-17  
clnt\_perrno, RPC RTL 9-18  
clnt\_perror, RPC RTL 9-19  
clnt\_spcreateerror, RPC RTL 9-17  
clnt\_sperrno, RPC RTL 9-18  
clnt\_sperror, RPC RTL 9-19  
clntraw\_create, RPC RTL 9-20  
clnttcp\_create, RPC RTL 9-22  
clntudp\_bufcreate, RPC RTL 9-24  
clntudp\_create, RPC RTL 9-24  
connect() 1-3, 1-5, 3-1

---

## D

Distributed Application Components 6-1  
DNS  
    resolver routines 2-10  
documentation  
    comments xxi  
    online help xviii  
    structure xv

---

## E

errno 3-1

---

## F

FAQs xviii  
files  
    PROGRAM.H 7-4  
    PROGRAM\_CLNT.C 7-4  
    PROGRAM\_SVC.C 7-4  
    PROGRAM\_XDR.C 7-4

---

## G

get\_myaddress routine, RPC RTL 8-3  
gethostbyaddr() 1-2  
gethostbyname() 1-2, 1-3, 2-1  
getrpcbynumber, RPC RTL 8-4  
getrpcport, RPC RTL 8-5  
getservbyname() 1-2, 1-3, 1-4  
getservbyport() 1-2

## H

h\_errno 2-10  
help  
    by electronic mail xvii  
    by fax xviii  
htonl() 1-2  
htons() 1-2

---

## I

INADDR\_ANY 1-4, 1-5  
inet\_addr() 1-2  
inet\_ntoa() 1-2  
Input/Output Status Block (IOSB) 3-1  
IO\$M\_EXTEND 1-6

---

## L

listen() 1-4  
logical  
    MULTINET\_HOST\_NAME 2-20  
    MULTINET\_HOSTALIASES 2-34  
    MULTINET\_NETWORK\_IMAGE 2-47  
    MULTINET\_SNMP\_DEBUG 4-3

---

## M

MultiNet  
    public mailing list xviii  
    software patches xix

---

## O

online help xviii

---

## P

pmap\_getmaps, RPC RTL 10-2  
pmap\_getport, RPC RTL 10-3  
PMAP\_PROT.H file 8-2  
pmap\_rmtcall, RPC RTL 10-4  
pmap\_set, RPC RTL 10-5  
pmap\_unset, RPC RTL 10-6  
Port Mapper  
    binding 5-2  
    broadcast RPC 5-3

---

registration 5-2  
requesting a listing 6-4

---

## Q

QIO interface call  
    IO\$\_ACCEPT 3-2  
    IO\$\_ACCEPT\_WAIT 3-4  
    IO\$\_BIND 3-5  
    IO\$\_CONNECT 3-6  
    IO\$\_GETPEERNAME 3-7  
    IO\$\_GETSOCKNAME 3-8  
    IO\$\_GETSOCKOPT 3-9  
    IO\$\_IOCTL 3-11  
    IO\$\_LISTEN 3-12  
    IO\$\_READVBLK 3-13  
    IO\$\_RECEIVE 3-13  
    IO\$\_SELECT 3-15  
    IO\$\_SEND 3-17  
    IO\$\_SENSEMODE 3-19  
    IO\$\_SENSEMODE | IO\$M\_CTRL 3-23  
    IO\$\_SETMODE|IO\$M\_ATTNAST 3-33  
    IO\$\_SETSOCKOPT 3-34  
    IO\$\_SHUTDOWN 3-36  
    IO\$\_SOCKET 3-37  
SYS\$CANCEL 3-39  
SYS\$DASSGN 3-40

---

## R

recv() 1-4, 1-5  
recvfrom() 1-4, 1-5  
registerrpc, RPC RTL 11-3  
Remote Procedure Call (RPC) 5-2  
RPC  
    protocol compiler, RPCGEN 7-1  
RPC Run-Time Library (RTL) 9-1  
    conventions 8-1  
RPC Services  
    broadcast RPC 5-8  
    client 5-3  
    client stub 5-4  
    components 5-2  
        Port Mapper 5-2  
        RPCGEN compiler 5-2  
        Run-Time Libraries (RTLs) 5-2  
    definition 5-1  
    distributed applications 5-1  
    compile all files 6-3  
    design 6-2  
    execute client and server programs 6-4  
    link object code 6-3  
    start port mapper 6-3

- write and compile definition 6-2
  - write code 6-3
- error handling 5-4
- External Data Representation (XDR) 5-3
- global variables
  - svc\_fdset 11-7
- implementation 5-1
- local calls vs. remote calls 5-4
- management routines 8-1
- marshalling 5-4
- Port Mapper 5-2
  - binding 5-2
  - registration 5-2
- port mapper routines 10-1
- processing flow 5-3
- program listing, requesting 6-4
- program version numbers 5-9
- remote procedure call (RPC) 5-2
- remote procedure numbers 5-9
- remote programs/procedures, identifying 5-8
- RFCs 5-1
- routines
  - high-level 5-5
  - low-level 5-6
  - mid-level 5-5
- RPC information 5-3, 6-4
- RPC language 7-2
- RPCGEN compiler 5-2
  - error handling 7-6
  - input files 7-2
  - interface definitions 7-2
  - invoking 7-4
  - output files 7-3
  - preprocessor directives 7-3
  - restrictions 7-6
  - software requirements 7-1
- RPCINFO utility
  - sample 6-4
- RTL client routines
  - auth\_destroy 9-3
  - authnone\_create 9-4
  - authunix\_create 9-5
  - authunix\_create\_default 9-6
  - callrpc 9-6, 9-7
  - clnt\_broadcast 9-8
  - clnt\_call 9-10
  - clnt\_control 9-11
  - clnt\_create 9-13
  - clnt\_destroy 9-15
  - clnt\_geterr 9-16
  - clnt\_pcreateerror 9-17
  - clnt\_perrno 9-18
  - clnt\_perror 9-19
  - clnt\_spcreateerror 9-17
  - clnt\_sperrno 9-18
  - clnt\_sperror 9-19
- clntraw\_create 9-20
  - clnttcp\_create 9-22
  - clntudp\_bufcreate 9-24
  - clntudp\_create 9-24
  - common arguments 9-1
  - reference 9-2
- RTL management routines
  - get\_myaddress 8-3
  - getrpcbynumber 8-4
  - getrpcport 8-5
  - header files 8-1
  - reference 8-2
  - routine name conventions 8-1
- RTL Port Mapper routines
  - arguments 10-1
  - pmap\_getmaps 10-2
  - pmap\_getport 10-3
  - pmap\_rmtcall 10-4
  - pmap\_set 10-5
  - pmap\_unset 10-6
- RTL Server routines
  - svcerr\_systemerr 11-13
- RTL server routines
  - registerrpc 11-3
  - svc\_destroy 11-4
  - svc\_freeargs 11-5
  - svc\_getargs 11-6
  - svc\_getreqset 11-7
  - svc\_register 11-9
  - svc\_run 11-10
  - svc\_sendreply 11-11
  - svc\_unregister 11-12
  - svcerr\_auth 11-13
  - svcerr\_decode 11-13
  - svcerr\_noproc 11-13
  - svcerr\_noprogram 11-13
  - svcerr\_progvers 11-13
  - svcerr\_weakauth 11-13
  - svcfld\_create 11-15
  - svccraw\_create 11-16
  - svctcp\_create 11-17
  - svcudp\_create 11-18
  - svcudp\_enablecache 11-19
  - xprt\_register 11-20
  - xprt\_unregister 11-21
- RTL XDR routines
  - reference 12-2
  - xdr\_accepted\_reply 12-5
  - xdr\_array 12-6
  - xdr\_authunix\_parms 12-7
  - xdr\_bool 12-8
  - xdr\_bytes 12-9
  - xdr\_callhdr 12-10
  - xdr\_callmsg 12-11
  - xdr\_char 12-12
  - xdr\_double 12-13

- xdr\_enum 12-14
- xdr\_float 12-15
- xdr\_free 12-16
- xdr\_hyper 12-17
- xdr\_int 12-18
- xdr\_long 12-19
- xdr\_netobj 12-20
- xdr\_opaque 12-21
- xdr\_opaque\_auth 12-22
- xdr\_pmap 12-23
- xdr\_pmaplist 12-24
- xdr\_pointer 12-25
- xdr\_reference 12-27
- xdr\_rejected\_reply 12-28
- xdr\_replymsg 12-29
- xdr\_short 12-30
- xdr\_string 12-31
- xdr\_u\_char 12-32
- xdr\_u\_hyper 12-33
- xdr\_u\_int 12-34
- xdr\_u\_long 12-35
- xdr\_u\_short 12-36
- xdr\_union 12-37
- xdr\_vector 12-38
- xdr\_void 12-39
- xdr\_wrapstring 12-40
- xdrmem\_create 12-41
- xdrrec\_create 12-42
- xdrrec\_endofrecord 12-44
- xdrrec\_eof 12-45
- xdrrec\_skiprecord 12-46
- xdrstdio\_create 12-47
- server 5-3
- system crashes 5-4
- transport protocols 5-6
- unmarshalling 5-4
- XDR language 7-2
- XID cache 5-7
- RPCGEN
  - file naming conventions 7-3
  - output files 7-3

---

## S

- sa\_data 1-1
- sa\_family 1-1
- select() 2-1
- send() 1-4, 1-5
- sendto() 1-4, 1-5
- SIGURG 3-1
- sin\_addr 1-2, 1-5
- sin\_family 1-2, 1-6
- sin\_len 1-6
- sin\_port 1-2, 1-5
- sin\_zero 1-2
- SNMP extendible agent API routines
  - debugging code 4-3
  - initializing SNMP subagent 4-4
  - installing the extension agent image 4-3
  - linking the extension agent image 4-2
  - prerequisites 4-2
  - programming 4-1
  - querying SNMP subagent 4-8
  - reference 4-3
  - registering multiple subtrees 4-6
  - sending trap from subagent 4-10
  - SnmExtensionInitEx 4-6
  - SnmExtensionQuery 4-8
  - SnmExtensionTrap 4-10
- SOCK\_STREAM 1-2
- sockaddr 1-1, 1-2, 1-5
- sockaddr\_in 1-1, 1-2, 1-3, 1-4, 1-5
- socket definition 1-1
- socket library function
  - accept() 2-3
  - bcmp() 2-5
  - bcopy() 2-6
  - bind() 2-7
  - bzero() 2-8
  - connect() 2-9
  - endhostent() 2-11
  - endnetent() 2-12
  - endprotoent() 2-13
  - endservent() 2-14
  - getdtablesize() 2-15
  - gethostbyaddr() 2-16
  - gethostbyname() 2-18
  - gethostbynameaddr() 2-19
  - gethostname() 2-20
  - getnetbyaddr() 2-21
  - getnetbyname() 2-22
  - getpeername() 2-23
  - getprotobyname() 2-24
  - getprotobynumber() 2-25
  - getprotoent() 2-26
  - getservbyname() 2-27
  - getservbyport() 2-28
  - getservent() 2-29
  - getsockname() 2-30
  - getsockopt() 2-31
  - gettimeofday() 2-33
  - hostalias() 2-34
  - htonl() 2-35
  - htons() 2-36
  - inet\_addr() 2-37
  - inet\_lnaof() 2-38
  - inet\_makeaddr() 2-39
  - inet\_netof() 2-40
  - inet\_network() 2-41
  - inet\_ntoa() 2-42

- 
- klread() 2-43
  - klseek() 2-44
  - klwrite() 2-45
  - listen() 2-46
  - multinet\_kernel\_nliith 2-47
  - nlist() 2-48
  - ntohl() 2-49
  - ntohs() 2-50
  - recv() 2-51
  - recvfrom() 2-53
  - recvmsg() 2-55
  - select() 2-57
  - select\_wake() 2-60
  - send() 2-61
  - sendmsg() 2-62
  - sendto() 2-64
  - sethostent() 2-66
  - setnetent() 2-67
  - setprotoent() 2-68
  - setservent() 2-69
  - setsockopt() 2-70
  - shutdown() 2-72
  - socket ioctl
    - FIONBIO 2-77
    - FIONREAD 2-78
    - SIOCADDRT 2-79
    - SIOCATMARK 2-83
    - SIOCDDARP 2-84
    - SIOCDELRT 2-81
    - SIOCGARP 2-85
    - SIOCGIFADDR 2-87
    - SIOCGIFBRDADDR 2-89
    - SIOCGIFCONF 2-91
    - SIOCGIFDSTADDR 2-92
    - SIOCGIFFLAGS 2-94
    - SIOCGIFMETRIC 2-96
    - SIOCGIFNETMASK 2-98
    - SIOCSARP 2-86
    - SIOCSIFADDR 2-88
    - SIOCSIFBRDADDR 2-90
    - SIOCSIFDSTADDR 2-93
    - SIOCSIFFLAGS 2-95
    - SIOCSIFMETRIC 2-97
    - SIOCSIFNETMASK 2-99
  - socket option
    - SO\_BROADCAST 2-100
    - SO\_DEBUG 2-101
    - SO\_DONTROUTE 2-102
    - SO\_ERROR 2-103
    - SO\_KEEPALIVE 2-104
    - SO\_LINGER 2-105
    - SO\_OOINLINE 2-106
    - SO\_RCVBUF 2-107
    - SO\_RCVLOWAT 2-108
    - SO\_RCVTIMEO 2-109
    - SO\_REUSEADDR 2-110
    - SO\_SNDBUF 2-111
    - SO\_SNDLOWAT 2-112
    - SO\_SNDTIMEO 2-113
    - SO\_TYPE 2-114
    - TCP\_KEEPALIVE 2-115
    - TCP\_NODELAY 2-116
  - socket() 2-73
  - socket\_close() 2-75
  - socket\_ioctl() 2-76
  - socket\_perror() 2-117
  - socket\_read() 2-118
  - socket\_write() 2-119
  - vms\_errno\_string() 2-120
  - socket() 1-2, 3-1
  - socket\_read() 1-3, 1-4
  - socket\_write() 1-3, 1-4
  - svc\_destroy, RPC RTL 11-4
  - svc\_freeargs, RPC RTL 11-5
  - svc\_getargs, RPC RTL 11-6
  - svc\_getreqset, RPC RTL 11-7
  - svc\_register, RPC RTL 11-9
  - svc\_run, RPC RTL 11-10
  - svc\_sendreply, RPC RTL 11-11
  - svc\_unregister, RPC RTL 11-12
  - svcerr\_auth, RPC RTL 11-13
  - svcerr\_decode, RPC RTL 11-13
  - svcerr\_noproc, RPC RTL 11-13
  - svcerr\_noprog, RPC RTL 11-13
  - svcerr\_progvers, RPC RTL 11-13
  - svcerr\_systemerr, RPC RTL 11-13
  - svcerr\_weakauth, RPC RTL 11-13
  - svcf\_create, RPC RTL 11-15
  - svcraw\_create, RPC RTL 11-16
  - svctcp\_create, RPC RTL 11-17
  - svcdup\_bufcreate, RPC RTL 11-18
  - svcdup\_create, RPC RTL 11-18
  - svcdup\_enablecache, RPC RTL 11-19
- 
- ## T
- TCP
    - client 1-3
      - program A-1
    - server 1-4
      - programs B-1
  - TCP SNMP counters function
    - reading the 3-31
  - typographical conventions xx
- 
- ## U
- UDP 1-4
    - client program C-1

- server programs D-1
- UDP SNMP counters function
  - reading the 3-31

---

## X

- XDR encoding and decoding routines 12-2
- XDR routines, upper layer 12-4
- XDR support routines 12-3
- xdr\_accepted\_reply, RPC RTL 12-5
- xdr\_array, RPC RTL 12-6
- xdr\_authunix\_parms, RPC RTL 12-7
- xdr\_bool, RPC RTL 12-8
- xdr\_bytes, RPC RTL 12-9
- xdr\_callhdr, RPC RTL 12-10
- xdr\_callmsg, RPC RTL 12-11
- xdr\_char, RPC RTL 12-12
- xdr\_double, RPC RTL 12-13
- xdr\_enum, RPC RTL 12-14
- xdr\_float, RPC RTL 12-15
- xdr\_free, RPC RTL 12-16
- xdr\_hyper, RPC RTL 12-17
- xdr\_int, RPC RTL 12-18
- xdr\_long, RPC RTL 12-19
- xdr\_netobj, RPC RTL 12-20
- xdr\_opaque, RPC RTL 12-21
- xdr\_opaque\_auth, RPC RTL 12-22
- xdr\_pmap, RPC RTL 12-23
- xdr\_pmaplist, RPC RTL 12-24
- xdr\_pointer, RPC RTL 12-25
- xdr\_reference, RPC RTL 12-27
- xdr\_rejected\_reply, RPC RTL 12-28
- xdr\_replymsg, RPC RTL 12-29
- xdr\_short, RPC RTL 12-30
- xdr\_string, RPC RTL 12-31
- xdr\_u\_char, RPC RTL 12-32
- xdr\_u\_hyper, RPC RTL 12-33
- xdr\_u\_int, RPC RTL 12-34
- xdr\_u\_long, RPC RTL 12-35
- xdr\_u\_short, RPC RTL 12-36
- xdr\_union, RPC RTL 12-37
- xdr\_void, RPC RTL 12-39
- xdr\_wrapstring, RPC RTL 12-40
- xdrmem\_create, RPC RTL 12-41
- xdrrec\_create, RPC RTL 12-42
- xdrrec\_endofrecord, RPC RTL 12-44
- xdrrec\_eof, RPC RTL 12-45
- xdrrec\_skiprecord, RPC RTL 12-46
- xdrstdio\_create, RPC RTL 12-47
- XID cache, enabling 5-8
- xprt\_register, RPC RTL 11-20
- xprt\_unregister, RPC RTL 11-21

## Reader's Comments

### MultiNet for OpenVMS Programmer's Reference, v4.4 Part Number: N-5003-44-NN-A

Your comments and suggestions will help us to improve the quality of our future documentation. Please note that this form is for comments on documentation only.

I rate this guide's:	Excellent	Good	Fair	Poor
Accuracy	0	0	0	0
Completeness (enough information)	0	0	0	0
Clarity (easy to understand)	0	0	0	0
Organization (structure of subject matter)	0	0	0	0
Figures (useful)	0	0	0	0
Index (ability to find topic)	0	0	0	0
Ease of use	0	0	0	0

1. I would like to see more/less: \_\_\_\_\_
2. Does this guide provide the information you need to perform daily tasks? \_\_\_\_\_
3. What I like best about this guide: \_\_\_\_\_
4. What I like least about this guide: \_\_\_\_\_
5. Do you like this guide's binding? If not, what would you prefer? \_\_\_\_\_

#### My additional comments or suggestions for improving this guide:

---

---

I found the following errors in this guide:

Page	Description
_____	_____
_____	_____

Please indicate the type of user/reader that you most nearly represent:

System Manager	<input type="radio"/>	Educator/Trainer	<input type="radio"/>
Experienced Programmer	<input type="radio"/>	Sales	<input type="radio"/>
Novice Programmer	<input type="radio"/>	Scientist/Engineer	<input type="radio"/>
Computer Operator	<input type="radio"/>	Software Support	<input type="radio"/>
Administrative Support	<input type="radio"/>	Other (please specify)	<input type="radio"/> _____

Name: \_\_\_\_\_ Dept. \_\_\_\_\_  
Company: \_\_\_\_\_ Date \_\_\_\_\_  
Mailing Address: \_\_\_\_\_

After filling out this form, FAX or mail it to:  
**Process Software, 959 Concord Street, Framingham, MA 01701-4682**  
**Attention: Marketing Manager FAX 508-879-0042 e-mail:techpubs@process.com**

