TCPware® for OpenVMS Network Control Utility Command Reference

Part Number: N-6002-60-NN-A

January 2014

This manual is a command reference to the Network Control Utility (NETCU) for managing the TCPware for OpenVMS family of software products.

Revision/Update: This is a revised manual.

Operating System/Version: VAX/VMS V5.5-2 or later, OpenVMS VAX V6.0 or later, OpenVMS Alpha V6.1 or later, or OpenVMS I64 V8.2 or later

Software Version: 6.0

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.

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 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.

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 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”).

Portions copyright 1988 - 1994 Epilogue Technology Corporation.

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

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

Introducing This Guide

This guide describes how to use the Network Control Utility (NETCU) to set up and manage a network and TCPware components. It is for end users and system managers.

What You Need to Know Beforehand

Before using TCPware, you should be familiar with:

- The TCPware for OpenVMS products, components, features, and capabilities (see the User's Guide for more information)
- Computer networks in general
- HP's OpenVMS operating system and file system

How This Guide Is Organized

This guide has the following contents:

- Chapter 1, *Introducing NETCU* — provides an overview of NETCU, a summary of commands as they relate to each TCPware component or function, how to run NETCU, and how to send NETCU output to a file.
- Chapter 2, *NETCU Commands* — is an alphabetically organized, detailed description of each NETCU command.
- Chapter 3, *MAIL-CONFIG Commands* — is an alphabetically organized, detailed description of each MAIL-CONFIG command.
- Index to this guide.

Obtaining Technical Support

You can use the following technical support services for information and help about TCPware and other Process Software products if you subscribe to Process Software’s Product Support Services. (If you bought TCPware products through an authorized TCPware reseller, contact your reseller for technical support.) Contact Customer Support directly using the following methods:

- **Electronic Mail**

  E-mail gets your questions to us quickly and allows us to respond as soon as we have information for you. Send e-mail to: **`support@process.com`**. Be sure to include your:

  – Name

  – Telephone number

  - Company name
  - Process Software product names and version numbers
  - Operating system name and version number

  Describe the problem in as much detail as possible. You will receive an immediate automated response telling you your call has been logged.

- **Telephone**

  If calling within the continental United States or Canada, call Process Software Technical Support toll-free at 1-800-394-8700. If calling from outside the continental United States or Canada, dial 1-508-628-5074. Please be ready to provide your name, company name, and telephone number.

- **World Wide Web**

  There is a variety of useful technical information available on our World Wide Web home page, **`http://www.process.com`** (select **Customer Support**).

- **Internet Newsgroup**

  You can also access the VMSnet newsgroup **`vmsnet.networks.tcp-ip.tcpware`**. Process Software's Engineering and Customer Support professionals monitor and respond to this open forum newsgroup on a timely basis.

Licensing Information

Each software product in the TCPware for OpenVMS family includes a software license which entitles you to install and use a TCPware for OpenVMS product on one computer. Please read and understand the *Software License Agreement* before installing the product. If you want to use a TCPware product on more than one computer, you need to purchase additional copies of the product. Contact Process Software or your distributor for details.

Maintenance Services

Process Software offers a variety of software maintenance and support services. Contact us or your distributor for details about these services.

Reader's Comments Page

In the back of each TCPware for OpenVMS guide is a Reader's Comments page. Return a completed copy of this page to Process Software or use e-mail to send us comments on the documentation.

Send e-mail to: **`techpubs@process.com`**. Please be as specific as possible about the location of your comments: include the exact title of the document, version, date, and page references as appropriate. Your comments about our documentation are very much appreciated.

Documentation Set

The documentation set for TCPware for OpenVMS consists of the following:

- **Error messages help** — Access help for TCPware error messages only as follows:

  ```
  $ HELP TCPWARE MESSAGES
  ```

  If the error message is included in the MESSAGES help, it identifies the TCPware component and provides a meaning and user action. See the `Instructions` under `MESSAGES`.

- **Installation & Configuration Guide** — for system managers and those installing the software. The guide provides installation and configuration instructions for the TCPware for OpenVMS products.
- **Management Guide** — for system managers. This guide contains information on functions not normally available to the general network end-user. It also includes implementation notes and troubleshooting

information.

- **Network Control Utility (NETCU) Command Reference** — for users and system managers. This reference covers all the commands available with the Network Control Utility (NETCU) and contains troubleshooting information.
- **Programmer's Guide** — for network application programmers. This guide gives application programmers information on the callable interfaces between TCPware for OpenVMS and application programs.
- **Release Notes** for the current version of TCPware for OpenVMS — for all users, system managers, and application programmers. The *Release Notes* are available online on your TCPware for OpenVMS media and are accessible before or after software installation.

You can use help at the DCL prompt to find the following:

- **Topical help** — Access TCPware help topics only as follows:

```
$ HELP TCPWARE [topic]
```

The topic entry is optional. You can also enter topics and subtopics at the following prompt and its subprompts:

TCPWARE Subtopic?

Online help is also available from within certain TCPware components: FTP-OpenVMS Client and Server, Network Control Utility, (NETCU), TELNET-OpenVMS Client, NSLOOKUP, and TRACEROUTE. Use the HELP command from within each component.

Example: NETCU> **HELP *[topic]***

- **User's Guide**— for all users. This guide includes an introduction to TCPware for OpenVMS products as well as a reference for the user functions arranged alphabetically by product, utility, or service.

Conventions Used

Convention	**Meaning**
host	Any computer system on the network. The local host is your computer. A remote host is any other computer.
`monospaced type`	System output or user input. User input is in `bold type`. Example: `Is this configuration correct? YES` Monospaced type also indicates user input where the case of the entry should be preserved.
italic type	Variable value in commands and examples. For example, *username* indicates that you must substitute your actual username. Italic text also identifies documentation references.
[*directory*]	Directory name in an OpenVMS file specification. Include the brackets in the specification.
[optional-text]	(Italicized text and square brackets) Enclosed information is optional. Do not include the brackets when entering the information. Example: `START/IP line address [info]` This command indicates that the *info* parameter is optional.

{*value* | *value*}	Denotes that you should use only one of the given values. Do not include the braces or vertical bars when entering the value.
Note!	Information that follows is particularly noteworthy.
CAUTION!	Information that follows is critical in preventing a system interruption or security breach.
`key`	Press the specified key on your keyboard.
`Ctrl/key`	Press the control key and the other specified key simultaneously.
`Return`	Press the Return or Enter key on your keyboard.

Chapter 1 Introducing NETCU

Introduction

The Network Control Utility (NETCU) is the utility program system managers and operators use to configure and control networks that run TCPware.

This chapter summarizes the NETCU commands, by category, and describes how to run NETCU and send NETCU output to a file. Each command is described in detail in the next chapter, NETCU Commands.

Running NETCU

Run NETCU directly from a terminal or from a command procedure. To run NETCU from your terminal, enter the following command at the DCL prompt:

```
NETCU
```

or

```
RUN TCPWARE:NETCU
```

The system displays the NETCU> prompt. NETCU is ready to accept your commands.

To have a startup command file execute each time you invoke NETCU, do the following:

1 Create a file containing the commands you want performed at the beginning of each NETCU session.

2 Define the NETCU_STARTUP logical to point to the file.

For example, you can include the following in your LOGIN.COM file:

```
ASSIGN SYS$LOGIN:NETCUSTART.COM NETCU_STARTUP
```

When you start NETCU, the NETCU_STARTUP logical points to the specified file (SYS$LOGIN:NETCUSTART.COM for example) and processes all the commands. Note that they system ignores all commands following an EXIT or QUIT command in the file. NETCU ignores any "commented-out" command lines in files (such as SERVICES.COM) that are used as input to NETCU. The commented-out line in the file should begin with the !, #, or ; character. NETCU does not execute the command line until you remove the character.

Summary of NETCU Commands

This section lists each NETCU command and summarizes its purpose. Related commands appear together.

ARP Commands

Use commands listed in Table 1-1 to maintain the Address Resolution Protocol (ARP) table. You rarely need to enter these commands since ARP maintains the table automatically.

Table 1-1 NETCU ARP Commands

Command	Purpose
ADD ARP	Adds an entry to the ARP table
FIND ARP	Displays an entry from the ARP table
FLUSH ARP	Flushes the ARP table
REMOVE ARP	Deletes an entry from the ARP table
SET INTERFACE/ARP_*	Sets various ARP parameters for an interface
SHOW ARP	Displays the ARP table for the specified line
SHOW INTERFACE	Displays the ARP parameters set

Dynamic Host Configuration Commands

Use commands listed in Table 1-2 to maintain the Dynamic Host Configuration Protocol (DHCP) server. Note that to maintain the DHCP V4 server, use “DHCP4” in the following commands instead of “DHCP”.

Table 1-2 NETCU Dynamic Host Configuration Commands

Command	Purpose
RELEASE DHCP RELEASE DHCP4	Releases an address lease record

SET DHCP
SET DHCP4
	Performs various DHCP operations

SHOW DHCP SHOW DHCP4	Displays various DHCP information
STOP/DHCP STOP/DHCP4	Shuts down the DHCP server

UPDATE DHCP
UPDATE DHCP4
	Instructs the Dynamic Host Configuration Protocol (DHCP) server to process the update file and add or remove the specified host and subclass declarations.

Multicasting Commands

Use commands listed in Table 1-3 to join, leave, or show multicast host groups.

Table 1-3 NETCU Multicasting Commands

Command	**Purpose**
ADD MULTICAST_GROUP	Adds (joins) a multicast host group address to an interface or all interfaces
REMOVE MULTICAST_GROUP	Removes (leaves) a multicast host group address from an interface or all interfaces
SHOW MULTICAST_GROUPS	Displays the multicast host groups joined for an interface or all interfaces

NFS Commands

Table 1-4 lists the NFS-related commands in NETCU. Each entry indicates whether the command is relevant to the NFS-OpenVMS Client, NFS-OpenVMS Server, or both.

Table 1-4 NETCU NFS Commands

Command	**Purpose**	**Relevant to**
ADD EXPORT	Adds an OpenVMS directory and associated NFS pathname to the EXPORT database	Server
ADD GROUP	Adds an NFS group to the GROUP database	Client
ADD PROXY	Adds an NFS user to the PROXY database	Client/Server
ADD SM*[_BAK]*	Adds a host to the Network Status Monitor file (SM.DAT or SM_BAK.DAT)	Server
CREATE EXPORT	Creates an empty EXPORT database	Server
CREATE GROUP	Creates an empty GROUP database	Client
CREATE PROXY	Creates an empty PROXY database	Client/Server
FIND PROXY	Finds and displays a PROXY database entry	Client/Server

RELOAD GROUP	Implements changes made to the GROUP database	Client
RELOAD PROXY	Implements changes made to the PROXY database	Client/Server
REMOVE EXPORT	Removes an entry from the EXPORT database	Server
REMOVE GROUP	Removes an entry from the GROUP database	Client
REMOVE PROXY	Removes an entry from the PROXY database	Client/Server
REMOVE SM*[_BAK]*	Removes a host from the Network Status Monitor file (SM.DAT or SM_BAK.DAT)	Server
SHOW EXPORT	Shows entries in the EXPORT database	Client/Server
SHOW GROUP	Shows entries in the GROUP database	Client
SHOW MOUNT	Shows the pathnames of exported directories and the hosts that mounted them	Client/Server
SHOW PROXY	Shows entries in the PROXY database	Client/Server
SHOW SM*[_BAK]*	Shows entries in the Network Status Monitor file (SM.DAT or SM_BAK.DAT)	Server
SHOW STATISTICS	Displays statistics information on the NFS Server	Server
STOP/SERVER	Stops the NFS Server	Server
UNMOUNT ALL	Removes the client’s mount list entries from one or more NFS servers	Client

Parameter Setting Command

Table 1-5 contains the TCPware parameters you can set using the NETCU SET command. You usually do not need to enter these commands because they are issued during configuration.

Table 1-5 NETCU SET Command

Command	**Sets**
SET *parameter*	Connection backlog values Default IP datagram time-to-live value IP datagram time-out time Default type of service used Whether subnets are local Maximum size of TCP segments sent Minimum TCP retransmission time Maximum TCP retransmission time TCP persistence timer's initial value Default time zone offset or name

Routing Commands

Table 1-6 lists the commands that configure and maintain routes. If you enter the necessary routing commands in the TCPWARE:ROUTING.COM file, TCPware executes them automatically at startup. If using GateD, do not also include routes in the ROUTING.COM file by using the ADD ROUTE command.

Table 1-6 NETCU Routing Commands

Command	**NETCU Routing Commands**
ADD ROUTE	Adds an entry to the routing table
CHECK GATED CONFIG	Checks a GateD configuration file for syntax errors
DUMP GATED STATE	Dumps the state of the GATED process to a file
ENABLE FORWARDING	Allows this host to act as a router between networks
DISABLE FORWARDING	Disables this host from acting as a router between networks
ENABLE REDIRECTS	Allows this host to return ICMP redirects to source hosts
DISABLE REDIRECTS	Disables this host from returning ICMP redirects to source hosts

FIND ROUTE	Displays an existing route from the routing table
FLUSH/ROUTE	Flushes the entire routing table
LOAD GATED CONFIGURATION	Loads a GateD configuration file
REMOVE ROUTE	Deletes an entry from the routing table
SET GATED TRACE	Controls tracing in GateD
SET GATEWAY	Defines the internet address of the default gateway
SHOW GATED TRACE	Displays tracing in GateD
SHOW OSPF	Queries Open Shortest Path First (OSPF) gateways
SHOW RIP	Queries Routing Information Protocol (RIP) gateways
SHOW ROUTES	Displays the routing table
STOP/GATED	Stops the GateD process
TOGGLE GATED TRACING	Toggles tracing in GateD
UPDATE GATED INTERFACES	Rescans the GateD network interfaces

Service Commands

Table 1-7 lists the commands that manage the master server of TCPware.

Table 1-7 NETCU Service Commands

Command	**Purposes**
ADD ACCESS_LIST	Lets you control host access to services
ADD SERVICE	NETCP listens for TCP or UDP connections on the specified port
MODIFY SERVICE	Modifies information associated with a service

REMOVE ACCESS_LIST	Removes server access restrictions
REMOVE SERVICE	NETCP stops listening for connections on the specified port(s)
SHOW ACCESS_LIST	Prints or displays server access restrictions
SHOW SERVICES	Displays information for the specified port(s) and protocol(s)

Starting and Stopping Commands

Table 1-8 lists the commands that start and stop the network. You do not need to enter these commands under normal circumstances. STARTNET.COM and SHUTNET.COM perform these functions automatically.

Table 1-8 NETCU Starting and Stopping Commands

Command	**Purpose**
KILL CONNECTIONS	Resets the TCP connection on specified device, address, or port
START/DNIP	Starts a DECnet-over-IP line
START/INET	Starts the INET device driver
START/IP	Starts the IP protocol for a particular interface
START/PWIP	Starts the PWIPDRIVER
START/TCP	Starts the TCP protocol
START/UCX	Starts UCX compatibility support
START/UDP	Starts the UDP protocol
STOP/DNIP	Stops a DECnet-over-IP line or lines
STOP/GATED	Stops the GateD process
STOP/INET	Stops the INET device driver
STOP/IP	Stops the IP protocol for a particular interface

STOP/NETCP	Stops the Network Control Process (NETCP)
STOP/PWIP	Stops the PWIPDRIVER
STOP/SERVER	Stops the NFS Server
STOP/TCP	Stops the TCP protocol
STOP/UCX	Stops UCX compatibility support
STOP/UDP	Stops the UDP protocol

Token Authentication Commands

Table 1-9 lists the commands that manage the TCPware ACE/Client user database used by Token Authentication. The TCPware ACE/Client user database is stored in the TCPWARE:ACECLIENT_USER.DAT file. If you create a new database, the existing database file is renamed to TCPWARE:ACECLIENT_USER_OLD.DAT.

Table 1-9 NETCU Token Authentication Commands

Command	**Purpose**
ADD ACE_USER	Adds a username to the TCPware ACE/Client database
CREATE ACE_USER_DATABASE	Creates a new database and renames the old one
REMOVE ACE_USER	Removes an entry from the database
SHOW ACE_USER	Shows the entries in the database

Status Commands

Table 1-10 lists the commands that show the status of various network activities. The table also lists the UNIX netstat command that shows similar information. The DEBUG commands require LOG_IO privilege along with either SYSPRV or BYPASS privilege.

Table 1-10 NETCU Status Commands

Command	**Purpose**
DEBUG/IP	Displays information about IP datagrams sent and received over the network
DEBUG/TCP	Displays information about TCP segments sent and received over the network
DEBUG/UPD	Displays information about UDP datagrams sent and received over the network
SET *[*NO*]*LOG	Controls logging of non-error events in the NETCP.LOG file or another specified log file.
SHOW *parameter*	Shows values set using the SET *parameters* command
SHOW ACCESS_LIST	Prints or displays server access restrictions
SHOW ARP	Displays the entire ARP table for the specified lines
SHOW CONNECTIONS	Displays a list of the active internet connections (similar to the `netstat -a` command)
SHOW COUNTERS	Displays statistics counters for TCPDRIVER and UDPDRIVER
SHOW DHCP SHOW DHCP4	Displays the current DHCP address lease records
SHOW DNIP	Displays information about currently configured DECnet over IP tunnels
SHOW GATED TRACE	Displays tracing in GateD
SHOW HOST	Displays the official host name, internet address(es), and alias host names for a specified host name or IP address
SHOW INTERFACE	Displays packet rate information for an interface
SHOW MULTICAST_GROUPS	Displays the multicast host groups joined for an interface or all interfaces

SHOW NETWORKS	Displays IPDRIVER network information for each line and IPDRIVER datagram counters (similar to the `netstat -i` command)
SHOW OSPF	Queries Open Shortest Path First (OSPF) gateways
SHOW RIP	Queries Routing Information Protocol (RIP) gateways
SHOW ROUTES	Displays the routing table
SHOW SERVICES	Displays information about protocols and ports NETCP services
SHOW SNMP	Displays the SNMP counters maintained by the local host
SHOW STATISTICS	Displays statistics information on the NFS Server

Security Commands

Table 1-11 lists the commands that control various security functions. Many of these commands are only available with the TCPware Security-Plus product.

Table 1-11 NETCU Security Commands

Command	**Purpose**
ADD KACL	Adds a Kerberos access control list (ACL) for accessing the Kerberos database (KDB)
ADD KDB	Adds an entry to the KDB
ADD KERBEROS USER	Used by the Kerberos administrator to remotely add a user to the KDB
CREATE KDB	Creates (initializes) the KDB
CREATE SRVTAB	Creates an encrypted service table file for authenticating principals
DUMP KDB	Dumps the contents of the KDB into an ASCII text file
GET TGT	Gets the ticket-granting ticket (TGT) used to obtain Kerberos service tickets

LOAD KDB	Loads the KDB from an ASCII text file
MODIFY KDB	Modifies an entry in the KDB
MODIFY KERBEROS USER	Used by the Kerberos administrator to remotely modify a Kerberos user's password
REMOVE KACL	Removes a Kerberos ACL for gaining access to the KDB
REMOVE KDB	Removes an entry from the KDB
REMOVE TICKETS	Removes outstanding tickets from the KERBV4.TICKET file
SET [NO]FILTER	Loads the specified address filter file and associates the filter list with the specified line, or removes a previously associated filter list from specified line
SET IPS	Starts/stops the Intrusion Protection System (IPS), or sets the debug level for IPS reporting.
SET [NO]IPSO	Enables (or disables) processing of IPSO labels (levels and protection authorities) for specific lines (ports or network interfaces) or for system processing
SET KERBEROS_PASS	Remotely changes a Kerberos user password
SET MASTER_PASS	Changes the KDB master password
SET [NO]OUTGOING	Loads (or removes) an outgoing access restrictions file
SHOW FILTER	Displays the current address filter list for specified line
SHOW IPS	Write the IPS configuration and status to a file.
SHOW IPSO	Displays IPSO information on datagrams
SHOW KACL	Shows the Kerberos ACL entries for access to the ID
SHOW KDB	Shows entries in the KDB
SHOW KERBEROS USER	Used by Kerberos administrator to remotely show users added to the KDB
SHOW OUTGOING	Shows all outgoing access restrictions

SHOW TICKETS	Displays a list of active user tickets in the KERBV4.TICKET file
STASH MASTER_PASS	Stashes the master password in a protected file

Miscellaneous Commands

NETCU supports the miscellaneous commands listed in Table 1-12.

Table 1-12 Miscellaneous NETCU Commands

Command	**Purpose**
ADD SECONDARY	Adds a secondary address, such as to implement cluster alias failover
REMOVE SECONDARY	Removes a secondary address
DEFINE/KEY	Associates an equivalence string and a set of attributes with a key on the keyboard
EXIT	Exits from NETCU and returns to DCL
HELP	Displays NETCU online help
SET DOMAINNAME	Sets the local host’s domain name
SET/SHOW INTERFACE	Sets (shows) interface related parameters and options
SET *[*NO*]*LOG	Starts (or stops) NETCP logging
SET PASSWORD	Sets the TCPware software password for your system
SHOW SNMP	Display the SNMP counters maintained by the local host
SHOW TIMEZONE	Displays the local time zone
SHOW VERSION	Displays the current version of TCPware for OpenVMS
SPAWN	Executes DCL commands without exiting from NETCU

For details on configuring electronic mail, refer to the *Management Guide*.

MAIL-CONFIG Command Summary

Table 1-13 lists the commands you can run from the MAIL-CONFIG prompt.

The DCL command `$ TCPWARE CONFIGURE/MAIL` brings up the MAIL-CONFIG prompt.

Table 1-13 MAIL-CONFIG Command Summary

MAIL-CONFIG Command	Description
ADD GATEWAY	Adds a mail gateway to another domain.
ADD LOCAL-DOMAIN	Adds a domain to a list of domains that the TCPware SMTP symbiont considers to be local. If users send mail to hosts beyond the local domains, TCPware forwards the mail to the mail hub specified by the FORWARDER parameter. The local domain list affects mail forwarding only when the FORWARD-REMOTE-MAIL parameter is TRUE.
ADD QUEUE-GROUP	Forms a mail queue grouping of nodes in a cluster, or adds new nodes to an existing queue group.
ATTACH	Attaches your terminal to another process.
CLEAR	Erases all information from the current configuration; same as ERASE.
DELETE GATEWAY	Deletes a mail gateway.
DELETE LOCAL-DOMAIN	Deletes a domain from TCPware's list of local domains.
DELETE QUEUE-GROUP	Deletes a queue group or removes a node from a queue group. When a node is removed from a named queue group, it becomes part of the default queue group.
ERASE	Erases all information from the current configuration; same as CLEAR.
EXIT	Saves the configuration file and exits from MAIL-CONFIG.
GET	Reads in a TCPware SMTP configuration file. (Functionally equivalent to USE.)
HELP	Invokes MAIL-CONFIG command help.

PUSH	Accesses the DCL command interpreter.
QUIT	Prompts you to save the configuration file if it has been modified, then exits MAIL-CONFIG.
REMOVE GATEWAY	Functionally equivalent to DELETE GATEWAY.
REMOVE QUEUE-GROUP	Functionally equivalent to DELETE QUEUE-GROUP.
SAVE	Saves the current configuration file.
SET ALIAS-FILE	Identifies the file that holds mail aliases.
SET DECNET-DOMAIN	Sets the domain name for DECnet mail.
SET DELIVERY-RECEIPTS	Specifies whether mail receipts are sent when incoming mail containing Delivery-Receipt-To: or Return-Receipt-To: headers is submitted to the SMTP queue.
SET DISABLE-PSIMAIL	When TRUE, the TCPware SMTP symbiont looks for messages addressed through PSImail, usually of the form PSI%address::user, and returns them to the sender marked user unknown.
SET DISALLOW-USER-REPLY-TO	When set to TRUE, prevents VMS MAIL users from setting a Reply-To: header address with the logical name TCPWARE_SMTP_REPLY_TO.
SET FORWARDER	Specifies the host that will forward mail messages to other hosts.
SET FORWARD-LOCAL-MAIL	Forwards mail addressed to users on the local host to a central mail hub specified by the FORWARDER parameter.
SET FORWARD-REMOTE-MAIL	Forwards mail addressed to users on non-local hosts to a central mail hub specified by the FORWARDER parameter.
SET HEADER-CONTROL	Specifies which RFC-822 message headers should be included in messages delivered to local VMS MAIL users.

SET HOST-ALIAS-FILE	Specifies a file from which TCPware obtains a list of host aliases.
SET LOCAL-MAIL-FORWARDER	Forwards local mail to a specific host.
SET POSTMASTER	Identifies the user responsible for mail on the system.
SET QUEUE-COUNT	Specifies the number of mail processing queues that should be created on a particular system.
SET REPLY-CONTROL	Specifies how Internet mail headers should be mapped to the VMS MAIL "From" header.
SET RESENT-HEADERS	When FALSE, the TCPware SMTP symbiont omits the Resent-From, Resent-To, and Resent-Date headers that are usually included when a message is forwarded using a VMS MAIL forwarding address.
SET RETRY-INTERVAL	Specifies the amount of time that elapses before another attempt is made to send a message after a failed attempt.
SET RETURN-INTERVAL	Specifies the amount of time that a message can remain in the processing queue before it is returned to sender.
SET SEND-BROADCAST-CLASS	Specifies the broadcast class to use to deliver immediate SEND messages.
SET SMTP-HOST-NAMES	Sets the host name from which all outgoing mail appears to be sent and aliases for which this host accepts incoming mail.
SET START-QUEUE-MANAGER	Determines whether START_SMTP.COM starts the VMS queue manager if it is not already running.
SHOW	Displays the current configuration.
SPAWN	Executes a single DCL command.
STATUS	Indicates whether the SMTP configuration has been modified.
USE	Reads in a non-standard configuration file.

VERSION	Displays the MAIL-CONFIG version and release information.
WRITE	Saves the current configuration file.

Creating Output Files

You can send output to a file for the DEBUG command and any SHOW command except SHOW EXPORT, SHOW GROUP, SHOW MOUNT, SHOW PROXY, and SHOW STATISTICS. Enter the /OUTPUT=*filespec* qualifier after the command. For example, the following command sends all output for the SHOW CONNECTIONS command to the file MYFILE.TXT:

```
SHOW CONNECTIONS/OUTPUT=MYFILE.TXT
```

Exiting NETCU

To exit NETCU, use the EXIT command or type `Ctrl/Z`. NETCU exits with the last error status, if any. DCL command procedures can use the $STATUS and $SEVERITY symbols to test for success or failure of the NETCU commands issued. A success status indicates that all commands succeeded. A warning, error, or severe status indicates that one or more commands failed to execute, either because of syntax errors or because of operational problems.

When possible, the status code is a System Service (defined in $SSDEF), RMS (defined in $RMSDEF), or shared (defined in $SHRDEF) status. In some cases, status codes are TCPware private codes with a facility number of 1577.

Command Reference

Each NETCU command is described in detail in the next chapter, NETCU Commands. The command descriptions include the command:

- Purpose, and any suggestions or restrictions that may apply
- Format
- Parameters (if any)
- Qualifiers (if any)
- Examples (when possible)

Troubleshooting NETCU

This section describes:

- Error messages that NETCU and NETCP can display at startup time
- NETCP error messages that OPCOM displays
- The NETCP.LOG file

NETCU and NETCP Startup Messages

This section lists messages that NETCU and NETCP may issue when you start-up the network.

```
%TCPWARE_NETCU-E-LPCNF, error configuring line port
-SYSTEM-F-BADPARAM, bad parameter
```

Meaning: Software other than TCPware might be using a TCP/IP protocol or your system might be running LAT without DECnet.

Action: Be sure TCPware is the only software using the TCP/IP protocols. If LAT is running without DECnet, perform one of the following steps:

- Start TCPware before starting LAT.

```
%TCPWARE_NETCU-E-LPSTART, error starting line port
-SYSTEM-F-IVADDR, invalid media address
```

Meaning: Two local lines have the same internet address.

Action: Be sure the internet addresses for all lines are valid, and that no duplicates exist. No two lines can use the same network (or subnet) number. Check the host for a bad SLIP line definition or ask if the host has two Ethernet interface cards. If there are two Ethernet cards, they cannot have the same network number, for example, 192.15.10.1 and 192.15.20.1.

NETCP OPCOM Messages

OPCOM messages inform you when a major event occurs on the network. Some messages are informational (such as when an Ethernet line is being restarted after a fatal error), while others alert you to a problem (such as when an error occurs in trying to restart a port).

NETCP sends a message to OPCOM when a network event occurs. OPCOM formats the messages and adds some information (such as a timestamp). It then displays the messages on the operator's console and writes them to the SYS$MANAGER: OPERATOR.LOG file. OPCOM messages should rarely occur.

All messages from NETCP OPCOM have the following prefix:

```
Status report from TCPware(R) for OpenVMS NETCP:
```

Most Important OPCOM Messages

The following are the most important NETCP OPCOM messages.

Line *line-id* restarted after fatal error

Meaning: The network controller reported a fatal error. The line was restarting automatically.

Action: Investigate the controller error, especially if it occurs repeatedly.

Error restarting line *line-id* (prot-id protocol) after fatal error

Meaning: The network controller reported a fatal error and TCPware could not recover from the error. An accompanying message displays the error reported by the controller during the restart attempt. After some failures, TCPware may periodically try to restart the controller. The prot-id value is IP, ARP, RARP, LTP (long trailer packets), or STP (short trailer packets).

Action: Investigate the controller error.

OPCOM Message for Interfaces

CAUTION! Maximum receive packet rate exceeded on line line-id (rate packets/second).

Meaning: The interface specified by line-id received more packets than were allowed. This may indicate that either the receive packet rate limit is too low or that a flood of packets were sent to the system and a network problem exists that should be corrected.

Action: If the limit is too low, raise it using SET INTERFACE /RECEIVE_LIMIT. If a network problem exists, investigate it and correct it.

OPCOM Messages for IP-over-DECnet Lines

OPCOM may display the following messages for IP-over-DECnet lines.

DECnet link lost on line *line-id*

Meaning: The communication path between systems is lost. Some possible causes can be that a modem line is down, a cable has been unplugged, or the peer system is shut down.

Action: If the problem persists, investigate the cause for the lost line.

DECnet line *line-id* reconnected to peer

Meaning: The lost line was reconnected. Network operation is back to normal.

MTU for line *line-id* too small, ignoring packets larger than mtu bytes

Meaning: The peer end of the IP over DECnet line is sending datagrams that are larger than TCPware can handle.

Action: Increase the maximum transmission unit (MTU) for the IP-over-DECnet line at the receiving host, or lower it at the sending host. You can reset the MTUs for the receiving host by using the NETCU START/IP command or by reconfiguring the network.

Shutting down line *line-id* after receiving fatal error

Meaning: A fatal error was detected. This message is usually accompanied by another OpenVMS message which specifies the exact error.

Action: See your OpenVMS documentation.

NETCP.LOG File

The TCPWARE:NETCP.LOG file logs each NETCP master server connection. You can use this file to obtain details on server errors, and to monitor access and security violations.

The NETCP.LOG file shows:

- When the connection was established
- Which protocol is servicing the connection
- The internet addresses of both hosts
- The name of the server process created

Before you examine the NETCP.LOG file, issue the NETCU SHOW SERVICES command. This command writes the current server information to the NETCP.LOG file.

NETCP.LOG File shows part of a sample NETCP.LOG file.

Example 1-1 NETCP.LOG File

```
TCPware(R) for OpenVMS  NETCP  Copyright (c) Process Software
** 1-JAN-2014 09:24:18 NETCP Master Server started.
```

Chapter 2 NETCU Commands

This chapter contains a detailed description of each NETCU command. The commands are in alphabetical order.

The commands are summarized by category in Chapter 1. That chapter also describes how to run NETCU and how to send NETCU output to a file.

The descriptions include the command:

- Purpose and any suggestions or restrictions that apply
- Format
- Parameters (if any)
- Qualifiers (if any)
- Examples, when possible

ADD ACCESS_LIST

Controls incoming access restrictions for a remote host. Incoming access restrictions affect only TCP connections for servers the master server process starts. Requires OPER privilege.

Define a service using the ADD SERVICE or MODIFY SERVICE command with the /ACCESS_LIST qualifier that points to the appropriate list number. The access list should be defined in SERVERS.COM.

Format

ADD ACCESS_LIST *list condition ia [mask]*

Parameters

list

Number of the incoming access restrictions list (1 to 65535).

condition

Condition of permitting or denying access. Valid keywords are PERMIT and DENY.

Any host you enter on the PERMIT list can access services. TCPware denies services to all other hosts. Use the DENY parameter when:

- You grant a network or group of hosts access to services, and
- You want to deny one or more hosts within the network or group from access to services

TCPware places (and honors) DENY entries before PERMIT entries except when there are duplicate host or network entries with a PERMIT that has a more restrictive mask, in which case the PERMIT entry comes first.

ia

Internet address of the network or host you enter on the list.

mask

Internet address mask. Specifies which bits are used when matching hosts against the incoming access list. TCPware uses the bits set when matching hosts against the ia. If you omit mask and the host portion of the ia is 0, TCPware uses the network or subnet mask. If the host portion is not 0, TCPware uses 255.255.255.255, where it matches the entire Internet address against *ia*.

Qualifier

/MESSAGE=*”text”*

Text message sent over the connection when TCPware denies access. Place the text in quotation marks (" "). Define one message for each incoming access list. If a message previously exists, the new text replaces it.

The message you define affects all hosts to which the specified list denies access. If omitted, TCPware closes the connection if the list denies the host access.

Table 2-1 lists special characters you can use that have special meaning in the message.

Table 2-1 Special Characters

Use this character...	In place of this character...
\\	\

\r	carriage return
\n	line feed
\t	tab
\0	NULL

Examples

1 Denies host 192.168.95.6 access to the server associated with list 56. Any host denied access by list 56 receives the message

```
550 You are not authorized to have access to this host
```

followed by a line feed and carriage return.

```
ADD ACCESS_LIST 56 DENY 192.168.95.6 /MESSAGE="550 You are not authorized to gain
access to this host.\n\r"
```

2 Permits hosts on network 192.168.95.0 access to the server associated with list 56.

```
ADD ACCESS_LIST 56 PERMIT 192.168.95.0
```

3 Permits all hosts on network 172.16 access to the server associated with list 1203.

```
ADD ACCESS_LIST 1203 PERMIT 172.16.0.0 255.255.0.0
```

ADD ACE_USER

Token Authentication only.

Adds a username to the TCPware ACE/Client user database (the TCPWARE:ACECLIENT_USER.DAT file). The ACE/Client authenticates the user if there is an entry in the database. You can only add one username with each command. Requires SYSPRV or BYPASS privilege.

To show the usernames added, use the SHOW ACE_USER command. To remove a username, use the REMOVE ACE_USER command. To create a new database and preserve the existing one under a new name, use the CREATE ACE_USER_DATABASE command.

Format

ADD ACE_USER *username*

Parameter

username

Name of the user to add to the ACE/Client database.

Example

Shows a sequence of adding new users to the TCPware ACE/Client user database and showing the results, showing the database file created, removing a user and showing the results, and creating a new database.

```
NETCU>ADD ACE_USER DIAMONDS
NETCU>ADD ACE_USER HEARTS
NETCU>ADD ACE_USER CLUBS
NETCU>ADD ACE_USER SPADES
NETCU>SHOW ACE_USER
TCPware ACE/Client Username Database

Username

CLUBS
DIAMONDS
HEARTS
SPADES

NETCU>ADD ACE_USER JOKER
NETCU>SHOW ACE_USER
TCPware ACE/Client Username Database

Username

CLUBS
DIAMONDS
HEARTS
JOKER
SPADES

NETCU>SPAWN DIR ACECLIENT_USER*

Directory SYS$COMMON:[TCPWARE] ACECLIENT_USER.DAT;1

NETCU>REMOVE ACE_USER JOKER
NETCU>SHOW ACE_USER
```

```
TCPware ACE/Client Username Database

Username

CLUBS
DIAMONDS
HEARTS
SPADES

NETCU>CREATE ACE_USER_DATABASE
NETCU>SPAWN DIR ACECLIENT_USER*

Directory SYS$COMMON:[TCPWARE]

ACECLIENT_USER.DAT;1      ACECLIENT_USER_OLD.DAT;1
```

ADD ARP

Adds an entry to an Address Resolution Protocol (ARP) table. Each ARP table entry consists of an internet address paired with a physical address. Requires OPER privilege.

Note! You do not need to use this command under normal circumstances. ARP maps internet addresses to physical addresses automatically. Use this command in rare instances when a particular host does not support ARP.

Format

ADD ARP *destination-ia physical-address*

Synonym

SET ARP *destination-ia physical-address*

Parameters

destination-ia

Internet address or host name of the ARP table entry.

physical-address

Ethernet, FDDI, or HYPERchannel address of the host specified by the *destination-ia*.

The standard physical address is in the format aa-bb-cc-dd-ee-ff, where for HYPERchannel physical addresses:

aa	is the global network address domain
bb	is the global network address network
cc	is the physical unit
dd	is the logical unit
ee	is the trunks-to-try mask
ff	is the flags mask

If *ee-ff* is 00-00, the value becomes FF-00.

If you do not specify an ARP server address when configuring the HYPERchannel line (HYP-n) and use the ADD ARP command to populate the ARP Table, a TCPware host can act as an ARP server. A TCPware host responds to ARP requests it receives for addresses in the ARP table that you add using the /PUBLISH qualifier.

Qualifiers

/LINE=*line*

Line id of the ARP table where you want NETCU to place the entry. When not specified, NETCU determines the ARP table on the basis of the internet address.

You must specify the /LINE qualifier when the internet address is not a local address.

/LOCK

Prevents ARP messages from changing the value of the physical address.

/PERMANENT

Makes the entry permanent in the ARP table. Without /PERMANENT, the entry may disappear from the ARP table if:

- The host does not receive a datagram within 10 minutes that has the destination-internet-address/ physical-address pair
- The ARP table is full and the entry is the oldest entry in the table

If you enable Reverse Address Resolution Protocol (RARP) support for an Ethernet or FDDI line, TCPware only responds to RARP requests for entries marked /PERMANENT.

/PUBLISH

The local host responds to ARP requests for the specified internet address.

Example

Places an entry in the ARP table for line QNA-0 (/LINE=QNA-0) that defines the Ethernet address for host ALPHA. This entry is permanent (/PERMANENT).

```
ADD ARP ALPHA AA-02-04-06-08-10/PERMANENT/LINE=QNA-0
```

ADD EXPORT

NFS Server only.

Adds an entry to the EXPORT database that lets the NFS server export the server filesystems to a remote NFS client. Users at the NFS-Client can then mount the server filesystems. Requires write access to the TCPWARE:NFS_EXPORT.DAT file. The EXPORT database is dynamic. Entries you add to the database become valid immediately. You do not need to restart the server.

If you are adding entries to the EXPORT database for the first time, read the EXPORT Database section in Chapter 14 of the *TCPware for OpenVMS Management Guide*.

Format

ADD EXPORT *"nfs-path" vms-directory*

Parameters

"nfs-path"

NFS-style pathname used to reference the exported directory. Typically expressed as a UNIX-style pathname. Enclose in quotation marks (" ").

Although nfs-path can be arbitrary, it usually reflects the actual OpenVMS directory path. The NFS client user must refer to the same nfs-path in naming the mount point.

vms-directory

Directory on the local OpenVMS server that you want to export. The directory must include the device specification, as in the following example:

```
$DISK1:[SALES.RECORDS]
```

When you export a directory, the NFS client user can potentially have access to all files and directories below the export point. The device you export should be a "public" device. The Server does not implement volume protection. Also, the Server only supports Files-11 ODS-2 structure level disks.

Qualifiers

Note! Many of the following qualifiers are specific to applications running on certain hosts. In these cases, it is critical to use the /HOST qualifier in combination with these qualifiers.

/HOST=*(host[,host...])*

Only specified host(s) can have access to the exported OpenVMS directory. NETCU allows either host names or internet addresses. Use the parentheses only if you specify a list of hosts (separated by commas). If you omit /HOST, any host can mount the exported directory.

/CONVERT={STREAM_LF (default) **| STREAM_CRLF**}
/NOCONVERT (for use with TCPware's NFS Client)

/CONVERT converts files on reads to either STREAM_LF (the default) for UNIX systems or STREAM_CRLF for PC systems.
/NOCONVERT disables this conversion and must be specified when using the Server together with TCPware's NFS-OpenVMS Client.

/EXPLICIT_MOUNT
/NOEXPLICIT_MOUNT (default)

/EXPLICIT_MOUNT prevents users from subsequently mounting subdirectories of the mount point.
/NOEXPLICIT_MOUNT allows subdirectory mounts.

/FILENAME={ SRI (default) **| ODS5 | PATHWORKS | PATHWORKS_CASE }**

Uses the SRI International, or ODS5, or PATHWORKS filename mapping schemes.
SRI is the default scheme between UNIX and OpenVMS systems.
ODS5 uses minimal mapping to get around ODS-5 file naming restrictions. If the disk or system doesn't support ODS-5, it falls through to SRI.
PATHWORKS specifies non-case-sensitive filename mapping.
PATHWORKS_CASE specifies case-sensitive filename mapping.

/HIGHEST_VERSION
/NOHIGHEST_VERSION (default)

/HIGHEST_VERSION returns only the highest version of files in directory requests.
/NOHIGHEST_VERSION does not. All file versions still exist in either case.

/PRIVILEGED_PORT
/NOPRIVILEGED_PORT (default)

/PRIVILEGED_PORT requests that incoming requests originate from privileged ports only.
/NOPRIVILEGED_PORT does not.

/PROXY_CHECK
/NOPROXY_CHECK (default)

/PROXY_CHECK specifies that mount requests only originate from users having mappings in the PROXY database.
/NOPROXY_CHECK does not.

/RFM=*option*

Record format (RFM) of newly created files. The options are **STREAMLF, STREAMCR, STREAM, FIXED,** and **UNDEFINED**.

/SERVER_ACCESS
/NOSERVER_ACCESS (default)

/SERVER_ACCESS requests the server to do access checking.
/NOSERVER_ACCESS requests that both the server and client do the checking.

/SUPERUSER_MOUNT
/NOSUPERUSER_MOUNT (default)

/SUPERUSER_MOUNT requests that only the superuser can mount a file system. /NOSUPERUSER_MOUNT does not.

/VERSION={ DOT | SEMICOLON (default) **| ALL | HIGHEST }**

DOT changes the file version display for exported filesystems to *file.ext.version* (a dot) for UNIX compatibility instead of the usual *file.extension****;****version* (a semicolon).
SEMICOLON (default) uses the regular semicolon.
ALL exports files with version numbers intact rather than the default of leaving the highest numbered version unnumbered.
HIGHEST is a synonym for /HIGHEST_VERSION. Do not use DOT with SEMICOLON.

/WRITE (default)
/NOWRITE

/WRITE requests that the client have read-write access to the filesystem.
/NOWRITE requests that the client have read access only.

Example

Exports the directory SALES.RECORDS on device $DISK1: as path /vax/records to hosts ORCHID and ROSE. Any subdirectories below SALES.RECORDS are also accessible. However, hosts ORCHID and ROSE cannot have access to or mount directories above SALES.RECORDS or other SALES subdirectories.

```
ADD EXPORT “/vax/records” $DISK1:[SALES.RECORDS] /HOST=(ORCHID,ROSE)
```

ADD GROUP

NFS Client only.

Adds an entry to the GROUP database that associates an OpenVMS user with an NFS group or list of groups. Requires SYSPRV privilege and write access to the TCPWARE:GROUP.DAT file.

If the GROUP database does not exist, use the CREATE GROUP command first to create an empty one. Use the REMOVE GROUP command to remove a group from the database.

Note! The GROUP database is static. Use the REL command when you modify it.

Format

ADD GROUP *nfs-group vms-identifier*

Parameters

nfs-group

NFS group number found in the /etc/group file on the server. For example, if the users group appears in the /etc/group file as:

```
users:x:15:
```

use 15 as the *nfs-group*.

vms-identifier

Associates either an OpenVMS rights identifier or UIC (or wildcarded UIC) with the NFS group. Only associate one vms-identifier per NFS group. Use either of the following formats to enter the value:

Format	**Description**
"Name"	OpenVMS rights identifier or username
"Value"	UIC value in [group,member] or %Xnnnnnnnn format; you can use wildcard entries such as [200,*].

"Name" and "value" correspond to the columns associated with entries in the OpenVMS rights database. To have access to this database, use the commands:

```
$ SET DEFAULT SYS$SYSTEM
$ RUN AUTHORIZE
UAF>SHOW/IDENTIFIER *
```

For example, the following line may appear in the rights database:

```
Name          Value                 Attributes
-----         -----                 ----------
USER        [000200,000200]
```

Qualifier

/HOST=(host[,host...])

Server host(s) on which the group identification is valid. If omitted, any remote host is valid for the group. /HOST accepts either host names or internet addresses. Use the parentheses with multiple host entries.

Examples

1 Associates NFS group number 15 on server host IRIS with the "value" [200,*], meaning "any user in group 200."

```
ADD GROUP /HOST=IRIS
_Group: 15
_Identifier: [200,*]
```

The *nfs-group* number derives from the entry in the /etc/group file on the server for the users group:

```
>cat /etc/group
staff:*:10:
users:*:15:
```

2 Associates NFS group number 15 with the OpenVMS rights identifier, USERS. As in Example 1, the *nfs-group* number derives from the entry in the /etc/group file on the server. Assuming that the USERS rights identifier exists in the rights database, any user granted this identifier would be in the group corresponding to GID 15 in NFS.

```
ADD GROUP 15 USERS
```

The resulting ADD GROUP entry would appear in the GROUP database as follows:

```
NFS GROUP Database V5.8 Copyright (c) Process Software
Group  Name     Value        Host(s)
-----  ----     -----        ------
15     USERS    %X8001000C
```

ADD KACL

Used by the Kerberos master administrator. Adds a Kerberos access control list (KACL) entry for access from a remote host to the Kerberos database using the Kerberos Administration Server. This ACL entry allows the Kerberos administrator to add (using ADD KERBEROS USER), modify (using MODIFY KERBEROS USER), or view (using SHOW KERBEROS USER) users' entries in the Kerberos database.

This command may only be executed if the local host is configured as a Kerberos Server. Requires OPER or SYSPRV privilege and entry of the Kerberos master password.

Format

ADD KACL *access-type admin-username instance [realm]*

Enter Kerberos master password: **master-password**
Verifying, please re-enter: **master-password**

Parameters

access-type

One of the following ACL access types:

Access type	**Description**
ADD	Kerberos administrator can add to the Kerberos database from a remote host (TCPware adds the username to the TCPWARE:ADMIN_ACL.ADD file)
MODIFY	Kerberos administrator can modify the Kerberos database from a remote host (TCPware adds the username to the TCPWARE:ADMIN_ACL.MOD file)
SHOW	Kerberos administrator can show entries in the Kerberos database from a remote host (TCPware adds the username to the TCPWARE:ADMIN_ACL.GET file)

admin-username

Kerberos administrator's username to add to the Kerberos database. Converted to lowercase unless you enclose it in quotes. The Kerberos administrator entered must also have an administrator's entry in the Kerberos database (see ADD KDB for details).

instance

Value should be **admin** since the username is for a Kerberos administration user.

realm

Alternate Kerberos realm to use instead of the TCPWARE_KERBV4_REALM logical value. Converted to lowercase unless you enclose it in double quotes.

master-password

Kerberos password used for access to the Kerberos database. Converted to lowercase unless you enclose it in double quotes.

Qualifiers

/PROMPT (default)
/NOPROMPT

Specifies whether the system should prompt you for the master password. /NOPROMPT reads the master password from the file created by STASH MASTER_PASSWORD.

Examples

The three commands combined add KACLs for administrator account persephone to add, modify, and show entries, respectively, in the Kerberos database. The last command (with /NOPROMPT) does not prompt for the master password but rather causes it to be read from the file created by STASH MASTER_PASSWORD.

```
ADD KACL ADD PERSEPHONE ADMIN HADES.COM
Enter Kerberos master password:
Verifying, please re-enter:
ADD KACL MODIFY PERSEPHONE ADMIN HADES.COM
Enter Kerberos master password:
Verifying, please re-enter:
ADD KACL SHOW PERSEPHONE ADMIN HADES.COM /NOPROMPT
```

ADD KDB

Used by the Kerberos master administrator. Adds an entry to the Kerberos database after the database was created (using CREATE KDB) and the master password stashed (using STASH MASTER_PASSWORD).

This command can only be executed if the local host is configured as a Kerberos Server. Requires OPER or SYSPRV privilege and entry of the Kerberos master password.

Format

ADD KDB *principal password [instance]*

Enter Kerberos master password: ***master-password***
Verifying, please re-enter: ***master-password***

Parameters

principal

Kerberos user's login name, or name of the Kerberos application service provided. Converted to lowercase unless you enclose it in double quotes.

password

Kerberos user's, administrator's, or application service's password. Specify **"NULL"** for a null password (not recommended, but allowed), or **"RANDOM"** to have a randomly generated password selected (recommended only for application services, not users or administrators). Converted to lowercase unless you enclose it in double quotes.

instance

Usually omitted for a general Kerberos user; **admin** for an administrative user; or name of the machine on which the Kerberos application resides for an application service. Converted to lowercase unless you enclose it in double quotes.

master-password

Kerberos password used for access to the Kerberos database. Converted to lowercase unless you enclose it in double quotes. Use the /NOPROMPT qualifier if you do not want to be prompted for the password and want it read from TCPWARE:KSTASH.KEY file instead.

Qualifiers

/ATTRIBUTE=*attribute*

Attribute number from 0 to 65535. The default is 0.

/EXP_DATE=*date*

Expiration date of the KDB entry. The default is 31-DEC-2099 23:59.

/KDBFILE=*file*

Name of the KDB file. The default is TCPWARE:PRINCIPAL.OK.

/MAX_LIFE=*minutes*

Maximum lifetime of the KDB entry, in minutes. The default is 255 minutes.

/PROMPT (default)
/NOPROMPT

Specifies whether TCPware prompts you for the master password.
/NOPROMPT reads the master password from the file created by the STASH MASTER_PASSWORD command.

Example

1 Creates an entry for username hermes, which has the Kerberos password herald. This entry will be used to grant username hermes a ticket-granting ticket from any remote host.

```
ADD KDB HERMES HERALD
Enter Kerberos master password:
Verifying, please re-enter:
```

2 Creates an entry for username zeus, who has a Kerberos password of olympus. This entry only grants username zeus a ticket-granting ticket from remote host athens (zeus must be on athens to get a **TGT**).

```
ADD KDB ZEUS OLYMPUS ATHENS
Enter Kerberos master password:
Verifying, please re-enter:
```

3 Creates an entry for the Berkeley R services on remote host bart. The "rcmd" is the name of the Kerberos application service provided on remote host bart.

```
ADD KDB “rcmd” “RANDOM” BART
Enter Kerberos master password:
Verifying, please re-enter:
```

4 Creates a Kerberos Administrator account for principal persephone, which has the Kerberos Administrator password spring, and an instance of admin. In this case, admin does not indicate the name of the machine from which persephone can access the Kerberos database; rather, it indicates that persephone is a Kerberos Administrator who can access the database from any remote host.

```
ADD KDB PERSEPHONE SPRING ADMIN
Enter Kerberos master password:
Verifying, please re-enter:
```

ADD KERBEROS USER

For Kerberos client administrators. Adds a user to the Kerberos Server database. The default Kerberos administrator account name is the name of the OpenVMS account using this command. Requires OPER or SYSPRV privilege and entry of the Kerberos administrator’s password.

Format

ADD KERBEROS USER *username user-password*

Administrator password for *admin-account:**admin-password***

Parameters

username

Kerberos user’s login name. Converted to lowercase unless you enclose it in quotes.

user-password

Kerberos user’s password. Converted to lowercase unless you enclose it in quotes.

admin-password

Kerberos administrator’s password. Converted to lowercase unless you enclose it in quotes.

Qualifier

/ADMINISTRATOR=*admin-username*

Alternate Kerberos administrator name. Converted to lowercase unless you enclose it in quotes. The default is the current OpenVMS account name, in lowercase.

Example

Adds a new Kerberos user, achilles, to the Kerberos database. The password for user achilles is running.

```
ADD KERBEROS USER ACHILLES RUNNING /ADMIN=PERSEPHONE
Administrator password for ‘persephone’:
```

ADD MULTICAST_GROUP

Adds a multicast host group address to the table of joined addresses for the interface or all interfaces. Once you add a multicast group address to an interface, applications can receive datagrams sent to that address. Requires OPER privilege.

Format

ADD MULTICAST_GROUP *internet-address*

Parameter

internet-address

Internet address or host name of the multicast host group address.

Qualifier

/LINE=*line-id*

Line ID of the interface on which to add the address. If omitted, TCPware adds the address to all active interfaces.

Example

Adds the all-routers multicast address (224.0.0.2) to all active interfaces. Once added, applications receive datagrams sent to the multicast address.

```
ADD MULTICAST_GROUP 224.0.0.2
```

ADD PROXY

NFS Client and NFS Server.

Registers an NFS or remote user as an OpenVMS username in the PROXY database. Requires SYSPRV privilege and write access to the TCPWARE:NFS_PROXY.DAT file.

Note! If you omit the /CLIENT or /SERVER qualifier, or do not define the TCPWARE_NFS_DYNAMIC_PROXY logical accordingly, you must use the RELOAD PROXY command to reload the database. (For details, see *Reloading the PROXY Database* in Chapter 14 of the *TCPware for OpenVMS Management Guide*.)

Format

ADD PROXY *vms-username*

Parameter

vms-username *(required)*

OpenVMS username to which you want to map an NFS userid. The username must appear as in the OpenVMS User Access File (SYSUAF.DAT).

Qualifiers

The /HOST, /UID, /GID, or /NFS qualifiers make the PROXY entry more restrictive. When you omit a qualifier, NFS-OpenVMS interprets it as a wildcard. For example, the command ADD PROXY SMITH/UID=210 creates an entry that lets a user with UID=210, but with any GID and from any host, use OpenVMS username SMITH.

/HOST=*(host[,host...])*

Host(s) from which the UID/GID identification is valid. Specify at least one host name. If omitted, NETCU allows any remote host with the matching identification.

/HOST accepts either host names or internet addresses. Use parentheses for multiple hosts.

/UID=*uid*

User's ID (UID). If omitted, NETCU accepts any UID for the *vms-username*.

/GID=*gid*

User's group ID (GID). If omitted, NETCU accepts any GID for the *vms-username*.

/CLIENT
/NOCLIENT (default)

/CLIENT notifies the Client to immediately update its loaded PROXY database with an entry for *vms username*.
/NOCLIENT does not notify the Client. This overrides any default action specified using the TCPWARE_NFS_DYNAMIC_PROXY logical.

/SERVER
/NOSERVER (default)

/SERVER notifies the Server to immediately update its loaded PROXY database with an entry for *vms-username*.
/NOSERVER does not notify the Server. This overrides any default action specified using the TCPWARE_NFS_DYNAMIC_PROXY logical.

Examples

The following examples range from most restrictive to least restrictive:

1 Registers a user with UID=210 and GID=5 at host ROSE to OpenVMS username SMITH for the NFS Server only.

```
ADD PROXY SMITH /UID=210 /GID=5 /HOST=ROSE /SERVER
```

2 Registers a user with UID=210 and GID=5 to OpenVMS username SMITH and dynamically reloads the PROXY database on both the Client and Server.

```
ADD PROXY SMITH /UID=210 /GID=5 /CLIENT /SERVER
```

3 Registers any user with GID=5, any UID, and at any host to OpenVMS username JONES.

```
ADD PROXY JONES /GID=5
```

4 Registers any user from host ORCHID to OpenVMS username JONES.

```
ADD PROXY JONES /HOST=ORCHID
```

ADD ROUTE

Adds an entry to the routing table. Requires OPER privilege. (See also REMOVE ROUTE.)

Format

ADD ROUTE *destination-ia {line | gateway-ia}*

Synonym

SET ROUTE *destination-ia {line | gateway-ia}*

Parameters

destination-ia

Internet address or host name of the destination host or network. Specify 0.0.0.0 to add a default gateway or use the SET GATEWAY command.

line *(default)*

Line ID of the direct route interface. If you specify a value for *line*, you cannot specify a *gateway-ia*.

gateway-ia

Internet address or host name of the gateway for the host or network (see the /GATEWAY qualifier below).

Qualifiers

/GATEWAY

Datagrams sent to the gateway. Do not use if specifying a line ID. If omitted, TCPware sends the datagrams to the destination IP address over the interface specified by *line*.

{/HOST | /NETWORK}

Use either one of these qualifiers to specify the type of route.

/HOST creates a host route for the host *destination-ia* identifies. /NETWORK creates a network route that leads to the network *destination-ia* identifies.

If you omit both, TCPware determines the type of route by looking at the host number part of *destination-ia*. If the host number is zero (0), TCPware assumes the route is a network route.

/LOCK

Disables ICMP redirect messages from changing the specified route.

/MASK=*mask*

Internet address mask for the Classless Inter-domain Routing (CIDR) protocol. The mask specifies the bits to use for the network portion of a mask. Thus the traditional network masks would be specified as:

Class A Network 255.0.0.0 Class B Network 255.255.0.0 Class C Network 255.255.255.0

If the mask is omitted, the destination address is derived by first checking interfaces for the same network number and, if one is found, the mask for that interface is used. Otherwise, the address is examined to determine if it is Class A, B, C, D, or E and a mask is created based on the class.

Network routes are sorted such that the routes with the most restrictive mask are searched before routes with a less restrictive mask. For example, a route with mask 255.255.255.0 is searched before a route with mask 255.255.0.0.

Do not create noncontiguous subnet masks. For example, a mask of 255.0.255.0 is not allowed.

Examples

1 Places a new route in the local host’s routing table. This route indicates that any traffic for network 172.16.10.0 (/NETWORK) must use gateway 172.16.1.5 (/GATEWAY). /LOCK indicates that an ICMP redirect message cannot modify this route.

```
ADD ROUTE 172.16.10.0 172.16.1.5/NETWORK/GATEWAY/LOCK
```

2 Adds a host route to the routing table (/HOST) and directs all datagrams for host 172.16.4.3 to gateway 172.16.1.16 (/GATEWAY).

```
ADD ROUTE 172.16.4.3 172.16.1.16/HOST/GATEWAY
```

3 Adds a route for the directly connected 172.16 network through the QNA-0 line.

```
ADD ROUTE 172.16.0.0 QNA-0
```

4 Adds a default route to gateway 172.16.0.5 (equivalent to SET GATEWAY 0.0.0.0)

```
ADD ROUTE 0.0.0.0 172.16.0.5/GATEWAY
```

ADD SECONDARY

Adds an additional internet address recognized as a local address. Requires OPER privilege

Note! It may be necessary to add a route to have the address be reachable from the system that the address is added to.

Format

ADD SECONDARY *ia*

Parameter

ia

Internet address you want recognized as a local address.

Qualifier

/CLUSTER_LOCK

Instructs the VMScluster node to take the OpenVMS cluster-wide resource lock before adding the secondary address. If another node in the VMScluster holds the lock, the node queues for the lock and adds the address when it acquires the lock.

Examples

1 192.168.95.101 becomes an additional local address for the interface address(es).

```
ADD SECONDARY 192.168.95.101
```

2 The VMScluster node queues for a resource lock on the specified address. When the node takes the lock, it adds the address as an additional local address. This node acquires the lock when no other node holds the lock or the node that holds the lock releases it (such as when you shut down TCPware or the node).

```
ADD SECONDARY 192.168.95.101 /CLUSTER_LOCK
```

ADD SERVICE

Instructs NETCP to start listening for connections on the specified port for the TCP or UDP protocol. Requires OPER privilege.

The TCPWARE:NETCP.LOG file logs each connection serviced. You can review this file for details on server errors and to monitor access and security violations.

Format

ADD SERVICE ***port protocol [image]***

Parameters

port

Name or port number the service uses. Any service name or port number (except 0) defined in the TCPWARE:SERVICES. file.

protocol

Protocol that services the connection. Table 2-2 lists the valid values.

Table 2-2 Protocol Values

Enter this value...	For...
BG_TCP	UCX-based servers on TCP
BG_UDP	UCX-based servers on UDP
TCP	TCPDRIVER-based servers
UDP	UDPDRIVER-based servers
STREAM, DGRAM	INETDRIVER-based servers

If you use the BG_TCP or BG_UDP protocol values:

- You MUST specify /USERNAME=username and /INPUT=file. The file in this case is the name of the service’s startup command file. DO NOT use the image parameter. BG_TCP and BG_UDP run images from the startup command file only.
- Use only the default create_server_process internal action routine (see the /ROUTINE qualifier).
- DO NOT use the /OUTPUT or /ERROR qualifier.

image

File specification of the server you want executed. DO NOT use with BG_TCP or BG_UDP; use the /INPUT qualifier instead.

Qualifiers

/ACCESS_LIST=*list*

Incoming access restrictions list that controls which hosts have access to the server. Access restrictions affect TCP connections only.

If you define a list using this qualifier and do not add entries to the list, no hosts have access to this server. If the list contains entries, only the specified hosts have access. If you do not define an incoming access restrictions list, all hosts have access. The list value must be a number between 1 and 65535. 0 (no list) is the default.

Use the ADD ACCESS_LIST command to define list entries, the REMOVE ACCESS_LIST command to remove list entries, and the SHOW ACCESS_LISTS command to display entries.

/ADDRESS=*ip-address*

Adds the service for the specified address or hostname only. The default is 0.0.0.0.

/BACKLOG=*number-backlogged-connections*

Number of backlogged connections allowed for listening TCP services. If omitted, the value /BACKLOG=0 is used to indicate the default connection backlog (usually 128).

/INACTIVITY_TIMER=*(TIME:minutes, CHECK_INTERVAL:minutes)*

Sets an inactivity timer to kill idle NOLISTEN server processes (see the /NOLISTEN qualifier) for the TCP protocols (not used for UDP). A process is idle if there is no CPU activity for the amount of minutes specified:

TIME:*minutes*	Idle NOLISTEN processes are terminated after this amount of time (the default is infinite)
CHECK_INTERVAL:*minutes*	Checks for idle NOLISTEN processes each of these time intervals (the default is one minute)

/LIMIT=*number-servers*

Maximum number of active servers that can reside on this host for the specified port(s). TCPware always uses /LIMIT=1 for UDP ports, regardless of what you enter. For example, to add a service on port 21 supporting one active server, use /LIMIT=1. NETCP waits for the current service to process before it listens for a new connection on the same port.

/LOG (default)
/NOLOG

/LOG starts logging of non-error events to the NETCP.LOG file. /NOLOG stops logging.

/NOLISTEN

Instructs NETCP to create the server process only when it detects a connection and not to hand off a socket or I/O channel. The default is to create the server process while listening for a connection. Use for the TCP protocols only (not for UDP).

/OPTION=*option*

Passes the process's STREAM device (INET*n*:) created using one of the following options:

Option	**Description**
NONE (default)	No special options

HANDOFF	Specifies to use a special handoff mechanism for passing the INETn: device to the created server process.
***[*NO*]*KEEPALIVE**	Specifies whether to use keep-alives for a STREAM (INET) or BG_TCP service. By default, these services are NOKEEPALIVE.
***[*NO*]*MULTITHREADE D**	Specifies whether the BG_TCP server is a multithreaded one; if so, the master server, once started, does not listen for additional connections. By default, all servers are NOMULTITHREADED.
SHARE	Specifies that TCPware set the INET device for shared access, allowing another process to assign the channel. This option is primarily for WIN/TCP servers.

TCPware ignores this qualifier if specified for non-STREAM services or services that do not use the create_server_process routine (see the /ROUTINE qualifier).

/ROUTINE=*routine-name*

NETCP internal action routine called when TCPware establishes a connection for the service. Table 2-3 lists the available routines.

Table 2-3 Internal Action Routines

Routine	**Purpose**	**Protocol**
create_rservice	Creates a Berkeley R service using NORMAL authorization checks	STREAM
create_rservice_kerberos	Creates a Berkeley R service using Kerberos authentication	STREAM
create_rservice_secure	Creates a Berkeley R service using SECURE authorization checks	STREAM
create_server_process	Creates a detached process	Any
create_telnet_session	Creates an interactive TELNET session	TCP or STREAM
ident_protocol	Starts the IDENT Server	TCP, UDP
port_mapper_server	Starts the Port Mapper	TCP, UDP
report_tclb_metric	Creates a load balancing reply service	UDP

time_protocol	Starts the Time service	Any

The default routine is create_server_process. This routine is appropriate for all user-written servers (and must be used for BG_TCP and BG_UDP protocol values).

/USERNAME=*username*

Use primarily with UCX devices (BG_TCP or BG_UDP protocol). If used with other devices, creates a detached process under the specified username.

Other Qualifiers

The following qualifiers are a subset of those the DCL RUN/DETACHED command uses. In most cases, OpenVMS provides default values for any qualifiers that you do not specify.

Always use /UIC and /PRIVILEGES to ensure that the new process has OPER privilege. All server processes should have at least TMPMBX and NETMBX privileges.

See the DCL documentation for complete details on each of the following qualifiers.

/ACCOUNTING (default)
/NOACCOUNTING

/AST_LIMIT=*quota*

/AUTHORIZE
/NOAUTHORIZE (default)

/BUFFER_LIMIT=*quota*

/DUMP
/NODUMP (default)

/ENQUEUE_LIMIT=*quota*

/ERROR=*filespec* (DO NOT use with BG_TCP or BG_UDP protocol)

/EXTENT=*quota*

/FILE_LIMIT=*quota*

/INPUT=*filespec* (Use with BG_TCP and BG_UDP protocols as the name of the service's startup command file)

/IO_BUFFERED=*quota*

/IO_DIRECT=*quota*

/JOB_TABLE_QUOTA=*quota*

/MAXIMUM_WORKING_SET=*quota*

/OUTPUT=*filespec* (DO NOT use with BG_TCP or BG_UDP protocol)

/PAGE_FILE=*quota*

/PRIORITY=*n*

/PRIVILEGES=(privilege[,...])

/PROCESS_NAME=*process-name*

/QUEUE_LIMIT=*quota*

/RESOURCE_WAIT (default)

/NORESOURCE_WAIT

/SERVICE_FAILURE
/NOSERVICE_FAILURE (default)

/SUBPROCESS_LIMIT=*quota*

/SWAPPING (default)
/NOSWAPPING

/UIC=*uic*

/WORKING_SET=*quota*

If you omit /INPUT, /OUTPUT, or /ERROR, NETCP supplies the TCP, UDP, or INET device name for the connection when it creates the process. If you use /PROCESS_NAME=*process-name*, NETCP uses up to 10 characters of the *process-name*. In addition, NETCP appends an underscore (_) and an ASCII decimal server number to the *process-name* to ensure that the *process-name* is unique.

Examples

1 Starts the DAYTIMED server for host BART only. Since the qualifiers do not specify any values, NETCU uses the OpenVMS default values.

```
ADD SERVICE DAYTIME TCP TCPWARE:DAYTIMED /ADDRESS=BART-
/PROCESS_NAME=DAYTIMED-

/NOACCOUNTING-
/NOAUTHORIZE-
/INPUT=NLA0:-
/OUTPUT=NLA0:-
/ERROR=NLA0:-
/UIC=[SYSTEM]-
/PRIVILEGES=(NOSAME,NETMBX,TMPMBX)
```

2 Starts the MYSERV service (defined in the TCPWARE:SERVICES. file) running over the BG_TCP (UCX) protocol, using the MYSERV_STARTUP.COM file, and creating a detached process under username SMITH.

```
ADD SERVICE MYSERV BG_TCP /INPUT=TK100:[MYSERV]MYSERV_STARTUP.COM
/USER=SMITH
```

CHECK GATED CONFIGURATION

Checks the syntax of a GateD configuration file. If no input file is specified, TCPware checks the default configuration file, TCPWARE:GATED.CONF. This command does not affect a running GateD process.

Format

CHECK GATED CONFIGURATION *[file]*

Parameter

file

Name of the configuration file to check. If omitted, defaults to TCPWARE:GATED.CONF.

Example

Checks the syntax of a GateD configuration file called TEST.CONF located in the user's current working directory.

```
CHECK GATED CONFIGURATION TEST.CONF
```

CREATE ACE_USER_DATABASE

Token Authentication only.

Creates a new ACE/Client user database and preserves the existing one under a new name. The new database is created in the TCPWARE:ACECLIENT_USER.DAT file and is empty. If a previous database file exists, it is re to TCPWARE:ACECLIENT_USER_OLD.DAT. Requires SYSPRV or BYPASS privilege.

To...	**Use this command...**
add users to the database	ADD ACE_USER
show the usernames added	SHOW ACE_USER
remove a username	REMOVE ACE_USER

Format

CREATE ACE_USER_DATABASE

Example

Creates a new ACE/Client user database and renames the current one to _OLD.DAT.

```
NETCU>CREATE ACE_USER_DATABASE
NETCU>SPAWN DIR ACECLIENT_USER*

Directory SYS$COMMON:[TCPWARE]

ACECLIENT_USER.DAT;1     ACECLIENT_USER_OLD.DAT;1
```

CREATE EXPORT

NFS Server only.

Creates an empty EXPORT database. Requires write access to the TCPWARE:NFS_EXPORT.DAT file.

Note! NFS Server installations create an empty EXPORT database. Use this command to supersede an existing EXPORT database only.

Format

CREATE EXPORT

Example

Shows the current EXPORT database, overwrites it, and shows that the database is now empty.

```
SHOW EXPORT
NFS EXPORT Database V5.8 Copyright (c) Process Software

Path   Directory                Host(s)
----   ---------                -------
/usr   $DISK1:[SALES.RECORDS]   SIGMA


CREATE EXPORT
SHOW EXPORT
%TCPWARE-NETCU-I-NOENTRIES, no EXPORT entries found
```

CREATE GROUP

NFS Client only.

Creates an empty GROUP database. Requires write access to the TCPWARE:NFS_GROUP.DAT file.

Note! Client installation creates an empty GROUP database. Only use this command to supersede an existing GROUP database.

Format

CREATE GROUP

Example

Shows the current GROUP database, overwrites it, and shows that the database is now empty.

```
SHOW GROUP
NFS GROUP Database V5.8 Copyright (c) Process Software

Group    Name      Value        Host(s)
-----    ----      -----        -------
15       GROUP     %X8001000B
15       GROUP_16  %X8001000E


CREATE GROUP
SHOW GROUP
%TCPWARE-NETCU-I-NOENTRIES, no GROUP entries found
```

CREATE KDB

Used by the Kerberos master administrator. Creates and initializes the Kerberos database (KDB). You must use CREATE KDB before starting the Kerberos Server or Administration Server. This command can only be executed if the local host is configured as a Kerberos Server. Requires OPER or SYSPRV privilege and entry of the Kerberos master password. See the SHOW KDB command for the output from CREATE KDB.

Format

CREATE KDB

Enter Kerberos master password: ***master-password***
Verifying, please re-enter: ***master-password***

Parameter

master-password

New Kerberos password to be used for access to the Kerberos database. Converted to lowercase unless you enclose it in double quotes.

Note! Keep the master password as secure as the password to the SYSTEM account. The Kerberos Server requires the KDB and a stashed Kerberos master password. See the STASH MASTER_PASSWORD command for details.

Qualifiers

/KDBFILE=*file*

Name of the KDB file. The default is TCPWARE:PRINCIPAL.OK.

/REALM=*realm*

Kerberos realm to use instead of the one defined by the default logical TCPWARE_KERBV4_REALM. Converted to lowercase unless you enclose it in double quotes.

Example

Creates and initializes the Kerberos database while entering the Kerberos master password in the new KDB.

```
CREATE KDB
Enter Kerberos master password:
Verifying, please re-enter:
```

CREATE PROXY

NFS Client and Server.

Creates an empty PROXY database. Requires write access to the TCPWARE:NFS_PROXY.DAT file.

Note! Client and Server installation creates an empty PROXY database. Only use this command to supersede an existing PROXY database.

Format

CREATE PROXY

Example

Shows the current PROXY database, overwrites it, and shows that the database is now empty.

```
SHOW PROXY
NFS PROXY Database V5.8 Copyright (c) Process Software

Username    UID     GID   Host(s)
--------    ---     ---   -------
BART        1116    15
MARGE       1115    15
LISA        1117    16
HOMER       -2      -2

CREATE PROXY
SHOW PROXY
%TCPWARE-NETCU-I-NOENTRIES, no PROXY entries found
```

CREATE SRVTAB

Used by the Kerberos master administrator. Creates an encrypted service table file for a host to allow its Kerberos application services to authenticate principals.

If the application service is not on the local host, you should specify an *instance*, and the file will be named *instance*-NEW-SRVTAB. in the local directory. The file should then be copied (preferably hand-carried) to the remote host and renamed there to TCPWARE:SRVTAB. if an OpenVMS machine, /etc/srvtab if a UNIX machine, or some other file if another type of machine (check their documentation for details).

Make sure the necessary services were previously added for the instance in the Kerberos database (see ADD KDB). Otherwise the service table file will be empty. Requires OPER or SYSPRV privilege and entry of the Kerberos master password.

Format

CREATE SRVTAB *[instance]*

Enter Kerberos master password: ***master-password***
Verifying, please re-enter: ***master-password***

Parameters

instance

Name of the host on which the Kerberos application services reside. The necessary services must have been added for that host in the Kerberos database or the service table file will be empty. Converted to lowercase unless you enclose it in quotes. If omitted, creates a service table for the local host and automatically creates the file TCPWARE:SRVTAB..

master-password

Kerberos password used for access to the Kerberos database. Converted to lowercase unless you enclose it in quotes.

Qualifiers

/KDBFILE=*file*

Name of an alternate KDB file. The default is TCPWARE:PRINCIPAL.OK.

/PROMPT (default)
/NOPROMPT

Specifies whether TCPware prompts you for the master password. /NOPROMPT reads the master password from the file created by the STASH MASTER_PASSWORD command.

/REALM=*realm*

Kerberos realm to use instead of the one defined by the TCPWARE_KERBV4_REALM logical. Converted to lowercase unless you enclose it in quotes.

Examples

1 Creates the service table for the current host in the TCPWARE:SRVTAB. file.

```
CREATE SRVTAB
Enter Kerberos master password:
Verifying, please re-enter:
```

2 Creates the service table for remote host BART. Since /NOPROMPT was used, the master password is read from the file created by the STASH MASTER_PASSWORDNO TAG command. (A service ticket entry for BART was previously created using ADD KDB rcmd “RANDOM” BART.) The name of the service table file will be BART-NEW-SRVTAB. and will be hand-carried to BART and renamed there to TCPWARE:SRVTAB., since BART is an OpenVMS system.

```
CREATE SRVTAB BART /NOPROMPT
```

DEBUG/IP

Displays information about IP datagrams sent and received over the network. Use this information to debug IP network problems. Requires LOG_IO privilege, along with either SYSPRV or BYPASS privilege.

The DEBUG/IP command displays the system time for the packet as mm:ss.cc (minutes, seconds, and hundredths of a second).

Press `Ctrl/C` to end the display and return to the NETCU prompt.

Note! To use the command output, you must understand the IP protocol and its header fields (see RFC 791). Contact Process Software if you need help.

Format

DEBUG/IP

Qualifiers

/DATA=*byte-count*

Maximum number of data bytes to display (the default is 16 bytes).

/DECODE

Shows all IP packets in TCPDUMP output format. You can combine /DECODE with any other qualifier except /OCTAL and /DECIMAL, since TCPDUMP output is in hex format.

/HEADER

Displays the IP header in bytes. By default, TCPware does not display the header since the important information contained in it appears in a decoded format.

{/OCTAL | /DECIMAL | /HEXADECIMAL}

Displays the data bytes in octal, decimal, or hexadecimal format. Hexadecimal is the default, which also displays printable ASCII characters for the bytes

You can only specify one of these qualifiers.

/LINE=*line-id*

Displays IP datagrams for the indicated line only.

{/SIA | /LIA}=(ia[,mask])

For transmitted packets, displays only packets the specified local internet address(es) sends. For received packets, displays only packets the specified local internet address(es) receives. For example, you can use this on a system with multiple interfaces to capture traffic to and from any particular interface.

This flag is optional if only one interface exists on the local system. If you omit the *mask* value, the parentheses are optional.

{/DIA | /RIA | /FIA}=(ia[,mask])

For transmitted packets, displays only packets the specified internet address(es) receives. For received packets, displays only packets the specified internet address(es) sends.

If you omit the *mask* value, the parentheses are optional.

Note! For the /SIA (/LIA) and /DIA (/RIA, /FIA) qualifiers, if you do not specify the mask value, TCPware determines the mask based on whether the host number portion of the address is 0 or non-zero. If non-zero, the mask is 255.255.255.255. If zero, the mask is the address mask for the network.

/PROTOCOL=*n*

Displays only packets for the specified IP protocol.

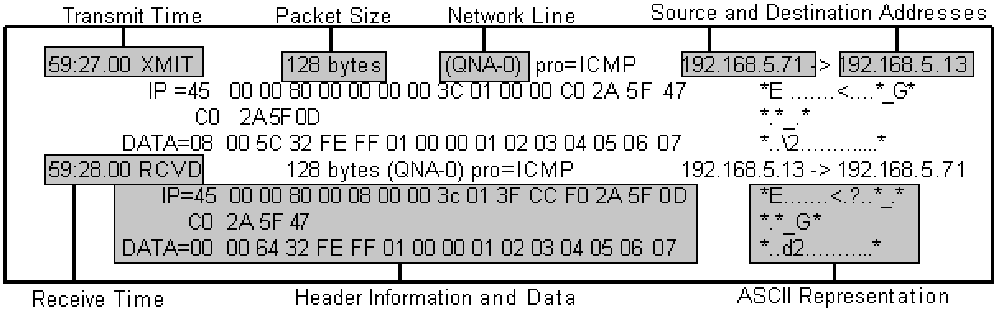
/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Example

`DEBUG/IP/HEADER`

Returns information such as the following about IP datagrams for all network connections:



```
59:27.00 XMIT        128 bytes     (QNA-0) pro=ICMP      192.168.5.71 -> 192.168.5.13
         IP =45   00 00 80 00 00 00 00 3C 01 00 00 C0 2A 5F  47         *E .......<....*_G*
                C0   2A5F0D                                              *.*_.*
         DATA=08  00 5C 32 FE FF 01 00 00 01 02 03 04 05 06  07          *..\2...........*
59:28.00 RCVD              128 bytes (QNA-0) pro=ICMP           192.168.5.13 -> 192.168.5.71
            IP=45  00 00 80 00 08 00 00 3c 01 3F CC F0 2A 5F 0D          *E.......<.?..*_.*
                C0  2A 5F 47                                             *.*_G*
         DATA=00  00 64 32 FE FF 01 00 00 01 02 03 04 05 06  07          *..d2..........*
```

DEBUG/TCP

Displays information about TCP segments sent and received over the network. Use this information to debug TCP network problems. Requires LOG_IO privilege, along with either SYSPRV or BYPASS privilege.

The DEBUG/TCP command displays the system time for the packet as *mm:ss.cc* (minutes, seconds, and hundredths of a second).

Press `Ctrl/C` to end the display and return to the NETCU prompt.

Note! To use the command output, you must understand the TCP protocol and its header fields (see RFC 793). Contact Process Software if you need help.

Format

DEBUG/TCP

Qualifiers

/DATA=*byte-count*

Maximum number of data bytes to display (the default is 16 bytes).

/DECODE

Shows all IP packets in TCPDUMP output format. You can combine /DECODE with any other qualifier except /OCTAL and /DECIMAL, since TCPDUMP output is in hex format.

/HEADER

Displays the TCP header in bytes. By default, TCPware does not display the header since the important information contained in it appears in a decoded format.

{/OCTAL | /DECIMAL | /HEXADECIMAL}

Displays the data bytes in octal, decimal, or hexadecimal format. Hexadecimal is the default, which also displays printable ASCII characters for the bytes. You can only specify one of these qualifiers.

{/SIA | /LIA}=(ia[,mask])

For transmitted packets, displays only packets the specified local internet address(es) sends. For received packets, displays only packets the specified local internet address(es) receives. For example, you can use this on a system with multiple interfaces to capture traffic to and from any particular interface.

This flag is optional if only one interface exists on the local system. If you omit the *mask* value, the parentheses are optional.

{/DIA | /RIA | /FIA}=(ia[,mask])

For transmitted packets, displays only packets the specified internet address(es) receives. For received packets, displays only packets the specified internet address(es) sends. If you omit the *mask* value, the parentheses are optional.

Note! For the /SIA and /DIA qualifiers, if you do not specify the mask value, TCPware determines the mask based on whether the host number portion of the address is 0 or non-zero. If non-zero, the mask is 255.255.255.255. If zero, the mask is the address mask for the network.

{/SPN | /LPN}=*port*

For transmitted packets, displays only packets the specified port number sends. For received packets, displays only packets you the specified port number receives.

{/DPN | /RPN | /FPN}=*port*

For transmitted packets, displays only packets the specified port number receives. For received packets, displays only packets the specified port number sends.

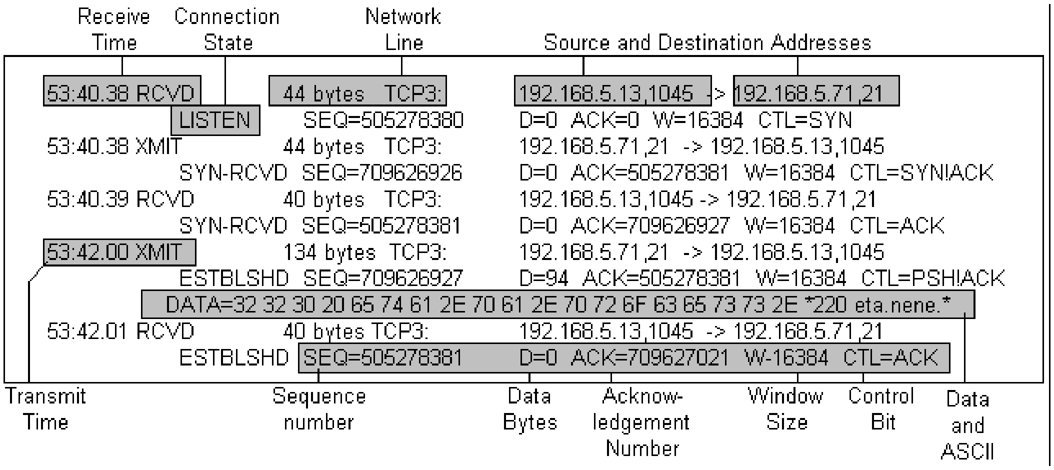
/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Example

`DEBUG/TCP`

Returns information such as the following about TCP segments for all network connections:



```
53:40.38 RCVD          44 bytes   TCP3:       192.168.5.13,1045 -> 192.168.5.71,21
            LISTEN       SEQ=505278380        D=0  ACK=0  W=16384  CTL=SYN
53:40.38 XMIT          44 bytes   TCP3:       192.168.5.71,21  -> 192.168.5.13,1045
            SYN-RCVD  SEQ=709626926        D=0  ACK=505278381  W=16384  CTL=SYN!ACK
53:40.39 RCVD          40 bytes   TCP3:       192.168.5.13,1045 -> 192.168.5.71,21
            SYN-RCVD  SEQ=505278381        D=0  ACK=709626927  W=16384  CTL=ACK
53:42.00 XMIT          134 bytes  TCP3:       192.168.5.71,21  -> 192.168.5.13,1045
            ESTBLSHD  SEQ=709626927        D=94  ACK=505278381  W=16384  CTL=PSH!ACK
           DATA=32 32 30 20 65 74 61 2E 70 61 2E 70 72 6F 63 65 73 73 2E *220 eta.nene.*
53:42.01 RCVD          40 bytes TCP3:         192.168.5.13,1045  -> 192.168.5.71,21
            ESTBLSHD  SEQ=505278381        D=0  ACK=709627021  W-16384  CTL=ACK
```

The system can display the following control bits after CTL=:

URG	Urgent pointer
ACK	Acknowledgment; if set, the ACK field contains the value of the next sequence number the sender expects to receive
PSH	Push function
RST	Reset the connection
SYN	Synchronize sequence numbers
FIN	Finished connection: no more data from the sender

DEBUG/UDP

Displays information about UDP datagrams sent and received over the network. Use this information to debug UDP network problems. Requires LOG_IO privilege, along with either SYSPRV or BYPASS privilege.

The DEBUG/UDP command displays the system time for the packet as *mm:ss.cc* (minutes, seconds, and hundredths of a second). Press `Ctrl/C` to end the display and return to the NETCU prompt.

Note! To use the command output, you must understand the UDP protocol and its header fields (see RFC 768). Contact Process Software if you need help.

Format

DEBUG/UDP

Qualifiers

/DATA=*byte-count*

Maximum number of data bytes to display (the default is 16 bytes).

/DECODE

Shows all IP packets in TCPDUMP output format. You can combine /DECODE with any other qualifier except /OCTAL and /DECIMAL, since TCPDUMP output is in hex format.

/HEADER

Displays the UDP header in bytes. By default, TCPware does not display the header since the important information contained in it appears in a decoded format.

{/OCTAL | /DECIMAL | /HEXADECIMAL}

Displays the data bytes in octal, decimal, or hexadecimal format. Hexadecimal is the default, which also displays printable ASCII characters for the bytes. You can only specify one of these qualifiers.

{/SIA | /LIA}=(ia[,mask])

For transmitted packets, displays only packets the specified local internet address(es) sends. For received packets, displays only packets the specified local internet address(es) receives. For example, you can use this on a system with multiple interfaces to capture traffic to and from any particular interface.

This flag is optional if only one interface exists on the local system. If you omit the *mask* value, the parentheses are optional.

{/DIA | /RIA | /FIA}=(ia[,mask])

For transmitted packets, displays only packets the specified internet address(es) receives. For received packets, displays only packets the specified internet address(es) sends. If you omit the *mask* value, the parentheses are optional.

Note! For the /SIA and /DIA qualifiers, if you do not specify the mask value, TCPware determines the mask based on whether the host number portion of the address is 0 or non-zero. If non-zero, the mask is 255.255.255.255. If zero, the mask is the address mask for the network.

{/SPN | /LPN}=*port*

For transmitted packets, displays only packets the specified port number sends. For received packets, displays only packets the specified port number receives.

{/DPN | /RPN | /FPN}=*port*

For transmitted packets, displays only packets the specified port number receives. For received packets, displays only packets the specified port number sends.

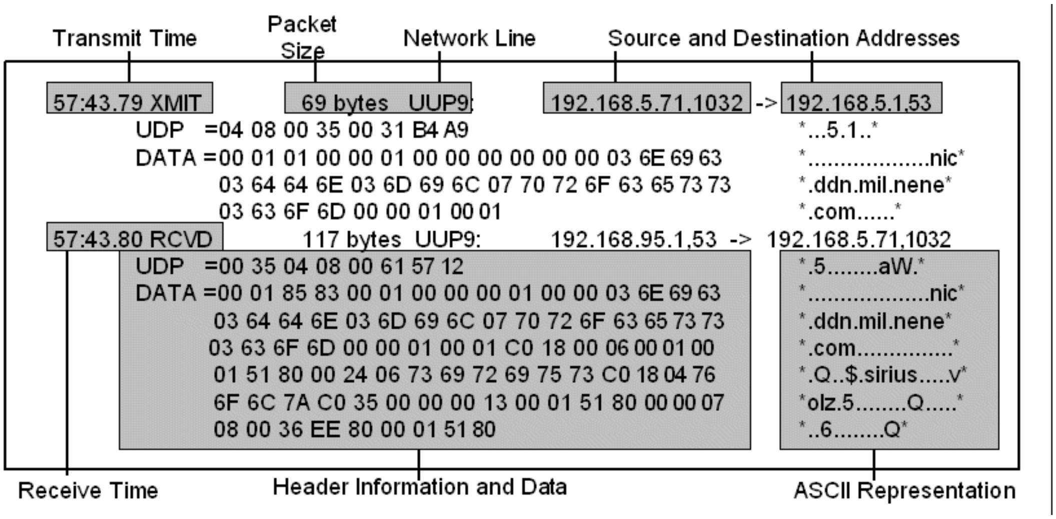
/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Example

`DEBUG/UDP/HEADER/DATA=1000`

Displays information about UDP datagrams for all network connections, includes the IP header information in bytes, and specifies the maximum number of data bytes to display (1,000), as in the following example:



```
57:43.79 XMIT          69 bytes   UUP9:       192.168.5.71,1032 -> 192.168.5.1,53
       UDP   =04 08 00 35 00 31 B4 A9                              *...5.1..*
       DATA =00 01 01 00 00 01 00 00 00 00 00 00 03 6E 69 63       *..................nic*
             03 64 64 6E 03 6D 69 6C 07 70 72 6F 63 65 73 73       *.ddn.mil.nene*
             03 63 6F 6D 00 00 01 00 01                            *.com......*
57:43.80 RCVD          117 bytes  UUP9:       192.168.95.1,53  ->  192.168.5.71,1032
       UDP   =00 35 04 08 00 61 57 12                              *.5........aW.*
       DATA =00 01 85 83 00 01 00 00 00 01 00 00 03 6E 69 63       *..................nic*
             03 64 64 6E 03 6D 69 6C 07 70 72 6F 63 65 73 73       *.ddn.mil.nene*
            03 63 6F 6D 00 00 01 00 01 C0 18 00 06 00 01 00        *.com...............*
             01 51 80 00 24 06 73 69 72 69 75 73 C0 18 04 76       *.Q..$.sirius.....v*
             6F 6C 7A C0 35 00 00 00 13 00 01 51 80 00 00 07       *olz.5........Q.....*
             08 00 36 EE 80 00 01 51 80                            *..6........Q*
```

DEFINE/KEY

Associates an equivalence string and a set of attributes with a key on the terminal keyboard. You must use the /KEY qualifier in this command.

Format

DEFINE/KEY *key-name equivalence-string*

Parameters

key-name

Name of the key you want to define.

Table 2-4 lists the key-names in the first column. The remaining three columns indicate the key designations on the keyboards for the three different types of terminals that allow key definitions. All definable keys on VT52 terminals are on the numeric keypad. On VT100-type terminals, you can define the # and % keys as well as all the keys on the numeric keypad.

You can define three types of keys on terminals with LK201 keyboards: keys on the numeric keypad, on the editing keypad (except the $ and ^ arrow keys), and on the function key row across the top of the terminal. You cannot define function keys F1 through F5.

The # and % keys and the F6 through F14 VT200 keys are reserved for command line editing. You must issue the DCL command SET TERMINAL/ NOLINE_EDITING before defining these keys. You can also press ^V to enable keys F7 through F14 (^V does not enable the F6 key).

Table 2-4 Key-Names

Key-name	**LK201**	**VT100-type**	**VT52**
PF1	PF1	PF1	[blue]
PF2	PF2	PF2	[red]
PF3	PF3	PF3	[gray]
PF4	PF4	PF4	n/a
KP0,...,KP9	0,...9	0,...9	0,...9
PERIOD	.	.	.
COMMA	,	,	n/a
MINUS	-	-	n/a
ENTER	Enter	ENTER	ENTER

LEFT	‹	‹	‹
RIGHT	fi	fi	fi
Find (E1)	Find	n/a	n/a
Insert Here (E2)	Insert_Here	n/a	n/a
Remove (E3)	Remove	n/a	n/a
Select (E4)	Select	n/a	n/a
Prev Screen (E5)	Prev_Screen	n/a	n/a
Next Screen (E6)	Next_Screen	n/a	n/a
HELP	Help	n/a	n/a
DO	Do	n/a	n/a
F6, ..., F20	F6, ..., F20	n/a	n/a

equivalence-string

String that you want to appear when you press the key. If the string contains spaces, enclose the equivalence string in quotation marks (" ").

Qualifiers

/ECHO (default)
/NOECHO

/ECHO echoes the equivalence string on your screen after you press the key. /NOECHO does not echo the equivalence string on your screen. Do not use /NOECHO with the /NOTERMINATE qualifier.

/IF_STATE=*(state-name,...)*
/NOIF_STATE (default)

/IF_STATE defines which if-state you establish with the /SET_STATE qualifier is in effect. If you omit /IF_STATE or use /NOIF_STATE, TCPware uses the current if-state. See the /SET_STATE qualifier for details.

/LOCK_STATE
/NOLOCK_STATE (default)

/LOCK_STATE specifies that the state set by the /SET_STATE qualifier remains in effect until explicitly changed. /NOLOCK_STATE specifies that the state set by /SET_STATE is in effect only for the next definable key that you press or for the next read terminating character that you type. Use /LOCK_STATE only with /SET_STATE.

/SET_STATE=*(state-name,...)*
/NOSET_STATE (default)

/SET_STATE defines the if-state to use when you press the defined key. The state-name is any alphanumeric string. The parentheses are for establishing multiple states. By including several state-names, you can define a key to have the same function in all the specified states. If you omit /SET_STATE or use /NOSET_STATE, the currently locked state is in effect.

/TERMINATE
/NOTERMINATE (default)

/TERMINATE terminates the current equivalence string when you press the defined key. Terminating the string usually executes the string. /NOTERMINATE lets you create key definitions that insert text into command lines, after prompts, or into other text you type.

Example

Sets the F1 key on the keyboard to the “SMITH SECRET”::[USERS] string, sets the state to 1, and locks the state for that definition.

```
DEFINE/KEY F1 “““SMITH SECRET””::[USERS]” /SET_STATE=1/LOCK_STATE
```

DEFINE TIMEZONE

Specifies the local time zone name that was either previously compiled into TCPware or is a name from a selected time zone in the time zone database files.

Format

DEFINE TIMEZONE *localzone*

Parameter

localzone

The name of the local time zone; for example, "MST."

Qualifiers

/LOG
/NOLOG (default)

Displays a list of the time zones that are loaded, and a list of the compiled-in zones that were selected but not loaded because they were compiled-in.

/SELECT
/SELECT=(rule1 [,rule2 [...]])

Specifies a list of countries or time zones to load. Specifying a country loads all time zones in that country.

/FILES
/FILES=(FILE1 [,FILE2 [...]])

Specifies a list of files from which to load the time zone data. The default is TCPWARE:TIMEZONES.DAT. Locally-written rules are normally added to TCPWARE:TIMEZONES.LOCAL.

Example

1 This example defines the time zone to use as the United States local time zone MST.

```
NETCU DEFINE TIMEZONE mst
```

2 This example defines the time zone to MST and loads Arizona time zone rules.

```
NETCU DEFINE TIMEZONE mst/SELECT="us/arizona"
```

DISABLE FORWARDING

Disables forwarding of IP datagrams not destined for this host. Requires OPER privilege. TCPware disables forwarding by default. You should normally disable forwarding to prevent TCPware from routing datagrams between networks.

Format

DISABLE FORWARDING

Synonym

DISABLE GATEWAY

DISABLE REDIRECTS

Disables returning ICMP redirect messages to sending hosts. This can be set if this host is to act as a router. Requires OPER privilege. Disabling redirects is only valid if forwarding is also enabled through ENABLE FORWARDING. ENABLE REDIRECTS is the default if forwarding is enabled.

Format

DISABLE REDIRECTS

DUMP GATED STATE

Tells GateD to dump its internal state into a text file. If you omit the filename, the default is TCPWARE:GATED.DUMP.

Note! The NETCU processing of this command is completed before GateD finishes processing it.

Format

DUMP GATED STATE [file]

Parameter

file

Name of the file to which to dump. If omitted, defaults to TCPWARE:GATED.DUMP.

Example

Tells the GateD process to dump its internal state information to a file called TEMP.DUMP in the user's current working directory.

```
DUMP GATED STATE TEMP.DUMP
```

DUMP KDB

Used by the Kerberos master administrator. Dumps the contents of the Kerberos database (KDB) into an ASCII text file. This command is useful for transferring the KDB from one machine to another. This command can only be executed if the local host is configured as a Kerberos Server. Requires OPER or SYSPRV privilege and entry of the Kerberos master password.

Format

DUMP KDB *output-file*

Enter Kerberos master password: ***master-password***
Verifying, please re-enter: ***master-password***

Parameters

output-file

Output file for the dump.

master-password

Kerberos password used for access to the Kerberos database. Converted to lowercase unless you enclose it in double quotes.

Qualifiers

/KDBFILE=*file*

Name of an alternate Kerberos database file from which the contents are dumped into an ASCII text file. The default is TCPWARE:PRINCIPAL.OK.

/PROMPT (default)
/NOPROMPT

Specifies whether TCPware prompts you for the master password. /NOPROMPT reads the master password from the file created by the STASH MASTER_PASSWORD command.

Example

Dumps the contents of the KDB into the foobar.txt file.

```
DUMP KDB FOOBAR.TXT
Enter Kerberos master password:
Verifying, please re-enter:
```

DUMP NAMED

These commands are used for debugging NameD:

Commands	Description
DUMP NAMED CACHE	Dumps the current contents of the NameD cache to a file, TCPWARE:NAMED_DUMP.DB, in an RFC 883 format
DUMP NAMED STATISTICS (STATS)	Dumps the current NameD statistics to the TCPWARE:NAMED.STATS and the TCPWARE:NAMED.MEMSTATS files

Format

DUMP NAMED CACHE
DUMP NAMED STATISTICS
DUMP NAMED STATS

Examples

```
DUMP NAMED CACHE
%TCPWARE_NETCU-S-NORMAL, normal successful completion
```

1 The NameD cache is dumped to the TCPWARE:NAMED_DUMP.DB file, as in the following example:

```
; Dumped at Thu May  1 09:14:39 2014
;; ++zone table++
;95.168.192.in-addr.arpa (type 2, class 1, source NAMED.temp_sirius_rev)
;       time=862478265,lastupdate=862396837, serial=237,
;       refresh=86400, retry=600, expire=3600000, minimum=86400
;       ftime=862396837, xaddr=[0.0.0.0], state=0041, pid=0
;       z_addr[1]: [192.168.1.92]
; nene.com (type 1, class 1, source NAMED.HOSTS)
;       time=0, lastupdate=862396105, serial=6002,
;       refresh=0, retry=1800, expire=3600000, minimum=86400
;       ftime=862396105, xaddr=[0.0.0.0], state=0041, pid=0
; 48.168.198.in-addr.arpa (type 1, class 1, source NAMED.REV)
;       time=0, lastupdate=862321422, serial=91,
;       refresh=0, retry=600, expire=3600000, minimum=86400
;       ftime=862321422, xaddr=[0.0.0.0], state=0041, pid=0
; 0.0.127.in-addr.arpa (type 1, class 1, source NAMED.LOCAL)
;       time=0, lastupdate=850919099, serial=6001,
; refresh=0, retry=600, expire=3600000, minimum=86400
; ftime=850919099, xaddr=[0.0.0.0], state=0041, pid=0
;; --zone table--
; Note: Cr=(auth,answer,addtnl,cache) tag only shown for non-auth RR’s
; Note: NT=milliseconds for any A RR which we’ve used as a nameserver
; --- Cache & Data ---
$ORIGIN .. 279304  IN   NS  D.ROOT-SERVERS.NET.
;Cr=answer [198.168.48.105]
     279304  IN   NS   E.ROOT-SERVERS.NET.
;Cr=answer [198.168.48.105]
```

```
.
.
.
The NAMESERVER.LOG file shows the following SIGNAL entries:
%%%%%%%%%%%% NAMED  1-MAY-2014 10:55:57.73  %%%%%%%%%%%%
%TCPWARE_NAMED-I-SIGNAL, Request to dump current cache received.

%%%%%%%%%%%% NAMED  1-MAY-2014 10:55:57.77  %%%%%%%%%%%%
%TCPWARE_NAMED-I-SIGNAL, dumping nameserver cache

%%%%%%%%%%%% NAMED  1-MAY-2014 10:55:58.13  %%%%%%%%%%%%
%TCPWARE_NAMED-I-SIGNAL, nameserver cache dump completed
```

```
DUMP NAMED STATS
%TCPWARE_NETCU-S-NORMAL, normal successful completion
```

2 Dumps the current NameD statistics in the NAMESERVER.LOG file, as in the following example:

```
%%%%%%%%%%%% NAMED  1-MAY-2014 10:55:57.72  %%%%%%%%%%%%
%TCPWARE_NAMED-I-SIGNAL, Request to dump statistics received.
%%%%%%%%%%%% NAMED  1-MAY-2014 10:55:57.73  %%%%%%%%%%%%
%TCPWARE_NAMED-I-STATUS, dumping nameserver stats

+++ Statistics Dump +++ (862478765) Thu May  1 09:26:05 2014
723     time since boot (secs)
723     time since reset (secs)
0       Unknown query types
++ Name Server Statistics ++
(Legend)
        RQ      RR      RIQ     RNXD    RFwdQ
        RFwdR   RDupQ   RDupR   RFail   RFErr
        RErr    RTCP    RAXFR   RLame   ROpts
        SSysQ   SAns    SFwdQ   SFwdR   SDupQ
        SFail   SFErr   SErr
(Global)  0 1 0 0 0  0 0 0 0 0  0 0 0 0 0  1 0 0 0 0  0 0 0
[192.168.12.34]  0 1 0 0 0  0 0 0 0 0  0 0 0 0 0  1 0 0 0 0  0 0 0
-- Name Server Statistics --
--- Statistics Dump --- (862478765) Thu May  1 09:26:05 2014
%%%%%%%%%%%% NAMED  1-MAY-2014 09:26:05.87 %%%%%%%%%%%%
%%TCPWARE_NAMED-I-STATUS, done dumping nameserver stats
```

ENABLE FORWARDING

Enables the forwarding of IP datagrams not destined for this host. This is necessary if this host is to act as a router. Requires OPER privilege. TCPware disables forwarding by default. When you enable forwarding, the host receiving IP datagrams forwards them to another network if needed.

Format

ENABLE FORWARDING

Synonym

ENABLE GATEWAY

Qualifier

/ARP
/NOARP (default)

Enables, or disables, ARP reply messages for remote internet addresses (also referred to as PROXY ARP). The network sends a reply only if there is a known route to the target internet address of the ARP request.

ENABLE REDIRECTS

Enables ICMP redirects to notify sending hosts to redirect IP datagrams to another host. This can be set if this host is to act as a router. Requires OPER privilege. Enabling redirects is only valid if forwarding is also enabled through ENABLE FORWARDING. ENABLE REDIRECTS is the default if forwarding is enabled. To disable redirects, use the DISABLE REDIRECTS command.

Format

ENABLE REDIRECTS

EXIT

Saves the current configuration, if it has been modified, then quits.

Exits NETCU and returns to the DCL level.

Format

EXIT

FIND ARP

Displays a single entry from an ARP table. ARP tables map internet addresses to physical hardware addresses for FDDI, Ethernet, and HYPERchannel interfaces. You can display the entire ARP table for a network device using the SHOW ARP command. For the format of the ARP table entries, see the SHOW ARP command.

Format

FIND ARP *destination-ia*

Parameter

destination-ia

Internet address or host name of the ARP table entry.

Qualifier

/LINE=*line*

Line ID of the ARP table where you want NETCU to locate the entry. You must use this qualifier if the internet address is not a local network address. If omitted, TCPware determines the ARP table based on the internet address.

Example

Finds the hardware (physical) address of the FLOWER.DAISY. COM internet address.

```
FIND ARP
_Internet address: FLOWER.DAISY.COM

Internet Address     Physical Address      Flags
----------------     ----------------      -----
192.168.5.1          AA-00-04-00-01-08
```

FIND PROXY

NFS Client and Server.

Locates and displays a single entry in the PROXY database. Requires read access to the TCPWARE:NFS_PROXY.DAT file.

On the Client, use this command to find the UIC assigned a specific user.

On the Server, use this command to determine which OpenVMS username the server uses when it receives a request from the specified UID, GID, and host name.

Format

FIND PROXY

Qualifiers

Note! You must specify *all three* of the following qualifiers.

/HOST=*host-name*(required)

Host on which the user is valid. This qualifier is required.

/UID=*uid*(required)

User's ID (UID). This qualifier is required.

/GID=*gid*(required)

User's group ID (GID). This qualifier is required.

Example

Locates an OpenVMS username for an NFS user with UID=210, GID=5, at host ROSE.

```
FIND PROXY /UID=210 /GID=5 /HOST=ROSE
NFS PROXY Database V5.8 Copyright (c) Process Software

Username    UID    GID    Host(s)
--------    ---    ---    -------
SMITH       210    15     ROSE
```

FIND ROUTE

The FIND ROUTE command displays an existing route from the routing table for a specified host or network.

Format

FIND ROUTE *destination-ia*

Parameter

destination-ia

The internet address or host name of the host or network of the routing table entry.

Example

Finds the routing table entry for the 192.168.5.21 host internet address.

The UNIL flag entry indicates that the route is "up" (functional), that it is a network (N) route, that the route is a network interface (I), and that someone locked the route (L) using the /LOCK qualifier. The number 2300 indicates that many datagrams have been transmitted using this route.

```
FIND ROUTE
_Destination internet address: 192.168.5.21

Destination    Gateway          Flags    RefCnt   UseCnt   Line
-----------    -------          _____    ______   ______   _____
192.168.5.0    192.168.5.21     UNIL     0        2300     SVA-0
```

FLUSH

Flushes the entire ARP table or routing table. Requires OPER privilege.

Format

FLUSH

Qualifiers

/ARP

Flushes the ARP tables and removes all but permanent entries. /NETWORK is an equivalent qualifier. Use the REMOVE command to remove a permanent ARP entry.

/LINE=*line*

Line ID of the ARP table to flush. If omitted, NETCU flushes all the ARP tables.

/ROUTE

Flushes the routing table by removing all non-interface routes. An interface route is for an actual network interface.

GET TGT

For Kerberos users. Gets the ticket-granting ticket (TGT) that allows you to get application service tickets. This process authenticates you to the Kerberos Server, which is considered to be a trusted, secure machine. TGTs are required to obtain an application service ticket from the Kerberos Server. The name of the ticket file is determined by the TCPWARE_KERBV4_TKFILE logical, usually set to SYS$LOGIN:KERBV4.TICKET. You must enter your Kerberos password with the command. Your OpenVMS login name is used for the Kerberos username unless the /USERNAME qualifier specifies otherwise. GET TGT is equivalent to the UNIX command *kinit*.

Format

GET TGT
Password:***password***

Parameter

password

User's Kerberos password that authenticates the user to the Kerberos Server. Converted to lowercase unless you enclose it in double quotes.

Qualifiers

/INSTANCE=*instance*

Usually omitted for a general Kerberos user; **admin** for an administrative user. (See your Kerberos administrator to determine your Kerberos instance name.) Converted to lowercase unless you enclose it in double quotes.

/LIFETIME=*minutes*

Lifetime of the TGT in minutes ranging from 5 to 1275 minutes. The default lifetime is 480 minutes (8 hours).

/REALM=*realm*

Optional Kerberos realm to use instead of the one determined by the value of the logical TCPWARE_KERBV4_REALM. Converted to lowercase unless you enclose it in double quotes.

/USERNAME=*login-name*

Alternate login name. Converted to lowercase unless you enclose it in double quotes.

Example

Gets a ticket-granting ticket for the logged-in user. If you logged in as SYSTEM, SYSTEM is used as the Kerberos username. If you logged in as FRED, FRED is used as the Kerberos username.

```
GET TGT
Password:
```

HELP

Brings up the NETCU online help. NETCU uses the OpenVMS interactive help facility. To exit the help facility, press `Return` until you return to the NETCU> prompt.

Format

HELP *[topic]*

Parameter

topic

(Optional) Topic for which you want help.

KILL CONNECTIONS

Resets the TCP connection on the specified device or the connections matching the internet address or port specification. Requires PHY_IO and either SYSPRV or BYPASS privileges.

Format

KILL CONNECTIONS *[device | qualifier]*

Specify either a device or one or both of the qualifiers listed below.

Parameter

device

One of the following devices: TCP*n,* BG*n,* INET*n.*

When specifying a device, KILL CONNECTIONS kills active and listening connections for that device. TCPware resets the TCP connection and completes any pending QIOs with the SS$_THIRDPARTY status. When you omit the device, KILL CONNECTIONS kills only active connections (those not in a CLOSED or LISTEN state) that match the local or remote specification.

Qualifiers

/LOCAL=*ia.port*

Local address and port for incoming connections, in the format *ia.port*, where *ia* is the IP address or host name followed by a period, and *port* is the port number or service name. Use an asterisk (*) as a wildcard in place of *ia* or *port*.

/REMOTE=*ia.port*

Remote address and port for outgoing connections, in the format *ia.port*, where *ia* is the IP address or host name followed by a period, and *port* is the port number or service name. Use an asterisk (*) as a wildcard in place of *ia* or *port*.

Examples

1 Kills all outgoing TELNET (port 23) connections.

```
KILL CONNECTIONS /REMOTE=*.23
```

2 Kills all outgoing connections to host NIC.NEAR.NET.

```
KILL CONNECTIONS /REMOTE=NIC.NEAR.NET.*
```

3 Kills all incoming connections to any local IP address and port.

```
KILL CONNECTIONS /LOCAL=*.*
```

LOAD GATED CONFIGURATION

Tells the GateD process to load a configuration file. If no file is specified, the default file TCPWARE:GATED.CONF is loaded.

CAUTION! If the GateD process detects an error in the configuration file being loaded, it stops running.

Note! The NETCU processing of this command is completed before GateD finishes processing it.

Format

LOAD GATED CONFIGURATION *[file]*

Parameter

file

Name of the configuration file to load. If omitted, defaults to TCPWARE:GATED.CONF.

Example

This example tells the GateD process to load a new configuration file called TEST_CONFIG.CONF from the system manager's current working directory.

```
LOAD GATED CONFIGURATION TEST_CONFIG.CONF
```

LOAD KDB

Used by the Kerberos master administrator. Loads the Kerberos database from an ASCII text file, such as the one created using DUMP KDB. Useful for transferring the Kerberos database from one machine to another. The Kerberos database is in TCPWARE:PRINCIPAL.OK. This command can only be executed if the local host is configured as a Kerberos Server. Requires OPER or SYSPRV privilege and entry of the Kerberos master password.

Format

LOAD KDB *input-file*

Enter Kerberos master password: ***master-password***
Verifying, please re-enter: ***master-password***

Parameter

input-file

Name of the ASCII text file from which the Kerberos database contents are loaded.

master-password

Kerberos password used for access to the Kerberos database. Converted to lowercase unless you enclose it in double quotes.

Qualifiers

/KDBFILE=*file*

Name of an alternate Kerberos database file into which the contents are loaded from an ASCII text file. The default is TCPWARE:PRINCIPAL.OK.

/PROMPT (default)
/NOPROMPT

Specifies whether TCPware prompts you for the master password. /NOPROMPT reads the master password from the file created by the STASH MASTER_PASSWORD command.

Example

Loads the KDB using the foobar.txt file created with DUMP KDB.

```
LOAD KDB FOOBAR.TXT
Enter Kerberos master password:
Verifying, please re-enter:
```

MODIFY KDB

Used by the Kerberos master administrator. Modifies an entry in the Kerberos database (KDB). Use qualifiers to make modifications to an entry. The Kerberos database is in TCPWARE:PRINCIPAL.OK. This command can only be executed if the local host is configured as a Kerberos Server. Requires OPER or SYSPRV privilege and entry of the Kerberos master password.

Format

MODIFY KDB ***principal [instance]***

Enter Kerberos master password: ***master-password***
Verifying, please re-enter: ***master-password***

Parameters

principal

Kerberos user's login name, Kerberos administrator's login name, or name of the Kerberos application service. Converted to lowercase unless you enclose it in double quotes. You can enter * to modify all principals.

instance

Usually omitted for a general Kerberos user; **admin** for an administrative user; or name of the machine on which the Kerberos application resides for an application service. Converted to lowercase unless you enclose it in double quotes. You can enter ***** to modify all instances.

master-password

Kerberos password used for access to the Kerberos database. Converted to lowercase unless you enclose it in double quotes.

Qualifiers

/ATTRIBUTE=*attribute*

Attribute number, from 0 to 65535.

/EXP_DATE=*date*

Expiration date of the KDB entry.

/KDBFILE=*file*

Name of the KDB file. The default is TCPWARE:PRINCIPAL.OK.

/MAX_LIFE=*minutes*

Maximum lifetime of the KDB entry, in minutes.

/PASSWORD=*new-kerberos-password*

Kerberos user’s new password or application service’s new password (usually **"RANDOM"**, which generates a random password for the service). Specify **"NULL"** for a null password. Converted to lowercase unless you enclose it in double quotes.

/PROMPT (default)
/NOPROMPT

Specifies whether TCPware prompts you for the master password. /NOPROMPT reads the master password from the file created by the STASH MASTER_PASSWORD command.

Examples

1 Modifies the password used for charon’s entry in the database.

```
MODIFY KDB CHARON /PASSWORD=monday
Enter Kerberos master password:
Verifying, please re-enter:
```

2 Changes all instances of rcmd services to have a randomly-generated password.

```
MODIFY KDB RCMD * /PASSWORD=”RANDOM”
Enter Kerberos master password:
Verifying, please re-enter:
```

MODIFY KERBEROS USER

Used by the Kerberos administrator to modify a user password in the Kerberos database. The default Kerberos administrator account name is the name of the OpenVMS account using this command. Requires OPER or SYSPRV privilege and entry of the Kerberos administrator's password.

Format

MODIFY KERBEROS USER *username new-password*

Administrator password for *'admin-account':* ***admin-password***

Parameters

username

Kerberos user's login name. Converted to lowercase unless you enclose it in quotes.

new-password

New password of the Kerberos user account to change. Converted to lowercase unless you enclose it in quotes.

admin-password

Kerberos administrator's password. Converted to lowercase unless you enclose it in quotes.

Qualifier

/ADMINISTRATOR=*admin-username*

Alternate Kerberos administrator name. Converted to lowercase unless you enclose it in quotes. The default name is the OpenVMS account name, in lowercase.

Example

Administrator fred changes smith's Kerberos password.

```
MODIFY KERBEROS USER SMITH FOOBAR /ADMINISTRATOR=FRED
Administrator password for 'fred':
```

MODIFY SERVICE

Modifies information associated with an existing service. Requires OPER privilege.

Format

MODIFY SERVICE ***port protocol [image]***

Parameters

port

Name or port number for the service to modify. Any service name or port number (except 0) defined in the TCPWARE:SERVICES. file. The service must be active.

protocol

Protocol to service the connection. Table 2-5 lists the valid values.

Table 2-5 Protocol Values

Enter This Value...	**For...**
BG_TCP	UCX-based servers on TCP
BG_UDP	UCX-based servers on UDP
TCP	TCPDRIVER-based servers
UDP	UDPDRIVER-based servers
STREAM, DGRAM	INETDRIVER-based servers

image

File specification of the server you want executed. DO NOT use with BG_TCP or BG_UDP.; use the /INPUT qualifier instead.

Qualifiers

See the ADD SERVICE command for valid qualifiers. Remove an access list for a service by specifying /ACCESS_LIST=0 (see Example 2).

Examples

The commands in this example:

- Add access list number 1, permitting access for the host given.
- Modify the service on port 23 (creating a TELNET session) to correspond to access list number 1. This allows access only to those hosts on that access list (in this case just the host at address 192.168.5.3).

```
ADD ACCESS_LIST 1 PERMIT 192.168.5.3
MODIFY SERVICE 23 TCP /ACCESS_LIST=1
```

SHOW SERVICE /FULL 23 TCP

```
TCPware(R) for OpenVMS NETCP Services:

Protocol  Port     Active   Limit   Connects   Errors  Image
--------  ----     ------   -----   --------   ------  ----
TCP       TELNET   0        NONE    0          0
                    /ROUTINE=CREATE_TELNET_SESSION
                    /ACCESS_LIST=1
```

SHOW ACCESS_LISTS 1

```
TCPware(R) for OpenVMS NETCP Access Lists:
List Condition InternetAddress AddressMask     Access Denied Message
---- --------- --------------- --------------  ---------------------
1    PERMIT    192.168.5.3     255.255.255.255
```

RELOAD GROUP

NFS Client only.

Implements changes made to the GROUP database without having to restart the client system. Requires SYSLCK privilege.

Note! The GROUP database is normally static. The REL command puts the changes into effect. Use this command sparingly. The Client can take a significant amount of time to reload the database. The reloading process blocks NFS activity.

Format

RELOAD GROUP

RELOAD NAMED

Reloads the Domain Name Services (DNS) name server's database files, if needed, by reading the NAMED.BOOT file and checking the zone information.

For example, if your name server is primary for five zones and you change the SOA record for one zone, RELOAD NAMED notices the change and reloads that zone. If you add a zone in the NAMED.BOOT file (for example, a secondary), it notices the change and starts a zone transfer to the primary to gain that zone.

Format

RELOAD NAMED

Examples

1
```
RELOAD NAMED
%TCPWARE_NETCU-S-NORMAL, normal successful completion
```

If executing this command after editing NAMED.BOOT and adding a secondary zone 95.168.192.in-addr.arpa with the primary nameserver to be 192.168.95.1, the following entry displays in the NAMESERVER.LOG file:

```
%%%%%%%%%%%% NAMED  30-APR-2014 10:40:36.11 %%%%%%%%%%%%
%TCPWARE_NAMED-I-SIGNAL, Request to reload databases received.

%%%%%%%%%%%% NAMED  30-APR-2014 10:40:36.12 %%%%%%%%%%%%
%TCPWARE_NAMED-I-RELOAD, reloading name server

%%%%%%%%%%%% NAMED 30-APR-2014 10:40:36.16 %%%%%%%%%%%%
%TCPWARE_NAMED-I-MAIN, Ready to answer queries.

%%%%%%%%%%%% NAMED  30-APR-2014 10:40:36.48 %%%%%%%%%%%%
%TCPWARE_NAMED-I-SUBPROC, created process 000001D4 to transfer zone
95.42.192.in-addr.arpa

%%%%%%%%%%%% NAMED  30-APR-2014 10:40:37.51 %%%%%%%%%%%%
%TCPWARE_NAMED-I-XFERSUCCESS, zone 95.42.192.in-addr.arpa
transferred successfully

%%%%%%%%%%%% NAMED 30-APR-2014 10:40:37.65 %%%%%%%%%%%%
%TCPWARE_NAMED-I-ZONEINFO,secondary zone “95.42.192.in-addr.arpa” loaded (serial
237)
```

2
```
  RELOAD NAMED
%TCPWARE_NETCU-S-NORMAL, normal successful completion
```

If executing this command after editing NAMED.BOOT and increasing the Serial Number, the following entry displays in the NAMESERVER.LOG file:

```
%%%%%%%%%%%% NAMED  30-APR-2014 10:28:39.84 %%%%%%%%%%%%
%TCPWARE_NAMED-I-SIGNAL, Request to reload databases received.
%%%%%%%%%%%% NAMED  30-APR-2014 10:28:39.84 %%%%%%%%%%%%
%TCPWARE_NAMED-I-RELOAD, reloading name server

%%%%%%%%%%%% NAMED 30-APR-2014 10:28:40.04 %%%%%%%%%%%%
%TCPWARE_NAMED-I-ZONEINFO, primary zone “yours.com” loaded (serial 6002)

%%%%%%%%%%%% NAMED 30-APR-2014 10:28:40.07 %%%%%%%%%%%%
%TCPWARE_NAMED-I-MAIN, Ready to answer queries.
```

RELOAD PROXY

NFS Client and Server.

Implements changes made to the PROXY database without having to restart the Client or Server. Not necessary if the TCPWARE_NFS_DYNAMIC_PROXY logical was defined as CLIENT or SERVER. Requires SYSLCK privilege.

Note! The PROXY database is normally static. The RELOAD PROXY command puts the changes into effect. Use this command sparingly. The Client can take a significant amount of time to reload the database. The reloading process blocks NFS activity.

Format

RELOAD PROXY *[vms-username[, vms-username, ...]*

Parameter

vms-username

Reloads only the PROXY database entries for the specified username (or list of usernames separated by commas). This is useful for notifying the Client or Server of changes to the OpenVMS SYSUAF.DAT file, such as changes to the rights list or user privileges.

Qualifiers

Note! If you omit both qualifiers, the PROXY database reloads on both the Client and Server.

/CLIENT
/NOCLIENT

/CLIENT reloads the PROXY database on the Client only. /NOCLIENT does not reload the database on the Client.

/SERVER
/NOSERVER

/SERVER reloads the PROXY database on the Server only. /NOSERVER does not reload the database on the Server.

REMOVE ACE_USER

Token Authentication only.

Removes a username from the TCPware ACE/Client user database (in the TCPWARE:ACECLIENT_USER.DAT file). Requires SYSPRV or BYPASS privilege.

To...	**Use this command...**
add a new username to the database	ADD ACE_USER
show the usernames added	SHOW ACE_USER
create a new database	CREATE ACE_USER_DATABASE

Format

REMOVE ACE_USER *username*

Parameter

username

Name of the user to remove from the ACE/Client database.

Example

Shows a sequence of removing a user from the ACE/Client user database and showing the results.

```
NETCU>REMOVE ACE_USER JOKER
NETCU>SHOW ACE_USER
TCPware ACE/Client Username Database

Username
--------
CLUBS
DIAMONDS
HEARTS
SPADES
```

REMOVE ACCESS_LIST

Removes an incoming access restrictions list or a specific entry from a list. Requires write access to the appropriate file.

Format

REMOVE ACCESS_LIST ***list [condition [ia [mask]]]***

Parameters

list

Number of the incoming access restrictions list (1 to 65535).

condition

Sets the condition if access is permitted or denied. Valid keywords are PERMIT and DENY. DENY is the default for hosts not specified on the list.

ia

Internet address of the network or host specified on the list.

mask

Internet address mask, which specifies which bits to use when matching hosts against the incoming access restrictions list. Use set bits when matching hosts against the ia.

If you omit *mask* and the host portion of *ia* is 0, NETCU uses the network or subnet mask. If the host portion of *ia* is not 0, NETCU uses 255.255.255.255, where only the specified host is allowed access.

Examples

1 Removes list 56.

```
REMOVE ACCESS_LIST 56
```

2 Removes all PERMIT entries from list 56.

```
REMOVE ACCESS_LIST 56 PERMIT
```

3 Removes the specified entry from list 56.

```
REMOVE ACCESS_LIST 56 PERMIT 192.168.5.0 255.255.255.0
```

REMOVE ARP

Deletes an entry from an ARP table. Requires OPER privilege.

Each ARP table entry consists of an internet address paired with a physical address.

Note! You do not need to use this command under normal circumstances. ARP automatically maps internet addresses to physical addresses. Use this command in rare instances when a particular host does not support ARP.

Format

REMOVE ARP *destination-ia*

Synonym

SET NOARP *destination-ia*

Parameter

destination-ia

Internet address or host name of the ARP table entry.

Qualifier

/LINE=*line*

Line id of the ARP table that contains the entry you want removed. If omitted, NETCU determines the ARP table on the basis of the internet address. You require /LINE when the internet address is not a local network address.

Note! Unlike some software, if you try to remove entries that do not exist you will not receive an error message.

RELEASE DHCP

Forces the Dynamic Host Configuration Protocol (DHCP) server to act as if it heard a DHCP release message from a client. This command can be used for dynamically assigned IP addresses only. Requires SYSPRV or OPER privilege.

To address the DHCP V4 server, use “DHCP4” instead of “DHCP” in the command.

Note! The DHCP Protocol has no way for the server to tell the client that the address has been released, so this command must be used with caution.

Format

RELEASE DHCP *ip-address*

RELEASE DHCP4 *ip-address*

Synonym

REMOVE DHCP *ip-address*

REMOVE DHCP4 *ip-address*

Parameter

ip-address

The IP address of the lease to release.

Example

Releases the lease for IP address 192.168.5.220.

```
RELEASE DHCP 192.168.5.220
```

REMOVE EXPORT

NFS Server only.

Removes an entry from the EXPORT database so that you can remove access to an exported directory for a single host or a list of hosts. Requires write access to the TCPWARE:NFS_EXPORT.DAT file.

Note! The EXPORT database is dynamic. Any path that you remove from the database becomes invalid immediately. You do not need to restart the Server.

Format

REMOVE EXPORT *"nfs-path"*

Parameter

"nfs-path"

NFS-style pathname used to reference the exported directory. Typically expressed as a UNIX-style pathname. Enclose the pathname in quotation marks (" "). You must enclose the nfs-path in quotation marks (" ").

Qualifier

/HOST=*(host[,host...])*

Removes access to an *nfs-path* for a single host or a list of hosts. If omitted, NETCU removes *nfs-path* for all hosts.

Example

Removes a record from the EXPORT database so that NFS host ORCHID can no longer mount an OpenVMS directory on the /vax/records pathname.

```
REMOVE EXPORT "/vax/records" /HOST=ORCHID
```

REMOVE GROUP

NFS Client only.

Removes a group mapping from the GROUP database. Requires write access to the TCPWARE:NFS_GROUP.DAT file.

Note! The GROUP database is static. The REL command puts changes into effect.

Format

REMOVE GROUP *nfs-group [vms-identifier,...]*

Parameters

nfs-group

NFS group number. If you specify nfs-group alone, NETCU removes the entire group from the database.

vms-identifier

OpenVMS rights identifier(s) or UIC(s) associated with the NFS group. If you specify one, NETCU removes only that identifier from the database; NETCU does not change the remaining entries for that group. See the ADD command for the valid format of *vms-identifier* entries.

Qualifier

/HOST=*(server[,server...])*

Server host(s) on which the group number is valid. Either host names or internet addresses are valid. This qualifier removes the GROUP entry for the specified host(s) only. Use the parentheses with multiple *server* specifications.

Example

Removes a record from the GROUP database so that you can no longer associate group number 15 with a group account on the client.

```
REMOVE GROUP 15
```

REMOVE KACL

Used by the Kerberos master administrator. Removes a Kerberos access control list (KACL) entry for access to the Kerberos database. This entry disallows a Kerberos administrator from adding, modifying, or showing a Kerberos user's entry in the Kerberos database from a remote host.

This command can only be executed if the local host is configured as a Kerberos Server. Requires OPER or SYSPRV privilege and entry of the Kerberos master password.

Format

REMOVE KACL *access-type admin-username instance [realm]*

Enter Kerberos master password: ***master-password***
Verifying, please re-enter: ***master-password***

Parameters

access-type

Specify one of the following ACL types:

ACL Type	Description
ADD	Removes the ability to add to the Kerberos database (ADD KERBEROS USER)
MODIFY	Removes the ability to modify the Kerberos database (MODIFY KERBEROS USER)
SHOW	Removes the ability to show the Kerberos database (SHOW KERBEROS USER)

admin-username

Kerberos administrator's username. Converted to lowercase unless you enclose it in double quotes.

instance

Value should be admin since the username is for a Kerberos administration user.

realm

Alternate Kerberos realm to use instead of the one determined by the value of the logical TCPWARE_KERBV4_REALM. Converted to lowercase unless you enclose it in double quotes.

master-password

Kerberos password used to access the Kerberos database. Converted to lowercase unless you enclose it in double quotes.

Qualifier

/PROMPT (default)
/NOPROMPT

Specifies whether TCPware prompts you for the master password. /NOPROMPT reads the master password from the file created by the STASH MASTER_PASSWORD command.

Example

Removes the KACL entry that allows Kerberos administrator persephone within the HADES.COM realm to show entries in the Kerberos database.

```
REMOVE KACL SHOW PERSEPHONE ADMIN HADES.COM

Enter Kerberos master password:
Verifying, please re-enter:
```

REMOVE KDB

Used by the Kerberos master administrator. Removes an entry from the Kerberos database (KDB). This command can only be executed if the local host is configured as a Kerberos Server. Requires OPER or SYSPRV privilege and entry of the Kerberos master password.

Format

REMOVE KDB ***principal [instance]***

Enter Kerberos master password: ***master-password***
Verifying, please re-enter:***master-password***

Parameters

principal

Kerberos user's login name, Kerberos administrator's login name, or name of the Kerberos application service. You can enter ***** to remove all principals. Converted to lowercase unless you enclose it in double quotes.

instance

Usually omitted for a general Kerberos user; **admin** for an administrative user; or name of the machine on which the Kerberos application resides for an application service. You can enter ***** to remove all instances of the specified principal. Converted to lowercase unless you enclose it in double quotes.

master-password

Kerberos password used for access to the Kerberos database. Converted to lowercase unless you enclose it in double quotes.

Qualifiers

/KDBFILE=*file*

Name of the alternate KDB file. The default is TCPWARE:PRINCIPAL.OK.

/PROMPT (default)
/NOPROMPT

Specifies whether TCPware prompts you for the master password. /NOPROMPT reads the master password from the file created by the STASH MASTER_PASSWORD command.

Examples

1 Removes the Kerberos user entry, charon, from the database.

```
REMOVE KDB CHARON
Enter Kerberos master password:
Verifying, please re-enter:
```

2 Removes all instances of admin from the database.

```
REMOVE KDB * ADMIN
Enter Kerberos master password:
Verifying, please re-enter:
```

REMOVE MULTICAST_GROUP

Removes a multicast host group address from the table of joined addresses for the interface or all interfaces. Requires OPER privilege.

Once you remove a multicast from an interface, applications can no longer receive datagrams sent to that address.

Multicast host group address entries have a reference count. This command decrements the reference count and, if zero, removes the address.

Note! TCPware does not issue an error message if you try to remove an address you never added.

Format

REMOVE MULTICAST_GROUP *internet-address*

Parameter

internet-address

Internet address or host name of the multicast host group address.

Qualifier

/LINE=*line-ID*

Line ID of the interface for which to remove the address. If omitted, TCPware removes the address from all active interfaces.

Example

Removes the all-routers multicast address (224.0.0.2) from the SVA-0 Ethernet interface.

```
REMOVE MULTICAST_GROUP 224.0.0.2 /LINE=SVA-0
```

REMOVE PROXY

NFS Client and Server.

Removes an entry from the PROXY database. Requires SYSPRV privilege and write access to the TCPWARE:NFS_PROXY.DAT file.

Note! If you omit the /CLIENT or /SERVER qualifier, or do not define the TCPWARE_NFS_DYNAMIC_PROXY logical accordingly, you must use the RELOAD PROXY command to reload the database. (For details, see *Reloading the PROXY Database* in Chapter 14 of the *TCPware for OpenVMS Management Guide*.)

Format

REMOVE PROXY *vms-username*

Parameter

vms-username

OpenVMS account you want to remove from the PROXY database. You can use the wildcard * in place of *vms-username* as long as you use one of the qualifiers below to be more selective about the update.

Qualifiers

If you omit a /HOST, /GID, or /UID qualifier, the command removes all entries containing the *vms-username* account from the database.

/HOST=*(server[,server...])*

Server host(s) on which the user is valid. NETCU removes the PROXY entry for the specified host(s) only. Use the parentheses with multiple *server* specifications.

/GID=*gid*

User's group ID (GID). NETCU removes the PROXY entry for the specified GID only.

/UID=*uid*

User's ID (UID). NETCU removes the PROXY entry for the specified UID only.

/CLIENT
/NOCLIENT (default)

/CLIENT notifies the Client to immediately update its loaded PROXY database with an entry for *vms-username*. /NOCLIENT does not notify the Client. This overrides any default action specified using the TCPWARE_NFS_DYNAMIC_PROXY logical.

/SERVER
/NOSERVER (default)

/SERVER notifies the Server to immediately update its loaded PROXY database with an entry for *vms-username*. /NOSERVER does not notify the Server. This overrides any default action specified using the TCPWARE_NFS_DYNAMIC_PROXY logical.

Examples

1 Removes authorization for an NFS user at host MARIGOLD with UID=210 and GID=5 to use the OpenVMS username SMITH.

```
REMOVE PROXY SMITH /UID=210 /GID=5 /HOST=MARIGOLD
```

2 Removes authorization for all users at host CROCUS to use OpenVMS username JONES.

```
REMOVE PROXY JONES /HOST=CROCUS
```

3 Removes authorization for any user at host MARIGOLD to use any OpenVMS username.

```
REMOVE PROXY * /HOST=MARIGOLD
```

4 Removes all entries containing the OpenVMS username SMITH.

```
REMOVE PROXY SMITH
```

5 Removes authorization for a user with UID=210 and GID=5 to use the OpenVMS username SMITH and dynamically reloads the PROXY database on both the Client and Server.

```
REMOVE PROXY SMITH /UID=210 /GID=5 /CLIENT /SERVER
```

REMOVE ROUTE

Deletes an entry from the routing table. Requires OPER privilege. (See also ADD.)

Format

REMOVE ROUTE *destination-ia gateway-ia*

Synonym

SET NOROUTE *destination-ia gateway-ia*

Parameters

destination-ia

Internet address or host name of the destination host or network.

gateway-ia

Gateway used to reach the host or network identified by the *destination-ia* parameter.

Note! If you added a route by specifying a line, specify 0.0.0.0 as the gateway address when removing the route.

Qualifiers

{/HOST | /NETWORK}

Type of route. If omitted, NETCU determines the type of route by looking at the host number portion of the *destination-ia*. If the host number is zero (0), NETCU assumes the route is a network route.

/MASK=*mask*

Internet address mask for the Classless Inter-domain Routing (CIDR) protocol. The mask specifies the bits to use for the network portion of a mask. Thus the traditional network masks would be specified as:

Class A Network	255.0.0.0	Class B Network	255.255.0.0	Class C Network	255.255.255.0

If the mask is omitted, the destination address is derived by first checking interfaces for the same network number, and if one is found, the mask for that interface is used. Otherwise, the address is examined to determine if it is a class A, B, C, D, or E address and a mask will be created based on the class.

Network routes are sorted such that the routes with the most restrictive mask are searched before routes with a less restrictive mask. For example, a route with mask 255.255.255.0 is searched before a routes with mask 255.255.0.0.

Do not create noncontiguous subnet masks. For example, a mask of 255.0.255.0 is not allowed.

REMOVE SECONDARY

Removes a secondary address previously added with the ADD SECONDARY command. If holding a cluster lock, you must use the /ABORT qualifier to force the removal of the secondary address. Requires OPER privilege.

Format

REMOVE SECONDARY *ia*

Parameter

ia

Internet address to remove and no longer recognize as a local address.

Qualifier

/ABORT

Forces the release of a cluster lock and the removal of the secondary address. If omitted, TCPware removes only queued requests for the resource lock. /ABORT has no effect when someone added the secondary address without the /CLUSTER_LOCK qualifier. TCPware always removes the secondary address.

Example

Release the cluster lock on the address 192.168.5.101 and no longer recognize the address as a local address.

```
REMOVE SECONDARY 192.168.5.101 /ABORT
```

REMOVE SERVICE

Stops listening for connections on the specified port. Requires OPER privilege. Removes non-active server connections only unless you use the /ABORT qualifier, which removes all active connections. The TCPWARE:NETCP.LOG file logs each connection serviced. Review this file to obtain details on server errors, and to monitor access and security violations.

CAUTION! If you omit both port and protocol, NETCP removes all services from all ports.

Format

REMOVE SERVICE *[port protocol]*

Parameters

port

Service name or port to stop servicing. Any port number is acceptable. A service name must be defined in the TCPWARE:SERVICES. file. If specifying a *port* or *protocol*, you must use both. Use **0** as a wildcard to stop servicing all ports for the specified *protocol*.

protocol

Protocol for the service you want removed: **TCP, UDP, STREAM, DGRAM, BG_TCP,**or **BG_UDP**.

Qualifier

/ABORT

Deletes all created active server processes.

/ADDRESS=*ip-address*

Removes the service for the specified address or hostname only. The default is 0.0.0.0.

Examples

1 Stops listening for UDP connections on all ports.

```
REMOVE SERVICE 0 UDP
```

2 Stops listening for UDP connections on the TFTP port. NETCP retrieves the TFTP port number from the TCPWARE:SERVICES. file.

```
REMOVE SERVICE TFTP UDP
```

3 Stops listening for connections on all ports on host BART. Does not affect connections that are currently active.

```
REMOVE SERVICE/ADDRESS=BART
```

4 Stops listening for connections on all ports, and removes all active server processes.

```
REMOVE SERVICE/ABORT
```

REMOVE TICKETS

For Kerberos users. Removes your ticket-granting ticket and application service tickets, if any. See the SHOW TICKETS command to view the user's ticket-granting ticket and any application service tickets contained in the user's ticket file. The name of the ticket file is determined by the value of the TCPWARE_KERBV4_TKFILE logical, usually set to SYS$LOGIN:KERBV4.TICKET. REMOVE TICKETS is equivalent to the UNIX command kdestroy.

Format

REMOVE TICKETS

Qualifiers

/BELL
/NOBELL (default)

Specifies whether the terminal bell should sound when an error occurs when trying to remove tickets. The default is /NOBELL.

/STATUS (default)
/NOSTATUS

Specifies whether to display a message when removing tickets. The default is /STATUS.

Example

Removes the ticket-granting ticket and application service tickets, if any.

```
REMOVE TICKETS
```

Troubleshooting

```
%TCPWARE_NETCU-W-NTKTTODES, no tickets to destroy
```

Meaning: The ticket file does not exist.

Action: Use the GET TGT command to create a ticket file entry.

```
%TCPWARE_NETCU-I-TKTDESTR, tickets destroyed
```

Meaning: The ticket was successfully removed.

```
%TCPWARE_NETCU-E-TKTNODES, tickets NOT destroyed
```

Meaning: Some error occurred while trying to delete the ticket file. Possible reasons are that the ticket file does not grant delete access, or you are not its actual owner.

SET

Sets the value for the networking parameters described below. Requires OPER privilege.

CAUTION! Be careful when using SET to change parameter values. Make sure you fully understand the effect of these changes before making them. Use the defaults whenever possible.

Format

SET *parameter value*

Parameters and Values

BACKLOG_DROP_THRESHOLD *connections*

Sets the connection backlog threshold at which TCPware's "random drop" feature is enabled to address half-open connection flooding problems. When there are more half-open TCP connections on the backlog of a socket than the value set for the BACKLOG_LIMIT parameter, and the BACKLOG_DROP_THRESHOLD value is equal to or less than the BACKLOG_LIMIT value, TCPware drops the oldest half-open connection from the request queue. This makes room for new connections. (If you set BACKLOG_DROP_THRESHOLD greater than BACKLOG_LIMIT under the same conditions, TCPware drops each new connection request.) The default BACKLOG_DROP_THRESHOLD value is 64.

BACKLOG_LIMIT *connections*

Sets the maximum backlog of waiting connections that can be requested for a listening socket. (For a listen request on a socket that specifies a backlog value higher than the BACKLOG_LIMIT, the latter value is still used, with no error returned.) Set BACKLOG_LIMIT relatively high (together with a relatively lower value for BACKLOG_DROP_THRESHOLD) to deal with half-open connection flooding problems that denial-of-service attacks can cause. The default BACKLOG_ LIMIT value is 1024. Use the following formula to set an optimum BACKLOG_LIMIT value in view of denial-of-service attacks:

```
Backlog-limit> (Attack-rate x Average-round-trip-time-per-connection)
```

For example, if the attack rate is 1000 connections per second and the average round trip time is 0.1 seconds, you should set the backlog limit to greater than 100 (=1000 x 0.1).

GATEWAY_MTU *maximum-transmission-unit*

Maximum transmission units (MTU) of the interface, which determines the size of TCP segments for connections to non-local hosts. The default value is 0.

IPDEFAULTTOS *default-type-of-service*

Default type-of-service used for all outgoing datagrams that do not explicitly specify a value. The default value is 0.

IPDEFAULTTTL *default-time-to-live-hops*

Default time-to-live value transmitted in outgoing IP datagrams. The default value is 60.

IPMAXFRAGMENTS ***max-fragmented-datagrams***

Maximum number of fragmented datagrams IPDRIVER holds for reassembly. TCPware discards any fragmented datagrams above the indicated value. The default value is 24. (Use SHOW IPXMAXFRAGMENTS to check the current value.)

IPMAXROUTES ***max-routing-table-entries***

Maximum number of routing table entries allowed by IPDRIVER. The default value is 512. (Use SHOW IPMAXROUTES to check the current value.)

IPMTTL ***default-multicast-time-to-live***

Default multicast time-to-live value used when sending multicast datagrams directly using IP. The default value is 1.

IPREASMTIMEOUT ***reassembly-timeout-time***

IP datagram reassembly timeout time. If you do not receive all the datagrams for a fragment within this time interval, the system discards the partially received datagram. The default value is 30 seconds.

SUBNETSARELOCAL (default)
NOSUBNETSARELOCAL

SUBNETSARELOCAL treats subnets as being local, where the MTU of the interface determines the maximum segment size of TCP segments for connections to other subnets on the same local network. NOSUBNETSARELOCAL specifies to use the GATEWAY_MTU parameter value for the size of TCP segments.

TCPDEFAULTTOS ***default-type-of-service***

Default type-of-service used for TCP connections. The default value is 0.

TCPDEFAULTTTL ***default-time-to-live-hops***

Default time-to-live used for TCP connections. The default value is 64.

TCPPERSIST ***persistence-timer-value***

TCP persistence timer's initial value (in milliseconds). The default value is 400 milliseconds (0.4 seconds).

TCPRTOMAX ***maximum-retransmission-time***

Maximum TCP retransmission time (in milliseconds). The default value is 62,000 milliseconds (62 seconds). If you configure TCPware with IP-over-X.25 support, you should reset the maximum retransmission time to 15000.

TCPRTOMIN ***minimum-retransmission-time***

Minimum TCP retransmission time (in milliseconds). The default value is 600 milliseconds (0.6 seconds). If you configure TCPware with IP-over-X.25 support, you should reset the minimum retransmission time to 2000.

UDPRECVLIMIT *unsolicited-receives*

Default limit of UDP unsolicited receives, or datagrams buffered on a socket if there is no outstanding read before they are dropped.

XMIT_QUEUE_LIMIT *maximum-queue-length*

Maximum transmit queue length. The default value is 100.

SET BG_

Sets the TCP, UDP, and IP (raw) parameters for the BGDRIVER devices for UCX compatibility.

Formats

SET BG_TCP {DROP_TIMER | PROBE_TIMER} ***seconds***
SET BG_TCP {SEND | RECEIVE} ***bytes***
SET BG_UDP {SEND | RECEIVE} ***bytes***
SET BG_RAW {SEND | RECEIVE} ***bytes***

BG_TCP Parameters and Values

BG_TCP DROP_TIMER ***seconds***

Maximum number of seconds to probe for idle TCP connections before a TCP connection close times out.

BG_TCP PROBE_TIMER ***seconds***

Number of seconds between probes for idle TCP connections. Also indicates the maximum number of seconds before a TCP connection request times out.

BG_TCP SEND ***bytes***

Sets the message queue size for sending TCP messages.

BG_TCP RECEIVE ***bytes***

Sets the message queue size for receiving TCP messages.

BG_UDP Parameters and Values

BG_UDP SEND ***bytes***

Sets the message queue size for sending UDP messages.

BG_UDP RECEIVE ***bytes***

Sets the message queue size for receiving UDP messages.

BG_RAW Parameters and Values

BG_RAW SEND ***bytes***

Sets the message queue size for sending IP messages.

BG_RAW RECEIVE ***bytes***

Sets the message queue size for receiving IP messages.

SET DHCP

Performs the operations listed here (/debug, /newlog, /partnerdown) on the Dynamic Host Configuration Protocol (DHCP) server. Requires SYSPRV or OPER privileges.

To address the DHCP V4 server, use “DHCP4” instead of “DHCP” in the command.

Format

SET DHCP

SET DHCP4

Qualifiers

/DEBUG=*value*

Sets the debug logging level to the given value. The value is a decimal integer that is a bitmask of debugging levels used to select messages to log to the debug log file and OPCOM (if configured). The debugging levels are (in decimal):

1	Severe Errors
3	Warnings
7	Informationals
15	Debug Messages
31	Dump Packets (Formatted)
63	Dump Packets (Hex)

By default, Severe Errors and Warnings are logged.

/NEWLOG

Starts a new debug log file. The existing log file is closed immediately. A new log file is created when the next log message is ready to be written.

/PARTNERDOWN

For DHCP Failover: Causes the DHCP server to transition into Partner Down state, which indicates that its failover DHCP partner is down.

Example

Sets the debug logging level to log severe error, warning, and informational messages.

```
SET DHCP/DEBUG=7
```

SET DOMAINNAME

Sets the local host's domain name. Requires SYSNAM or SYSPRV privilege, and uses the setdomainname Socket Library subroutine.

Note! The TCPware startup command procedure, STARTNET.COM, sets the domain name to the name specified during network configuration.

Format

SET DOMAINNAME *domain-name*

Parameter

domain-name

Domain name or host name of the local host. Must be the name of the local host as other systems within the network know it.

SET FILTER

SET FILTER loads the specified packet filter file and associates the filter list with the specified line(s). SET NOFILTER removes a previously associated filter list from the specified line(s). SET FILTER and SET NOFILTER require OPER privilege.

Formats

SET FILTER ***line[, line...] file [/LOG=logfile/INTERVAL=interval/FORMAT=format]***
SET NOFILTER ***line[, line...]***

Parameters

line

Line ID of the network device.

file

Packet filter file that contains the packet filter list. The default file extension is .DAT.

See Chapter 21, *Packet Filtering*, of the *TCPware for OpenVMS Management Guide* for the format of a packet filter file.

Note! An implicit deny terminates the list of entries in the packet filter file. Therefore, an entry in the list must explicitly permit a datagram. If the file has no entries and you set filtering for a line based on that file, it implicitly filters out all datagrams on that line. You can also filter out all traffic on a line using the command **SET FILTER line NLA0**:.

Qualifiers

/LOG=logfile

/NOLOG

Defines the destination for logged filter activity. This may be a file name or OPCOM to log the information to OPCOM. When logging to OPCOM, the operator console must be enabled with either NETWORK or SECURITY.

/INTERVAL=interval

Sets the logging interval in seconds.

/FORMAT=format

Sets the output format of the logged data. If set to ***normal,*** the output will be the same as displayed via **NETCU SHOW FILTER**

If set to ***comma***, the output will be in comma-separated (CSV) format, which may be imported into a spreadsheet or other program. The file contains a header line (comma-separated) which describes each field.

Examples

1 Sets lines ESA-0 and FZA-0 to check the filters in the TCPWARE:FILTER-1.DAT file.
SET FILTER ESA-0,FZA-0 TCPWARE:FILTER-1.DAT

2 Removes an associated filter list from lines ESA-0 and FZA-0.
SET NOFILTER ESA-0,FZA-0

3 Filters out all traffic on line ESA-0.
SET FILTER ESA-0 NLA0:

SET GATED TRACE

Tells the GateD process to turn on or off various tracing flags. This controls what is placed in the TCPWARE:GATED.LOG file. By default, minimal tracing is done.

Note! The NETCU processing of this command is completed before GateD finishes processing it.

Format

SET GATED TRACE *qualifier*

Qualifiers

/ADVERTISE
/NOADVERTISE

Sets tracing of route advertising.

/ALL

Turns on all tracing.

/DETAILS
/NODETAILS

Sets tracing of all send and receive information.

/RECV_DETAILS
/NORECV_DETAILS

Sets tracing of receive information.

/SEND_DETAILS
/NOSEND_DETAILS

Sets tracing of send information.

/EVENTS
/NOEVENTS

Sets tracing of normal events.

/INTERFACES
/NOINTERFACES

Sets tracing of network interface information.

/NONE

Turns off all tracing.

/PACKETS
/NOPACKETS

Sets tracing of packet sends and receives.

/RECV_PACKETS
/NORECV_PACKETS

Sets tracing of packet receives.

/SEND_PACKETS
/NOSEND_PACKETS

Sets tracing of packet sends.

/PARSING
/NOPARSING

Sets tracing of configuration file parsing.

/POLICY
/NOPOLICY

Sets tracing of policy decisions.

/ROUTING
/NOROUTING

Sets tracing of routing table changes.

/STATES
/NOSTATES

Sets tracing of state machine transitions.

/SYMBOLS
/NOSYMBOLS

Sets tracing of kernel symbols.

/TASKS
/NOTASKS

Sets tracing of task and job functions.

/TIMER
/NOTIMER

Sets tracing of timer functions.

Example

This example tells the GateD process to turn on tracing of policy decisions and turn off tracing of state machine transitions.

```
SET GATED TRACE /POLICY /NOSTATES
```

SET GATEWAY

Defines a default gateway. Requires OPER privilege.

The system uses a default gateway whenever you need to send an IP datagram to a host that is not on a local network and for which no other route is known.

Note! Traffic for a host routes through a default gateway unless a routing table entry exists for that host or its network. You can add entries to the routing table manually (see the ADD command) or you can add them automatically (using ICMP redirect messages from a gateway).

Format

SET GATEWAY *ia [ia...]*

Parameter

ia

Internet address or host name of a default gateway on one of the local networks.

- You can have any number of default gateways. Subsequent SET GATEWAY commands add an additional default gateway. To remove an individual default gateway, use the REM command. To remove all default gateways, use the SET GATEWAY 0.0.0.0 command.

When you use multiple SET GATEWAY commands, TCPware uses the first gateway on the list. If TCPware finds that the gateway is marked possibly down, it goes to the next gateway on the list in a round robin fashion until one responds.

SET INET

Sets the TCP parameters for the INET devices. These commands affect services added using the STREAM protocol.

Formats

SET INET_TCP DROP_TIMER *value*

SET INET_TCP PROBE_TIMER *value*

INET_TCP Parameters and Values

INET_TCP DROP_TIMER *value*

Maximum number of seconds to probe for idle TCP connections before a TCP connection close times out.

INET_TCP PROBE_TIMER *value*

Number of seconds between probes for idle TCP connections. Also indicates the maximum number of seconds before a TCP connection request times out.

SET INTERFACE

Sets interface related parameters and options. The command is only meaningful if used with one or more of the qualifiers.

The /ARP_ , /COMMON_LINK, and /RECEIVE_LIMIT qualifiers are only valid for Ethernet, FDDI, Token Ring, and Classical IP over ATM or LAN Emulation over ATM devices.

The /RECEIVE_LIMIT qualifier is only valid for interfaces that use the VMS Communications Interface (VCI). If issued for other interfaces, the limit is set but not honored. Interfaces that do not implement this support show 0 for the maximum receive packet rate displayed by the SHOW INTERFACE command.

Format

SET INTERFACE *line-id qualifier [qualifier ...]*

Parameter

line-id

Line ID of the interface.

Qualifiers

/ARP_AGE_INTERVAL=*seconds*

Controls how often to check the Address Resolution Protocol (ARP) times. The default is 30 seconds.

/ARP_AGE_LIMIT=*seconds*

Controls how long an unused ARP entry is left in the cache. The default is 600 seconds (10 minutes).

/ARP_WAIT_LIMIT=*seconds*

Controls how long to wait for an initial ARP entry that is unresolved to be removed from the cache, or when a CONFPEND entry times out and is removed from the cache. The default is 20 seconds, which translates into 30 seconds under most instances because a check is done only every 30 seconds (see /ARP_AGE_INTERVAL).

Note! Use the above /ARP_ qualifiers carefully. They should not normally be changed.

/ARP_ENTRY_LIMIT=*entries*

Controls the size of the ARP cache (number of ARP entries) for an interface. The default is 512 entries.

/COMMON_LINK=*line-ids*

The /COMMON_LINK qualifier works for systems that have multiple interfaces on a common Ethernet, FDDI, or Token Ring cable. The system manager configures this support using the following new NETCU SET command:

```
$ NETCU SET INTERFACE line-id/COMMON_LINK=(line-id,line-id,...)
```

With this command TCPware adds ARP entries for each device into the other device's ARP caches and internally links the interfaces together. A performance benefit of this linking occurs if data is to be transmitted on an interface that happens to be busy, TCPware assigns the data to the least busy linked interface for transmission.

This linking also provides a level of redundancy. If a linked interface is shut down using NETCU STOP/IP or if a fatal error is detected with the interface and an automatic restart can not be attempted, then any routing table entries or pseudo devices associated with the shut down interface will be failed over to one of the common link interfaces.

Note! If failover does occur, the interface is removed from the list of interfaces on the common link. If the interface is restarted, you must re-issue the NETCU SET INTERFACE/COMMON_LINK command.

Restrictions:

- The joined interfaces must be connected to the same cable.
- The joined interfaces must have the same MTU.
- The NETCU DEBUG/IP command shows the interface that a write is queued to. However, with linked interfaces, the datagram might actually be transmitted from a linked interface.
- If an interface on the common link is shut down and restarted via the NETCU START/IP command, you must re-issue the NETCU SET INTERFACE/COMMON_LINK command to rejoin the interfaces.

  It is also possible that when the interface is restarted some ARP entries for the interface may remain in other interfaces' ARP caches leading to a "Duplicate IP address!" message on the console. If the address reported is for another interface on the same machine, you can ignore this warning.

/RECEIVE_LIMIT=*packets-per-second*

Sets the receive packet rate to the specified limit. Can be used to impose a limit on the number of packets to be received per second on an interface. If more than the specified number of packets are received in any one second period, the additional packets are dropped and, in some cases, an OPCOM message is generated (see below). If the value is set to 0, limiting is turned off (the default).

While you should not normally use a limit, you can in some situations do so where the network is unstable or prone to packet storms. In these cases, you need to determine an appropriate normal packet rate so as to determine the proper receive limit.

Use the SHOW INTERFACE command to display the packet rate limit and maximum receive packet rate values. The maximum receive packet rate can be useful in determining an appropriate limit for a system.

The OPCOM message Warning - maximum receive packet rate exceeded on line line-id (rate packets/second) is generated only when both the limit and previous maximum rate are exceeded. TCPware keeps a maximum rate for each interface and SET resets this rate.

The line ID for the offending interface is displayed in numeric form. To convert this to an ASCII line ID, use the SHOW FILTER numeric-id command to display the corresponding ASCII line ID, or see (Line ID Values) in Chapter 5, *IPDRIVER Services*, of the *TCPware for OpenVMS Programmer's Guide*.

Example

The SET INTERFACE command in this example resets the receive packet rate for the SVA-0 interface to 400 packets/second, with a resulting maximum receive packet rate change from 484 to 309 packets/second. The ARP entry limit parameter was reset to 1024 entries.

1
```
SHOW INTERFACE SVA-0
For Network Line SVA-0:
No receive packet rate limit has been set.
The maximum receive packet rate was 484 packets/second.
The ARP entry limit is 512 entries.
The ARP age check interval is 30 seconds.
The ARP entry age limit is 600 seconds.
The ARP entry wait limit is 20 seconds.
```

2
```
SET INTERFACE SVA-0 /RECEIVE_LIMIT=400 /ARP_ENTRY_LIMIT=1024
SHOW INTERFACE SVA-0
For Network Line SVA-0:
The receive packet rate limit is set at 400 packets/second.
The maximum receive packet rate was 309 packets/second.
The ARP entry limit is 1024 entries.
```

```
  The ARP age check interval is 30 seconds.
  The ARP entry age limit is 600 seconds.
  The ARP entry wait limit is 20 seconds.
```

3 **`SET INTERFACE EWA-0 /COMMON_LINK=(EWA-1, PSD-0)`**

SET IPS

Enables or disables line-specific or system-specific processing of DoD Security Options (IPSO). Requires OPER privilege.

Format

SET IPS *{ /DEBUG=n* | */RELOAD* | */RESTART* | */START* | */STOP }*

Qualifiers

/DEBUG=n

Change the debug level for the server. Levels above 4 should never be set without instructions from Process Software.

/RELOAD

Re-read and parse the configuration files. Note that this will not wipe out existing state (event and rule) information; it will simply update it so no potential filter information will be lost.

/RESTART

Stop and restart the FILTER_SERVER process. All existing event and rule information will be lost and reloaded from the configuration file.

/START

Start the FILTER_SERVER process if it's not already running.

/STOP

Stop the FILTER_SERVER process from running. All existing event and rule information will be lost.

Examples

```
$ NETCU SET IPS /DEBUG=3
```

This causes the debug level of the server to be set to 3.

SET IPSO

Enables or disables line-specific or system-specific processing of DoD Security Options (IPSO). Requires OPER privilege.

Format

SET [NO]IPSO *{ /LINE | /SYSTEM }*

Qualifiers

/LINE[=*(line-id, line-id ...)]*

Defines the line or set of lines for which to set security options. (Lines are equivalent to ports or network interfaces, such as SVA-0.) Use parentheses for multiple lines separated by commas. If you omit line-id, the SET IPSO command affects all lines. You must use /LINE if you do not use
/SYSTEM.

/[IN_ | OUT_]LABEL=(LEVEL=*(min-level[,max-level])* -
,AUTHORITY=*{(auth1[,auth2,...]) | ANY | NONE})*

Sets the minimum and maximum security levels and list of authorities for incoming or outgoing datagrams. /IN_LABEL specifies a label for incoming datagrams. /OUT_LABEL specifies a label for outgoing datagrams. /LABEL by itself specifies a label for both incoming and outgoing datagrams. Use parentheses for multiple parameters separated by commas.

LEVEL sets the single (if just min-level) or minimum and maximum security levels. Use parentheses if setting both min-level and max-level separated by a comma. Valid security levels appear in Table 2-6. Specify the level either by its name (such as Top_Secret) or hexadecimal value (such as %X3D). If you omit the LEVEL keyword (or, for that matter, the entire /LABEL type qualifier), the default level is Unclassified.

Table 2-6 IPSO Security Levels

Security Level	**Hexadecimal Value**
Top_Secret	%X3D
Secret	%X5A
Confidential	%X96
Unclassified	%XAB

AUTHORITY sets a protection authority (authority) or a list of authorities. Use parentheses for multiple authorities separated by commas. The predefined authorities appear in Table 2-7. Specify the authority either by its name (such as GENSER) or its hexadecimal value (such as %X80).

Table 2-7 IPSO Protection Authorities

Protection Authority	**Hexadecimal Value**	**Point of Contact**
GENSER	%X80	Designated Approving Authority per DOD 5200.28
SIOP-ESI	%X40	DoD Joint Chiefs of Staff
SCI	%X20	Director of Central Intelligence
NSA	%X10	National Security Agency
DOE	%X08	Department of Energy

A single *authority* field can also be in the form ***"auth1+auth2+..."*** (such as "GENSER+SCI"), with a plus sign (+) between values embedded in quotes. Alternatively, you can use the logically OR'd hexadecimal value of the combined authorities (such as %X30 for "SCI+NSA"), or you can use the site-specific value from the TCPWARE:IPSO_AUTHORITIES. file.

An AUTHORITY value of ANY means that the port will accept all authority fields in datagrams. If you omit the AUTHORITY keyword (or, for that matter, the entire /LABEL type qualifier), the default is a null authority (NONE).

/SYSTEM

Specifies that the parameters on the command line are SYSTEM parameters. If set, these parameters are the first ones tested on outgoing datagrams and the last ones tested on incoming datagrams destined for the host. You must use /SYSTEM if you do not use /LINE.

/ERROR_LABEL=*{(LEVEL=level, AUTH={auth | NONE}) | NONE}*

Sets labels for ICMP error messages to allow originators of out-of-range datagrams to receive these messages. Set a single level and single authority only. If omitted, the default is LEVEL=Unclassified and AUTHORITY=NONE. /ERROR_LABEL=NONE means that the system should not return ICMP errors.

/EXTENDED_ALLOWED[=([NO]IN, [NO]OUT)] (default)
/NOEXTENDED_ALLOWED[=(IN, OUT)]

/EXTENDED_ALLOWED specifies that you want Extended Security Option fields allowed on incoming or outgoing datagrams. You can selectively disallow security options using the NOIN and NOOUT keywords, or disallow them more generally using /NOEXTENDED_ALLOWED. The default is /EXTENDED_ALLOWED=(IN, OUT).

/FIRST
/NOFIRST (default)

Specifies that the IPSO Basic Option be the first option in the datagram header on outgoing datagrams. Some security systems require this.

If you previously specified /STRIP on a line, make sure to /NOSTRIP before using /FIRST. You cannot use /FIRST with /STRIP in a single command.

/RECEIVE_IMPLICIT_LABEL=*{(LEVEL=level, AUTHORITY=auth -*

[, {REQUIRED | NOREQUIRED}]) | NONE}

Associates an implicit label with a received datagram. Use a single level and single authority only. REQUIRED specifies that you require a label and not to use an implicit one. NOREQUIRED specifies that you do not require a label and to use an implicit one. The default is NONE, which is Unclassified and a null authority.

/TRANSMIT_IMPLICIT_LABEL=*{(LEVEL=level, AUTHORITY=auth -*
[, {ADD | NOADD}][, {REQUIRED | NOREQUIRED}]) |NONE}

Associates (or adds) an implicit label with a transmitted datagram. Use a single level and single authority only. See /RECEIVE_IMPLICIT_LABEL for a description of keywords and values.

The additional ADD keyword ensures that you actually add the basic security option containing this label to the datagram header.

If you previously specified /STRIP on a line, make sure to /NOSTRIP before using /TRANSMIT_IMPLICIT. You cannot use the ADD keyword with /TRANSMIT_IMPLICIT together with the /STRIP qualifier in a single command.

/STRIP
/NOSTRIP (default)

/STRIP strips security options from the datagram header on outgoing datagrams. Useful for routers and forwarding datagrams on which you do not want to impose security restrictions. Be careful using /STRIP if you want to have further IPSO checks performed.

Examples

1 Sets the IPSO system parameters with a security level of Secret and a protection authority of DOE for both incoming and outgoing datagrams.

```
SET IPSO /SYSTEM /LABEL=(LEVEL=SECRET, AUTHORITY=DOE)
```

2 Sets a Secret security level and a DOE protection authority for incoming labeled datagrams on lines SVA-0 and ENA-0.

```
SET IPSO /LINE=(SVA-0,ENA-0) /IN_LABEL=(LEVEL=SECRET, AUTHORITY=DOE)
```

3 Specifies that all incoming datagrams on line SVA-0 should have a Secret security level and a protection authority of either SCI+NSA or just DOE.

```
SET IPSO /LINE=SVA-0 /IN_LABEL=(LEVEL=SECRET, AUTHORITY=("SCI+NSA",DOE))
```

4 Identical to the previous example except that the command uses hexadecimal values for the level and authorities.

```
SET IPSO /LINE=SVA-0 /IN_LABEL=(LEVEL=%X3D, AUTHORITY=(%X30,%X08))
```

5 Sets an error label value for ICMP error messages in response to out-of-range datagrams. Note that you can specify only one level and one authority.

```
SET IPSO /ERROR_LABEL=(LEVEL=SECRET, AUTHORITY=DOE)
```

6 Specifies that any unlabeled transmitted datagrams implicitly use a "Secret DOE" label and to process any unlabeled received datagrams with an "Unclassified Null Authority" label.

```
SET IPSO /LINE=SVA-0 /TRANSMIT_IMPLICIT_LABEL=(LEVEL=SECRET, AUTHORITY=DOE)
/RECEIVE_IMPLICIT_LABEL=NONE
```

7 Similar to example 6 except that this actually adds a basic security option with the specified label to the transmitted datagram.

```
SET IPSO /LINE=SVA-0 /TRANSMIT=(LEVEL=SECRET, AUTHORITY=DOE, ADD)
/RECEIVE=NONE
```

8 Specifies requiring a label and not using an implicit one.

```
SET IPSO /LINE=SVA-0 /RECEIVE_IMPLICIT_LABEL=REQUIRED
```

9 Specifies not to process datagrams with Extended Security Option fields. The default is /EXTENDED_ALLOWED.

```
SET IPSO /LINE=SVA-0 /NOEXTENDED_ALLOWED
```

SET KERBEROS_PASSWORD

For Kerberos users. Changes your Kerberos password.

Note! If you change your Kerberos password, your ticket-granting ticket (TGT) is deleted from your ticket file. You need to create a new TGT using the GET command.

SET KERBEROS_PASSWORD is equivalent to the UNIX command *kpasswd*.

Format

SET KERBEROS_PASSWORD *[username [instance]]*

Old password for username: ***old-password***
New password for username: ***new-password***
Verifying, please re-enter: ***new-password***

Parameters

username

Kerberos username for which to change the Kerberos password. If omitted, the OpenVMS username under which the user logged in is used. Converted to lowercase unless you enclose it in double quotes.

instance

Usually omitted for a general Kerberos user but can be the name of the machine from which you can obtain ticket-granting tickets and service tickets. Specify admin for an administrative user. (See your Kerberos administrator to determine your Kerberos instance.) Converted to lowercase unless you enclose it in double quotes.

old-password
new-password

Old and new user passwords. Converted to lowercase unless you enclose them in double quotes.

Example

Changes the Kerberos password for user persephone.

```
SET KERBEROS_PASSWORD PERSEPHONE
Old password for 'persephone':
New password for 'persephone':
Verifying, please re-enter:
```

SET LOG

Sets the NETCP file for logging Network Control Program (NETCP) activity. When TCPware starts, it automatically logs to the TCPWARE:NETCP.LOG file. SET NOLOG stops NETCP logging. If no logging is set, SET LOG resets NETCP logging to another log file.

SET LOG/FTP/NEW

Causes FTP_LISTENER to open a new log file without being restarted.

SET LOG /NFS

Sets the NFSSERVER file for logging NFS server activity. When TCPware starts, it automatically logs to the TCPWARE:NFSSERVER.LOG file. SET NOLOG /NFS stops NFSSERVER logging. If no logging is set, SET LOG /NFS resets NFSSERVER logging to another log file.

SET NOLOG/FTP

Causes FTP_LISTENER to stop logging anonymous connection information.

Format

SET LOG
SET NOLOG
SET LOG/FTP/NEW
SET LOG /NFS
SET NOLOG/FTP
SET NOLOG /NFS

Qualifiers

/NEW [*file*]

Closes the current NETCP log file and creates a new revision of that file. If a filename is indicated, the new log file name will be used for logging.

/NEW/NFS [*file*]

Closes the current NFSSERVER.LOG file and creates a new revision of that file. If a filename is indicated, the new log file name will be used for logging.

/NEW/FTP *file*

Closes the current FTP_LISTENER.LOG file and opens a new file with the specified name.

Examples

- Closes the current NETCP log file (if open) and creates a new NETCP2.LOG file.
  SET LOG /NEW TCPWARE:NETCP2.LOG
- Closes the current NETCP log file and creates a new revision of that file.
  SET LOG /NEW
- Closes the current NFSSERVER log file (if open) and creates a new NFSSERVER2.LOG file.
  SET LOG /NEW /NFS TCPWARE:NFSSERVER2.LOG
- Closes the current NFSSERVER log file and creates a new revision of that file.
  SET LOG /NEW /NFS

SET MASTER_PASSWORD

Used by the Kerberos master administrator. Changes the Kerberos master password.

This command copies the contents of the current Kerberos database (or the contents of the alternate Kerberos database if the /KDBFILE qualifier is used) into a new ASCII text file (PRINCIPAL.TXT, located in your local directory). This new file also contains the new Kerberos master password.

Use LOAD KDB to load this new ASCII file into the Kerberos database using the old Kerberos password. Verification comes from matching the password typed to the one listed in the "old" Kerberos database.

After loading in the new database, use STASH MASTER_PASSWORD to update the stashed, encrypted Kerberos master password file, TCPWARE:KSTASH.KEY. The master password entered must match the new master password created with SET MASTER_PASSWORD.

Requires OPER or SYSPRV privilege and entry of the master password.

Format

SET MASTER_PASSWORD

Enter Kerberos master password: ***old-master-password***
Verifying, please re-enter: ***old-master-password***
Enter Kerberos master password: ***new-master-password***
Verifying, please re-enter: ***new-master-password***

Parameter

old-master-password

Old Kerberos password used for access to the Kerberos database. Converted to lowercase unless you enclose it in double quotes.

new-master-password

New Kerberos password used for access to the Kerberos database. Converted to lowercase unless you enclose it in double quotes.

Qualifier

/KDBFILE=*file*

Name of an alternate KDB file from which the old master password is verified. The default is TCPWARE:PRINCIPAL.OK.

Example

Changes the Kerberos master password from tigger to pooh (not displayed).

```
SET MASTER_PASSWORD
Enter Kerberos master password: tigger [not displayed]
Verifying, please re-enter: tigger [not displayed]
Enter Kerberos master password: pooh [not displayed]
Verifying, please re-enter: pooh [not displayed]
%TCPWARE_NETCU-I-DORELOAD, do not forget to issue a NETCU LOAD KDB PRINCIPAL.TXT
command to reload the database
```

SET NAMED DEBUG

This command is used for debugging NameD:

Command	**Description**
SET NAMED DEBUG *n*	Sets the debug level. The larger the value of *n*, the more verbose the output. A debug value of 0 sets the debug level to off.

When the server is busy, NETCU sends a message stating that your request has been queued, and it will be acted upon when it is the next one in the queue to be serviced. When the server is not busy, it performs your request while NETCU waits (except for the case of REREAD).

Format

SET NAMED DEBUG

Example

Defines the debug logical.

```
$ NETCU SET NAMED DEBUG 2
%TCPWARE_NETCU-S-NORMAL, normal successful completion
```

SET NAMED MAXIMUM_TTL

This command changes the maximum time-to-live (TTL) that resource records are cached from the default 604800 seconds (1 week) to the value given.

Format

SET NAMED MAXIMUM_TTL *n*
(SET NAMED MAX_TTL *n*)

Parameter

n

is an integer value representing the maximum number of seconds the nameserver should cache a non-authoritative answer.

Example

```
SET NAMED MAXIMUM_TTL 302400
```

SET NAMED MINIMUM_TTL

This command changes the minimum time-to-live (TTL) that resource records are cached from the default of zero (0) seconds to the value given.

Note! It is recommended you use this command only if there is a specific need. This could cause problems in that you may be caching resource records for longer than the authoritative administrator intended.

Format

SET NAMED MINIMUM_TTL *n*
(SET NAMED MIN_TTL *n*)

Parameter

n

is an integer value representing the minimum number of seconds the nameserver should cache a non-authoritative answer.

Example

```
SET NAMED MINIMUM_TTL 0
```

SET OUTGOING_ACCESS_RESTRICTIONS

SET OUTGOING_ACCESS_RESTRICTIONS loads the specified outgoing access restrictions file. The default file specification is TCPWARE:TCPWARE_OUTGOINGRESTRICT.DAT.

Note! An outgoing access restrictions list loaded using this command supersedes any previously existing one.

SET NOOUTGOING_ACCESS_RESTRICTIONS removes the outgoing access restrictions file. Both commands require OPER privilege.

Formats

SET OUTGOING_ACCESS_RESTRICTIONS *file*
SET NOOUTGOING_ACCESS_RESTRICTIONS

Parameter

file

Outgoing access restrictions file. The default file is TCPWARE:TCPWARE_OUTGOINGRESTRICT.DAT. You can locate the file in system-specific directories such as TCPWARE_SPECIFIC.

See Chapter 20, *Access Restrictions*, of the *TCPware for OpenVMS Management Guide* for the format of an outgoing access restrictions file entry. You can also deny all access using the command:

```
SET OUTGOING_ACCESS_RESTRICTIONS NLA0:
```

Examples

1 Loads the BARTRESTRICT.DAT file that contains outgoing access restrictions in the system-specific directories.

```
SET OUTGOING_ACCESS_RESTRICTIONS TCPWARE_SPECIFIC:BARTRESTRICT.DAT
```

2 Restricts all outgoing access on the local system.

```
SET OUTGOING_ACCESS_RESTRICTIONS NLA0:
```

3 Removes all outgoing access restrictions for the local system.

```
SET NOOUTGOING_ACCESS_RESTRICTIONS
```

SET SSH /DEBUG

Sets the debug level.

Format

SET SSH /DEBUG

Parameter

level

Entering zero turns off all debug information in the SSHD.LOG file. Entering a non-zero number turns on debug.

Example

```
$ NETCU SET SSH /DEBUG=2

Debug level now 2
```

Note! Enabling higher levels of debug may have serious performance impacts on a system, as well as consuming significant disk space for logs. Therefore, debug levels higher than 4 should only be used when recommended by Process Software Technical Support.

SET TIMEZONE

Sets the offset from universal time and optional time zone name for the IP layer (used for ICMP timestamp replies). Requires SYSNAM and OPER privilege.

Formats

SET TIMEZONE *+hh[mm[ss]] [name]*
SET TIMEZONE *name*

Parameters

+hh[mm[ss]]

Hours, minutes, and seconds offset from the universal time (UT). Use "+" for east of the central meridian, "-" for west. For example, +0400 is 4 hours east of the central meridian at Greenwich. In another example, Eastern Standard Time (EST) is five hours west of UT, so the offset is -0500.

name

(Optional) Name of the time zone. For example, EDT is for Eastern Daylight time. When using the SET TIMEZONE *name* syntax, use only the following known time zone names:

Time	Time Zone Name
Universal Time	"UT", "UTC" or "GMT"
North American Time	"EST", "EDT", "CST", "CDT", "MST", "MDT", "PST", "PDT"
Military Time	Any single uppercase letter "A" through "Z" except "J." ***Note!*** We do not recommend using this format.

Examples

1 `SET TIMEZONE -0500`

2 `SET TIMEZONE EDT`

3 `SET TIMEZONE +0100 MET`

4 `SET TIMEZONE +0100 BST`

SHOW

Shows the values for a variety of networking parameters. See the SET command for additional details on these parameters.

Format

SHOW *parameter*

Parameters

BACKLOG_DROP_THRESHOLD

Minimum backlog limit required on a listening port for "random" drop to take effect. (See the SET BACKLOG_DROP_THRESHOLD command.)

BACKLOG_LIMIT

Maximum listen backlog allowed for listening ports. (See the SET BACKLOG_LIMIT command.)

BG_TCP {DROP_TIMER | PROBE_TIMER | SEND | RECEIVE}

DROP_TIMER, PROBE_TIMER, SEND, and RECEIVE parameters for BG_TCP devices. (See the SET BG_ commands for details on these parameters.)

BG_UDP {SEND | RECEIVE}

SEND and RECEIVE parameters for BG_UDP devices. (See the SET BG_ commands for details on these parameters.)

BG_RAW {SEND | RECEIVE}

SEND and RECEIVE parameters for BG_RAW (IP) devices. (See the SET BG_ commands for details on these parameters.)

GATEWAY_MTU

Maximum size of TCP segments for connections to non-local hosts. A value of 0 means that TCPware uses the maximum transmission unit (MTU) of the interface to determine the size.

IPDEFAULTTOS

Type-of-service used for all outgoing datagrams that do not explicitly specify a value.

IPDEFAULTTTL

Time-to-live value transmitted in outgoing IP datagrams.

IPMAXFRAGMENTS

Maximum number of fragmented datagrams IPDRIVER holds for reassembly.

IPMAXROUTES

Maximum number of routing table entries allowed by IPDRIVER.

IPMTTL

Default multicast time-to-live value used when sending multicast datagrams directly using IP.

IPREASMTIMEOUT

IP datagram reassembly time-out time (in seconds).

INET_TCP {DROP_TIMER | PROBE_TIMER}

DROP_TIMER and PROBE_TIMER parameters for INET devices. (See the SET commands for details on these parameters.)

SM[_BAK]

Shows the contents of the NFS-OpenVMS Server Network Status Monitor file, SM.DAT (or in the case of SHOW SM_BAK, the backup file, SM_BAK.DAT, that appears after a reboot). Use ADD SM[_BAK] or REMOVE SM[_BAK] to add nodes to or remove nodes from the file. (Do not edit the file directly.)

SHOW SM and SHOW SM_BAK truncate host names at the 120th character so it is good practice to limit names to less than 120 characters when adding hosts to the table.

SUBNETSARELOCAL

Shows if the system treats subnets as being local. A value of 1 means to treat subnets as being local. 0 means not to treat subnets as being local.

TCPDEFAULTTOS

Default type-of-service value used for TCP connections.

TCPDEFAULTTTL

Default time-to-live value used for TCP connections.

TCPPERSIST

TCP persistence timer's initial value (in milliseconds).

TCPRTOMAX

Maximum TCP retransmission time (in milliseconds).

TCPRTOMIN

Minimum TCP retransmission time (in milliseconds)

UDPRECVLIMIT

Default limit of UDP unsolicited receives, or datagrams buffered on a socket if there is no outstanding read before they are dropped.

Qualifier

/OUTPUT=*filespec*

Sends output to the specified file. If omitted, output displays on the terminal screen.

Troubleshooting

```
%TCPWARE_NLM-F-TIMEOUT, device timeout
UDP send timeout
%TCPWARE_NLM-F-TIMEOUT, device timeout
NLM_RPC: Portmapper call failed
```

```
%TCPWARE_NLM-F-NOSUCHNODE, remote node is unknown
NLM_RPC: network error
```

One or more of these messages may indicate that a node being monitored by the NFS-OpenVMS Server Network Status Monitor has gone down or is unreachable. Use the SHOW SM (or SHOW SM_BAK) command as indicated under the SM[_BAK] parameter description.

SHOW ACE_USER

Token Authentication only.

Shows the authenticated users in the TCPware ACE/Client user database (the TCPWARE:ACECLIENT_USER.DAT file). Requires SYSPRV or BYPASS privilege.

To...	**Use This Command**
add a new username to the database	ADD ACE_USER
remove a username from the database	REMOVE ACE_USER
create a new database	CREATE ACE_USER_DATABASE

Format

SHOW ACE_USER *[username]*

Parameter

username

Name of the user to show in the ACE/Client database. If omitted, shows all the users in the database.

Example

Shows a sequence of adding new users to the TCPware ACE/Client user database and showing the results.

```
NETCU>ADD ACE_USER DIAMONDS
NETCU>ADD ACE_USER HEARTS
NETCU>ADD ACE_USER CLUBS
NETCU>ADD ACE_USER SPADES
NETCU>SHOW ACE_USER
TCPware ACE/Client Username Database

Username
---------
CLUBS
DIAMONDS
HEARTS
SPADES
```

SHOW ACCESS_LISTS

Displays all incoming access restrictions lists or a specific list. Requires OPER privilege.

DENY entries usually appear before PERMIT entries for each list number. The exception is when there is a duplicate address (or network part of the address) with a more restrictive address mask, in which case the PERMIT entry comes first.

The Access Denied Message always appears next to the first entry for a list number, although the message may originally have been entered with another item in that list (using ADD ACCESS_LIST /MESSAGE).

Format

SHOW ACCESS_LISTS *[list]*

Parameter

list

Incoming access restrictions list number, from 1 to 65535.

Qualifier

/OUTPUT=*filespec*

Sends output to the specified file. If omitted, output displays on the terminal screen.

Example

Shows access entries for list 16 and prints them in the ACCESS.TXT file.

```
SHOW ACCESS_LISTS 16 /OUTPUT=ACCESS.TXT

TCPware(R) for OpenVMS NETCP Access Lists:
List Condition Internet Address  Address Mask     Access Denied Message
---- --------- ----------------  ---------------  ---------------------
16   DENY      192.168.5.23      255.255.255.255  "access not authorized"
     PERMIT    192.168.45.21     255.255.255.255
     PERMIT    192.168.5.0       255.255.255.0
     PERMIT    192.168.30.0      255.255.255.0
```

SHOW ARP

Displays the entire Address Resolution Protocol (ARP) table for the specified Ethernet, FDDI, or HYPERchannel line. Returns and displays the internet address, its corresponding physical address (or incomplete if the address has not been resolved), and a flags field. The flags field can consist of:

Flags Field	**Description**
PERM	You cannot remove the entry from the table (created using ADD ARP /PERMANENT)
PUBL	Local host can respond to ARP requests for this entry (created using ADD ARP /PUBLISH)
LOCK	ARP messages cannot change the entry's physical address (created using ADD ARP /LOCK)
LASU	Last reference to this entry was a use rather than an update
CONF	Next use of this entry requires confirmation
PEND	Confirmation attempt is pending

The first table entry is for the local host's internet address.

Format

SHOW ARP *line*

Parameter

line

Network device line ID for the ARP table. You can only display one ARP table.

Qualifiers

/HOST_NAMES

Shows host names, if available, instead of IP addresses.

/OUTPUT=*filespec*

Sends output to the specified file. If omitted, output displays on the terminal screen.

Example

This command displays the ARP table for the QNA-0 network device. The Flags entries in this example indicate that the system manager used the /PERMANENT, /PUBLISH, and /LOCK qualifiers to set up the ARP table.

```
SHOW ARP QNA-0
TCPware(R) for OpenVMS Address Resolution Table for Network Line QNA-0:

Internet Address   Physical Address     Flags
----------------   -----------------    ------
192.168.5.21       AA-00-04-00-15-08    PERM, PUBL, LOCK
192.168.5.1        AA-00-04-00-01-08    LASU, PEND
192.168.5.8        AA-00-04-00-08-08    CONF
```

SHOW CONNECTIONS

Displays a list of the currently active internet connections (equivalent to the UNIX netstat -a command). The following information appears for each connection:

- Connection ID — TCP, UDP, INET, or BG device name.
- Receive queue count — Number of bytes in the receive queue.
- Send queue count — Number of bytes in the transmit queue.
- Local host internet address and port number.
- Remote host internet address and port number.
- State — Displayed for TCP connections only. See Table 3-2 in the *TCPware for OpenVMS Programmer's Guide*.

NETCU SHOW CONNECTIONS displays 1024 TCP connections and 512 UDP connections before displaying ???. These characters mean there are more connections than NETCU SHOW CONNECTIONS can print.

Format

SHOW CONNECTIONS

Qualifiers

/ALL (default)
/NOALL

Displays all (/ALL) or does not display (/NOALL) listening connections.

/CONTINUOUS

Display of the information uses the OpenVMS Screen Management Facility, which updates it every two seconds. (NETCU does not highlight areas of change.) Do not use together with /OUTPUT. See the /CONTINUOUS qualifier for the SHOW COUNTERS command for the commands to use in the display.

/HOST_NAMES

Displays the host name for an internet address, if it is available. TCPware ignores /CONTINUOUS if SYS$OUTPUT is not a terminal class device or the terminal is not a scope.

/LOCAL

Includes the address and port for incoming and outgoing connections.

/NUMERIC

Displays port numbers in numeric form. If omitted, NETCU tries to translate these numbers into service names using the TCPWARE:SERVICES. file.

/PID

Displays the process ID associated with each device.

/REMOTE

Includes the address and port for incoming and outgoing connections.

/TCP (default)
/NOTCP

Displays (/TCP) or does not display (/NOTCP) TCP connections.

/UDP (default)
/NOUDP

Displays (/UDP) or does not display (/NOUDP) UDP connections.

/OUTPUT=*filespec*

Sends output to the specified file. If omitted, output displays on the terminal screen. Do not use together with /CONTINUOUS.

SHOW COUNTERS

Displays the TCPDRIVER and UDPDRIVER statistics counters.

Format

SHOW COUNTERS

Qualifiers

/CONTINUOUS

Display of the information uses the OpenVMS Screen Management Facility, which updates it every two seconds. (NETCU does not highlight areas of change.) Do not use together with /OUTPUT. Use the following commands when in the display:

`Ctrl/B`	Scroll display back one line
`Ctrl/B`	Scroll display one line
`Ctrl/W`	Repaint the screen
`Ctrl/C` or **`Ctrl/Z`**	Return to the NETCU> prompt

TCPware ignores /CONTINUOUS if SYS$OUTPUT is not a terminal class device or the terminal is not a scope.

/OUTPUT=*filespec*

Sends output to the specified file. If omitted, output displays on the terminal screen. Do not use together with /CONTINUOUS.

/RESET

Resets the counters after their display. Requires OPER privilege.

Example

For details on the TCP counters in the above example, see the IO$_SENSEMODE | IO$M_RD_COUNT description in Chapter 3, *TCPDRIVER Services*, in the *TCPware for OpenVMS Programmer's Guide*. For details on the UDP counters in the above example, see the IO$_SENSEMODE | IO$M_RD_COUNT descriptions in Chapter 4, *UDPDRIVER Services*, in the *TCPware for OpenVMS Programmer's Guide*.

```
SHOW COUNTERS
TCPware(R) for OpenVMS Counters:
Seconds since zeroed:     1776384
TCP segments transmitted:    2814      TCP segments received:2214
   Delayed ACKS:             1491      Out of sequence:        28
   Window updates:             18      Receive errors:          0
Segments retransmitted:        58      Concatenated RDBs:      10
   Keep-alives/Persists:       56
Transmit errors:                0
Concatenated XDBs:             10

Seconds since zeroed:     1776382
```

```
UDP datagrams transmitted:     15      UDP datagrams received:3008
Transmit errors: 0  Receive errors: 0  Undelivered datagrams: 2923
```

SHOW DHCP

Displays a variety of information about the Dynamic Host Configuration Protocol (DHCP) server and its configuration, depending on the qualifiers specified. The /LEASES qualifier is the default.

To address the DHCP V4 server, use “DHCP4” instead of “DHCP” in the command.

Format

SHOW DHCP
SHOW DHCP4

Qualifier

/ALL

Displays SHOW DHCP/SUBNET output for all subnets in the DHCP server configuration, then it displays brief information about all static assignments.

/CLIENT_IDENTIFIER=*client-id*

Displays details about all leases and static assignments that match the given client ID. Clients can have leases on multiple subnets simultaneously.

/CONFIGURATION

Writes all DHCP server configuration and lease information to a dump file. The default dump file is TCPWARE:DHCPD.DUMP. Use the /OUTPUT qualifier to specify a different dump file.

/HARDWARE_ADDRESS=*hardware-address*

Displays details about all leases and static assignments that match the given hardware address. Clients can have leases on multiple subnets simultaneously.

/IP_ADDRESS=*ip-address*

Displays the current lease binding details for the given IP address. The IP address must be in the dynamic pool. Statically-bound IP addresses are not supported.

/ISKNOWN

After specifying the /ISKNOWN qualifier, specify one of the following:

HOST *hardware-address-or-client-id*
SUBCLASS *class-name subclass-data*

If HOST is specified, shows whether the given hardware address or client identifier is "known", that is if there is a *host* declaration for that hardware address or client identifier. If SUBCLASS is specified, shows whether the given subclass data exists as a subclass within the given class.

/LEASES

For all subnets, displays brief information about the IP addresses that have leases (pending, active, or expired). Statically-assigned IP addresses are not shown. This is the default for the SHOW DHCP command if no qualifiers are specified.

/OUTPUT=*filespec*

Sends output to the specified file. If not specified, output appears on the terminal screen (except for the SHOW DHCP/CONFIGURATION command; see the separate description).

/POOLS

Displays a table showing the number of IP addresses that are available for each IP address pool. An IP address pool corresponds to a shared-network statement, a subnet statement, or a *pool* statement in the DHCP configuration file.

/STATUS

Verifies whether the DHCP server is running and displays a message accordingly.

/SUBNET=*ip-address*

Displays brief information about each IP address in the same shared network as the given IP address. Statically-assigned IP addresses are not shown.

/VERIFY=(option, [option...])

Inspects the syntax of the DHCP server configuration file and optionally the lease file and update file and displays any errors found. By default, the standard DHCP configuration file (TCPWARE:DHCPD.CONF) is checked. The options are as follows:

config[=*filename*]	Specifies the name and location of the configuration file to verify. If not specified, the default configuration file is used.
lease[=*filename*]	Specifies the name and location of the lease file to verify. If the filename is not specified, the default lease file is used (TCPWARE:DHCPD.LEASES). If the *lease* option is not specified, the lease file is not checked.
update[=f*ilename*]	Specifies the name and location of the update file to verify. If the filename is not specified, the default update file is used (TCPWARE:DHCPD.UPDATES). If the *update* option is not specified, the update file is not checked.

/VERSION

Displays the version of the DHCP server.

Examples

1 **SHOW DHCP/VERIFY**

```
Process Software DHCP Server 4.2.5-P1 for TCPWARE
Copyright Process Software. Internet Systems Consortium DHCP Server 4.2.5-P1
Copyright 2004-2013 Internet Systems Consortium.
For info, please visit https://www.isc.org/software/dhcp/
reading config file: tcpware:dhcpd.conf
tcpware:dhcpd.conf line 8: Expecting numeric value
ping-retries no;
             ^
exiting.
```

2 **SHOW DHCP/IP_ADDRESS=10.10.10.100**

```
TCPware(R) for OpenVMS DHCP IP Address Information
IP Address          10.10.10.100
Subnet Mask         255.255.255.0
Default Gateway     10.10.10.1
State               Leased (expired)
Lease Length        300 secs
Lease Obtained      10-Mar-2014 20:29:56 GMT
Lease Expires       10-Mar-2014 20:34:56 GMT (-33 secs)
Hardware Address    11 22 33 44 55 66
Client ID           74 65 73 74
                    "test"
```

3 **SHOW DHCP/ISKNOWN HOST 01:02:03:04:05:06**

```
Host 01:02:03:04:05:06 is known by hardware address
```

4 **SHOW DHCP/SUBNET=10.10.10.100**

```
TCPware(R) for OpenVMS DHCP Configured Addresses on Subnet

Address          Expires (GMT)          Client Address/Identifier
--------         -------------          -------------------------
Shared Network   10.10.10.0
Pool 1
10.10.10.104     <available>
10.10.10.102     <abandoned>
10.10.10.100     <expired>              74 65 73 74        "test"
10.10.10.103     10-Mar-2014 18:49:26   00 00 F8 00 00 BB  "..ø..»"
```

Column	**Content**
Address	Shows the IP address.
Expires	Identifies the date and time the lease expires in Greenwich Mean Time (GMT), also known as Universal Coordinated Time (UTC). If there is no active lease, this column shows the state of the IP address.
Client Address/Identifier	Shows either the hardware address or the client identifier in two-digit hexadecimal groupings followed by the ASCII text equivalent.

5 **SHOW DHCP/POOLS**

```
TCPware(R) for OpenVMS DHCP Address Pool Availability

< Shared Network   Pool     Total  Abandoned  Reserved   Available
< --------------   ----     -----  ---------  --------   ---------
<  local           total      44       5          0          15
<                  1          44       5          0          15
<  10.12.1.0       total      128      2          0          57
<                  1          111      0          0          54
<                  2          11       2          0          0
<                  3          6        0          0          3
```

Pool Heading	**Description**
Shared Network	The name from the *shared-network* statement or the subnet number from the *subnet* statement.
Pool	“Total” for the complete information for the shared network, otherwise a number identifying the pool. You can see which IP addresses are in which pools using the SHOW DHCP/ALL or SHOW DHCP/SUBNET command.
Total	The total number of IP addresses in the pool.
Abandoned	The number of IP addresses in the pool which were found in use on the network when they were thought to be free.
Reserved	If DHCP Safe-failover is in use, the number of IP addresses in the pool reserved for the secondary DHCP server. These addresses are unassigned but reserved for the secondary.
Available	The number of IP addresses in the pool available to be leased.

SHOW DNIP

Displays information about the currently configured DECnet over IP tunnels.

Format

SHOW DNIP

Qualifier

/OUTPUT=*filespec*

Sends output to the specified file. If omitted, output displays on the terminal screen.

Example

The status displayed by this command is the status of the TCP connection associated with the DNIP tunnel. NETCU has no knowledge of the state of the DECnet line and circuit associated with this tunnel. Use the DECnet NCP utility to show information about the DECnet state.

```
SHOW DNIP
TCPware(R) for OpenVMS DECnet-over-IP Tunnels:

DECnet Line  Remote Host      Local Port   Remote Port  Status
-----------  -----------      ----------   -----------  ------
DNIP-0-0     alpha.nene.com   64215        64215        Established
DNIP-0-1     beta.yours.com   777          654          Established
```

SHOW EXPORT

NFS Client and Server. Displays the NFS server's EXPORT database, the filesystem pathnames that the server exports, and any access restrictions that the server imposes on each pathname. If a local file, requires read access to the TCPWARE:NFS_EXPORT.DAT file.

Format

SHOW EXPORT *[server-host]*

Parameter

server-host

NFS server host for which you want to display the EXPORT database. If omitted, NETCU examines the local server's EXPORT database.

Qualifiers

/BINDINGS

Shows the device bindings for the NFS Server, as a device name and 32-bit value.

/FULL

Shows the full range of options. (See the ADD EXPORT command description for details on the qualifiers used for these options.)

/PATH=*"server-path"*

Displays only filesystems matching the specified server path. You can include the standard OpenVMS wildcard characters (* and %). Enclose the pathname in quotation marks (" ").

/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

/UDP

Use UDP (instead of TCP) to contact the remote system for the export list. When using UDP the TCPware RPC processing has a limit of 8800 bytes in the response.

Examples

1 Displays the local NFS server's EXPORT database. If there is no local NFS server, NETCU displays an error message. The display for a local NFS server includes the Directory header for the device and directory to which each exported pathname is equivalent on the local OpenVMS system.

```
SHOW EXPORT
NFS EXPORT Database V5.8 Copyright (c) Process Software

Path        Directory                 Host(s)
----        ---------                 -------
/user       SYS$SYSDEVICE:[USER]
/root       SYS$SYSDEVICE:[000000]
```

2 Displays a remote NFS server's export database. The display for the remote server does not include the Directory header.

```
SHOW EXPORT IRIS.NENE.COM
NFS EXPORT Database V5.8 Copyright (c) Process Software

Server: iris.nene.com

Path          Host(s)
----          -----
/user         lambda.nene.com
/root
```

SHOW FILTER

Displays the current packet filter list for the specified line(s). Requires OPER privilege. The display also includes the number of permitted and denied packet hits so that you can flag potential access violations.

In addition, if the /EXTRACT qualifier is used, the current filters loaded in the kernel for the specified interface are written in packet filter file format to the specified output file.

Format

SHOW FILTER *line[, line...]* [/OUTPUT=<*filespec*>][/EXTRACT=<*filespec*>]

Parameter

line

Line ID of the network device.

Qualifier

/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

/EXTRACT=*filespec*

Writes the list of filters currently loaded in the kernel on the specified interface, to the specified file. The format of the output information is the same as that used as input to the **NETCU SET FILTER <interface><file>** command. If a list of interfaces is specified, only the filters for the first interface are output.

Example

Displays the filters for lines SVA-0. Note that source and destination address masks appear on the second line of each entry. In this partial filter list example, the entries:

- Permit local traffic. The number of packets permitted has been 47.
- Deny UDP datagrams on NFS port 2049. The number of packets denied has been 3.
- Permit TCP datagrams on ports greater than 1023 at a particular destination address. The number of packets permitted has been 11.
- Permit TCP datagrams at the same address on SMTP port 25. The number of packets permitted has been 19.
- Permit UDP datagrams at the same address on DNS port 53. The number of packets permitted has been 12.
- Permit all ICMP datagrams at the same address. The number of packets permitted has been 2.

```
SHOW FILTER SVA-0
TCPware(R) for OpenVMS Packet Filter List for SVA-0:

               Source         Source Destination    Destination
Action   Proto Address/Mask   Port   Address/Mask   Port   Option  Hits
------   ----- -------------  ------ -------------  -----  ------  ----
permit   ip    192.168.5.0           0.0.0.0
               255.255.255.0         0.0.0.0                       47
deny     udp   0.0.0.0               0.0.0.0        eq 2049
               0.0.0.0               0.0.0.0                       3
permit   tcp   0.0.0.0               192.168.5.0    gt 1023
               0.0.0.0               255.255.255.0                 11
permit   tcp   0.0.0.0               192.168.5.0    eq 2519
               0.0.0.0               255.255.255.0                 19
permit   udp   0.0.0.0               192.168.5.0    eq 53\
                 0.0.0.0             255.255.255.0                 12
  permit   icmp  0.0.0.0             192.168.5.0
                 0.0.0.0             255.255.255.0                 2
```

SHOW GATED TRACE

Shows what GateD tracing TCPware is currently doing. There may be a delay of several seconds before the GateD process returns the tracing information.

Format

SHOW GATED TRACE

Example

This example shows how to get the GateD tracing status.

```
SHOW GATED TRACE
     Summary of GateD tracing
---------------------------------------------
State Machine Transitions Logging  is :  'ON'
Internal Events Logging            is :  'ON'
Policy Decision Logging            is :  'ON'
Task Information Logging           is :  'ON'
Timer Logging                      is :  'ON'
Routing Information Logging        is :  'ON'
General Send and Receive Logging   is :  'ON'
General Receive Logging            is :  'ON'
General Send Logging               is :  'ON'
Packet Send and Receive Logging    is :  'ON'
Packet Receive Logging             is :  'ON'
Packet Send Logging                is :  'ON'
Configuration File Parsing Logging is :  'ON'
Route Advertisement Logging        is :  'ON'
Kernel Symbols Logging             is :  'ON'
Network Interface Logging          is :  'ON'
```

SHOW GROUP

NFS Client only.

Displays entries in the client's GROUP database. Requires read access to the TCPWARE:NFS_GROUP.DAT file.

Format

SHOW GROUP *[nfs-group]*

Parameter

nfs-group

NFS group number for which to show database entries. If omitted, NETCU displays entries for all groups on the local client.

Qualifiers

/HOST=*(server[,server...])*

Server host(s) on which the group number is valid. NETCU accepts either host names or internet addresses. Use the parentheses with multiple server specifications.

/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Example

Shows the NFS group number on host IRIS and corresponding OpenVMS group name and value.

```
SHOW GROUP /HOST=IRIS
NFS GROUP Database V6.0 Copyright (c) Process Software

Group    Name     Value      Host(s)
-----    ----     -----      -------
15       USER     [200,*]    IRIS
```

SHOW HOST

Displays the official host name, internet address (or addresses), and alias host names for a host, if found.

Format

SHOW HOST *host[,host...]*

Synonym

FIND HOST *host[,host...]*

Parameter

host

Host name or internet address of the host whose information you want displayed.

Qualifier

/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Example

Displays the official host name, internet address(es), and alias host names for a host.

```
SHOW HOST
_Host name or Internet address: DAISY

Host                DAISY.FLOWER.COM
Internet address    192.168.5.16
```

SHOW INTERFACE

Displays the following information for the specified interface:

- Packet rate limit (if set)
- Maximum rate seen since the interface was started or the last SET command was issued
- Address Resolution Protocol (ARP) entry limit, age check interval, entry age limit, and entry wait limit values
- The interface data rage (Mega bits per second)
- The buffer size (bytes) of the interface.

For details on packet rate and ARP setting, see the SET command.

Format

SHOW INTERFACE *line-id*

Parameter

line-id

Line ID of the interface.

Qualifier

/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Example

This example shows the packet rate limit and maximum receive packet rate for the SVA-0 interface. The subsequent SET command resets the receive packet rate to 400 packets/second. The final SHOW INTERFACE command shows the reset values. The ARP entry limit parameter was reset to 1024 entries.

```
SHOW INTERFACE SVA-0
For Network Line SVA-0:
No receive packet rate limit has been set.
The maximum receive packet rate was 484 packets/second.
The ARP entry limit is 512 entries.
The ARP age check interval is 30 seconds.
The ARP entry age limit is 600 seconds.
The ARP entry wait limit is 20 seconds.

SET INTERFACE SVA-0 /RECEIVE_LIMIT=400 /ARP_ENTRY_LIMIT=1024


SHOW INTERFACE SVA-0
For Network Line SVA-0:
The receive packet rate limit is set at 400 packets/second.
The maximum receive packet rate was 309 packets/second.
The ARP entry limit is 1024 entries.
The ARP age check interval is 30 seconds.
The ARP entry age limit is 600 seconds.
The ARP entry wait limit is 20 seconds.
The linespeed is 100 (Mbps).
The MTU is 1500.
```

SHOW IPS

Write the current FILTER_SERVER configuration to a file. Requires OPER privilege.

Format

SHOW IPS /CONFIG{=*filename*}

If you omit the filename for the /CONFIG qualifier, the output will be written to SYS$DISK:[]FILTER_SERVER.TXT.

Qualifiers

/CONFIG_FILE=filename

Write the configuration information to the specified filename.

Example

Displays the full IPSO information for the system, including counter information.

```
$ netcu show ips/config
$ type filter_server.txt
Filter server snapshot      2-JUN-2014 09:34:42.43

Debug level 6
Block at destination port or system: PORT
Log to:
    OPCOM via OPCOM targets "NETWORK,DEVICES,OPER3,OPER12,SECURITY"
    SNMP trap, specific ID "38", generic ID "24", enterprise string "this is the string"
    Logfile (tcpware:filter_logfile.log)
Component: ftp
         Rule: ftp_invaliduser
              IPV6 address      = FALSE
              Dest address      = 192.168.0.11/32
              Dest port         = 21
              Interface name    = se0
              Max event count   = 10
              Delta time        =    0 00:05:00.00
              Filter durations  = 300  600  1800  3600  -1
              hourly hits       =   0    0    0    0    0    0    0    0
                                    0    0    0    0    0    0    0    0
                                    0    0    0    0    0    0    0    0
              hourly filters    =   0    0    0    0    0    0    0    0
                                    0    0    0    0    0    0    0    0
                                    0    0    0    0    0    0    0    0
         Rule: ftp_userauth
              IPV6 address      = FALSE
              Dest address      = 192.168.0.11/32
              Dest port         = 21
              Interface name    = se0
              Max event count   = 21
              Delta time        =    0 00:03:00.00
              Filter durations  = 300  600  1800  3600  -1
              hourly hits       =   0    0    0    0    0    0    0    0
                                    0    0    0    0    0    0    0    0
                                    0    0    0    0    0    0    0    0
              hourly filters    =   0    0    0    0    0    0    0    0
```

```
                           0    0    0    0    0    0    0    0
                           0    0    0    0    0    0    0    0
Rule: ftp_authfailed
     IPV6 address      = FALSE
     Dest address      = 192.168.0.11/32
     Dest port         = 21
     Interface name    = se0
     Max event count   = 21
     Delta time        =    0 00:01:30.00
     Filter durations  = 300  600  1800  3600  -1
     hourly hits       =   0    0    0    0    0    0    0    0
                           0    0    0    0    0    0    0    0
                           0    0    0    0    0    0    0    0
     hourly filters    =   0    0    0    0    0    0    0    0
                           0    0    0    0    0    0    0    0
                           0    0    0    0    0    0    0    0
Rule: ftp_timeout
     IPV6 address      = FALSE
     Dest address      = 192.168.0.11/32
     Dest port         = 21
     Interface name    = se0
     Max event count   = 21
     Delta time        =    0 00:01:30.00
     Filter durations  = 300  600  1800  3600  -1
     hourly hits       =   0    0    0    0    0    0    0    0
                           0    0    0    0    0    0    0    0
                           0    0    0    0    0    0    0    0
     hourly filters    =   0    0    0    0    0    0    0    0
                           0    0    0    0    0    0    0    0
                           0    0    0    0    0    0    0    0
```

SHOW IPSO

Displays IPSO information on datagrams. Requires OPER privilege.

Format

SHOW IPSO

If you omit all qualifiers, displays basic information for all lines and SYSTEM. You must use the /FULL qualifier to display additional counter information.

Qualifiers

/FULL

Displays additional counter information.

/LINE[=*(line-id, line-id...)]*

Shows the IPSO options for a specific line or lines.

/SYSTEM

Shows the SYSTEM options.

Example

Displays the full IPSO information for the system, including counter information.

```
SHOW IPSO /SYSTEM /FULL
TCPware(R) for OpenVMS IPSO Configuration for line SVA-0:

Label      Level                          Authorities
-----      -----                          -----------
In:        UNCLASSIFIED to SECRET         SIOP-ESI
                                          GENSER
Out:       SECRET to SECRET               C1(DOE+SCI+SIOP-ESI)
Implied
  Receive:   None                         None
  Transmit:  SECRET                       None
 ICMP Error: SECRET                       C1(DOE+SCI+SIOP-ESI)
Label on received datagrams is required
          Incoming datagrams screened by IPSO
              0 contained a BSO
              0 were delivered to receivers
              0 contained extended options
              0 used implicit labeling
              0 were rejected as out-of-range
              0 were rejected due to containing ESO
           3226 lacked a required BSO
          Outgoing datagrams screened by IPSO
             12 contained a BSO
              8 were successfully transmitted
              0 contained extended options
              0 used implicit labeling
              0 were rejected as out-of-range
              0 were rejected due to containing ESO
              0 lacked a required BSO
```

SHOW KACL

Used by the Kerberos master administrator. Shows the Kerberos access control list (KACL) entries for accessing the Kerberos database. Requires OPER or SYSPRV privilege and entry of the Kerberos master password.

Format

SHOW KACL *admin-username instance [realm]*

Enter Kerberos master password: ***master-password***
Verifying, please re-enter: ***master-password***

Parameters

admin-username

Kerberos administrator's username to remove from the Kerberos database. Converted to lowercase unless you enclose it in double quotes.

instance

Enter **admin**, since the username is for an administration user.

realm

Optional Kerberos realm to use instead of the TCPWARE_KERBV4_REALM logical value. Converted to lowercase unless you enclose it in double quotes.

master-password

Kerberos password used for access to the Kerberos database. Converted to lowercase unless you enclose it in double quotes.

Qualifiers

/PROMPT (default)
/NOPROMPT

Specifies whether TCPware prompts you for the master password. /NOPROMPT reads the master password from the file created by the STASH MASTER_PASSWORD command.

Example

Shows the KACLs for Kerberos administrator account persephone, who has ADD, MODIFY, and SHOW privileges to the Kerberos database from any remote host within the hades.com realm.

```
SHOW KACL PERSEPHONE ADMIN HADES.COM
Enter Kerberos master password:
Verifying, please re-enter:

ACL Type     Kerberos user
--------     -------------
ADD          persephone.admin@hades.com
MODIFY       persephone.admin@hades.com
SHOW         persephone.admin@hades.com
```

SHOW KDB

Shows the entries in the Kerberos database (KDB). Requires OPER or SYSPRV privilege and entry of the Kerberos master password.

Format

SHOW KDB *principal [instance]*

Enter Kerberos master password: ***master-password***
Verifying, please re-enter: ***master-password***

Parameters

principal

Kerberos user's login name, or the name of the Kerberos application service provided. Converted to lowercase unless you enclose it in double quotes.

instance

Usually omitted for a general Kerberos user; admin for an administrative user; name of the machine on which the Kerberos application resides for an application service. Converted to lowercase unless you enclose it in double quotes.

master-password

Kerberos password used for access to the Kerberos database. Converted to lowercase unless you enclose it in double quotes.

Qualifiers

/KDBFILE=*file*

Name of the alternate KDB file. The default is TCPWARE:PRINCIPAL.OK.

/PROMPT (default)
/NOPROMPT

Specifies whether TCPware prompts you for the master password. /NOPROMPT reads the master password from the file created by the STASH MASTER_PASSWORD command.

Example

Shows the entry for the Kerberos administrator account persephone in the Kerberos database by reading the master password from the file created by the STASH MASTER_PASSWORD command.

```
SHOW KDB PERSEPHONE ADMIN /NOPROMPT

Name :              persephone
Instance :          admin
Expiration Date :   31-DEC-2099 23:59
Modification Date : 1-FEB-2014 09:21:09
Attributes :        0
Maximum Lifetime :  255
Key Version :       1
```

SHOW KERBEROS USER

For Kerberos administrators. Shows users added to the Kerberos database. The default Kerberos administrator account name is the name of the OpenVMS account using this command. Requires OPER or SYSPRV privilege and entry of the Kerberos administrator's password.

Format

SHOW KERBEROS USER *username*

Administrator password for *admin-account:* ***admin-password***

Parameters

username

Kerberos user's login name. Converted to lowercase unless you enclose it in quotes.

admin-password

Kerberos administrator's password. Converted to lowercase unless you enclose it in quotes.

Qualifier

/ADMINISTRATOR=*admin-username*

Alternate Kerberos administrator name. Converted to lowercase unless you enclose it in quotes. The default name is the current OpenVMS account name, in lowercase.

Example

Shows an entry for user Smith in the Kerberos Server database. persephone is the current Kerberos administrator's OpenVMS account name.

```
show kerberos user "Smith"
Administrator password for 'persephone':
```

SHOW MOUNT

NFS Client and Server.

Displays a list of client hosts that mounted a file system served by a specified NFS server. Returns the mounted directories by the pathnames NETCU uses to export them, not the directory names as the OpenVMS system knows them.

Format

SHOW MOUNT *[server-host]*

Parameter

server-host

NFS server host from which to get the list of mounted file systems. If omitted, NETCU uses the local server.

Qualifier

/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Examples

1 Because the user did not specify the server host name, the system displays the full domain name for the local server ZETA. In this example no client hosts have mounted any of the server file system.

```
SHOW MOUNT
NFS Mount List V5.8 Copyright (c) Process Software

Server: ZETA.nene.com
Path         Host
----         ----
```

2 Displays the list of client hosts and directories by pathnames for mounted file systems served by the specified server IRIS.

```
SHOW MOUNT IRIS
NFS Mount List V5.8 Copyright (c) Process Software

Server: IRIS
Path                Host
----                ----
/sales/records      bart.nene.com
/exported/spool     bart.nene.com
```

SHOW MULTICAST_GROUPS

Displays the joined multicast host group address table for the specified interface or all interfaces.

Format

SHOW MULTICAST_GROUPS *[line-id]*

Parameter

line-id

Line ID of the interface for which to display the table. If omitted, the table includes all active interfaces.

Qualifier

/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Example

Displays the multicast host groups for the SVA-0 Ethernet interface. Note that the RefCnt (reference count) for 224.0.0.1, the all-hosts group address, is -perm-, which means that it is permanent and you cannot remove it.

```
SHOW MULTICAST_GROUPS
TCPware(R) for OpenVMS Multicast Host Groups:

Host Group Address   RefCntLine      Name
------------------   ----------      ----
224.0.0.1            -perm-SVA-0     ALL-SYSTEMS.MCAST.NET
226.1.1.1            1SVA-0?
```

SHOW NETWORKS

Displays the IPDRIVER network information for each line, any active secondary addresses, and the IPDRIVER datagram counters. The network information consists of the following:

SHOW NETWORKS is equivalent to the UNIX netstat -i command.

Format

SHOW NETWORKS

Qualifiers

/CONTINUOUS

Display of the information uses the OpenVMS Screen Management Facility, which updates it every two seconds. (NETCU does not highlight areas of change.) Do not use together with /OUTPUT.

TCPware ignores /CONTINUOUS if SYS$OUTPUT is not a terminal class device or the terminal is not a scope. See the SHOW COUNTERS command for the screen commands to use.

/OUTPUT=*filespec*

Sends output to the specified file. If omitted, output displays on the terminal screen. Do not use together with /CONTINUOUS.

Example

```
SHOW NETWORKS
TCPware(R) for OpenVMS Internet Network Information:
Line  Local Address  Subnet MaskMTU  Xmits  Errs  Recvs  Errs   RBU
----  -------------  --------------  -----  ----  -----  ----   ---
SVA-0 192.168.5.33   255.255.255.0   1500   1     0      1197   0  0
LPB-0 127.0.0.1      255.0.0.0       64512  0     0      0      0  0

Secondary Address    State
-----------------    -----
192.168.5.102        Active, holding cluster lock
192.168.5.101        Inactive, queued for cluster lock
        0    IP datagrams were transmitted, of which
             0 were fragmented
             0 were forwards
             0 were ICMP requests/replies
             0 were IGMP reports
        263  IP datagrams/fragments were received, of which
             0 were fragments
             0 were forwarded
             0 were ICMP requests/replies
             0 were IGMP queries/reports
        259  IP datagrams were delivered to receivers.
```

SHOW OSPF

Queries OSPF routers. You can obtain a wide variety of detailed information from these routers using these commands.

All of the SHOW OSPF commands use a file called TCPWARE:OSPF_DESTS.DAT. This is a file of OSPF destination records. Each record is a single line entry listing the destination IP address, the destination host name, and an optional OSPF authentication key (if the destination activates authentication).

CAUTION! Since the OSPF_DESTS.DAT file may contain authentication information, you should restrict access to it.

Note! To stop the output of this command, enter a **`Ctrl/C`** at the command line.

Format

SHOW OSPF *option*

Options

ADVERTISE ***area-id***
type
ls-id
adv-router
index
/OUTPUT=file
/FILE=file
/TIMEOUT=seconds

Displays link state advertisements. The parameters and qualifiers for SHOW OSPF ADVERTISE are as follows:

Parameter and Qualifier	**Description**
area-id	OSPF area for which the query is directed.

type	The available types are **INTERFACES** — Requests the router links advertisements. Describes the collected states of the router's interfaces. For this request, the ls-id field should be set to the originating router's Router ID. **ROUTERS** — Requests the network links advertisements. Describes the set of routers attached to the network. For this request, the ls-id field should be set to the IP interface address of the network's Designated Router. **NETWORK_ROUTES** — Requests the summary link advertisements describing routes to networks. Describes the inter-area routes and enables the condensing of routing information at area borders. For this request, the ls-id field should be set to the destination network's IP address. **BOUNDARY_ROUTES** — Requests the summary link advertisements describing routes to AS boundary routers. Describes the inter-area routes and enables the condensing of routing information at area borders. For this request, the ls-id field should be set to the Router ID of the described AS boundary router. **EXTERNAL_ROUTES** — Requests the AS external link advertisements. Describes routes to destinations external to the AS. For this request, the ls-id field should be set to the destination network's IP address.
ls-id	See the type parameter.
adv-route	Router ID of the router that originated this link state advertisement.
index	Indexes into a file of OSPF destination records.
/OUTPUT=*file*	Name of an output file to write the results to.
/FILE=*file*	Alternate file of OSPF destination records to use.
/TIMEOUT=*seconds*	Interval to wait for a response. Default is 20 seconds.

AS ***index***
/OUTPUT=file
/FILE=file
/TIMEOUT=seconds

Shows the Autonomous System (AS) external database entries. This table reports the advertising router, forwarding address, age, length, sequence number, and metric for each AS external route. The parameters and qualifiers for SHOW OSPF AS are as follows:

index	Indexes into a file of OSPF destination records.
/OUTPUT=*file*	Name of an output file to write the results to.
/FILE=*file*	Alternate file of OSPF destination records to use.
/TIMEOUT=*seconds*	Interval to wait for a response. Default is 20 seconds.

DESTINATIONS/OUTPUT=*file*

/FILE=*file*

This command displays the list of destinations and their indices described in an OSPF destination records file. The parameters and qualifiers for SHOW OSPF DESTINATIONS are as follows:

/OUTPUT=*file*	Name of an output file to write the results to.
/FILE=*file*	Alternate file of OSPF destination records to use.

ERRORS ***index***
/OUTPUT=file
/FILE=file
/TIMEOUT=seconds

Shows the error log. This reports the different error conditions that can happen between OSPF routing neighbors and shows the number of occurrences for each. The parameters and qualifiers for SHOW OSPF ERRORS are as follows:

index	Indexes into a file of OSPF destination records.
/OUTPUT=*file*	Name of an output file to write the results to.
/FILE=*file*	Alternate file of OSPF destination records to use.
/TIMEOUT=*seconds*	Interval to wait for a response. Default is 20 seconds.

HOPS ***index***
/OUTPUT=file
/FILE=file
/TIMEOUT=seconds

Shows the set of next hops for the OSPF router being queried. The parameters and qualifiers for SHOW OSPF HOPS are as follows:

index	Indexes into a file of OSPF destination records.
/OUTPUT=*file*	Name of an output file to write the results to.
/FILE=*file*	Alternate file of OSPF destination records to use.
/TIMEOUT=*seconds*	Interval to wait for a response. Default is 20 seconds.

INTERFACES ***index***
/OUTPUT=file
/FILE=file
/TIMEOUT=seconds

Displays all interfaces. This shows all the interfaces configured for OSPF. The information includes the area, interface IP address, interface type, interface state, cost, priority and the IP address of the DR and BDR of the network. The parameters and qualifiers for SHOW OSPF INTERFACES are as follows:

index	Indexes into a file of OSPF destination records.
/OUTPUT=*file*	Name of an output file to write the results to.
/FILE=*file*	Alternate file of OSPF destination records to use.
/TIMEOUT=*seconds*	Interval to wait for a response. Default is 20 seconds.

LOG ***index***
/OUTPUT=file
/FILE=file
/TIMEOUT=seconds

Shows the cumulative log. This log includes input and output statistics for monitor requests, hellos, database descriptions, link state updates, and link state ACK packets. Area statistics are provided that describe the total number of routing neighbors and number of active OSPF interfaces. Routing table statistics are summarized and reported as the number of intra-area routes, inter-area routes, and AS external database entries.

The parameters and qualifiers for SHOW OSPF LOG are as follows:

index	Indexes into a file of OSPF destination records.
/OUTPUT=*file*	Name of an output file to write the results to.
/FILE=*file*	Alternate file of OSPF destination records to use.
/TIMEOUT=*seconds*	Interval to wait for a response. Default is 20 seconds.

NEIGHBORS ***index***
/OUTPUT=file
/FILE=file
/TIMEOUT=seconds
/RETRANSMIT

This command shows all OSPF routing neighbors. The information shown includes the area, local interface address, router ID, neighbor IP address, state and mode. The parameters and qualifiers for SHOW OSPF NEIGHBORS are as follows:

index	Indexes into a file of OSPF destination records.
/OUTPUT=*file*	Name of an output file to write the results to.
/FILE=*file*	Alternate file of OSPF destination records to use.
/TIMEOUT=*seconds*	Interval to wait for a response. Default is 20 seconds.
/RETRANSMIT	Displays the retransmit list of neighbors.

ROUTING ***index***
/OUTPUT=file
/FILE=file
/TIMEOUT=seconds

Shows the OSPF routing table. This table reports the AS border routes, area border routes, summary AS border routes, and the networks managed using OSPF. The parameters and qualifiers for SHOW OSPF ROUTING are as follows:

index	Indexes into a file of OSPF destination records.
/OUTPUT=*file*	Name of an output file to write the results to.
/FILE=*file*	Alternate file of OSPF destination records to use.
/TIMEOUT=*seconds*	Interval to wait for a response. Default is 20 seconds.

STATE ***index***
/OUTPUT=file
/FILE=file
/TIMEOUT=seconds
/RETRANSMIT

Shows the link state database (except for ASEs). This describes the routers and networks making up the AS. The parameters and qualifiers for SHOW OSPF STATE are as follows:

index	Indexes into a file of OSPF destination records.
/OUTPUT=*file*	Name of an output file to write the results to.
/FILE=*file*	Alternate file of OSPF destination records to use.
/TIMEOUT=*seconds*	Interval to wait for a response. Default is 20 seconds.
/RETRANSMIT	Displays the retransmit link state database.

Examples

1 Displays the OSPF cumulative log for index 1 in the OSPF_DESTS.DAT file.

```
SHOW OSPF LOG 1
          Source <<192.168.5.31     izar.nene.com>>
IO stats
        Input  Output   Type
             2       0  Monitor request
             0       0  Hello
             0       0  DB Description
             0       0  Link-State Req
             0       0  Link-State Update
             0       0  Link-State Ack
       ASE:  0 checksum sum 0

       LSAs originated: 39   received: 0
                Router: 39

       Area 0.0.0.0:
                Neighbors: 0    Interfaces: 0
                Spf: 1 Checksum sum CE9D
                DB: rtr: 1 net: 0 sumasb: 0 sumnet: 0

Routing Table:
         Intra Area: 0   Inter Area: 0     ASE: 0
```

2 Displays the OSPF interface log for index 1 in the OSPF_DESTS.DAT file.

```
SHOW OSPF INTERFACE 1
          Source <<192.168.5.31      izar.nene.com>>
IO stats
        Input  Output   Type
             6       0  Monitor request
             0       0  Hello
             0       0  DB Description
             0       0  Link-State Req
             0       0  Link-State Update
             0       0  Link-State Ack
        ASE: 0 checksum sum 0

        LSAs originated: 39   received: 0
                 Router: 39
        Area 0.0.0.0:
                 Neighbors: 0    Interfaces: 0
                 Spf: 1  Checksum sum CE9D
                 DB: rtr: 1 net: 0 sumasb: 0  sumnet: 0

Routing Table:
        Intra Area: 0   Inter Area: 0   ASE: 0
```

3 Displays the OSPF destination records in the OSPF_DESTS.DAT file.

```
SHOW OSPF DESTINATIONS
1: 192.168.5.31    izar.nene.com
```

4 Displays the OSPF link state database log for index 1 in the OSPF_DESTS.DAT file.

```
SHOW OSPF STATE 1
          Source <<192.168.5.31    izar.nene.com>>
LS Data Base:
Area: 0.0.0.0
Type LinkState ID   AdvRouter    Age  Len Sequence Metric Where
----------------------------------------------------------------
Rtr  192.168.5.31   192.168.5.31 986  24  80000027 0      SpfTree
```

5 Displays the OSPF next hops log for index 1 in the OSPF_DESTS.DAT file.

```
SHOW OSPF HOPS 1
          Source <<192.168.5.31    izar.nene.com>>
Next hops:

Address         Type      Refcount  Interface
---------------------------------------------------------
192.168.5.31    Direct    1         192.168.5.31    SVA-0
```

6 Displays the OSPF error log for index 1 in the OSPF_DESTS.DAT file.

```
SHOW OSPF ERRORS 1
        Source <<192.168.5.31  izar.nene.com>>
Packets Received:
   3: Monitor request              0: Hello
   0: DB Description               0: Link-State Req
   0: Link-State Update            0: Link-State Ack

Packets Sent:
   0: Monitor response             0: Hello
   0: DB Description               0: Link-State Req
   0: Link-State Update            0: Link-State Ack

Errors:
   0: IP: bad destination          0: IP: bad protocol
   0: IP: received my own packet   0: OSPF: bad packet type
   0: OSPF: bad version            0: OSPF: bad checksum
   0: OSPF: bad area id            0: OSPF: area mismatch
   0: OSPF: bad virtual link       0: OSPF: bad authentication type
   0: OSPF: bad authentication key 0: OSPF: packet too small
   0: OSPF:packet size > ip length 0: OSPF: transmit error
   0: OSPF: interface down         0: OSPF: unknown neighbor
   0: HELLO: netmask mismatch      0: HELLO: hello timer mismatch
```

```
0: HELLO: dead timer mismatch   0: HELLO: extern option mismatch
0: HELLO: router id confusion   0: HELLO: virtual neighbor unknown
0: HELLO: NBMA neighbor unknown 0: DD: neighbor state low
0: DD: router id confusion      0: DD: externoption mismatch
0: DD: unknown LSA type         0: LS ACK: neighbor state low
0: LS ACK: bad ack              0: LS ACK: duplicate ack
0: LS ACK: Unknown LSA type     0: LS REQ: neighbor state low
0: LS REQ: empty request        0: LS REQ: bad request
0: LS UPD: neighbor state low   0: LS UPD: newer self-gen LSA
0: LS UPD: LSA checksum bad     0: LS UPD:received less recent LSA
0: LS UPD: unknown LSA type
```

SHOW OUTGOING_ACCESS_RESTRICTIONS

Displays all outgoing access restrictions. Requires OPER privilege. You can also direct output to a file that you can subsequently load as a new outgoing access restrictions file.

Format

SHOW OUTGOING_ACCESS_RESTRICTIONS

Qualifier

/OUTPUT=*file*

File output for the outgoing access restrictions. TCPware formats the information in the output file so that you can use it as an input file for the SET OUTGOING_ACCESS_RESTRICTIONS command.

See Chapter 20, *Access Restrictions*, in the *TCPware for OpenVMS Management Guide* for the format of an outgoing access restrictions file entry.

Example

Logs all connections, denies local users access to the SMTP port (25) over the network, and only permits general outgoing access for users with the INTERNET_USER rights identifier.

```
SHOW OUTGOING_ACCESS_RESTRICTIONS
TCPware(R) for OpenVMS Outgoing Access Restrictions List

Actions  Userid        Destination  Address  Destination Mask  Port
-------  ------        --------------------  ----------------  ----
LOG      *             0.0.0.0               0.0.0.0
DENY     *             0.0.0.0               0.0.0.0           EQ 25
PERMIT   INTERNET_USER 0.0.0.0               0.0.0.0
```

SHOW PROXY

NFS Client and Server.

Displays the contents of the PROXY database. Requires read access to the TCPWARE:NFS_PROXY.DAT file.

Format

SHOW PROXY *[vms-username]*

Parameter

vms-username

OpenVMS account entries you want to display. If omitted, the system displays the contents of the PROXY database determined by the qualifiers listed below.

Qualifiers

/HOST=*(server[,server...])*

Displays the PROXY entries restricted to the specified server host(s) only, or for which there are no host restrictions given. Specify one or more server hosts (if multiple, separate by a comma and use the parentheses).

/GID=*gid*

NFS user's group ID (GID). NETCU displays only entries containing the specified GID.

/UID=*uid*

NFS user's ID (UID). The system displays only entries containing the specified UID.

/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Example

Displays the PROXY database entries for user SMITH.

```
SHOW PROXY SMITH
NFS PROXY Database V5.8 Copyright (c) Process Software

Username    UID    GID    Host(s)
--------    ---    ---    -------
SMITH       100    101
```

SHOW RIP

Used to request all routes known by a RIP gateway. The routing information in any routing packets returned is displayed numerically and symbolically. This command is intended to be used as a tool for debugging gateways, not for network management.

Note! To stop the output of this command, enter a **`Ctrl/C`** at the command line.

Format

SHOW RIP *gateway-ia*

Parameter

gateway-ia

Internet address or name of the gateway to be queried.

Qualifiers

/AUTHENTICATION=*authkey*

Authentication password to use for queries. If specified, an authentication type of **SIMPLE** is used. The default authentication type is **NONE**.

/NONAME

Prevents the responding host's address from being looked up to determine the symbolic name.

/POLL

Requests information from the gateway's routing table. This is the default. If there is no response to the /POLL qualifier, the /REQUEST qualifier is tried.

/REQUEST

Requests information from the gateway's routing table. Unlike the /POLL qualifier, all gateways should support this command. If there is no response, the /POLL qualifier is tried.

/TIMEOUT=*seconds*

Number of seconds to wait for the initial response from a gateway. Default is 5 seconds.

/TRACE

Traces the RIP packets being sent and received by this command.

/V1

Sends the query as a RIP version 1 packet.

/V2

Sends the query as a RIP version 2 packet.

Example

Shows the routers known by RIP gateway 192.33.23.2.

SHOW RIP 192.33.23.2

```
24 bytes from omega1.foobar.com(192.33.23.2):
              net/mask               router        metric   tag
        192.168.5.0/255.255.255.0    192.33.23.1   2        0000
```

SHOW ROUTES

Displays the following internet routing information for each route:

- Destination internet address
- Gateway internet address
- Mask — Destination mask (displayed with /FULL only)
- Flags — Each flag is a one character code. The following list defines each flag:

Flag	**Description**
U =	Route is "up" (functional)
D =	Route may be “down”
N =	Network route
H =	Host route
G =	Gateway — Route uses a specific gateway
I =	Interface route — Route is an actual network interface
L =	Locked — Someone created the route with the /LOCK qualifier
R =	Dynamic route — Someone created the route using an ICMP redirect message
A =	Automatic route — Someone created the route using RIP or RAP
X =	Route marked for delete, will be deleted when no longer referenced

- Reference count — Number of connections currently using the route
- Use count — Number of datagrams transmitted using this route
- Line id — Line identification of the network interface used to send datagrams to this route's destination
- Path_MTU associated with the route (displayed with /FULL only)

SHOW ROUTES is equivalent to the UNIX netstat -r command.

Format

SHOW ROUTES

Qualifiers

/CONTINUOUS

Display of the information uses the OpenVMS Screen Management Facility, which updates it every two seconds. (NETCU does not highlight areas of change.) Do not use together with /OUTPUT. See the SHOW

COUNTERS command for the screen commands to use. TCPware ignores /CONTINUOUS if SYS$OUTPUT is not a terminal class device or the terminal is not a scope.

/FULL

Displays the full routing information.

/HOST_NAMES

Shows host names, if available, instead of IP addresses.

/OUTPUT=*filespec*

Sends output to the specified file. If omitted, output displays on the terminal screen. Do not use together with /CONTINUOUS.

Examples

1 Displays the normal routing information for your current host.

```
SHOW ROUTES
TCPware(R) for OpenVMS Internet Routing Table:

Destination            Gateway         Flags    RefCnt   UseCnt   Line
------------           -------         -----    ------   ------   ----
255.255.255.255        192.168.5.0     UH       0        0        SVA-0
all others (default)   192.168.5.126   UNG      0        665      SVA-0
192.168.5.0            192.168.5.21    UNIL     0        2300     SVA-0
127.0.0.0              127.0.0.1       UNIL     0        0        LPB-0
```

2 Displays the full routing information for your current host.

```
SHOW ROUTES /FULL
TCPware(R) for OpenVMS Internet Routing Table:

Destination            Gateway         Flags    RefCnt   UseCnt   Line
-----------            -------         -----    ------   ------   ----
192.168.142.0          192.168.142.7   UNIL     0        2196     SVA-0
     MASK=255.255.255.0
     PATH_MTU=1500
127.0.0.0              127.0.0.1       UNIL     0        1        LPB-0
     MASK=255.0.0.0
     PATH_MTU=64512
```

SHOW SERVICES

Displays information on the protocols and ports the NETCP master server process services. Table 2-8 describes each piece of information SHOW SERVICES displays.

Table 2-8 Information Displayed by SHOW SERVICES

Output Heading	Provides
Protocol	Protocol name (TCP or UDP).
Port	Service name or number of the port.
Active	Count of how many servers are active for the port (except Server-TELNET).
Limit	Maximum number of servers that can be active for the port.
Connects	Total number of connections made to this service since someone added it.
Errors	Total number of errors associated with the service. (For example, errors result when resources are in sufficient to run the server, or the server image does not exist.) The TCPWARE:NETCP.LOG file logs each connection serviced. You can have this file obtain details on errors, and monitor access and security violations.
Image	Name of the server image.

Format

SHOW SERVICES *[port protocol]*

Parameters

port

Service name or port for which to display information. Accepts any service name defined in the TCPWARE:SERVICES. file. If you specify a port, you must also specify a *protocol*. If you omit both, shows service information for all ports and protocols. Use **0** as a wildcard.

protocol

Protocol for which to display information. Enter **TCP, UDP, STREAM, DGRAM, BG_TCP,** or **BG_UDP**. If you specify a port, you must also specify a *protocol*. If you omit both, NETCP shows service information for all ports and protocols.

Qualifiers

/FULL

Displays complete information for each service.

/NUMERIC

Displays port numbers in numeric form. If omitted, NETCU tries to translate these numbers into service names using the TCPWARE:SERVICES. file.

/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Examples

1 Displays a summary of activity for all ports using the STREAM protocol. This is especially useful for determining if the R Services are running so that you can use RCP.

```
SHOW SERVICES
TCPware(R) for OpenVMS TCP Services:

Protocol  Port     Active  Limit  Connects Errors Image
--------  ----     ------  ------ -------- ------ -----
TCP       discard  0       none   0        0      TCPWARE:DISCARDD
TCP       daytime  0       none   0        0      TCPWARE:DAYTIMED
TCP       telnet   0       none   2        0


SHOW SERVICES 0 STREAM
TCPware(R) for OpenVMS NETCP Services:

Protocol  Port   Active  Limit  Connects  ErrorsImage
--------  ----   ------  -----  --------  -----------
STREAM    exec   0       none   0         0
STREAM    login  0       none   0         0
STREAM    shell  0       none   1         1
```

2 Displays a full summary for the DISCARD service.

```
HOW SERVICES/FULL DISCARD TCP
TCPware(R) for OpenVMS NETCP Services:

Protocol  Port    Active Limit  Connects  Errors  Image
--------  ----    ------ -----  --------  ------  -----
TCP       discard 0      none   0         0       TCPWARE:DISCARDD
                 /ROUTINE=create_server_process
                 /PROCESS_NAME=DISCARDD
                 /LOG
                 /NOLISTEN
                 /INACTIVITY_TIMER=(TIME:30, CHECK_INTERVAL:5)
                 /INPUT=NLA0:
                 /OUTPUT=NLA0:
                 /ERROR=NLA0:
                 /PRIVILEGES=(TMPMBX,NETMBX)
                 /UIC=[SYSTEM]
                 /PRIORITY=4
                 /AST_LIMIT=10
                 /IO_BUFFERED=6
                 /BUFFER_LIMIT=10240
                 /IO_DIRECT=6
                 /ENQUEUE_LIMIT=6
```

```
/FILE_LIMIT=20
/PAGE_FILE=10000
/SUBPROCESS_LIMIT=0
/QUEUE_LIMIT=8
/WORKING_SET=200
/EXTENT=500
/MAXIMUM_WORKING_SET=300
/NOACCOUNTING
```

SHOW SNMP

Displays the SNMP counters maintained by the local host.

Note! This command can only display the local counters. It does not use the SNMP protocol to obtain the counters and therefore cannot display the counters maintained by a remote host.

Format

SHOW SNMP *group[,group...]*

Parameter

group

Can be one or more of **IP, ICMP, MIB_VARIABLE, TCP,** or **UDP** separated by commas.

MIB_VARIABLE[=*variable*]

MIB_VARIABLE returns the value of the variable specified, or the entire MIB tree if no variable is specified. When MIB_VARIABLE is used /HOST can be used to get information from a host other than the one that NETCU is running on. /COMMUNITY is used to specify the SNMP community string; the default value is public.

Qualifier

/COMMUNITY=*community_name*
/HOST=*host_name*

These are only valid when MIB_VARIABLE is specified.
The default value for /HOST is 127.0.0.1 (localhost).

/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Examples

1 Displays the TCP SNMP counters.

```
SHOW SNMP TCP
```

2 Displays the TCP and UDP SNMP counters.

```
SHOW SNMP TCP,UDP
```

SHOW STATISTICS

NFS Server only.

Displays statistics information on the NFS Server, useful in troubleshooting if problems occur. Appends the statistics to the TCPWARE:NAMED.STATS file and appends the memory statistics to the TCPWARE:NAMED.MEMSTATS file. See below for the statistics returned. The Server must be running.

Format

SHOW STATISTICS

Qualifiers

/RESET

Displays the counter information, then resets the counters. Requires OPER privilege.

/TIMES

Displays the additional average and maximum times (in milliseconds) for certain NFS requests listed.

/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Description

The NFS statistics returned by the command are:

Started	Date and time someone started the server.
Uptime	Total amount of time the server has been running.
Memory in use	Total amount of dynamic memory (in bytes) the NFS server uses. This includes memory allocated for the RPC server routines.
Threads	NFS thread counters give the *total* threads available, the *current* number of threads in use, and the *maximum* number of threads that have been in use at one time. These statistics can give an indication of server load. If the *maximum* number of threads in use at one time is equal to the *total* threads available, you may want to increase the number of threads defined by the parameter NFS_THREADS.
Files	File system counters include the number of *opens* and *closes* performed by the server, the number of files *currently open*, and the *maximum* open files at one time since someone started the server. The number of files *currently open* and the *maximum open* files at one time can be an indication of the load on the server.

NFS	NFS counters return the total NFS procedure calls, and the total calls for each NFS procedure since you started the server. These counters can give an indication of the load on the server. total is the total number of calls bad call is the number of bad calls fail is the number of failed calls null is the number of null calls getattr is the number of get attribute calls setattr is the number of set attribute calls read is the number of reads lookup is the number of lookups mkdir is the number of make directory calls write is the number of writes create is the number of creates remove is the number of removes rename is the number of renames rmdir is the number of directory removes readdir is the number of address reads statfs is the number of file system statistics calls link is the number of create link to file calls symlink is the number of create symbolic link calls readlink is the number of read from symbolic link calls other is the number of other calls
RPC	RPC counters provide information on RPC operations. This includes the total number of *receives, transmits, XID hits*, and *duplicate receives*. The *XID hits* counter gives the number of cached replies the NFS Server retransmitted. The *duplicate receives* counter gives the number of times the server received a duplicate request for an operation that was in progress at the time of the request. If either of these counters is excessive you may need to increase the timeout time on the NFS-Client host(s).
RPC Errors	RPC counters also returns the following error conditions: *receive* and *transmiterrors, authentication errors, decode errors,* and *RPC program errors*.
MOUNT	MOUNT counters return the total MOUNT procedure calls, the calls for each MOUNT procedure since someone started the server, the total number of directory mounts since someone started the server, and the number of directories currently mounted. total is the number of MOUNT calls bad call is the number of bad MOUNT calls fail is the number of failed MOUNT calls mount is the number of successful mounts unmount is the number of successful dismounts null is the number of null mounts dump is the number of dumps from MOUNT calls mnt export is the number of exported mounts cur mount is the number of current mounts

Example

The command description section describes the output parameters for this example. The /TIME qualifier includes the average and maximum times for the indicated NFS requests.

```
SHOW STATISTICS /TIME
NFS Show Statistics V5.8 Copyright (c) Process Software
Started:  1-FEB-2014 07:24:05 Uptime: 14 07:05:53  Memory in use: 1414850
Threads:       total       40 current     0 max         11
Files:         opens       54 closes     54 cur. open    0  max.open   5
NFS:           total     2519 bad call    0 fail         0
  null       6 getattr    149 setattr     6 read       396  lookup  1381
ave:      0 ms           7 ms         82 ms          78 ms          20ms
max:      0 ms          40 ms        100 ms         180 ms          50 ms
  mkdir      0 write      396 create      6 remove      12  rename    18
ave:      0 ms          38 ms         83 ms          38 ms         117 ms
max:      0 ms         510 ms         90 ms         120 ms         130 ms
  rmdir      0 readdir     51 statfs      1 link         0  symlink    0
ave:      0 ms          32 ms         10 ms           0 ms           0  ms
max:      0 ms         230 ms         10 ms           0 ms           0  ms
  readlink   0 other        0 adfread    97 adfwrite     6
ave:      0 ms           0 ms          7 ms          27 ms
max:      0 ms           0 ms         50 ms          30 ms

RPC:           recv      2520 xmit     2520 xid hits     0  dup recv    0
RPC errors:    recv         0 xmit        0
  authweak   0 authother    0 decode      0 noproc       0  noprog      0
  progvers   2 systemerr    0

MOUNT:         total        1 bad call     0 fail         0
mount        1 unmount      0 null         0 dump         0 mnt export  0
mounts       1 cur. mount   1
```

SHOW TICKETS

For Kerberos users. Displays your ticket-granting ticket (TGT) and any existing application service tickets. The name of the ticket file is determined by the value of the TCPWARE_KERBV4_TKFILE logical, usually set to SYS$LOGIN:KERBV4.TICKET. SHOW TICKETS is equivalent to the UNIX command klist. See the GET command for more information on getting ticket-granting tickets.

Format

SHOW TICKETS

Qualifiers

/BRIEF
/NOBRIEF (default)

/BRIEF lists only the acquired tickets and not the ticket files, principal names, issuance dates, or expiration dates.

/SRVTAB

Shows the contents of the TCPWARE:SRVTAB. file as a list of available Kerberos services. (See CREATE SRVTAB for more information on the TCPWARE:SRVTAB. file.)

/TGT_TEST
/NOTGT_TEST (default)

Checks whether the tickets are still valid and returns a success or failure exit status.

Examples

1 Displays the name of the ticket file; ticket owner's principal name, issue and expiration dates; and service principal name of each ticket.

```
SHOW TICKETS
Ticket file:    SYS$LOGIN:KERBV4.TICKET
Principal:      fred@daisy.com
Issued           Expires           Principal
--------------------------------------------
Jun 1 10:11:12   Jun 1 18:11:12    krbtgt.daisy.com@daisy.com
```

2 Lists the available Kerberos services on BART as listed in its TCPWARE:SRVTAB. file.

```
SHOW TICKETS /SRVTAB
Server key file:   TCPWARE:SRVTAB.
Service      Instance     Realm         Key Version
---------------------------------------------------
changepw     bart         daisy.com     1
rcmd         bart         daisy.com     1
```

SHOW TIMEZONE

Displays the offset from universal time and optional timezone name.

Format

SHOW TIMEZONE

Examples

1 This is displayed if the time was set by the numerical value -0500.

```
SHOW TIMEZONE
Offset from universal time (UT) is -05:00:00
```

2 This is displayed if the time was set by the value **EST**.

```
SHOW TIMEZONE
Offset from universal time (UT) is -05:00:00 (EST)
```

SHOW NAMED VERSION

Prints the current DNS server version number. (This is the version of BIND from which the TCPware DNS server is derived.)

When the server is busy, NETCU sends a message stating that your request has been queued, and it will be acted upon when it is the next one in the queue to be serviced. When the server is not busy, it performs your request while NETCU waits (except for the case of RELEAD). For example,

```
NETCU>show named version
Domain Name Server Version = named 8.1.2 for TCPware V5.8
        Process Software
tcpware_named_root:named.conf =
         sys$sysdevice:[engineering.schreiber.zonefiles]named.conf
```

Format

SHOW NAMED VERSION

Qualifiers

/ALL

Displays any patch versions of the executables along with their link date and times.

/OUTPUT=*filespec*

Uses the specified file instead of the terminal for output.

Example

Shows the current TCPware version along with any patches and their link and date times.

```
SHOW NAMED VERSION /ALL
TCPware(R) for OpenVMS V6.0 Copyright (c) Process Software

Build Revision 31

TCPware Image           Version         Link Date/Time
-------------------------------------------------------------
TCPWARE:BGDRIVER.EXE    TCPWARE V6.0    17-APR-2014 14:15:23
TCPWARE:CHARGEND.EXE    TCPWARE V6.0    17-APR-2014 14:17:23
TCPWARE:CHAT.EXE        TCPWARE V6.0    17-APR-2014 14:16:49
```

SHOW VERSION

Displays the current version of the TCPware for OpenVMS software.

Format

SHOW VERSION

Qualifiers

/ALL

Displays any patch versions of the executables along with their link data and times. Also shows your maintenance agreement number (MAS) if you entered it during CNFNET configuration.

/OUTPUT=*filespec*

Uses the specified instead of the terminal for output.

Example

```
SHOW VERSION /ALL

TCPware(R) for OpenVMS V6.0 Copyright (c) Process Software

Build Revision 31

MAS number : <none entered in configuration>

TCPware Image             Version           Link  Date/Time
-----------------------------------------------------------------
TCPWARE:BGDRIVER.EXE      TCPWARE V6.0      3-NOV-2014  14:15:23
TCPWARE:CHARGEND.EXE      TCPWARE V6.0      3-NOV-2014  14:17:23
TCPWARE:CHAT.EXE          TCPWARE V6.0      3-NOV-2014  14:16:49
```

Shows the current TCPware version along with any patches and their link and date times.

SPAWN

Executes DCL commands within NETCU.

Note! You cannot SPAWN with CAPTIVE accounts.

Format

SPAWN *[command-line]*

Parameter

command-line

DCL command line you want executed. If omitted, NETCU spawns an interactive subprocess. To return to NETCU from an interactive subprocess, enter **LOGOUT**.

Examples

1 Displays the time on your local host without leaving the NETCU utility.

```
SPAWN SHOW TIME
1-MAY-2014 14:02:48
NETCU>
```

2 Initiates DCL command mode and returns the DCL prompt.

```
NETCU>SPAWN
$ SHOW TIME
1-MAY-2014 14:02:51
$ LOGOUT
Process SMITH_1 logged out at 1-MAY-2014 14:02:54.34
```

SSHKEYGEN

Generates authentication key pairs. The format of the keys is incompatible between SSH1 and SSH2. Therefore, the correct format keys must be generated for each version of the protocol to be supported.

Each key may be protected via a passphrase, or it may be left empty. Good passphrases are 10-30 characters long and are not simple sentences or otherwise easily guessable. Note that the passphrase can be changed later, but a lost passphrase cannot be recovered, as a “one-way” encryption algorithm is used to encrypt the passphrase.

Refer to the section on SSHKEYGEN in the *TCPware Users Guide*, chapter 16, "Accessing Remote Systems with the Secure Shell (SSH) Utilies", for details on using SSHKEYGEN.

START/DNIP

Configures and starts a single DECnet over IP tunnel between the local host and another host.

Note! You would normally not use this command directly. Instead, you should configure DECnet over IP tunnels through CNFNET (as described in Chapter 28 of the *TCPware for OpenVMS Management Guide*). TCPware then issues the START/DNIP command during STARTNET.

If you decide to use this command directly, keep in mind that it only establishes the TCP connection for the tunnel. It does not inform DECnet that the tunnel exists. For DECnet to use the tunnel, perform the following commands:

```
$ MCR NCP SET LINE dev-n-u STATE ON
$ MCR NCP SET CIRCUIT dev-n-u STATE ON
```

Format

START/DNIP ***line-name remote-host local-port remote-port***

Parameters

line-name

DECnet line name (format dev-c-n) of the DECnet-over-IP tunnel to configure and start.

remote-host

Internet host name of the remote host establishing the tunnel.

local-port

TCP port number on the local host establishing the tunnel.

remote-port

TCP port number on the remote host establishing the tunnel.

Example

Configures the tunnel DNIP-0-1 to connect to node BETA using TCP port number 777 on the local host and TCP port 654 on BETA. Attempts to establish a connection and start up the tunnel.

```
START/DNIP DNIP-0-1 BETA 777 654
```

START/INET

Instructs the Network Control Process (NETCP) to start the INET device driver. Requires OPER privilege.

Note! Use the TCPware startup command procedure, STARTNET.COM, to start TCPware. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

START/INET

START/IP

Instructs NETCP to start the IP protocol. Issue this command for each network device that the local host supports. Requires OPER privilege.

Note! Use the TCPware startup command procedure, STARTNET.COM, to start TCPware. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

START/IP *line ia [line-specific-info]*

Parameters

line

Line ID for the network device. See Table 3-4 in the *TCPware for OpenVMS Installation & Configuration Guide* for a full list of the supported network devices. You can use a wildcard symbol for the specific device number. For example, you can specify:

```
START/IP SLIP-* ...
```

This assigns the lowest unused and unique line ID for the interface type. This also defines the TCPWARE_LINE (global) symbol with the assigned line ID. For example:

```
NETCU START/IP SLIP-* 1.2.3.4 TTA2:
SHOW SYMBOL TCPWARE_LINE
   TCPWARE_LINE = "SLIP-0"
```

Use this wildcard feature with any line type. However, it is less meaningful for line IDs related to physical device names (such as Ethernet and FDDI interfaces).

ia

Local host's internet address or host name for the line.

line-specific-info

Parameter used only for SLIP, IP-over-DECnet, HYPERchannel, and HP Wide Area Network Device Drivers lines, as in Table 2-9.

Table 2-9 Line-Specific Information for Various Line Types

For Line Type...	*Line-specific-info* is...
SLIP Lines	OpenVMS terminal device name for the SLIP line. If omitted for a SLIP line, NETCU assumes the TCPWARE_SLIP_*n* system logical defined the device (where *n* is the line's controller number).

IP-over-DECnet Lines	Required DECnet link information. Enter it in the format: ***node-name::"*****TASK=*****object-name"*** *node-name* is the listener node when issued from the master node, and the master node when issued from the listener node and *object-name* is the object used on the listener node; both the master and listener nodes must specify the same *object-name*: An IP-over-DECnet line has a master node at one end and a listener node at the other end.
HYPERchannel Lines	Local HYPERchannel interface address. The format for this parameter is *aa-bb-cc-dd*, where *aa, bb, cc,* and *dd* are hexadecimal values representing each byte of the address as follows: The value *aa* is the global network address domain (if none, specify 00) The value *bb* is the global network address network (if none, specify 00) The value *cc* is the physical unit The value *dd* is the logical unit NETCU uses the *cc-dd* portion of the address as the path address in the H269 driver's IO$_ATTACH function. Always specify the 32-bit HYPERchannel address.
HP Wide Area Network Device (WAN) Lines	Quoted string of the line configuration options shown in Table 2-10. An example of *line-specific-info* is: `"PROTO DDCMP POINT CLOCK INTER LINE SPEED 6400"` Note that for the option specifications: — You must include the quotation marks — You can use keyword abbreviations

Table 2-10 HP WAN Line Configuration Options

Parameter	Option/Value	Description
PROTOCOL	DDCMP POINT LAPBE LAPB SDLC	Line protocol used.
DUPLEX	HALF FULL	Defines whether the line operates in full or half duplex mode.

CLOCK	INTERNAL EXTERNAL	Defines whether the lines uses internal or external clocking.
CRC	*type*	Type of CRC used. *Not recommended*.
LINE SPEED	*speed*	Line speed. This setting is only useful if you specify CLOCK INTERNAL.
RECEIVE BUFFERS	*number*	Number of receive buffers.
RETRANSMIT TIMER	*time*	Retransmission time (for DDCMP only).

For details on these parameters, such as the possible values for the line speed or CRC, see the *HP VAX Wide Area Network Device Drivers Programmer's Guide.*

Qualifiers

/ARP_SERVER=*HC-address*

For HYPERchannel lines, the optional ARP server's HYPERchannel address. If specified, NETCU uses the ARP server to resolve all unknown addresses. If omitted, you must populate the Address Resolution Table before communicating with a peer.

The address format is the same as for the *line-specific-info* parameter for HYPERchannel lines. This must be a 32-bit HYPERchannel address.

/FLAGS=*(option[,option...])*

Table 2-11 includes the *options* for Ethernet, FDDI, and Token Ring, as well as LAN emulation in an Asynchronous Transfer Mode (ATM) network environment (known as Classical IP over ATM, or CLIP). Table 2-12 includes these options for PPP, SLIP, and CSLIP, and Table 2-13 includes them for DECnet over IP.

Table 2-11 /FLAGS Options for Ethernet, FDDI, Token Ring, and CLIP

/FLAGS Option	Description
NOBACKTOBACK	Disables transmitting back-to-back packets to the same physical address. TCPware uses back-to-back transmission by default.
NOBROADCAST	Disables receiving broadcast packets. Especially useful if an OpenVMS system has multiple Ethernet controllers connected to the same Ethernet. You must disable all but one controller to receive broadcasts.

*[NO]*RARP	Enables (RARP) or disables (NORARP) Reverse Address Resolution Protocol (RARP) support. The TCPware system only responds to RARP requests for permanent address entries in its ARP cache. RARP support is enabled by default for all Ethernet, FDDI, and Token Ring interfaces. RARP support is disabled for Classical IP over ATM (CLIP-*n*) lines.
*[NO]*TRAILERS	Enables (TRAILERS) or disables (NOTRAILERS) trailer packet support. NOTRAILERS is the default. ***Note!*** VCI and Classical IP over ATM do not support trailer packets.
*[NO]*VCI	Enables (VCI) or disables (NOVCI) VMS Communications Interface (VCI) support. If starting VCI fails or you use /FLAGS=NOVCI, TCPware uses the alternate interface.

Table 2-12 /FLAGS Options for SLIP and CSLIP

/FLAGS Option	Description
AUTOENABLE	Enables sending compressed TCP/IP headers in SLIP packets if receiving compressed TCP/IP headers from the peer.
COMPRESSED	Enables sending compressed TCP/IP headers in SLIP packets.
DOUBLEEND	Enables sending the “end” character at the start of SLIP packets. This action is optional. ***Note!*** We do not recommend the use of this option when both ends of the SLIP line connect to TCPware hosts increases processing overhead.
FLOWCONTROL	Enables a TCPware private extension to the SLIP protocol to allow use of XON/XOFF flow control over the serial ink. You can use this option only when both ends of the SLIP line connect to TCPware hosts. It is especially useful when using reliable compression modems.
(RCV=*n*)	Sets the number of receive buffers used for the serial line. *n* may be from 1 to 9. The default is 6.

Table 2-13 /FLAGS Options for DECnet over IP

/FLAGS Option	Description
LISTENER	Issues commands for the passive end of the DECnet link. If omitted, NETCU assumes you issued the command for the master node.
(RETRY=*seconds*)	Specifies the retry interval when losing a DECnet link. When entered for the master node, it is the time interval between retries to establish a link. When entered for the listener node, it is the time interval between retries to create the object. The maximum retry time is 65535 seconds (about 18 hours). The default is 60 seconds.

/MASK=*ia*

Sets the subnet mask to the specified address.

Use this qualifier to support subnets and supernets. If not specified, NETCU uses the default network mask for the internet address class. NETCU determines the network number from the internet address by ANDing the specified address with the mask.

Table 2-14 shows the default network masks for the network classes.

Table 2-14 Network Classes and Masks

Class	Network Mask	Internet Address Range
A	255.0.0.0	0.*rrr.rrr.rrr*—127.*rrr.rrr.rrr*
B	255.255.0.0	128.000.*rrr.rrr*—191.255.*rrr.rrr*
C	255.255.255.0	192.000.000.*rrr*—223.255.255.*rrr*

/MTU=*n*

Sets the maximum transmission unit (MTU) to n for the line.

The maximum transmission unit is the byte size of the data portion of the largest packet you can transmit. If omitted, TCPware uses the default value for the line. The maximum allowable MTU value is 64512 bytes. Table 2-15 lists the default MTU for the line type.

Table 2-15 Line Type Default MTU

Line Type	Default MTU	Comments
Classical IP over ATM	1500	

Ethernet	1500	
FDDI	4352	
HYPERchannel	4096	
IP-over-DECnet	2048	
IP-over-X.25	1500	Set the MTU to 576 bytes if the system should communicate with older version of IP-over-X.25 (RFC 877). Configure the MTU over 1500 bytes only be prearrangement with the other sites.
LAN Emulation over ATM	1500	
proNET	2040	
Token-Ring	4092	
WAN	1500	

/UNNUMBERED_INTERFACE

Use this qualifier when starting an unnumbered interface, especially for SLIP lines. NETCU does not assign unnumbered interfaces a local address. However, you must specify an internet address (*ia*), as TCPware uses this address when originating datagrams for the interface if you do not explicitly specify a source address.

Examples

1 Starts the IP protocol for the QNA-0 line and sets the line's local internet address to 10.0.0.1.

```
START/IP QNA-0 10.0.0.1
```

2 Starts the IP protocol for the SLIP-0 line on device TXA7: and sets the line's local internet address to 192.168.5.6.

```
START/IP SLIP-0 192.168.5.6 TXA7:
```

3 Starts the IP protocol for DECnet line 4 for the listener node. The internet address is 192.168.5.2. LILAC is the master node and DGCFF is the object name of the listener.

```
START/IP DECNET-4 192.168.5.2-LILAC::"TASK=DGCFF"/FLAGS=LISTENER
```

4 Starts the IP protocol for the HYPERchannel HYP-0 line and sets the local internet address to 10.0.0.1. The local HYPERchannel address is 01-01-13-01 and ARP server's HYPERchannel address is 01-01-12-11.

```
START/IP HYP-0 10.0.0.1 01-01-13-01/ARP_SERVER=01-01-12-11
```

5 Starts the IP protocol for SJA1: (the second line on the first DSV11 controller). The device will run the DDCMP protocol at 19200 baud.

```
    START/IP DSV-1 10.0.0.5 "PROTOCOL DDCMP POINT LINE SPEED 19200"
```

Pseudo devices

You can start pseudo devices by using the START/IP command.

Note! Refer to the *TCPware for OpenVMS Management Guide*, Chapter 1, for more information on pseudo devices.

Format

START/IP PSD-*n* *Internet-Address* *Real-Line-ID*

Parameters

n

This is the pseudo device line-id number (from 0 to 255). The number is not meaningful, but must be unique for each pseudo device; it identifies the instance of the pseudo device.

Internet-Address

This is the Internet address of the TCPware system on the network.

Real-Line-ID

This is the line-id of the physical device.

Note the following with respect to standard START/IP qualifiers:

Qualifiers

/MASK

This qualifier can be used to specify the network mask for the network.

/ARP, /FLAGS, and **/UNNUMBERED**

These qualifiers are not allowed and result in an error if specified.

/MTU

This qualifier, if specified, is ignored as the MTU used is that of the physical device.

Example

In this example, a pseudo device is started that is associated with the ISA-0 device (this is the Ethernet network to which the system is connected). The Ethernet network has two IP network numbers assigned to it (192.116.1.0 and 192.168.2.0) and the system has two Internet addresses assigned to it, one on each network, 192.168.1.1 and 192.168.2.1.

```
NETCU START/IP ISA-0 192.168.1.1
NETCU START/IP PSD-0 192.168.2.1 ISA-0
```

START/PWIP

Instructs NETCP to start the PWIPDRIVER. Requires OPER privilege.

PATHWORKS Version 5.0 and later and DECnet/OSI Version 6.0 and later use PWIPDRIVER for TCP/IP support.

Note! Use the TCPware startup command procedure, STARTNET.COM, to start TCPware. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

START/PWIP

START/TCP

Instructs NETCP to start the TCP protocol. Requires OPER privilege. You must start the Internet Protocol (IP) before you can start the TCP protocol. See the START/IP command.

Note! If you already started TCP, you can issue this command to change a parameter value. However, if you do not explicitly specify a parameter, it reverts to its default value as described below.

Use the TCPware startup command procedure, STARTNET.COM, to start TCPware. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

START/TCP

Qualifiers

/KEEPALIVE (default)
/NOKEEPALIVE

Determines if TCP sends KEEPALIVE probes to a peer to see if the peer is still there. If a connection is idle, TCP periodically sends KEEPALIVE probes to solicit a response. The KEEPALIVE probe assumes the peer is down and closes the connection if a specified time period elapses and there is no response. Process Software recommends that you set this qualifier to
/NOKEEPALIVE if you or part of your organization are on a tariff network. Charges on such a network can be very high; for example, some X.25 networks. To change this qualifier, edit the STARTNET.COM file or add the appropriate command to the ROUTING.COM file.

/MSS=*bytes*

Sets the maximum segment size (MSS) to bytes. MSS is a TCP parameter that specifies the maximum number of bytes that TCP transmits in a single segment, which is the IP datagram size minus 40 bytes. The minimum MSS value is 512 bytes, the maximum is 61440, and the default is 16384 bytes. A host cannot send datagrams larger than the lesser of MSS and the MTU the network interface uses. Path MTU discovery (see /PATH_MTU_DISCOVERY) may dynamically adjust the MSS to the value advertised by the peer, and will never exceed it. If omitted, the value is set to 0, which means no limit, which is the preferred setting for most cases.

/MWS=*bytes*

Sets the maximum window size (MWS) to bytes. The MWS is a TCP parameter that specifies the number of bytes the peer is willing to receive (in one or more segments). The default MWS is 24576 bytes. The TCP protocol allows a top maximum window size of 65535.

TCPware supports a maximum MWS value of 262144 bytes. Restrict use of a window size of more than 65535 bytes to situations where there is a high bandwidth-times-round-trip-delay product; for example, in some satellite links. TCPware uses the Window Scale option by default (see the
/WINDOW_SCALE qualifier).

Communication over a high bandwidth times round trip delay product (like some satellite links) works best if you:

- Configure all systems with the same window size.
- Choose a window size that matches the actual bandwidth and delay. For example, a window size of 112500 should be about optimum for a bandwidth of 1.5 Mbit and round trip delay of 600 msec as shown here.

$$\frac{1500000 \text{ bits/second} \times 0.6 \text{ seconds}}{8 \text{ bits/byte}} = 112500 \text{ bytes}$$

- Choose a window size that is slightly larger than the calculated value, rather than slightly smaller than the calculated value.

In some cases, a window size in excess of 65535 may slightly degrade Ethernet performance. This should not cause visible problems.

Note! You must configure the queue length of routers connected to the satellite link to buffer an entire window of data. TCPware sends the data on the Ethernet at full speed. Check the interface statistics on the satellite link route to see that it did not drop any packets.

/NODELAY

Normally TCP may delay a transmit for a short period of time so that if there are multiple rapid transmits, they can be coalesced into larger packets, placing fewer packets on the network and in general causing improved network performance. For some applications though, this ends up providing a poor user experience. /NODELAY allows this feature of the TCP protocol to be disabled.

/NODELACK

Normally TCP will delay the ACK of a received segment for a short period of time (up to 200ms) so that if multiple segments are received in that time and no data is being sent back, multiple received segments can all be ACKed in one ACK segment. This will (in general) lead to improved network performance. /NODELACK allows this feature of the TCP protocol to be disabled.

/PATH_MTU_DISCOVERY (default)
/NOPATH_MTU_DISCOVERY

Enables or disables Path MTU discovery logic, which prevents excessive datagram fragmentation by dynamically discovering the maximum transmission unit (MTU) of an arbitrary internet path. Path MTU discovery is enabled by default.

Path MTU discovery is an IP protocol (described in RFC 1191) that uses the least value of the MTUs it finds among the hops on a datagram's path. It starts with the MTU set for the interface and looks for a smaller value embedded in an ICMP reply from any traversed router, until it can estimate an MTU low enough to prevent fragmentation. The host also periodically sends out an increased MTU value to test for upward changes in MTUs along the path.

/PROTECTED_PORTS (default)
/NOPROTECTED_PORTS

Enables or disables protection for ports below 1024. When protected, an application program must have BYPASS or SYSPRV privilege to listen on a port below 1024.

/WINDOW_SCALE (default)
/NOWINDOW_SCALE

Enables or disables sending the Window Scale option (one of the TCP extensions for high performance options described in RFC 1323) when establishing connections. Some TCP/IP implementations cannot handle this option or need to be updated to do so. With /NOWINDOW_SCALE, TCPware does not send the Window Scale option, but continues to acknowledge its support for incoming connections specifying it.

START/UCX

Instructs NETCP to start the BGDRIVER protocols. Requires OPER privilege.

Note! Use the TCPware startup command procedure, STARTNET.COM, to start TCPware. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

START/UCX

START/UDP

Instructs NETCP to start the UDP protocol. Requires OPER privilege.

You must start the Internet Protocol (IP) before you start the UDP protocol. See the START/IP command.

Note! If you already started UDP, you can issue this command to change a parameter value. However, if you do not explicitly specify a parameter, it reverts to its default value as described below.
Use the TCPware startup command procedure, STARTNET.COM, to start TCPware. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

START/UDP

Qualifiers

/MDS=*n*

Sets the maximum datagram size (MDS) to n bytes. UDPDRIVER will not transmit datagrams larger than *n*. The default MDS value is 16384. The maximum MDS value is 61440 bytes.

/PROTECTED_PORTS (default)
/NOPROTECTED_PORTS

Enables or disables protection for ports below 1024.

When protected, an application program must have BYPASS or SYSPRV privilege to open a port for a port number below 1024.

/UNSOLICITED_RECEIVE_LIMIT=*n*

Sets the default limit of UDP unsolicited receives, or datagrams buffered on a socket if there is no outstanding read before they are dropped.

STASH MASTER_PASSWORD

Used by the Kerberos master administrator. Stashes the master password in the protected TCPWARE:KSTASH.KEY file.

You must use STASH MASTER_PASSWORD after creating the Kerberos database (see CREATE KDB) and before starting the Kerberos Server or Administration Server.

Requires OPER or SYSPRV privilege and entry of the Kerberos master password.

Note! You must execute this command before starting the Kerberos Server or Administration Server.

Format

STASH MASTER_PASSWORD

Enter Kerberos master password: ***master-password***
Verifying, please re-enter: ***master-password***

Parameter

master-password

Kerberos password used for access to the Kerberos database. Use the same password as the one created using CREATE KDB. Converted to lowercase unless you enclose it in double quotes.

Example

Stashes the master password in the encrypted TCPWARE:KSTASH.KEY file.

```
STASH MASTER_PASSWORD
Enter Kerberos master password:
Verifying, please re-enter:
```

STOP/DHCP

Shuts down the Dynamic Host Configuration Protocol (DHCP) server in an orderly manner. Requires SYSPRV or OPER privilege.

To address the DHCP V4 server, use “DHCP4” instead of “DHCP” in the command.

Format

```
STOP/DHCP
STOP/DHCP4
```

STOP/DNIP

Shuts down any or all DECnet over IP tunnel(s) currently configured and running on this host.

Note! You would normally not use this command directly. Instead, you should stop DECnet over IP tunnels through the SHUTNET.COM procedure described in the Chapter 26 of the *TCPware for OpenVMS Management Guide.*

Note! If you decide to use this command directly, keep in mind that it only shuts down the TCP connection for the tunnel. It does not inform DECnet that the tunnel no longer exists. For DECnet to stop trying to use the tunnel, perform the following commands:

```
$ MCR NCP SET LINE dev-n-u STATE OFF
$ MCR NCP SET CIRCUIT dev-n-u STATE OFF
```

Format

STOP/DNIP *dev-n-u*	**Shuts down DECnet tunnel dev-n-u**
STOP/DNIP/ALL	**Shuts down all DECnet over IP tunnels**

Parameter

dev-n-u

DECnet line name of the DECnet-over-IP tunnel to shut down.

Qualifier

/ALL

Shuts down all DECnet-over-IP tunnels on this host.

Examples

1 Shuts down the single DECnet-over-IP tunnel DNIP-0-0 on this host.

```
STOP/DNIP DNIP-0-0
```

2 Shuts down all DECnet-over-IP tunnels on this host.

```
STOP/DNIP/ALL
```

STOP/DNS

Instructs the nameserver to shut down. Stops the Domain Name Services (DNS) Resolver process (TCPware_DNS).

CAUTION! Do not use this command in most cases. The DNS Resolver process is the last one shut down with SHUTNET.COM and the first one started with STARTNET.COM. If you use STOP/DNS and then restart TCPware without the DNS Resolver process present, you will get a series of error messages beginning with:

```
%SYSTEM-F-NOLOGNAM, no logical name match
%TCPWARE_NETCU-E-IVPORT, invalid port number or service name
```

To restart the DNS Resolver after having used STOP/DNS, run TCPWARE:STARTUP_RESOLVER.COM as follows:

```
$ @TCPWARE:STARTUP_RESOLVER DETACH
```

Format

STOP/DNS

STOP/GATED

Tells the GateD process to halt in an orderly manner.

Note! Do not use this command in most cases. Use the SHUTNET.COM GATED command instead.

Format

STOP/GATED

STOP/INET

Instructs NETCP to stop the INET device driver. Requires OPER privilege.

Note! Use the TCPware shutdown command procedure, SHUTNET.COM, to stop TCPware. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

STOP/INET

STOP/IP

Instructs NETCP to stop a line. Requires OPER privilege.

Note! Use the TCPware shutdown command procedure, SHUTNET.COM, to stop TCPware. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

STOP/IP *line*

Parameter

line

Line ID of the network device to be stopped.

Examples

1 Stops the IP protocol on the SLIP-0 line.

```
STOP/IP SLIP-0
```

2 Stops the IP protocol on the SVA-0 ethernet interface.

```
STOP/IP SVA-0
```

STOP/NAMED

Stops the nameserver.

Format

STOP/NAMED

STOP/NETCP

Stops the Network Control Process (NETCP) process. Requires OPER privilege. When you enter this command, NETCP shuts down the network and terminates itself.

Note! This command is for use by the SHUTNET. COM procedure only. To stop TCPware, use the SHUTNET.COM procedure. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

STOP/NETCP

STOP/PWIP

Stops the PWIPDRIVER. Requires OPER privilege. PATHWORKS Version 5.0 and later and DECnet/OSI Version 6.0 and later use PWIPDRIVER for TCP/IP support.

Note! Use the TCPware shutdown command procedure, SHUTNET.COM, to stop TCPware. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

STOP/PWIP

STOP/SERVER

NFS Server only.

Stops the NFS Server. Requires OPER privilege.

Note! We recommend you use the NFS-OpenVMS Server shutdown command procedure, SHUTNET.COM NFS, to stop the NFS server.

Format

STOP/SERVER

STOP /SSH

Shuts down all SSH server processes, terminating all active SSH sessions to this system. Does not affect SSH sessions outgoing from this system to other systems.

Format

STOP /SSH

Example

```
$ NETCU STOP /SSH

Starting shutdown of SSH Master server
```

STOP/TCP

Instructs NETCP to stop the TCP protocol. Requires OPER privilege.

Note! Use the TCPware shutdown command procedure, SHUTNET.COM, to stop TCPware. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

STOP/TCP

STOP/UCX

Instructs NETCP to stop the BGDRIVER protocols. Requires OPER privilege.

Note! Use the TCPware shutdown command procedure, SHUTNET.COM, to stop TCPware. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

STOP/UCX

STOP/UDP

Instructs NETCP to stop the UDP protocol. Requires OPER privilege.

Note! Use the TCPware shutdown command procedure, SHUTNET.COM, to stop TCPware. See the *TCPware for OpenVMS Installation & Configuration Guide* for details.

Format

STOP/UDP

TCPDUMP

TCPDUMP prints out the headers of packets on a network interface that match the boolean expression. The OpenVMS implementation currently only works with HP-compatible Ethernet cards. Some of the command line switches were changed from the UNIX version to support OpenVMS's case-insensitive command line.

PHY_IO privilege is required to use TCPDUMP unless reading packets from a file. If using the TCPware drivers for packet capturing, LOG_IO and SYSPRV or BYPASS privileges are also needed.

Format

TCPDUMP *[options/qualifiers] [expressions]*

Options and Qualifiers

Note! The command qualifiers are not available if using TCPDUMP as a foreign command on the DCL level. You can mix and match options and qualifiers on the NETCU level only. For a full description of the TCPDUMP command and its options, qualifiers, and expressions, see the *TCPware for OpenVMS Management Guide*, Chapter 31, *Network Testing Tools*, the *TCPDUMP* section.

TOGGLE GATED TRACING

Toggles GateD tracing on and off. This command opens and closes the GateD log file TCPWARE:GATED.LOG as needed.

Note! The NETCU processing of this command is completed before GateD finishes processing it.

Format

TOGGLE GATED TRACING

UNMOUNT ALL

NFS Client only.

Removes all the mount list entries for the local client host on the specified NFS server or servers. Useful for notifying the remote server host that the server file systems are no longer mounted on the client in the event that the client system goes down and you need to reboot it.

Note! Unmounting is not the same as dismounting. UNMOUNT ALL does not dismount a mounted file system.

After using UNMOUNT, you can use SHOW MOUNT (in TCPware) or show mount (on a UNIX system server) to verify that the list entry you requested to be unmounted on the specified server(s) is no longer there. The mount list entries are in the /etc/rmtab file on most UNIX systems.

Format

UNMOUNT ALL

Qualifier

/HOST=*(server,server...)*

Server host or hosts. The parentheses are required for multiple servers. If omitted, the Client sends a broadcast message to all local network servers to remove the list entry for the local client host.

Examples

1 Sends a broadcast message to all local network servers to remove the mount list entry for the local client host.

```
UNMOUNT ALL
```

2 Sends a request to hosts TAU and SIGMA to remove the mount list entry for the local client host.

```
UNMOUNT ALL /HOST=(TAU,SIGMA)
```

Note! The following message can occur after an UNMOUNT ALL request sent to a UNIX system server:

```
%TCPWARE_NETCU_E-CLNTCALLFAIL, RPC Client call failed, RPC: Remote system error
```

Ignore this message. However, confirm through a SHOW MOUNT command that the mount list entry was, in fact, removed.

UPDATE DHCP

Instructs the Dynamic Host Configuration Protocol (DHCP) server to process the update file and add or remove the specified host and subclass declarations. See Chapter 4, *DHCP/BOOTP Server* of the *TCPware for OpenVMS Management Guide* for a description of the update file and commands.

To address the DHCP V4 server, use “DHCP4” instead of “DHCP” in the command.

Format

UPDATE DHCP
UPDATE DHCP4

Qualifiers

/OUTPUT=*filespec*

Sends output to the specified file. If not specified, output appears on the terminal screen.

/FILENAME=*filespec*

Specifies the name and location of the file containing the update commands. Optional. The default is TCPWARE:DHCPD.UPDATES.

UPDATE GATED INTERFACES

Tells the GateD process to rescan the network interfaces.

Note! The NETCU processing of this command is completed before GateD finishes processing it.

Format

UPDATE GATED INTERFACES

WRITE

Writes the current TCPware SMTP configuration to SMTP configuration files. (Functionally equivalent to SAVE.)

FORMAT

WRITE *config_file*

PARAMETERS

config_file

Specifies the name of the file to which to write the current TCPware SMTP configuration. By default, the configuration is saved to the same file from which it was read **.**

Chapter 3 MAIL-CONFIG Commands

MAIL-CONFIG lets you examine, modify, and save configuration files for the SMTP mail system.

To invoke MAIL-CONFIG:

```
$ TCPWARE CONFIGURE /MAIL
```

At any MAIL-CONFIG prompt, type ? to list the available commands. Use the MAIL-CONFIG HELP command to view online help for each MAIL-CONFIG command.

Changes do not take effect until you do one of the following:

- Restart the SMTP service with the @TCPWARE:START_SMTP.COM or @TCPWARE:START_SMTP_LOCAL.COM commands.
- Restart the SMTP component.
- Restart TCPware.
- Restart your system.

For details on configuring electronic mail, refer to the *TCPware for OpenVMS Management Guide*.

ADD GATEWAY

Adds a mail gateway to another domain. Specifies a gateway host to which mail for the specified host or domain will be forwarded.

Note! To define a mail gateway to an IP address (instead of a host name), you must enclose the IP address in square brackets.

FORMAT

ADD GATEWAY *domain_name hostname*

PARAMETERS

domain_name

Specifies the name of the domain for which the new gateway will handle mail. This can be a fully qualified host name (for example, WHORFIN.FLOWERS.COM) or a domain tag beginning with a dot (for example, .BITNET).

hostname

Specifies the name of the host that acts as a gateway for mail addressed to domain_name.

ADD LOCAL-DOMAIN

Adds a domain to a list of domains that the TCPware SMTP symbiont considers to be local. If users send mail to hosts beyond the local domains, TCPware forwards the mail to the mail hub specified by the FORWARDER parameter. The local domain list affects mail forwarding only when the FORWARD-REMOTE-MAIL parameter is TRUE.

FORMAT

ADD LOCAL-DOMAIN *domain_name*

PARAMETERS

domain_name

Specifies the name of a domain (for example, LOT-49.FLOWERS.COM) that TCPware considers to be local.

ADD QUEUE-GROUP

Forms a mail queue grouping of nodes in a cluster, or adds new nodes to an existing queue group. The SMTP queues on the nodes in the group you create will share responsibility for handling mail messages generated on nodes within the group. If a node is not placed in a named queue group, it is made part of the default queue group.

FORMAT

ADD QUEUE-GROUP *group_name [node_name_list]*

PARAMETERS

group_name

Specifies the name of the queue group to add, or the name of an existing group to which nodes will be added.

node_name_list

Contains a list of names of VMScluster (SCS) nodes to add to the queue group.

ATTACH

Detaches the terminal from the calling process and reattaches it to another process. Use the SPAWN SHOW PROCESS /SUBPROCESSES command to list the names of the subprocesses. Use the DCL LOGOUT command to return to the original process. If the TCPWARE_DISABLE_SPAWN logical is enabled, ATTACH does not work.

FORMAT

ATTACH *process-name*

PARAMETERS

process_name

Specifies the name of a process to which you want your terminal attached. (Not all subprocesses can be attached; some testing may be required.)

CLEAR

Clears all information from the current configuration. (Functionally equivalent to ERASE.)

FORMAT

CLEAR

DELETE GATEWAY

Deletes a mail gateway.

FORMAT

DELETE GATEWAY *domain_name*

PARAMETERS

domain_name

Specifies the name of the domain whose gateway will be deleted.

DELETE LOCAL-DOMAIN

Deletes a domain from TCPware's list of local domains.

FORMAT

DELETE LOCAL-DOMAIN *domain_name*

PARAMETERS

domain_name

Specifies the name of the domain to delete from the list of local domains.

DELETE QUEUE-GROUP

Deletes a queue group or removes a node from a queue group. When a node is removed from a named queue group, it becomes part of the default queue group.

FORMAT

DELETE QUEUE-GROUP *group_name [node_names]*

PARAMETERS

group_name

Specifies the name of the group to delete or the name of the group from which to remove the specified nodes.

node_names

Specifies the VMScluster (SCS) node name to remove from the specified queue group.

ERASE

Erases all information from the current configuration. (Functionally equivalent to CLEAR.)

FORMAT

ERASE

EXIT

Saves the configuration file and exits from MAIL-CONFIG.

Format

EXIT

GET

Reads in a TCPware SMTP configuration file. (Functionally equivalent to USE.) After a GET, you can use the various configuration commands to modify the SMTP configuration.

FORMAT

GET *config_file*

PARAMETERS

config_file

Specifies the name of the SMTP configuration file to read in.

HELP

Invokes MAIL-CONFIG command help.

Format

HELP *[topic]*

Parameter

topic

(Optional) Topic for which you want help.

PUSH

Starts and attaches a DCL subprocess. If a parent process exists, attach to it. To return from DCL, use the ATTACH or the LOGOUT command. To switch back from a DCL subprocess, use the ATTACH command.

If the TCPWARE_DISABLE_SPAWN logical is set, PUSH does not work.

FORMAT

PUSH

QUIT

If the configuration file has been edited, QUIT prompts you to save the file before quitting.

FORMAT

QUIT

REMOVE GATEWAY

Functionally equivalent to DELETE GATEWAY.

FORMAT

REMOVE GATEWAY *domain_name*

PARAMETERS

domain_name

Specifies the name of the gateway to remove.

REMOVE QUEUE-GROUP

Functionally equivalent to DELETE QUEUE-GROUP.

FORMAT

REMOVE QUEUE-GROUP *group_name [node_names]*

PARAMETERS

group_name

Specifies the name of the group to remove or the name of the group from which to remove the specified nodes.

node_names

Specifies the VMScluster (SCS) node name to remove from the specified queue group.

SAVE

Writes the current TCPware SMTP configuration to SMTP configuration files. (Functionally equivalent to WRITE.)

FORMAT

SAVE *config_file*

PARAMETERS

config_file

Specifies the name of the file to which to write the current TCPware SMTP configuration (by default, the same file from which it was read).

SET ALIAS-FILE

Identifies the file that holds system-wide mail aliases.

FORMAT

SET ALIAS-FILE *[file-spec]*

PARAMETERS

file-spec

Specifies the name of the file that contains system-wide mail aliases (by default, TCPWARE:SMTP_ALIASES).

SET DECNET-DOMAIN

Sets the domain name for DECnet mail.

FORMAT

SET DECNET-DOMAIN *domain_name*

PARAMETERS

domain_name

Specifies the domain name for DECnet mail.

SET DELIVERY-RECEIPTS

Specifies whether mail receipts are sent when incoming mail containing Delivery-Receipt-To: or Return-Receipt-To: headers is submitted to the SMTP queue. If TRUE, mail receipts are sent.

FORMAT

SET DELIVERY-RECEIPTS { TRUE | FALSE }

SET DISABLE-PSIMAIL

When TRUE, the TCPware SMTP symbiont looks for messages addressed through PSImail, usually of the form PSI%address::user, and returns them to the sender marked user unknown. The default is FALSE. This parameter does not affect mail delivery to local users who have set up forwarding entries to PSImail addresses with the VMS MAIL SET FORWARD command.

FORMAT

SET DISABLE-PSIMAIL { TRUE | FALSE }

SET DISALLOW-USER-REPLY-TO

When set to TRUE, prevents VMS MAIL users from setting a Reply-To: header address with the TCPWARE_SMTP_REPLY_TO logical name.

FORMAT

SET DISALLOW-USER-REPLY-TO { TRUE | FALSE }

SET FORWARDER

Specifies the host that will forward mail messages to other hosts.

FORMAT

SET FORWARDER *[host_name]*

PARAMETERS

host_name

Specifies the name of the host to which mail is forwarded when attempts by the local system to send mail to a remote system fail because of a host name lookup failure.

If no host name is specified, no forwarder is used, and failed messages are tried repeatedly (based on the RETRY-INTERVAL setting) until they are returned to sender (based on the RETURN-INTERVAL setting).

SET FORWARD-LOCAL-MAIL

When TRUE, TCPware forwards mail addressed to users on the local host to a central mail hub specified by the FORWARDER parameter.

FORMAT

SET FORWARD-LOCAL-MAIL { TRUE | FALSE }

DESCRIPTION

To configure TCPware to direct mail to a central mail hub, you must specify the IP address of the mail hub with the FORWARDER parameter, and define the scope of addresses that you want the mail hub to handle.

By default, when users on the same TCPware host send mail to each other, TCPware does not route the messages through the mail hub. When FORWARD-LOCAL-MAIL is TRUE, TCPware forwards local mail to the mail hub.

To exclude a specific user from the local mail-forwarding system, add the following type of mail alias to TCPWARE:SMTP_ALIASES:

```
username : *
```

SET FORWARD-REMOTE-MAIL

When TRUE, TCPware forwards mail addressed to non-local users on a central mail hub specified by the FORWARDER parameter.

FORMAT

SET FORWARD-REMOTE-MAIL { TRUE | FALSE }

DESCRIPTION

To configure TCPware to direct mail to a central mail hub, you must specify the IP address of the mail hub with the FORWARDER parameter, and define the scope of addresses that you want the mail hub to handle.

By default, when TCPware users send mail to users on other hosts, TCPware does not route the messages through the mail hub. When FORWARD-REMOTE-MAIL is TRUE, TCPware forwards non-local mail to the mail hub.

By default TCPware considers all remote hosts non-local. You can add hosts in other domains to the local-domain list with the ADD LOCAL-DOMAIN command.

SET HEADER-CONTROL

Specifies which RFC-822 message headers are included in messages delivered to local VMS MAIL users.

FORMAT

SET HEADER-CONTROL *header_type*

PARAMETERS

header_type

NONE, MAJOR, or ALL.

- NONE eliminates the RFC-822 message headers from locally delivered VMS MAIL messages.
- MAJOR (the default) includes all but Received and Return Path headers.
- ALL includes all headers.

SET HOST-ALIAS-FILE

Specifies a file from which TCPware obtains a list of host aliases. A common use for SMTP host names is when your system is a member of a homogeneous VMScluster, and you want all mail from any cluster member to appear to be from the same host (for example, the cluster alias).

Unlike the MAIL-CONFIG SET SMTP-HOST-NAMES command which has a limit of 16 host names, SET HOST-ALIAS-FILE lets you specify a host alias file containing as many host aliases as needed.

Note! The host name or alias you specify should be registered in the Domain Name System or in the host tables of any system to which you send mail; otherwise, the recipients of your mail will be unable to reply to it.

If this logical name is not defined, the SMTP software looks for the file TCPWARE:SMTP_HOST_ALIASES by default.

FORMAT

SET HOST-ALIAS-FILE *file_spec*

PARAMETERS

file_spec

Specifies the file that contains a list of SMTP host names.

SET LOCAL-MAIL-FORWARDER

Forwards failed local mail to a specific host.

FORMAT

SET LOCAL-MAIL-FORWARDER *hostname*

PARAMETERS

hostname

Specifies the name of the host to which failed local mail is directed.

SET LOCASE-USERNAME

When FALSE, disables the lower-casing of usernames on outgoing VMS mail.

FORMAT

SET LOCASE-USERNAME

SET POSTMASTER

Identifies the user responsible for mail on the system.

FORMAT

SET POSTMASTER *[username]*

PARAMETERS

username

Specifies the name of the user who will receive messages addressed to Postmaster on the local host. If omitted, the user name POSTMASTER is used.

To assign multiple users as the postmaster, enter POSTMASTER, then create an alias for postmaster in the alias file. For example, to make both "username1" and "username2" postmasters, enter the following line in the alias file:

```
postmaster:     username1, username2;
```

SET QUEUE-COUNT

Specifies the number of mail processing queues that should be created on a system.

FORMAT

SET QUEUE-COUNT *node_name [count]*

PARAMETERS

node_name

Specifies the VMScluster (SCS) node name of the node whose queue count you wish to set, or specifies DEFAULT to set the default for all nodes not specifically set. In a non-cluster environment, only the DEFAULT setting is used.

count

Specifies the number of queues to create on the specified node. If a count is omitted, the queue-count setting for the specified node is removed.

SET REPLY-CONTROL

Specifies how Internet mail headers are mapped to the VMS MAIL "From" header.

FORMAT

SET REPLY-CONTROL *[hdr_types]*

PARAMETERS

hdr_types

Specifies a comma-delimited list of SMTP headers (ENVELOPE-FROM, FROM, or REPLY-TO) that are mapped to the VMS MAIL "From" header. The default is "ENVELOPE-FROM, FROM, REPLY-TO."

SET RESENT-HEADERS

When FALSE, the TCPware SMTP symbiont omits the Resent-From, Resent-To, and Resent-Date headers that are usually included when a message is forwarded using a VMS MAIL forwarding address. The default is TRUE.

Use this option if mail user agents at your site cannot properly distinguish between normal "From" headers and "Resent-From" headers.

FORMAT

SET RESENT-HEADERS { TRUE | FALSE }

SET RETRY-INTERVAL

Specifies the amount of time that elapses before another attempt is made to send a message after a failed attempt.

FORMAT

SET RETRY-INTERVAL *[interval]*

PARAMETERS

interval

Specifies the interval, in minutes (by default, 30 minutes).

SET RETURN-INTERVAL

Specifies the amount of time that a message can remain in the processing queue before it is returned to the sender.

FORMAT

SET RETURN-INTERVAL *[interval]*

PARAMETERS

interval

Specifies the interval, in hours; by default, 96 (four days). A message typically only remains in the processing queue if it cannot be sent over the network to a remote host. When such a message is returned to its sender, the returned message includes the reason why it could not be sent.

SET RFC822-TO-HEADER

When FALSE, disables the use of the RFC 822 To: header value for the VMS mail To.

FORMAT

SET RFC822-TO-HEADER

SET SEND-BROADCAST-CLASS

Specifies the broadcast class to use to deliver immediate (SEND) messages.

FORMAT

SET SEND-BROADCAST-CLASS *[class_number]*

PARAMETERS

class_number

Specifies the class-number in a range from 1 to 16, corresponding to the VMS USER1 through USER16 broadcast classes (by default, 16).

SET SMTP-HOST-NAMES

Sets the host name from which all outgoing mail appears to be sent and the aliases for which this host accepts incoming mail.

A common use for SMTP HOST NAME is when your system is a member of a homogeneous VMScluster, and you want all mail from any cluster member to appear to be from the same host.

FORMAT

SET SMTP-HOST-NAMES *host_names*

PARAMETERS

host_names

Contains a comma-delimited list of host names. The first name in the list specifies the host name from which all outgoing mail appears to be sent. The remaining host names in the list specify the aliases for which this host accepts incoming mail.

The specified host name or alias should be registered in the Domain Name System or in the host tables of any system that you send mail to; otherwise, the recipients of your mail will be unable to reply to it.

SET START-QUEUE-MANAGER

Determines whether START_SMTP.COM starts the VMS queue manager if it is not already running. The default is TRUE.

FORMAT

SET START-QUEUE-MANAGER { TRUE | FALSE}

SHOW

Displays the current configuration.

Format

SHOW

SPAWN

Executes a single DCL command, or if entered without options, starts a subprocess with the same effect as PUSH. To return from DCL, use the LOGOUT command. If the TCPWARE_DISABLE_SPAWN logical is set, SPAWN does not work.

FORMAT

SPAWN *[command]*

PARAMETERS

command

Specifies a command to execute. If you omit command, a DCL command line subprocess is created.

QUALIFIERS

/INPUT=file-spec

Specifies an input file to the command you enter with SPAWN.

/LOGICAL_NAMES
/NOLOGICAL_NAMES

Specifies that logical names and logical name tables are not copied to the subprocess.

/SYMBOLS
/NOSYMBOLS

Specifies that global and local names are not passed to the subprocess.

/WAIT
/NOWAIT

Returns control without waiting for the command to complete. Do not use this qualifier with commands that have prompts or screen displays.

/OUTPUT=file-spec

Specifies a file that retains the output of the command invoked with SPAWN. This qualifier only works when a single command is entered without creating a DCL subprocess. In addition, this qualifier is positional; you must enter it immediately after SPAWN or other qualifiers.

STATUS

Indicates whether the SMTP configuration has been modified.

FORMAT

STATUS

USE

Reads in a TCPware SMTP configuration file. After a USE, you can use the various configuration commands to modify the SMTP configuration. (Functionally equivalent to GET.)

FORMAT

USE *config_file*

PARAMETERS

config_file

Specifies the name of the SMTP configuration file to read in.

VERSION

Displays the MAIL-CONFIG version and release information.

FORMAT

VERSION

WRITE

Writes the current TCPware SMTP configuration to SMTP configuration files. (Functionally equivalent to SAVE.)

FORMAT

WRITE *config_file*

PARAMETERS

config_file

Specifies the name of the file to which to write the current TCPware SMTP configuration. By default, the configuration is saved to the same file from which it was read.