Program Directory for

TCP/IP for z/VM®

Level 640

Program Number 5741-A07

for Use with
z/VM Version 6 Release 4

Document Date: November 2016

GI13-3474-00

Note!

Before using this information and the product it supports, be sure to read the general information under “Notices” on page 81.

This program directory, dated November 2016, applies to IBM® TCP/IP for z/VM, level 640, Program Number 5741-A07.

A form for reader's comments appears at the back of this publication. When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© **Copyright International Business Machines Corporation 1990, 2016. All rights reserved.**
Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 1990, 2016

Figures

1.0 Introduction

This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information that corresponds to the material and procedures for installation and service of the following:

- TCP/IP for z/VM

Note: It is recommended that you review this program directory in its entirety before you install or service this program, then keep this document for future reference.

The program directory contains the following sections:

- 2.0, “Program Materials” on page 5 identifies basic (and optional) TCP/IP for z/VM program materials and documentation
- 3.0, “Program Support” on page 8 describes the IBM support available for TCP/IP for z/VM
- 4.0, “Program and Service Level Information” on page 11 lists APARs (program level fixes) that have been incorporated within TCP/IP for z/VM
- 5.0, “Installation Requirements and Considerations” on page 13 identifies resources and considerations for installing and using TCP/IP for z/VM
- 6.0, “Installation Instructions” on page 41 provides detailed installation instructions for TCP/IP for z/VM
- 7.0, “Service Instructions” on page 54 provides detailed servicing instructions for TCP/IP for z/VM
- Appendix A, “TCP/IP Utilities” on page 57 provides information about various TCP/IP for z/VM utility programs
- Appendix B, “TCP/IP for z/VM Local Modifications” on page 68 provides information to help you implement local modifications to various TCP/IP for z/VM components
- Appendix C, “TCP/IP for z/VM Build Lists” on page 69 provides information about the VMSES/E build lists used to maintain TCP/IP for z/VM
- Appendix D, “Copying TCP/IP for z/VM Client Code to the Y-Disk” on page 71 provides considerations and optional instructions for copying client files to the system Product Code minidisk
- Appendix E, “Managing TCP/IP Files with Unique Service Requirements” on page 74 provides information about TCP/IP files for which extenuating service considerations and procedures are applicable.

Obtaining Updated Planning Information

Before you install TCP/IP for z/VM, read 3.1, “Preventive Service Planning” on page 8. This section describes how to obtain any updates to the information and procedures presented within this program directory.

© Copyright IBM Corp. 1990, 2016

1.1 Program Description

TCP/IP (Transmission Control Protocol/Internet Protocol) enables z/VM customers to participate in a multivendor, open networking environment using the TCP/IP protocol suite for communications and interoperability. The applications included in TCP/IP provide the ability to transfer files, send mail, log on a remote host, allow access from any other TCP/IP node in the network, and perform other network client and server functions.

Transmission Control Protocol/Internet Protocol for z/VM, level 640, (TCP/IP for z/VM) contains the functions provided by TCP/IP for z/VM, level 630, and provides the following enhancements:

- Upgrade of the **z/VM TLS/SSL server** to **z/OS V2.2 Equivalency**, which includes support for:
  - RFC 5280 Certificate Validation Upgrade (introduces support for Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)
  - PKCS #12 Certificate Store (function already introduced with z/VM version 6 release 3 APAR PI29130)
  - OCSP support, which enhances certificate revocation checking and flexibility, with:
    - support for retrieval of CRLs through HTTP URLs
    - more flexible processing of CRLs from LDAP
    - support for retrieval of revocation information through OCSP

  In addition, these z/VM TLS/SSL server changes have been implemented:
  - Inclusion of **z/OS V2.1 Equivalency** support (introduced with z/VM version 6 release 3 APAR PI40702), which facilitate exploitation of these functions:
    - AES Galois-Counter Mode (AES GCM), a TLS 1.2 symmetric key algorithm which is more secure than the current CBC mechanism employed today.
    - Enablement of DSA Certificates in MODE NIST-800-131a, an update to the size of the DSS certificates the server can support for asymmetric encryption
  - Inclusion of support to use PKCS #12 formatted files as certificate and key repositories. PKCS #12 is a more common format than the .kdb files used by gskkyman and System SSL today. Inclusion of this functionality allows for greater interoperability between platforms (including OpenSSL) and ease of use.
  - The default protocol levels for now are TLS 1.2 and TLS 1.1. All other protocols are disabled by default.
  - Inclusion of support for the VMSSL command **ENABLE** operand, which enables use of a specific cipher suite that is disabled by default — these being: 00, 01, 02, 03, 04, 05, 06 and 3B.
  - These fixed Diffie Hellman cipher suites now are disabled by default:

    0F, 0C, 10, 0D, 31, 30, 37, 36, 3F, 3E, 69, 68, A5, A1, A0 and A4.
  - Inclusion of secure RSCS TCPNJE links support (introduced with z/VM version 6 release 3 APAR PI56474).

- Upgrade of the **MPRoute** server to **z/OS V2.2 Equivalency**, which includes these functional enhancements:
  - Deprecates the **OMPROUTE_OPTIONS.hello_hi** environment variable.
  - Processes inbound OSPF hello packets from neighbors at the highest priority, for the purpose of maintaining OSPF adjacencies.
  - Modifications to avoid the potential for an abend when formatting or parsing OSPF packet content.
  - Enhancements to existing informational and debug messages, to cite more specific information when an IOCTL call has failed.
- Upgrade of the **z/VM LDAP Server and client utilities** to **z/OS V2.2 equivalency**, which includes these functional enhancements:
  - Group Search Limits updates, which enhances the setting of search limits by allowing search and time limits to be set on a group basis.
  - Admin Roles updates, which enhances the server to allow for multiple DNs, group or non-group, to be set as administration DNs. Currently, only one DN can be given administration privileges. The definitions can be in the LDAP directory or in SAF.
  - Page and Sort Search updates, which enhances the server and ldapsearch client utility to provide paged and/or sorted search results.

    Paged search results allows clients to receive just a subset of search results (a page) instead of the entire list. The next page of entries is returned to the client application for each subsequent paged results request submitted by the client until the operation is canceled or the last result is returned.

    Sorted search results allows clients to receive sorted search results based on a list of criteria, where each criterion represents a sort key.
  - TLS V1.2 Support, which makes use of the TLS V1.1, TLS V1.2 and NSA Suite B Cryptography support in System SSL.
  - Activity Log enhancements that provide improved activity log features by adding new records for events that were previously not logged, and useful information to existing records so that better auditing and problem determination can be done.
  - Dynamic Group Performance, which provides performance enhancements for Dynamic Groups.
  - Password Policy Attribute Replication, which provides consistent replication updates of password policy operational attributes on all servers when they get updated in a read-only server in a replication topology.
- **Domain Name Server (DNS) IPv6 support**, which:
  - accommodates use of IPv6 domain name server addresses as part of the **TCPIP DATA** configuration file **NSINTERADDR** statement
  - includes various CMS resolver IPv6 enhancements
  - adds TCP/IP stack support for UDP over IPv6
  - updates IPWIZARD configuration support to accommodate of IPv6 domain name server addresses
  - provides REXX Sockets toleration for IPv6 addresses specified for an **NSINTERADDR** statement
- Modification of the **SMTP server command exit (SMTPCMDX)** to reject VRFY and EXPN commands, by default.

- Inclusion of FTP client support for the FTP DATA file statement **EPSV4 TRUE/FALSE** (introduced with z/VM version 6 release 3 APAR PM90145). This statement, and corresponding **LOCSITE** command operands EPSV4 / NOEPSV4 allow one to control whether the FTP client attempts use of the EPRT/EPSV command when connections with a remote server are established for data transfer.

  Notes:

  1. The following servers (and associated resources) have been removed from TCP/IP for z/VM:

     – IBM zEnterprise Unified Resource Manager - Ensemble Management server (DTCENS1)
     – IBM zEnterprise Unified Resource Manager - Ensemble Management server (DTCENS2)

     and have been replaced with resources for additional virtual switch (VSWITCH) controller virtual machines:

     – Virtual switch controller virtual machine (DTCVSW3)
     – Virtual switch controller virtual machine (DTCVSW4)

     These changes are part of an ongoing effort to provide only those TCP/IP services that are required by customers to support their enterprise.

2.0 Program Materials

An IBM program is identified by a program number. The program number for TCP/IP for z/VM is 5741-A07.

The z/VM version 6 release 4 program announcement material provides detailed information about features supported by TCP/IP for z/VM. If you have not already received a copy of this information, contact your IBM marketing representative.

The following sections identify:

- basic and optional program materials that are applicable to this program
- publications useful during installation and service.

2.1 Basic Machine-Readable Material

TCP/IP for z/VM is distributed as part of the z/VM version 6 release 4 System deliverable. Refer to the z/VM version 6 release 4 Software Announcement for information about ordering z/VM and its features.

2.2 Optional Machine-Readable Material

There are no features or optional machine-readable materials associated with TCP/IP for z/VM.

2.3 Program Publications

The following sections identify the basic publications associated with TCP/IP for z/VM. There are no optional publications for this component of z/VM.

2.3.1 Basic Program Publications

Publications associated with TCP/IP for z/VM are listed in Figure 1:

Figure 1 (Page 1 of 2). Basic Material: Unlicensed Publications

Publication Title	Form Number
TCP/IP Planning and Customization	SC24-6238
TCP/IP LDAP Administration Guide	SC24-6236
TCP/IP User's Guide	SC24-6240
TCP/IP Messages and Codes	GC24-6237
TCP/IP Programmer's Reference	SC24-6239

© Copyright IBM Corp. 1990, 2016

Figure 1 (Page 2 of 2). Basic Material: Unlicensed Publications

Publication Title	Form Number
TCP/IP Diagnosis Guide	GC24-6235

2.3.2 Softcopy Publications

TCP/IP for z/VM publications are supplied in softcopy form as part of the *IBM Online Library: z/VM Collection* in both BookManager® and Adobe® Portable Document Format (PDF) file formats. One copy of the *IBM Online Library: z/VM Collection* DVD is included when you order the basic materials for z/VM version 6 release 4.

TCP/IP for z/VM softcopy publications, including this Program Directory, also are available as Adobe PDF files from the TCP/IP for z/VM home page and z/VM Library pages on the World Wide Web. The applicable URLs are:

```
www.vm.ibm.com/related/tcpip/
www.vm.ibm.com/library/
```

In addition, TCP/IP for z/VM publications (except this Program Directory) are available at the z/VM Information Center web site. The URL for this site is:

```
www.ibm.com/support/knowledgecenter/SSB27U
```

z/VM publications also can be separately ordered through the IBM Publications Center (for a fee), by using specific publication numbers. The URL for the IBM Publications Center is:

```
www.ibm.com/shop/publications/order
```

The IBM Publications Center is a world wide central repository for IBM product publications and marketing material. Note that a large number of publications are available as on-line files (in various formats, such as Adobe PDF), which currently can be downloaded free of charge.

2.4 Program Source Materials

No viewable program listings are provided for TCP/IP for z/VM.

2.5 Publications Useful During Installation and Service

The publications listed in Figure 2 on page 7 might be useful during the installation and servicing of TCP/IP for z/VM. Most such publications likely are available at the z/VM Library page on the World Wide Web. The URL for this page is:

```
www.vm.ibm.com/library/
```

To obtain copies of publications that are not available from the z/VM Library web page, contact your IBM representative or access the IBM Publications Center on the World Wide Web; the URL for the home page of this site is:

```
www.ibm.com/shop/publications/order
```

Figure 2. Publications Useful During Installation / Service on z/VM version 6 release 4

Publication Title	Form Number
TCP/IP Planning and Customization	SC24-6238
TCP/IP LDAP Administration Guide	SC24-6236
TCP/IP User's Guide	SC24-6240
z/VM: Installation Guide	GC24-6246
z/VM: Service Guide	GC24-6247
z/VM: VMSES/E Introduction and Reference	GC24-6243
z/VM: CMS Planning and Administration	SC24-6171
z/VM: CMS File Pool Planning, Administration, and Operation	SC24-6167
z/VM: CP Planning and Administration	SC24-6178
XL C/C++ for z/VM Run-Time Library Reference	SC09-7624
z/VM: CMS Callable Services Reference	SC24-6165
z/VM: CMS Commands and Utilities Reference	SC24-6166
z/VM: REXX/VM Reference	SC24-6221
z/VM: CMS and REXX/VM Messages and Codes	GC24-6161
z/VM: Other Components Messages and Codes	GC24-6207

3.0 Program Support

This section describes the IBM support available for TCP/IP for z/VM.

3.1 Preventive Service Planning

Before you install TCP/IP for z/VM, check with your IBM Support Center or use IBMLink™ to determine if Preventive Service Planning (PSP) information is available that you should know. To obtain this information, specify the appropriate UPGRADE and SUBSET values listed in Figure 3:

Figure 3. PSP Upgrade and Subset ID

RETAIN™				
COMPID	**Release**	**Upgrade**	**Subset**	**Component Name**
5735FAL00	640	TCPIP640	VM640	TCP/IP for z/VM
5735FAL00	640	TCPIP640	*yynn*RSU	RSU Service Recommendations

RSU-BY-LVL information can be obtained from the VM service RSU web site at this URL:

```
www.vm.ibm.com/service/rsu/
```

3.2 Statement of Support Procedures

With TCP/IP for z/VM, you are entitled to support under the basic warranty for z/VM version 6 release 4. Also, note that z/VM Software Subscription and Support is *automatically* added when you order z/VM — this provides zSeries service to which you are likely accustomed.

Note: You must take specific action when you order z/VM to decline z/VM Software Subscription and Support.

Report any difficulties you have using this program to your IBM Support Center. If an APAR (Authorized Program Analysis Report) is required, the Support Center will provide the address to which any needed documentation can be sent.

Figure 4 identifies IBM RETAIN information — the Component ID (COMPID), Release, and Field Engineering Service Number (FESN) — that corresponds to TCP/IP for z/VM:

Figure 4. Component IDs

RETAIN			
COMPID	**Release**	**Component Name**	**FESN**
5735FAL00	640	TCP/IP for z/VM	0461035

© Copyright IBM Corp. 1990, 2016

3.3 Service Information

The IBM Software Support Center provides telephone assistance for problem diagnosis and resolution. You can call the IBM Software Support Center at any time; you will receive a return call within eight business hours (Monday—Friday, 8:00 a.m.—5:00 p.m., local customer time). The number to call is:

1-800-426-7378 (or, **1-800-IBM-SERV**)

Outside of the United States or Puerto Rico, contact your local IBM representative or your authorized supplier.

Various installation and service-related items, such as the Preventive Service Planning (PSP) "bucket" and current RSU status/content information, are available from the TCP/IP for z/VM home page and z/VM RSU Content pages on the World Wide Web. The applicable URLs are:

```
www.vm.ibm.com/related/tcpip/
www.vm.ibm.com/service/rsu/
```

3.3.1 Problem Documentation

When working with TCP/IP for z/VM support personnel on problems associated with an active Problem Management Record (PMR), diagnostic information might occasionally be requested. In such cases, the support staff will work with you to determine how to best provide any requested documentation. In general, providing problem documentation in electronic format (such as to an FTP site or via e-mail) is the most effective (and expedient) manner to provide this information.

However, in the event that problem documentation must be provided using non-electronic media, the address that follows can be used.

Figure 5. Physical Media Problem Documentation Submission Address

Format	Address
Physical Media	IBM Corporation Attention: *IBM contact name* Dept. G37G 1701 North St. Endicott, NY 13760

3.3.2 Communicating Your Comments to IBM

If you have comments about or suggestions for improving the TCP/IP for z/VM program product, or this Program Directory, please provide them to IBM through one of the following means:

- If you prefer to send comments by mail, use the address provided with the Reader's Comments form (RCF) at the back of this document

- If you prefer to send comments electronically, please use the appropriate form provided by the "Contact z/VM development" link of the z/VM home page on the World Wide Web. The URL for this page is:

  `www.vm.ibm.com`

If you provide doumentation-related comments, please include:

- the title of this publication
- the section title, section number, or topic to which your comment applies.

4.0 Program and Service Level Information

This section identifies the program level and any relevant service levels of TCP/IP for z/VM. In this context, *program level* refers to APAR fixes incorporated within the TCP/IP for z/VM program; *service level* refers to PTFs that are supplied with this product. Information about the TCP/IP for z/VM cumulative service deliverable is provided as well.

4.1 Program Level Information - TCP/IP for z/VM

APAR fixes (for previous levels of IBM TCP/IP for VM) that have been incorporated into this level of TCP/IP for z/VM are:

PI04999	PI06241	PI06358	PI08085	PI08319	PI11640	PI13481	PI13614
PI16228	PI16680	PI19122	PI19560	PI20509	PI25555	PI26239	PI26525
PI28028	PI29130	PI29479	PI30085	PI30359	PI31200	PI31202	PI32316
PI32624	PI36658	PI36920	PI38574	PI38762	PI40702	PI41073	PI41317
PI41479	PI41480	PI43610	PI44132	PI50876	PI51726	PI52850	PI53104
PI56350	PI56474	PI56516	PI57886	PI59963	PI60636	PI61469	PM83945
PM88668	PM89511	PM90145	PM90851	PM93610	PM93619	PM93646	PM94969
PM95488	PM95516	PM96884	PM99762				

4.2 Service Level Information

Before you install and configure TCP/IP for z/VM, you should review the TCPIP640 PSP (Preventive Service Planning) “bucket” for updated installation information that you should be aware of, or for information about PTFs that should be installed. Specify upgrade and subset values of **TCPIP640** and **VM640**, respectively, when you request or obtain this information.

© Copyright IBM Corp. 1990, 2016

4.3 Cumulative Service (RSU) Information

Cumulative service for TCP/IP for z/VM is available through a periodic, preventive service deliverable, the Recommended Service Upgrade (RSU). The RSU is used to provide service updates for multiple z/VM components (including TCP/IP for z/VM) and is often referred to as a *stacked* RSU.

The current-level of the stacked z/VM RSU can be obtained using the information provided in Figure 6:

Figure 6. Cumulative Service (RSU) Information

	RETAIN	
COMPID	**Release**	**PTF**
568411202	RSU	**UM97640**

Note: Current RSU status and content information is available at the z/VM RSU Content pages on the World Wide Web. The URL for this home page is:

```
www.vm.ibm.com/service/rsu/
```

5.0 Installation Requirements and Considerations

The following sections identify system requirements for installing TCP/IP for z/VM.

5.1 Hardware Requirements

There are no special hardware requirements to install TCP/IP for z/VM. Additional hardware requirements for exploiting specific functions of TCP/IP for z/VM are documented in the announcement material and in *TCP/IP Planning and Customization* (SC24-6238).

5.2 Program Considerations

The following sections list programming considerations for installing TCP/IP for z/VM.

5.2.1 Operating System Requirements

TCP/IP for z/VM requires the following operating system:

- z/VM version 6 release 4
- CMS Level 28

5.2.2 Other Program Product Requirements

IBM VS Pascal Version 1 Release 2, Compiler and Library (5668-767) has been used to build the Pascal components that are part of TCP/IP for z/VM. If local modifications are to be made to the Pascal source files that pertain to Pascal-based TCP/IP servers or applications (such as the TCP/IP or SMTP server, or the FTP server and client), this compiler level is required.

IBM XL C/C++ for z/VM, V1.3 (5654-A22) has been used to build the C components that are part of TCP/IP for z/VM. If any local modifications are to be made to the C source files that pertain TCP/IP C-based TCP/IP servers or applications (such as the NFS server, or the PING client command), this compiler level, or greater, is required.

Language Environment® for z/VM, supplied as an installed component of z/VM version 6 release 4, is necessary to use the TCP/IP services listed here.

- Internet Message Access Protocol server (IMAP)
- Lightweight Directory Access Protocol server (LDAPSRV)
- Multiple Protocol ROUTE server (MPRoute)
- Portmapper server (PORTMAP)
- Remote Execution daemon (REXECD and RXAGENT*n*)
- Secure Socket Layer (SSL) Server (SSL*nnnnn* pool servers)
- SNMP Query Engine, Agent and Subagent (SNMPD, SNMPQE and SNMPSUBA)

© Copyright IBM Corp. 1990, 2016

- Sockets Applications Programming Interface
- Network File System server (VMNFS)

Various client functions also require Language Environment for z/VM support. Representative of these are:

- CMSRESOL and CMSRESXA
- DIG
- LDAP Client Applications
- NFS (client)
- NSLOOKUP
- PING
- RPCGEN and RPCINFO
- TRACERTE

Additional software requirements for exploiting specific TCP/IP for z/VM functions are documented in the announcement material and in *TCP/IP Planning and Customization* (SC24-6238).

5.2.3 Program Installation/Service Considerations

This section describes items that should be considered before you install or service TCP/IP for z/VM

- VMSES/E is required to install and service this product.
- **All TCP/IP for z/VM service activity** now must be performed using the appropriate MAINT*vrm* user ID. For this program level, this user ID is **MAINT640**.
- Any user ID that is used to perform TCP/IP for z/VM installation and service actions (such as to use the **SSLPOOL** utility to alter or add an SSL server pool) must have ***file pool administration authority*** for the **VMSYS** file pool. As supplied with the z/VM version 6 release 4 System deliverable, both the MAINT640 and TCP/IP service resource owner user ID (6VMTCP40) are enrolled as file pool administrators for this file pool.
- To allow for the installation of, and application of service updates for, BFS-resident TCP/IP LDAP components, **the z/VM system file pools** (**VMSYS**, **VMSYSU** and **VMSYSR**, by default) ***must*** **be available and in operation**.

Note! Minidisk and SFS Requirements

Certain minidisks or SFS directories **must** be defined for use by individual TCP/IP server machines, regardless of whether TCP/IP for z/VM is maintained using service minidisks or Shared File System directories. This requirement is explained further in item 7 of 5.3, "DASD Storage and User ID Requirements" on page 30.

- TCP/IP for z/VM source files are supplied in ***packed*** format. Use the CMS COPYFILE command (with its UNPACK option) to unpack TCP/IP source files prior to their use.

5.2.4 Migration Considerations

This section provides general information about changes to TCP/IP for z/VM that you should be aware of prior to its installation and use. The changes described herein are presented on a level-to-level basis, and grouped with respect to these topics:

- VMSES/E Migration Procedures
- Packaging
- General TCP/IP Usage
- FTP Client
- General TCP/IP Server Configuration
- FTP Server
- IMAP Server
- LDAP Server
- NETSTAT Command
- MPRoute Server
- Remote Execution Services
- SMTP Server
- SNMP Server and Client
- TLS/SSL Server
- **TCP/IP (Stack) Server**
- Telnet Server and Client

For the most part, these changes have been implemented to accommodate the introduction of new functions and improvements to existing functions. In some cases, existing functions might have been removed or replaced by alternative functions.

Migration Information for Levels not Listed

For information about changes that have been implemented in levels of TCP/IP for z/VM that are not listed here, check the *TCP/IP - End-of-Service Reference Information* and *Migration Considerations for End-of-Service Levels* sections of the TCP/IP for z/VM home page on the World Wide Web). The URL for this home page is:

```
www.vm.ibm.com/related/tcpip/
```

Note - Supported Environments

TCP/IP level 640 is supported on corresponding level 640 releases of CP and CMS only. Refer to section 5.2.1, “Operating System Requirements” on page 13 for details about the CP and CMS levels required for using TCP/IP level 640.

If TCP/IP level 640 services and functions are used with other CP or CMS levels (as might be the case for migration testing purposes), certain capabilities might be limited or might not function. In some instances, non-TCP/IP service updates ***might*** be available to facilitate the temporary use of TCP/IP in such a transitory environment.

5.2.4.1 VMSES/E Migration Procedures

5.2.4.1.1 General Information

- If the VMSES/E migration procedures (documented in *z/VM: Installation Guide*) are used to migrate from a supported z/VM system to z/VM version 6 release 4, then TCP/IP customizable files will be migrated to z/VM version 6 release 4, where possible.

  If certain customizable files (for example, a sample configuration file) have been changed by IBM on the new, serviced level of TCP/IP for z/VM, and you have modified these files for use on your prior-level system, the migration utilities will provide information about pertinent files for which your changes must be reworked.

  Note that when the VMSES/E migration procedures are used, no attempt is made to migrate data that resides on prior-level TCP/IP for z/VM minidisk or SFS directories that pertain to servers or resources that have been removed from the current level of TCP/IP for z/VM.

5.2.4.2 Packaging

5.2.4.2.1 General Information About TCP/IP Level 640

- TCP/IP level 640 is included as a pre-installed component of the z/VM product; its use is governed by your license for z/VM.
- TCP/IP level 640 is **not** separately orderable or installable from the z/VM product. However, service that is obtained for TCP/IP for z/VM can be *applied* separately from that for z/VM.
- TCP/IP level 640 RSU service is provided as part of a *stacked* z/VM RSU, and not as a separately orderable RSU. Corrective (COR) service for TCP/IP for z/VM can be obtained and applied separately from other z/VM service.
- This level of TCP/IP relies on the presence of certain functions in the z/VM version 6 release 4 levels of CP and CMS. The converse is also true — using z/VM version 6 release 4 CMS requires that TCP/IP level 640 be present, to accommodate those functions that use TCP/IP (DNS) resolver services.

  Abends and incorrect results are possible if you attempt to use mixed levels of TCP/IP, CP and CMS.
- TCP/IP softcopy publications are provided in the same manner as other z/VM softcopy publications, and are included with these z/VM publications.

5.2.4.2.2 Changes Introduced in TCP/IP Level 640

- Resources associated with the following servers have been removed:
  - IBM zEnterprise Unified Resource Manager - Ensemble Management server (DTCENS1)
  - IBM zEnterprise Unified Resource Manager - Ensemble Management server (DTCENS2)

  and have been replaced with resources for additional virtual switch (VSWITCH) controller virtual machines:
  - Virtual switch controller virtual machine (DTCVSW3)
  - Virtual switch controller virtual machine (DTCVSW4)

- The MAINT*vrm* user ID for performing TCP/IP for z/VM service activity is **MAINT640**, whereas the **6VMTCP40** user ID is the designated owner of TCP/IP minidisks and SFS resources.

5.2.4.2.3 Changes Introduced in TCP/IP Level 630

- Resources associated with the following services have been removed:
  - Dynamic Host Configuration Protocol server (DHCPD)
  - Line Printer Daemon server (LPSERVE)

  These changes are part of an ongoing effort to provide only those TCP/IP services that are required by customers to support their enterprise.

5.2.4.2.4 Changes Introduced in TCP/IP Level 620

- Significant packaging changes, which affect all of z/VM and its components, have been implemented with z/VM version 6 release 2 to provide support for a z/VM single system image (SSI) environment. With these changes, the role of the **6VMTCP20** user ID has changed. This user ID no longer is intended for use to service and maintain TCP/IP for z/VM. Instead, the **6VMTCP20** user ID serves only as the designated owner of the various minidisks and SFS resources required for product maintenance purposes.

  All TCP/IP for z/VM service activity must be performed using the MAINT*vrm* user ID (**MAINT620**).
- The **TCP2PROD** command no longer is used for placing TCP/IP files into production; instead, the VMSES/E **PUT2PROD** command now directly performs this function. With this change, the TCP2PROD command no longer is supplied with z/VM. The **PRODUTL** command, included as part of the VMSES/E component of z/VM, provides equivalent function and capabilities, and can be used (if needed) in place of TCP2PROD.
- The TCP/IP CATALOG file (**6VMTCP20 CATALOG**) no longer is used for control purposes when TCP/IP product files are placed into production. For the most part, this file now is used for select processing that pertains to TCP/IP for z/VM sample files..
- Resources associated with the following services (for which support was withdrawn from TCP/IP for z/VM, effective as of level 540) have been removed:
  - Network Database (NDB)
  - SNALINK
  - Trivial File Transfer Protocol (TFTP)
  - X.25 support

  Included with these changes is removal of these user IDs and any associated minidisks:
  - ADMSERV
  - GCSXA
  - NAMESRV
  - NDBPMGR
  - NDBSRV01
  - SNALNKA
  - TFTPD
  - VMKERB

  - VSMSERVE
  - X25IPI

- The **SSLSERV** user ID no longer is included as part of the z/VM version 6 release 4 System deliverable. In its place, an **SSL server "pool"** of five servers now is defined as part of the system. While continued use of a single-instance, minidisk-based server (such as SSLSERV) still is possible and remains supported, the preferred configuration for running a single SSL server is to alter the SSL pool definition such that only one pool sever is defined. This can readily be accomplished by a CP directory change to the SSL server **POOL** definition.
- The **SSLPOOL** utility, supplied as a sample exec with the PTFs for the SSL Server Performance and Scalability Enhancements, has been incorporated as a formally supported command. The SSLPOOL SAMPEXEC file no longer is supplied.
- Consult the **6VMTCP20 PLANINFO** file for detailed information about how specific TCP/IP user IDs have been defined. This file is located on the 6VMTCP20 191 minidisk.

5.2.4.2.5 Changes Introduced in TCP/IP Level 610

- No significant changes have been introduced with TCP/IP Level 610.

  Note: With TCP/IP Level 610, the PTF for APAR PK65850 (SSL Server Enablement) is ***not*** required — the CMS-based SSL server supplied with the z/VM version 6 release 4 System deliverable is fully enabled.

5.2.4.2.6 Changes Introduced in TCP/IP Level 540

- The default minimum virtual storage size defined for the **TCPIP** (stack) server virtual machines has been increased to **128M**, to better accommodate a wide variety of workloads without the need to redefine storage allocated for this server.
- The directory entries for the **MPROUTE** and the **SSLSERV** virtual machines now include a **SHARE RELATIVE 3000** statement, to allow these servers to better handle activity that is closely associated with TCP/IP server processing.
- With the PTF for **APAR PK65850**, a CMS-based SSL server is provided with TCP/IP for z/VM that no longer requires operation within a Linux guest. The components required for running this updated server implementation are installed and serviced through the same means as other CMS-based TCP/IP servers — installation of an updated RPM file within a Linux guest no longer is necessary. For this reason, the minidisks that follow have been deleted with this level of TCP/IP for z/VM:
  - 5VMTCP40 493
  - SSLSERV 201
  - SSLSERV 203
- The **GSKADMIN** user ID has been added. This user ID has been defined with appropriate authorization to perform certificate management operations for the SSL server key database, now maintained within the z/VM Byte File System (BFS). The GSKADMIN user ID is also defined as an SSL server administrative user ID.

5.2.4.3 General TCP/IP Usage

5.2.4.3.1 Changes Introduced in TCP/IP Level 640

- **Domain Name Server (DNS) IPv6 support** is added, which:
  - accommodates use of IPv6 domain name server addresses as part of the **TCPIP DATA** configuration file **NSINTERADDR** statement
  - includes various CMS resolver IPv6 enhancements
  - adds TCP/IP stack support for UDP over IPv6
  - updates IPWIZARD configuration support to accommodate of IPv6 domain name server addresses
  - provides REXX Sockets toleration for IPv6 addresses specified for an **NSINTERADDR** statement

5.2.4.3.2 Changes Introduced in TCP/IP Level 620

- The **IPFORMAT** diagnostic utility has been updated to support a **PCAP** operand, which causes which causes TYPE GT and TYPE LAN trace data to be formatted in PCAP data format, to allow for its review and evaluation using a GUI-based trace analysis tool.
- The CMS **NOTE** and **SENDFILE** commands (SMTP clients) have been updated to accommodate the use of **IPv6**.

  Note that IPv6 SMTP connections cannot be secured using SSL because the z/VM SSL server does not incorporate IPv6 support.

5.2.4.3.3 Changes Introduced in TCP/IP Level 540

- The **RPCINFO** function has been updated to use the **ETC HOSTS** file as the local site table when host names are resolved. If the ETC HOSTS file is not present, RPCINFO continues to use the HOSTS SITEINFO file.
- Processing of the **CERTNOCHECK** operand for TLS connections associated with the FTP and Telnet clients (and, the SMTP server) has been changed such that this operand is equivalent to the **CERTFULLCHECK** operand.
- The **TCPSLVL** utility has been modified such that results now are directed to a file (named *partname* SLVLDATA) by default. To direct command output to the console, a new **CONSOLE** option must be used. For more information, see Appendix A, “TCP/IP Utilities” on page 57.

5.2.4.4 FTP Client

5.2.4.4.1 Changes Introduced in TCP/IP Level 640

- Support for the FTP DATA file statement **EPSV4 TRUE/FALSE** (introduced with z/VM version 6 release 3 APAR PM90145) is included. This statement, and corresponding **LOCSITE** command operands EPSV4 / NOEPSV4 allow one to control whether the FTP client attempts use of the EPRT/EPSV command when connections with a remote server are established for data transfer.

5.2.4.4.2 Changes Introduced in TCP/IP Level 630

- The FTP client has been updated to accommodate the use of SSL to secure **IPv6** FTP connections.

5.2.4.4.3 Changes Introduced in TCP/IP Level 620

- The FTP client has been updated to accommodate the use of **IPv6**.

  Note that IPv6 FTP connections cannot be secured using SSL because the z/VM SSL server does not incorporate IPv6 support.

5.2.4.4.4 Changes Introduced in TCP/IP Level 540

- Support is added for changing an FTP control connection from a secure state to a clear state through use of the Clear Control Connection (**CCC**) subcommand.
- Processing of the **CERTNOCHECK** operand for TLS connections associated with the FTP client has been changed such that this operand is equivalent to the **CERTFULLCHECK** operand.

5.2.4.5 General TCP/IP Server Configuration

5.2.4.6 FTP Server

5.2.4.6.1 Changes Introduced in TCP/IP Level 630

- The FTP server has been updated to accommodate the use of SSL to secure **IPv6** FTP connections.

5.2.4.6.2 Changes Introduced in TCP/IP Level 620

- The FTP server has been updated to accommodate connections using **IPv6**.

  Note that IPv6 FTP connections cannot be secured using SSL because the z/VM SSL server does not incorporate IPv6 support.

5.2.4.7 IMAP Server

5.2.4.7.1 Changes Introduced in TCP/IP Level 540

- The mechanism for defining user IDs that are to be authorized to use the **IMAPADM EXEC** has changed. Instead of directly creating a $SERVER$ NAMES private resource registration file, authorized user IDs are now listed via the DTCPARMS file tag **:Admin_ID_List.**

5.2.4.8 LDAP Server

5.2.4.8.1 Changes Introduced in TCP/IP Level 640

- The **z/VM LDAP Server and client utilities** have been upgraded to **z/OS 2.2 Equivalency**, and include these functional enhancements:
  - Group Search Limits updates, which enhances the setting of search limits by allowing search and time limits to be set on a group basis.
  - Admin Roles updates, which enhances the server to allow for multiple DNs, group or non-group, to be set as administration DNs. Currently, only one DN can be given administration privileges. The definitions can be in the LDAP directory or in SAF.

- Page and Sort Search updates, which enhances the server and ldapsearch client utility to provide paged and/or sorted search results.

  Paged search results allows clients to receive just a subset of search results (a page) instead of the entire list. The next page of entries is returned to the client application for each subsequent paged results request submitted by the client until the operation is canceled or the last result is returned.

  Sorted search results allows clients to receive sorted search results based on a list of criteria, where each criterion represents a sort key.
- TLS V1.2 Support, which makes use of the TLS V1.1, TLS V1.2 and NSA Suite B Cryptography support in System SSL.
- Activity Log enhancements that provide improved activity log features by adding new records for events that were previously not logged, and useful information to existing records so that better auditing and problem determination can be done.
- Dynamic Group Performance, which provides performance enhancements for Dynamic Groups.
- Password Policy Attribute Replication, which provides consistent replication updates of password policy operational attributes on all servers when they get updated in a read-only server in a replication topology.

5.2.4.8.2 Changes Introduced in TCP/IP Level 540

- The Lightweight Directory Access Protocol (LDAP) server (**LDAPSRV**) has been updated to a function level equivalent to the z/OS level 1.10 Tivoli Directory Server.
- Server plug-in support has been added, to allow the functionality of the directory server to be extended.
- Support for RACF change logging and password/phrase enveloping is introduced.

5.2.4.9 NETSTAT Command

5.2.4.9.1 Changes Introduced in TCP/IP Level 630

- As part of the updates to provide SSL support for IPv6 secure connections, the NETSTAT IDENT SSL command has been enhanced to handle and display IPv6 secure connection data.

5.2.4.9.2 Changes Introduced in TCP/IP Level 620

- With the upgrade of MPROUTE to z/OS 1.12 equivalency, the following updates are included:
  - support for a **ROUTERADV** option for the **NETSTAT CONFIG** command. This option can be used to display the router advertisement configuration parameters of a TCP/IP server.
  - the **NETSTAT GATE** and **NETSTAT CONFIG HELP** commands include new output fields.
- Support for the **OSAINFO** option is introduced. This option displays basic information (such as IP and MAC addresses) from the OSA Address Table (OAT) for TCP/IP devices that are defined on supported OSA-Express cards.

5.2.4.9.3 Changes Introduced in TCP/IP Level 610

- With the PTFs for APAR PK75662, these enhancements are provided:
  - a new **SSL** option is added on the **NETSTAT IDENTIFY** command.
  - the results produced by the **NETSTAT CONFIG SSL** command are updated to accommodate multiple SSL server support.
  - a new **SSL START** command is added, which can be used to initiate TCP/IP server-managed startup of one or more SSL servers.
- Support is added for a **CONTROLLER** option for the **NETSTAT CONFIG** command. This option can be used to display current VSWITCH CONTROLLER settings.

5.2.4.9.4 Changes Introduced in TCP/IP Level 540

- **NETSTAT GATE** command output has been updated to include two new flags — one indicates if the MTU was modified by path MTU discovery for a given route; the other indicates whether a route was created as a result of path MTU discovery.
- **NETSTAT DEVLINKS** command output for an **OSD** device has been updated to include the OSA-Express port number, the designated transport type (**ETHERNET** or **IP**, for Layer 2 or Layer 3 mode, respectively), and local MAC address (for transport type ETHERNET only).
- (***IPv4 only***) **NETSTAT DEVLINKS** command output has been updated for all non-VIPA devices to display path MTU discovery status.

5.2.4.10 MPRoute Server

5.2.4.10.1 Changes Introduced in TCP/IP Level 640

- The **MPRoute** server has been upgraded to **z/OS 2.2 Equivalency**, and includes these functional enhancements:
  - Deprecates the **OMPROUTE_OPTIONS.hello_hi** environment variable.
  - Processes inbound OSPF hello packets from neighbors at the highest priority, for the purpose of maintaining OSPF adjacencies.
  - Modifications to avoid the potential for an abend when formatting or parsing OSPF packet content.
  - Enhancements to existing informational and debug messages, to cite more specific information when an IOCTL call has failed.

5.2.4.10.2 Changes Introduced in TCP/IP Level 630

- The **MPRoute** server has been upgraded to **z/OS 1.13 Equivalency**, and includes these functional enhancements:
  - support for RFC 2328 for IPv4 OSPF
  - support for RFC 2740 for IPv6 OSPF

5.2.4.10.3 Changes Introduced in TCP/IP Level 620

- The **MPRoute** server has been upgraded to **z/OS 1.12 Equivalency**, and includes these functional enhancements:

- support for RFC 4191 and RFC 5175
- support for MPRoute configuration file INCLUDE statements
- updates to report and help prevent futile neighbor state loops
- SMSG command updates to support DELETED, ACTIVATE, and SUSPEND keywords for selected commands
- **ROUTERADV** statement support changes that allow router advertisements to be sent with a HIGH, MEDIUM, or LOW preference value.

5.2.4.11 Remote Execution Services

5.2.4.11.1 Changes Introduced in TCP/IP Level 540

- The logon password default for the **RXAGENT1** virtual machine has been changed to **AUTOONLY**, to reinforce the concept that REXEC agents should be used for handling only anonymous requests.

5.2.4.12 SMTP Server

5.2.4.12.1 Changes Introduced in TCP/IP Level 640

- The **SMTP server command exit (SMTPCMDX)** has been modified to reject VRFY and EXPN commands, by default.

5.2.4.12.2 Changes Introduced in TCP/IP Level 630

- The SMTP server has been updated to accommodate the use of SSL to secure **IPv6** SMTP connections.

5.2.4.12.3 Changes Introduced in TCP/IP Level 620

- The SMTP server has been updated to accommodate connections using **IPv6**.

  Note that IPv6 SMTP connections cannot be secured using SSL because the z/VM SSL server does not incorporate IPv6 support.

5.2.4.12.4 Changes Introduced in TCP/IP Level 540

- Processing of the **CERTNOCHECK** operand for TLS connections associated with SMTP server has been changed such that this operand is equivalent to the **CERTFULLCHECK** operand.

5.2.4.13 SNMP Server and Client

5.2.4.13.1 Changes Introduced in TCP/IP Level 540

- An **SNMPTRAP** command is introduced that can be used to generate SNMP version 1 enterprise-specific traps for reporting events to an SNMP manager.

5.2.4.14 TLS/SSL Server

5.2.4.14.1 Changes Introduced in TCP/IP Level 640

- The **z/VM TLS/SSL server** has been upgraded to **z/OS V2.2 Equivalency**, which includes support for:
  - RFC 5280 Certificate Validation Upgrade (introduces support for Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)
  - PKCS #12 Certificate Store (function already introduced with z/VM version 6 release 3 APAR PI29130)
  - OCSP support, which enhances certificate revocation checking and flexibility, with:
    - support for retrieval of CRLs through HTTP URLs
    - more flexible processing of CRLs from LDAP
    - support for retrieval of revocation information through OCSP

  In addition, these z/VM TLS/SSL server changes have been implemented:

  - Inclusion of **z/OS V2.1 Equivalency** support (introduced with z/VM version 6 release 3 APAR PI40702), which facilitate exploitation of these functions:
    - AES Galois-Counter Mode (AES GCM), a TLS 1.2 symmetric key algorithm which is more secure than the current CBC mechanism employed today.
    - Enablement of DSA Certificates in MODE NIST-800-131a, an update to the size of the DSS certificates the server can support for asymmetric encryption
  - Inclusion of support to use PKCS #12 formatted files as certificate and key repositories. PKCS #12 is a more common format than the .kdb files used by gskkyman and System SSL today. Inclusion of this functionality allows for greater interoperability between platforms (including OpenSSL) and ease of use.
  - The default protocol levels for now are TLS 1.2 and TLS 1.1. All other protocols are disabled by default.
  - Inclusion of support for the VMSSL command **ENABLE** operand, which enables use of a specific cipher suite that is disabled by default — these being: 00, 01, 02, 03, 04, 05, 06 and 3B.
  - These fixed Diffie Hellman cipher suites now are disabled by default:

    0F, 0C, 10, 0D, 31, 30, 37, 36, 3F, 3E, 69, 68, A5, A1, A0 and A4.

5.2.4.14.2 Changes Introduced in TCP/IP Level 630

- The z/VM SSL server has been upgraded to **z/OS V1.13 equivalency**. This upgrade includes support for **Transport Layer Security (TLS) protocol, version 1.2**, which provides support for SHA-256

certificates. A new **PROTOCOL** operand on the VMSSL command allows the system administrator to enable and disable SSL and TLS protocols for cryptographic use in the operation of the SSL server.

- In addition, the SSL server has been updated to accommodate the use of SSL to secure **IPv6** connections.

  With this change, the SSLADMIN and NETSTAT IDENT SSL commands have been enhanced to handle and display IPv6 secure connection data.

5.2.4.14.3 Changes Introduced in TCP/IP Level 620

- Inclusion of the **SSL Server Performance and Scalability Enhancements** (introduced in TCP/IP for z/VM level 540 and level 610 via the PTFs for APARs PK97437, PK97438 and PK75662). These enhancements improve upon the ability of an SSL server to provide concurrent secure connectivity by increasing its overall performance and decreasing the amount of required system resources.

  Changes included as part of these enhancements include:

  – support for a new VMSSL command operand, CACHECLEANUP, and changes associated with support of the CACHELIFE operand
  – updates to the SSLADMIN command, with changes that affect the SSLADMIN QUERY, SSLADMIN REFRESH, and SSLADMIN TRACE/NOTRACE commands
  – support for new SSL server administration (SSLADMIN) commands — SSLADMIN CLEAR, SSLADMIN SET and SSLADMIN START
  – introduction of a new TCP/IP server configuration statement, SSLLIMITS, and changes that affect processing of the SSLSERVERID statement.

  With this change, the **SSLSERV** user ID no longer is included as part of the z/VM version 6 release 4 System deliverable. In its place, an **SSL server "pool"** of five servers now is defined as part of the system. While continued use of a single-instance, minidisk-based server (such as SSLSERV) still is possible and remains supported, the preferred configuration for running a single SSL server is to alter the SSL pool definition such that only one pool sever is defined. This can readily be accomplished by a CP directory change to the SSL server **POOL** definition.

- Inclusion of **SSL Server Federal Information Processing Standard (FIPS) 140-2 Support** (introduced in TCP/IP for z/VM level 610 via the PTF for APAR PM10616).

5.2.4.14.4 Changes Introduced in TCP/IP Level 610

- **SSL Server Federal Information Processing Standard (FIPS) 140-2 Support** is introduced with the the PTF for APAR PM10616.
- With the PTFs for APARs PK97437, PK97438 and PK75662, **SSL Server Performance and Scalability Enhancements** are introduced. These enhancements improve upon the ability of an SSL server to provide concurrent secure connectivity by increasing its overall performance and decreasing the amount of required system resources. With these enhancements, support for multiple SSL servers, defined as a server "pool" is introduced as well.
- With TCP/IP Level 610, the PTF for APAR PK65850 (SSL Server Enablement) is ***not*** required — the CMS-based SSL server supplied with the z/VM version 6 release 4 System deliverable is fully enabled.

5.2.4.14.5 Changes Introduced in TCP/IP Level 540

- With the PTF for **APAR PK65850**, a CMS-based SSL server is provided with TCP/IP for z/VM that no longer requires operation within a Linux guest. The components required for running this updated server implementation are installed and serviced through the same means as other CMS-based TCP/IP servers.

  With this implementation, the SSL server and TCP/IP stack server interfaces have been modified, as have SSL server command (**VMSSL**) and DTCPARMS file configuration operands and requirements. Due to the nature of these changes, **an SSL server implementation that is based on prior levels of TCP/IP for z/VM cannot be used with the TCP/IP level 540 TCP/IP server**. The converse is also true — the TCP/IP level 540 SSL server **cannot** be used with prior levels of TCP/IP for z/VM.

  For a summary of TCP/IP level 540 SSL and TCP/IP server compatibility, refer to Figure 7.

Figure 7. TCP/IP level 540 SSL / TCP/IP Server Compatibility

	TCP/IP level 540 SSL Server	**Prior-level SSL Server**
TCP/IP level 540 Stack Server	Compatible	**Not Compatible**
Prior-level TCP/IP Stack Server	**Not Compatible**	Compatible

  Additional changes associated with the level 540 SSL server include:

  – Use of z/OS V1.10 System SSL technology by the SSL server for encryption, decryption, and certificate management functions. Significant functional changes associated with the use of this technology include:

    - Implementation of Federal Information Processing Standard (**FIPS**) 140-2 is ***not*** available with this level of TCP/IP for z/VM.
    - Relaxed certificate checking, through use of selected application **CERTNOCHECK** options or operands, is not available at this level. Thus, self-signed certificates are accepted only if they are stored in both client- and-server-side certificate databases.
    - Addition of support for changing an FTP control connection from a secure state to a clear state through use of the FTP **CCC** subcommand.
    - Several cipher suites, including suites that provide 128-bit and 256-bit **AES encryption**, have been added. Two ciphers — RC4_EXP1024_56_SHA and DES_EXP1024_56_SHA have been removed. All other previously supported cipher suites have been renamed to more closely match specifications in RFCs 2246 and 4346.
    - z/OS System SSL will use hardware-assisted encryption and decryption through use of a processor-specific instruction, if it is available. Cryptographic cards are not supported.

  – Use of the **gskkyman** (previously introduced with LDAP server support) for SSL server certificate management functions.

- The z/VM SSL server now references a certificate database that is maintained in the z/VM Byte File System (BFS).
- A **GSKADMIN** user ID has been added. This user ID has been defined with appropriate authorization to perform certificate management operations for the SSL server key database. The GSKADMIN user ID is also defined as an SSL server administrative user ID.
- The **SSLADMIN** command has been revised such that a network connection no longer is used to perform server administrative functions. Thus, the server administrative port (previously defined at port number 9999) no longer is used and has been removed from the TCP/IP server configuration and ETC SERVICES sample files.
- **OBEY** authorization no longer is used to determine SSL server administrative authority. Such authorization now is controlled by DTCPARMS file **:Admin_ID_List.** tag entry.
- Additional or different DTCPARMS file configuration tags and SSL server command (**VMSSL**) parameters now are used for configuration of the SSL server. Detailed information about such changes are provided in *TCP/IP Planning and Customization* (SC24-6238).

5.2.4.15 TCP/IP (Stack) Server

5.2.4.15.1 Changes Introduced in TCP/IP Level 630

- Support for Common Link Access to Workstation (CLAW) and HYPERchannel A220 devices has been removed.

5.2.4.15.2 Changes Introduced in TCP/IP Level 620

- Inclusion of the TCP/IP server-specific changes associated with the **SSL Server Performance and Scalability Enhancements** (introduced in TCP/IP for z/VM level 540 and level 610 via the PTFs for APARs PK97437, PK97438 and PK75662). Stack specific updates introduced with the PTF for APAR PK75662 include:
  - support for the **SSLLIMITS** statement is added, which is used to specify the total number of secure connections that are to be supported by the TCP/IP server, as well as the connection limit for each SSL server.
  - support for the **SSLSERVERID** statement is modified to accept an asterisk (*) as a *user_id* value. In addition, a different **TIMEOUT** operand default (of 30 seconds, formerly 60 seconds) now is employed, with boundary values imposed.

5.2.4.15.3 Changes Introduced in TCP/IP Level 540

- The TCP/IP server has been updated such that the **OVERRIDEPRECEDENCE** operand of the **AssortedParms** configuration statement is always in effect. This change has been made in support of RFC 2873. The OVERRIDEPRECEDENCE operand continues to be accepted to maintain compatibility with prior levels of TCP/IP for z/VM, but will be reported as an obsolete parameter when encountered.
- The TCP/IP server has been updated such that the **EQUALCOSTMULTIPATH** and **EQUALCOSTIPV6MULTIPATH** operands of the **AssortedParms** configuration statement are always

in effect. These operands continue to be accepted to maintain compatibility with prior levels of TCP/IP for z/VM, but will be reported as no longer required, when encountered.

- The **OSD** and the **HIPERSockets DEVICE** statements have been updated to make **AUTORestart** the default. Thus, the TCP/IP server automatically will attempt to restart the device in the event of a device failure. AUTORestart is attempted only after successful data transfer has occurred.
- The **OSD DEVICE** statement has been updated to include a **PORTNUMBER** operand for which the additional port on each channel of an OSA-Express3 device can be specified. If a port number is not specified, the default port number is 0.
- The IFCONFIG command has been updated to allow a port number to specified for a QDIO (OSA-Express) device. Additionally, IFCONFIG command output now reports the transport type (**ETHERNET** or **IP**) for links that are associated with an **OSD** device.
- (***IPv4 only***) The **IFCONFIG** command has been updated to accept two new operands — **PATHMTU** and **NOPATHMTU** — to enable or disable path MTU discovery for a given link.
- (***IPv4 only***) Various LINK statements have been updated to include two new operands — **PATHMTU** and **NOPATHMTU** — that respectively enable or disable path MTU discovery on a link-by-link basis.
- (***IPv4 only***) The **PATHMTU** operand is accepted for the **ASSORTEDPARMS** statement, to enable path MTU discovery by default for links for which this has not explicitly been configured.
- Support for The **PATHMTUAGE** statement has been added, which allows for the specification of how long (in minutes) path MTU discovery information is to be retained for a given route.
- The **QDIOETHERNET LINK** statement has been updated to accept an **ETHERNET** or **IP** operand, which designates the transport type for the link (Layer 2 or Layer 3 mode, respectively).
- Due to **SSLADMIN** command revisions that eliminate the need for a network connection to perform SSL server administrative functions, an administrative port (previously defined at port number 9999, by default) no longer needs to be reserved for the SSL server.

5.2.4.16 Telnet Server and Client

5.2.4.16.1 Changes Introduced in TCP/IP Level 540

- The Telnet server and client have been updated to accommodate connections using **IPv6**. For the Telnet server, the telnet session connection and printer management exits (**SCEXIT** and **PMEXIT**, respectively) have been updated accordingly. The Telnet client includes support for a new **ADDRTYPE** option.

  Note that IPv6 Telnet connections cannot be secured using SSL because the z/VM SSL server does not incorporate IPv6 support.
- Processing of the **CERTNOCHECK** operand for TLS connections associated with the Telnet client has been changed such that this operand is equivalent to the **CERTFULLCHECK** operand.

5.3 DASD Storage and User ID Requirements

Figure 10 on page 33 lists the user IDs and minidisks used to install, service and use TCP/IP for z/VM.

Important Notes:

1. **All TCP/IP for z/VM service activity** now must be performed using the appropriate MAINT*vrm* user ID. For this program level, this user ID is **MAINT640**.
2. All user IDs necessary for installing, maintaining and using TCP/IP for z/VM have been defined as part of the installed z/VM version 6 release 4 System deliverable. Likewise, all required minidisks and SFS directories (dependent upon installation selections) have been defined. For a single system image (SSI) environment, these resources have been defined on all installed member systems that comprise this environment. These resources are listed in Figure 10 on page 33 and Figure 12 on page 38 so you are aware of the resources that have been allocated on your behalf.

   For information about specific user ID directory entry requirements, consult the **6VMTCP40 PLANINFO** file. This file is located on the 6VMTCP40 191 minidisk.
3. Any user ID that is used to perform TCP/IP for z/VM installation and service actions (such as to use the **SSLPOOL** utility to alter or add an SSL server pool) must have ***file pool administration authority*** for the **VMSYS** file pool. As supplied with the z/VM version 6 release 4 System deliverable, both the MAINT640 and TCP/IP service resource owner user ID (6VMTCP40) are enrolled as file pool administrators for this file pool.
4. If you modify or eliminate any of the IBM-supplied user IDs, minidisk addresses, or SFS directory names that are associated with TCP/IP for z/VM, you ***must*** create an appropriate PPF override for the **SERVP2P $PPF** file.

   Similarly, if additional TCP/IP user IDs and their associated resources are created (for example, to establish an alternate TCP/IP stack server and suite of TCP/IP protocol servers), appropriate PPF overrides for the **SERVP2P $PPF** file, as well as local modifications to the 6VMTCP40 CATALOG file, should be created. If such changes are not implemented, service updates might not be properly reflected for such servers.

   You also must use the **VMFUPDAT** command to update the VM SYSSUF software inventory file, so that your PPF override of SERVP2P PPF is used for automated service processing. For more information about PPF file overrides, see *z/VM: VMSES/E Introduction and Reference*.

   Before any user ID or resource changes are implemented, be certain to review the section titled “Implications of Assigning Different Server Virtual Machine Names” in Chapter 1 of *TCP/IP Planning and Customization* (SC24-6238), as well as the resource and user ID information provided in the remainder of this document.
5. **6VMTCP40** is the IBM-supplied user ID designated as the owner for the resources used to service and maintain TCP/IP for z/VM, whereas **TCPMAINT** is that designated for TCP/IP administration, and which separately owns TCP/IP production resources.

   If you choose to use different user IDs for these purposes, or you elect to use different minidisks and/or SFS directories to maintain TCP/IP for z/VM, appropriate **SERVP2P $PPF** file override changes must be implemented, as previously noted.

6. **All** resources associated with the 6VMTCP40 user ID (whether strictly minidisks, SFS directories, or a combination thereof) **must** be retained. This includes the TCP/IP service ***test build*** minidisks. If these resources are not retained, problems will be encountered during installation and service.
7. Note the following, with regard to the user ID and resource information provided in Figure 10:

   Minidisk Requirements and Restrictions

   Certain minidisks **must** be defined for the TCP/IP server machines used by your installation. Similarly, specific minidisks must be retained and used for maintaining TCP/IP for z/VM for your installation. These minidisks **cannot** be replaced with a Shared File System (SFS) SFS directory.

   Minidisks to which this requirement applies are listed in Figure 10, as **boldface** virtual device numbers. In addition, dashes are present in place of numeric SFS 4K block values, and alternate SFS directory name defaults have been omitted.

   Note that the minidisks identified using the aforementioned conventions also must be available to their respective user IDs with **Read/Write** (**R/W**) status, when those user IDs are in use. Read/Write access to a 191 minidisk is necessary so that writeable "work space" and other data critical to the operation of a given server are available.

   For the TCPMAINT user ID, R/W access to its 198, 591, and 592 disks is necessary only when these disks (or the files that reside upon them) are updated for customization purposes. Otherwise, Read-Only (R/O) access to these minidisks is sufficient for this user ID (as is the usual case for the various TCP/IP server user IDs). For TCP/IP client users, Read-Only (R/O) access to only the TCPMAINT 592 minidisk is necessary.

   SFS Directory Requirements

   Certain SFS directories **must** be defined and retained for use by SSL "pool" servers (such as SSL00001). These directories **cannot** be replaced with an equivalent minidisk.

   user IDs to which this requirement applies are listed in Figure 10 with **boldface** user ID values. In addition, dashes are present in place of all minidisk-related attributes, and the applicable SFS directory (cited in **Usage** column) is listed using **boldface** text.

8. Additional storage might need to be allocated for a given user ID or server minidisk, depending on your installation. Some examples of minidisks that might need to be increased, and possible reasons for so doing, are listed in Figure 8. Note that certain minidisks (not cited here) might also need to be increased to accommodate TCP/IP server configurations that regularly employ logging or tracing facilities that direct information to a server-owned minidisk.

Figure 8. Alternate Minidisk Storage Requirements

User ID / Minidisk	Rationale for Storage Revision
SMTP 191	Allow for SMTP processing of a high volume of e-mail
VMNFS 191	Provide support for a large number of NFS clients
6VMTCP40 2D2	Facilitate a high number of TCP/IP for z/VM maintenance files

For certain minidisks, storage requirements should be re-assessed locally, on a regular basis, for your specific environment. For example, the capacity of the **DELTA** minidisk (**6VMTCP40 2D2**, by default), periodically might need to be increased, based on the specific preventive and corrective service applied to your system.

9. If you choose to provide remote execution services through use of the rexec daemon (REXECD), you might find the need to define multiple agent virtual machines, named RXAGENT1, RXAGENT2, etc. Each RXAGENT*n* virtual machine you create should be defined similar to RXAGENT1 (defined as part of the installed z/VM version 6 release 4 System deliverable). However, note that the RXAGENT*n* virtual machines do not "own" any minidisks.
10. Source files are supplied in ***packed*** format. If you intend to unpack source files after installation, ensure that sufficient space is allocated for the unpacked files. Alternate storage requirements for storing unpacked files on the TCP/IP **SOURCE** minidisk (**6VMTCP40 2B3**, by default) are listed in Figure 9:

Figure 9. 6VMTCP40 2B3 Minidisk Storage Requirements — Unpacked Source Files

Type of Storage	Alternate Storage Requirement
3390 DASD	206 cylinders
FBA Device	296640 FB-512 blocks
SFS Directory	37080 SFS 4K blocks

To store unpacked files as described above, update the listed minidisk sizes to those cited in Figure 9 (which supersede the storage values cited in Figure 10).

5.3.1 DASD Requirements for TCP/IP for z/VM

Various minidisks and SFS directories necessary for installing, maintaining and using TCP/IP for z/VM have been defined as part of the installed z/VM version 6 release 4 System deliverable. For a single system image (SSI) environment, these resources have been defined on all installed member systems. These resources are listed in Figure 10 so you are aware of the resources that have been allocated on your behalf.

Notes:

1. With the exception of the TCP/IP service resource owner user ID (6VMTCP40), ***all*** of the TCP/IP server virtual machines cited in Figure 10 are defined using multiconfiguration virtual machine definitions. The 6VMTCP40 user ID is defined using a single-configuration virtual machine definition. See *z/VM: CP Planning and Administration* for more information about multiconfiguration and single-configuration virtual machine definitions.
2. The cylinder values defined in Figure 10 are based on a 4K block size. FB-512 block and SFS values are derived from the 3390 cylinder values in this table. FBA minidisk sizes are shown in 512-byte blocks; these minidisks should be CMS formatted at 1K size.
3. Additional storage might need to be allocated for certain minidisks, depending on your environment. For more information, see the accompanying notes on page 30.

Figure 10 (Page 1 of 4). DASD Storage Requirements for Target Minidisks - TCP/IP for z/VM

Minidisk owner (User ID)	Default Device Number	Storage in Cylinders		FB-512 Blocks	SFS 4K Blocks	Usage
		DASD	CYLS			Default SFS Directory Name
6VMTCP40	191	3390	20	28800	3600	6VMTCP40 user ID 191 minidisk **VMPSFS:6VMTCP40**
6VMTCP40	2B2	3390	150	216000	27000	Contains all base code shipped with TCP/IP for z/VM **VMPSFS:6VMTCP40.TCPIP.OBJECT**
6VMTCP40	2B3	3390	59	84960	10534	Source files disk. (1*) **VMPSFS:6VMTCP40.TCPIP.SOURCE**
6VMTCP40	29D	3390	5	7200	750	Contains TCP/IP CMS Help files **VMPSFS:6VMTCP40.TCPIP.HELP**

Notes:

1. Additional storage might need to be allocated for this minidisk. For more information, see the accompanying notes on page 30.

Figure 10 (Page 2 of 4). DASD Storage Requirements for Target Minidisks - TCP/IP for z/VM

Minidisk owner (User ID)	Default Device Number	Storage in Cylinders		FB-512 Blocks	SFS 4K Blocks	Usage
		DASD	CYLS			Default SFS Directory Name
6VMTCP40	2C4	3390	5	7200	750	Contains local modifications **VMPSFS:6VMTCP40.TCPIP.LOCAL**
6VMTCP40	2D2	3390	500	720000	90000	Contains serviced files (1*) **VMPSFS:6VMTCP40.TCPIP.DELTA**
6VMTCP40	2A6	3390	5	7200	750	Contains AUX files and software inventory tables that represent the test service level of TCP/IP for z/VM **VMPSFS:6VMTCP40.TCPIP.APPLYALT**
6VMTCP40	2A2	3390	5	7200	750	Contains AUX files and software inventory tables that represent the service level of TCP/IP for z/VM that is currently in production **VMPSFS:6VMTCP40.TCPIP.APPLYPROD**
6VMTCP40	**491**	3390	80	115200	_____	***Test*** build disk for server code; files from this disk are copied to a production disk (TCPMAINT 591) which also requires this amount of free space
6VMTCP40	**492**	3390	120	172800	_____	***Test*** build disk for client code; files from this disk are copied to a production disk (TCPMAINT 592) which also requires this amount of free space
TCPMAINT	**191**	3390	7	10080	_____	TCPMAINT user ID 191 minidisk
TCPMAINT	_____	____	__	_____	1000	TCPMAINT-owned SSL Pool Server user ID Work (and parent) Directory **VMSYS:TCPMAINT** **VMSYS:TCPMAINT.SSLPOOL_SSL.**
TCPMAINT	**198**	3390	9	12960	_____	Contains configuration files for clients and servers.
TCPMAINT	**591**	3390	160	230400	_____	***Production*** build disk for server code
TCPMAINT	**592**	3390	240	345600	_____	***Production*** build disk for client code

Notes:

1. Additional storage might need to be allocated for this minidisk. For more information, see the accompanying notes on page 30.

Figure 10 (Page 3 of 4). DASD Storage Requirements for Target Minidisks - TCP/IP for z/VM

Minidisk owner (User ID)	Default Device Number	Storage in Cylinders		FB-512 Blocks	SFS 4K Blocks	Usage
		DASD	CYLS			Default SFS Directory Name
GSKADMIN	**191**	3390	2	2880	_____	GSKADMIN user ID 191 minidisk
DTCSMAPI	**191**	3390	5	7200	_____	DTCSMAPI user ID 191 minidisk
DTCVSW1	**191**	3390	5	7200	_____	DTCVSW1 user ID 191 minidisk
DTCVSW2	**191**	3390	5	7200	_____	DTCVSW2 user ID 191 minidisk
DTCVSW3	**191**	3390	5	7200	_____	DTCVSW3 user ID 191 minidisk
DTCVSW4	**191**	3390	5	7200	_____	DTCVSW4 user ID 191 minidisk
FTPSERVE	**191**	3390	9	12960	_____	FTPSERVE user ID 191 minidisk
IMAP	**191**	3390	1	1440	_____	IMAP user ID 191 minidisk
IMAPAUTH	**191**	3390	6	8640	_____	IMAPAUTH user ID 191 minidisk
LDAPSRV	**191**	3390	5	7200	_____	LDAPSRV user ID 191 minidisk
MPROUTE	**191**	3390	2	2880	_____	MPROUTE user ID 191 minidisk
PORTMAP	**191**	3390	2	2880	_____	PORTMAP user ID 191 minidisk
REXECD	**191**	3390	2	2880	_____	REXECD user ID 191 minidisk
RXAGENT1	_____	3390	__	_____	_____	REXEC agent (a 191 minidisk is **not** required; REXEC agents utilize the REXECD 191 minidisk)
SMTP	**191**	3390	25	36000	_____	SMTP user ID 191 minidisk (1*)
SNMPD	**191**	3390	2	2880	_____	SNMPD user ID 191 minidisk
SNMPQE	**191**	3390	2	2880	_____	SNMPQE user ID 191 minidisk
SNMPSUBA	**191**	3390	2	2880	_____	SNMPSUBA user ID 191 minidisk
SSL00001	_____	____	__	_____	50	SSL00001 user ID Root Directory **VMSYS:SSL0001.**
SSL00002	_____	____	__	_____	50	SSL00002 user ID Root Directory **VMSYS:SSL0002.**
SSL00003	_____	____	__	_____	50	SSL00003 user ID Root Directory **VMSYS:SSL0003.**

Notes:

1. Additional storage might need to be allocated for this minidisk. For more information, see the accompanying notes on page 30.

Figure 10 (Page 4 of 4). DASD Storage Requirements for Target Minidisks - TCP/IP for z/VM

Minidisk owner (User ID)	Default Device Number	Storage in Cylinders		FB-512 Blocks	SFS 4K Blocks	Usage
		DASD	CYLS			Default SFS Directory Name
SSL00004	_____	____	__	_____	50	SSL00004 user ID Root Directory **VMSYS:SSL0004.**
SSL00005	_____	____	__	_____	50	SSL00005 user ID Root Directory **VMSYS:SSL0005.**
SSLDCSSM	**191**	3390	1	1440	_____	SSLDCSSM user ID 191 minidisk
TCPIP	**191**	3390	5	7200	_____	TCPIP user ID 191 minidisk
UFTD	**191**	3390	2	2880	_____	UFTD user ID 191 minidisk
VMNFS	**191**	3390	9	12960	_____	VMNFS user ID 191 minidisk (1*)

Notes:

1. Additional storage might need to be allocated for this minidisk. For more information, see the accompanying notes on page 30.

5.3.2 TCP/IP for z/VM Directory PROFILES and User IDs

The user IDs necessary for installing, maintaining and using TCP/IP for z/VM have been defined as part of the installed z/VM version 6 release 4 System deliverable. More information about these user IDs is provided in the sections that follow.

5.3.2.1 TCP/IP for z/VM Directory PROFILES

Two system directory PROFILE entries (PROFILE TCPCMSU and PROFILE TCPSSLU) are defined for TCP/IP for z/VM as part of the z/VM version 6 release 4 system directory. These entries are shown in Figure 11. Each TCP/IP service virtual machine directory includes one of these profiles, as follows:

- PROFILE TCPCMSU — used for the majority of TCP/IP for z/VM user IDs
- PROFILE TCPSSLU — used for only server virtual machines that are defined as an SSL server "pool."

Figure 11. TCP/IP for z/VM System Directory Profiles

```
PROFILE TCPCMSU
  IPL CMS
  MACHINE ESA
  SPOOL 000C 2540 READER *
  SPOOL 000D 2540 PUNCH  A
  SPOOL 000E 1403 A
  CONSOLE 0009 3215 T
  LINK MAINT 0190 0190 RR
  LINK MAINT 019D 019D RR
  LINK MAINT 019E 019E RR
  LINK MAINT 0402 0402 RR
  LINK MAINT 0401 0401 RR
```

```
PROFILE TCPSSLU
  IPL CMS PARM FILEPOOL VMSYS
  LOGONBY TCPMAINT GSKADMIN
  MACH ESA
  NAMESAVE TCPIP
  POSIXINFO UID 7 GNAME security
  IUCV ALLOW
  OPTION ACCT MAXCONN 1024 QUICKDSP SVMSTAT APPLMON
  SHARE RELATIVE 3000
  SPOOL 000C 2540 READER *
  SPOOL 000D 2540 PUNCH A
  SPOOL 000E 1403 A
  CONSOLE 0009 3215 T
  LINK MAINT 0190 0190 RR
  LINK MAINT 019D 019D RR
  LINK MAINT 019E 019E RR
  LINK MAINT 0402 0402 RR
  LINK MAINT 0401 0401 RR
  LINK TCPMAINT 0491 0491 RR
  LINK TCPMAINT 0492 0492 RR
  LINK TCPMAINT 0591 0591 RR
  LINK TCPMAINT 0592 0592 RR
  LINK TCPMAINT 0198 0198 RR
```

5.3.2.2 TCP/IP for z/VM User IDs

The user IDs listed in Figure 12 on page 38 have been defined for TCP/IP for z/VM as part of the z/VM version 6 release 4 system directory. For a single system image (SSI) environment, these user IDs have been defined on all installed member systems.

User ID Notes:

1. For information about specific user ID directory entry requirements, consult the **6VMTCP40 PLANINFO** file. This file is located on the 6VMTCP40 191 minidisk.
2. With the exception of the TCP/IP service resource owner user ID (6VMTCP40), ***all*** TCP/IP server virtual machines are defined using multiconfiguration virtual machine definitions. The 6VMTCP40 user ID is defined using a single-configuration virtual machine definition. See *z/VM: CP Planning and Administration* for more information about multiconfiguration and single-configuration virtual machine definitions.
3. The TCP/IP directory profiles include LINK statements for the MAINT 401 and 402 minidisks, to facilitate the use of CMS Kanji and Upper Case American English HELP files, for those environments in which these might be required.
4. The directory entries supplied for each TCP/IP for z/VM service virtual machine include LINK statements for the TCP/IP service test build minidisks, to better facilitate the ability to test newly applied service before it is placed into production.
5. The directory entry for the TCPIP virtual machine (and other select TCP/IP servers) includes the statement: `SHARE RELATIVE 3000`

   For most installations, the relative CPU share allocation of 3000 should be suitable. However, you are free to change this value to conform to local guidelines established for defining server and guest virtual machine share settings.
6. If you create additional RXAGENT*n* machines, duplicate the RXAGENT1 directory entry for each server that is added.

Figure 12 (Page 1 of 4). Default User IDs - TCP/IP for z/VM

TCP/IP User ID	Associated TCP/IP Function
6VMTCP40	Owns the resources used to service and maintain TCP/IP for z/VM.
TCPMAINT	TCP/IP system administration and configuration user ID. This user ID also owns the production resources used to provide TCP/IP services.
GSKADMIN	Administrative user ID for management of SSL key database (via use of **gskkyman** utility).
DTCSMAPI (2*)	SMAPI-exclusive TCP/IP Protocol server virtual machine.

Notes:

1. Additional changes might need to be made for some user IDs, depending on your environment. For more information, see the accompanying notes on page 38.
2. This server is supplied by IBM to support select system capabilities, such as Unified Resource Manager support; it should not be customized for your installation.

Figure 12 (Page 2 of 4). Default User IDs - TCP/IP for z/VM

TCP/IP User ID	Associated TCP/IP Function
DTCVSW1	System-default VSWITCH controller virtual machine.
DTCVSW2	System-default VSWITCH controller virtual machine (alternate, for provision of failover capability)
DTCVSW3	System-default VSWITCH controller virtual machine (alternate, for provision of failover capability)
DTCVSW4	System-default VSWITCH controller virtual machine (alternate, for provision of failover capability)
FTPSERVE	Implements the File Transfer Protocol (FTP) daemon, which controls access to files on the local host.
IMAP	Implements the Internet Message Access Protocol (IMAP) daemon, which allows a client to access and manipulate electronic mail messages on a server.
IMAPAUTH	Performs IMAP user authentication, when the IMAP server has been configured to make use of the IMAP Authentication Exit.
LDAPSRV	Implements the Lightweight Directory Access Protocol (LDAP) server.
MPROUTE	Implements the Multiple Protocol Routing (MPRoute) server, which uses OSPF and/or RIP protocols to manage network routing information.
PORTMAP	Runs the Portmapper function for RPC systems that support the Network File System protocol.
REXECD	Provides remote execution services for TCP/IP hosts that support the REXEC client.
RXAGENT1 (1*)	Agent virtual machine used by REXECD to process anonymous rexec client requests.
SMTP	Implements the Simple Mail Transfer Protocol (SMTP) server, which provides TCP/IP electronic mail support.
SNMPD	Virtual machine for the SNMP Agent.
SNMPQE	Virtual machine for the SNMP Query Engine.
SNMPSUBA	Subagent virtual machine for the SNMP Query Engine.
SSL*nnnnn*	An SSL “pool” server that provides Secure Sockets Layer (SSL) protocol support for TCP/IP servers and select clients. By default, a pool of five such servers (SSL00001-SSL00005) is defined as part of the z/VM version 6 release 4 System deliverable, via the **SSL** user ID definiton.
SSLDCSSM	The SSL DCSS Management Agent server, used in conjunction with Sockets Layer (SSL) protocol support.
TCPIP (1*)	Primary virtual machine that provides TCP/IP and Telnet services.

Notes:

1. Additional changes might need to be made for some user IDs, depending on your environment. For more information, see the accompanying notes on page 38.
2. This server is supplied by IBM to support select system capabilities, such as Unified Resource Manager support; it should not be customized for your installation.

Figure 12 (Page 3 of 4). Default User IDs - TCP/IP for z/VM

TCP/IP User ID	Associated TCP/IP Function
UFTD	Implements the Unsolicited File Transfer (UFT) server.
VMNFS	Implements the Network File System (NFS) server.

Notes:

1. Additional changes might need to be made for some user IDs, depending on your environment. For more information, see the accompanying notes on page 38.
2. This server is supplied by IBM to support select system capabilities, such as Unified Resource Manager support; it should not be customized for your installation.

6.0 Installation Instructions

Note

TCP/IP for z/VM is pre-installed as part of the z/VM version 6 release 4 System deliverable. This section provides procedures to complete the customization process for TCP/IP for z/VM.

The procedures that follow are presented in two-column format, where the steps to be performed are identified using numbered, **boldface** headings. Any sub-steps that correspond to a given procedure are presented on the right side of each page and are ordered using bold numerals, while the commands associated with these steps are presented on the left side of a page. Pertinent command information might exist to the right of a given command.

Instruction Notes:

1. Each step of these installation instructions must be followed. Do not skip any step unless directed otherwise.
2. These instructions describe actions for only a single z/VM system (a non-SSI system or a single-member SSI system). **For an SSI environment with multiple members, these steps must be repeated for each member system.**
3. Throughout these instructions, the use of IBM-supplied default minidisk device numbers and user IDs is assumed. If different user IDs, device numbers, or SFS directories are used to install TCP/IP for z/VM in your environment, adapt these instructions as needed.
4. For a complete description of all VMSES/E installation commands, operands and options, refer to:
   - *z/VM: VMSES/E Introduction and Reference* (GC24-6243)

Note!

Any sample console output presented throughout these instructions is based on a z/VM version 6 release 4 system; this output reflects an installation environment in which default values (PPF and component names, user IDs, and minidisks) are in use.

6.1 TCP/IP for z/VM Installation Process Overview

A brief description of the steps necessary to complete the installation of TCP/IP for z/VM follows:

- **Review the Default Installation** — Various resources have been defined and allocated for TCP/IP for z/VM, as part of the installed z/VM version 6 release 4 System deliverable. This default environment should be reviewed and, if necessary, modified for your installation.
- **Review TCP/IP for z/VM Content and Changes** — Review the topics presented in 5.2.4, “Migration Considerations” on page 16, so you are aware of changes that might affect your customization and use of TCP/IP level 640.

© Copyright IBM Corp. 1990, 2016

- **Configure TCP/IP for z/VM** — The configuration files associated with various TCP/IP services must be customized to effectively use TCP/IP for z/VM.

6.2 Customizing TCP/IP for z/VM

Note — All z/VM Customers

The material presented in the next few sections is provided mostly for informational and reference purposes. To complete the installation of TCP/IP for z/VM, continue with the instructions in section 6.2.2, “Configure TCP/IP for z/VM for Your Installation” on page 43.

6.2.1 Review the TCP/IP for z/VM Default Installation Environment

Because TCP/IP for z/VM is pre-installed as part of the z/VM version 6 release 4 System deliverable, several installation steps have already been performed on your behalf. Among these are the:

- inclusion of TCP/IP-specific user ID entries and PROFILES in the z/VM version 6 release 4 system directory
- creation of a simplified PROFILE EXEC for the 6VMTCP40 user ID
- allocation of TCP/IP-required minidisks
- creation of TCP/IP-required SFS directories and authorizations (for SSL pool servers)
- loading of TCP/IP for z/VM product files (run-time and sample configuration files) to service test build *and* production minidisks, using VMSES/E commands.

For a single system image (SSI) environment, these actions will have been completed for each member system that has been defined.

6.2.1.1 PPF Override and Other Modification Considerations

If you modify any of the IBM-supplied user IDs, minidisk addresses, or SFS directory names that are associated with TCP/IP for z/VM, then you ***must*** create an appropriate PPF override for the **SERVP2P $PPF** file.

You also must use the **VMFUPDAT** command to update the VM SYSSUF software inventory file, so that your PPF override of SERVP2P PPF is used for automated service processing. For more information about PPF file overrides, see *z/VM: VMSES/E Introduction and Reference*.

If you create your own TCP/IP for z/VM PPF override file, use the *ppfname* of your override file (instead of SERVP2P) throughout any procedures that require this file to be identified, unless noted otherwise.

6.2.2 Configure TCP/IP for z/VM for Your Installation

As previously mentioned, upon installation of the z/VM version 6 release 4 System deliverable, the various program files that comprise TCP/IP for z/VM reside on appropriate production minidisks. In addition, representative client and server *sample* configuration files are also present. See 6.2.2.5, “TCP/IP for z/VM Product and Sample Configuration Files” on page 47 for more information about these files and their default location.

Before any TCP/IP services can be used, certain configuration files **must** be created and customized for your installation.

Note: For a single system image (SSI) environment, such customization must be completed ***for each member system*** that has been defined.

See *TCP/IP Planning and Customization* (SC24-6238) for detailed information about the various TCP/IP services that can be established, and the configuration files that are associated with each service.

For convenience, the PRODUTL command can *optionally* be used to create an initial set of configuration files, as described in the next section. Such files might serve as a starting point for customizing TCP/IP services for your installation. For reference, the sample configuration files supplied by IBM are summarized in Figure 15 on page 50.

IPWIZARD Considerations

If the IPWIZARD command has been used to create an initial TCP/IP configuration, the following files have been created *and* customized:

- PROFILE TCPIP
- SYSTEM DTCPARMS
- TCPIP DATA

These files enable basic network connectivity for your z/VM system, with their content based on information supplied via the IPWIZARD panels. If you intend to provide more comprehensive TCP/IP services for your installation, further customization of the previously listed files is required. Additional TCP/IP configuration files will also require customization, dependent upon the specific services that are to be established.

Note: If the IPWIZARD command has **not** been used, the previously listed files are not present on your system.

6.2.2.1 Create a Starter Set of TCP/IP Configuration Files (Optional)

This section provides ***optional*** steps for using the PRODUTL command to create an initial (or, "starter") set of TCP/IP configuration files that then can be customized for the TCP/IP services selected for use by your installation. The files created by this procedure are listed in Figure 15 on page 50.

PRODUTL Command and Usage Notes:

1. The configuration files created by PRODUTL have the same content as the *sample* files on which they are based.
2. When the PRODUTL command is used as described in this section, a configuration file is created *only if the intended file does not already exist*. Existing (and presumably customized) configuration files are *not* replaced.
3. Any of the configuration files listed in Figure 15 can be (manually) created on an individual, as-needed basis if you choose to not use the PRODUTL command as described in this section.
4. For step 5 below, it is assumed that changes to the TCPCONFIG section of the 6VMTCP40 CATALOG are not required for your installation. If such changes are necessary, complete your modifications before you continue with the steps that follow. See 6.2.3, "TCP/IP for z/VM CATALOG Files" on page 52 for more information about TCP/IP for z/VM catalog files.

1 Log on the z/VM product maintenance user ID, **MAINT640**.

The PROFILE EXEC supplied with the z/VM version 6 release 4 System deliverable for this user ID contains ACCESS commands for VMSES/E minidisks that are necessary to run the commands cited in later steps. The minidisks required are the VMSES/E code minidisk (MAINT640 5E5, by default) and the VMSES/E Software Inventory minidisk (MAINT640 51D, by default).

2 Issue the CMS QUERY DISK command to verify the VMSES/E code and Software Inventory minidisks are correctly linked and accessed.

query disk

Verify the MAINT640 5E5 minidisk is accessed as file mode **B**.

Verify the MAINT640 51D minidisk is accessed as file mode **D**, and is linked **R/W**.

Note: If another user has the MAINT640 51D minidisk linked in write (R/W) mode, you'll obtain only read (R/O) access to this minidisk. If this occurs,

have that user re-link the 51D disk in read-only (RR) mode, after which you need issue the appropriate LINK and ACCESS commands for the 51D minidisk. Do not continue with these procedures until a R/W link is established to the 51D minidisk.

3. If necessary, establish the appropriate access to the VMSES/E minidisks.

   a. Establish read access to the VMSES/E code minidisk (to allow use of the PRODUTL command).

      link maint640 5e5 5e5 rr
      access 5e5 b

   b. Establish write access to the Software Inventory minidisk.

      link maint640 51d 51d mr
      access 51d d

4. Establish the appropriate working environment, to ensure the TCP/IP 6VMTCP40 CATALOG file is available.

vmfsetup servp2p {tcpipp2p | tcpipsfsp2p}

Use **tcpipp2p** if the TCP/IP for z/VM default minidisk environment has been maintained; use **tcpipsfsp2p** if the service minidisks were moved to Shared File System directories.

The 6VMTCP40 CATALOG file resides on the 491 minidisk that is obtained by this command.

5 Create initial TCP/IP for z/VM configuration files by using the PRODUTL command. For reference, files that can be processed using the TCPCONFIG section are listed in Figure 15 on page 50.

Verifying Your Environment

When you perform this step, it is suggested that you first invoke PRODUTL as illustrated, but with the **TEST** option also specified. This will verify that all resources can be accessed and that the appropriate files will be processed.

With the **TEST** option in effect, **no files are copied**.

Resolve any reported problems, then invoke PRODUTL (without the TEST option) as illustrated.

```
produtl servp2p {tcpipp2p | tcpipsfsp2p} 6vmtcp40 tcpconfig
```

Use **tcpipp2p** if the TCP/IP for z/VM default minidisk environment has been maintained; use **tcpipsfsp2p** if the service minidisks were moved to Shared File System directories.

6 Review the PRODUTL message log (PRODUTL $MSGLOG). If necessary, correct any problems before you proceed with the next step.

```
vmfview produtl
```

6.2.2.2 Configure TCP/IP Services

The various TCP/IP for z/VM services that are to be provided for your installation (such as the provision of SMTP or FTP protocol support) must be configured prior to use. For detailed information about configuring these services, see the appropriate chapters of *TCP/IP Planning and Customization*.

6.2.2.3 Initialize TCP/IP Services

Once TCP/IP for z/VM has been (fully) configured for your installation, the appropriate TCP/IP servers must be initialized. For more information, see the section that discusses “Starting and Stopping TCP/IP Servers” in the chapter titled “General TCP/IP Server Configuration,” of *TCP/IP Planning and Customization*.

In addition, the TCPMSMGR command is available to manage the startup and shutdown of the TCP/IP servers used by your installation. For more information about the TCPMSMGR command, see Appendix A, “TCP/IP Utilities” on page 57.

6.2.2.4 Copy TCP/IP Client Code to the z/VM Product Code Disk (Optional)

After TCP/IP for z/VM has been configured for your installation, you might want to consider copying TCP/IP client code (or a subset of this) to the z/VM Product Code minidisk. See Appendix D, “Copying TCP/IP for z/VM Client Code to the Y-Disk” on page 71 for additional information and instructions concerning this process.

Note: For a single system image (SSI) environment, this action must be completed ***for each member system*** that has been defined.

6.2.2.5 TCP/IP for z/VM Product and Sample Configuration Files

For summary purposes, various TCP/IP product and configuration files are identified within this section. In general, these files can be considered to belong to one of these groups:

- TCP/IP product files that are noteworthy, with resect to service updates; these files are summarized in Figure 13 on page 48
- TCP/IP server production run-time files, summarized in Figure 14 on page 48
- TCP/IP configuration files, summarized in Figure 15 on page 50

Figure 13 on page 48 lists the TCP/IP for z/VM product files for which notification of any service updates to these files is of importance. The production locations shown are those established by the TCP/IP for z/VM product packaging build lists. For reference, source and production file naming information is provided as well.

Figure 13. TCP/IP for z/VM Product Change Notification Files

Source Location (1*)	Production Location (2*)	Source File Name / Type	Production File Name / Type	Usage
491	591	TCPROFIL EXEC	TCPROFIL EXEC	All Servers
491	591	IBM DTCPARMS	IBM DTCPARMS	All Servers

Notes:

1. Device number for source minidisks owned by the 6VMTCP40 user ID.
2. Device number for production minidisks owned by the TCPMAINT user ID. minidisk.

Figure 14 lists the TCP/IP for z/VM product files that must reside on individual TCP/IP server virtual machine (SVM) minidisks. The production locations shown are those established with installation of the z/VM version 6 release 4 System deliverable. For reference, source and production file naming information is provided as well.

Notes:

1. Because of their use and composition, the files listed in Figure 14 ***usually*** are not processed or updated when TCP/IP for z/VM service is applied to your system.

   However, should the need arise to process these files — such as to restore them to their base-level, unmodified state for unique or extenuating circumstances, or if notification of a service change to these parts is received — this can be accomplished by using the TCP/IP for z/VM **PRODUTL** command, with the appropriate catalog section name (**tcpsvmcms**) specified as an operand. For more information, see Appendix E, “Managing TCP/IP Files with Unique Service Requirements” on page 74.

2. The TCPROFIL EXEC file should be copied to the 191 disk of any additional CMS-based TCP/IP for z/VM servers that are installed (or added at a later time).

3. The PROFILE EXEC used by all SSL*nnnnn* pool servers is an aliased file that is maintained (by default) in this SFS directory:

   - **VMSYS:TCPMAINT.SSLPOOL_SSL.**

   Use the SSLPOOL utility to establish the correct SFS aliases and authorizations if an alternate SFS directory is used for this purpose, of if any additional SSL server pools are defined for your installation.

Figure 14. TCP/IP for z/VM Production Run-Time Files (CMS SVM-Specific)

Source Location (1*)	Production Location (2*)	Source File Name / Type	Production File Name / Type	Associated Server
491	191	TCPROFIL EXEC	PROFILE EXEC	TCPIP
491	191	TCPROFIL EXEC	PROFILE EXEC	FTPSERVE
491	191	TCPROFIL EXEC	PROFILE EXEC	MPROUTE
491	191	TCPROFIL EXEC	PROFILE EXEC	PORTMAP
491	191	TCPROFIL EXEC	PROFILE EXEC	REXECD
491	191	TCPROFIL EXEC	PROFILE EXEC	SMTP
491	191	TCPROFIL EXEC	PROFILE EXEC	SNMPD
491	191	TCPROFIL EXEC	PROFILE EXEC	SNMPQE
491	191	TCPROFIL EXEC	PROFILE EXEC	SSLSERV
491	191	TCPROFIL EXEC	PROFILE EXEC	UFTD
491	191	TCPROFIL EXEC	PROFILE EXEC	VMNFS
491	191	TCPROFIL EXEC	PROFILE EXEC	IMAP
491	191	TCPROFIL EXEC	PROFILE EXEC	IMAPAUTH
491	191	TCPROFIL EXEC	PROFILE EXEC	DTCVSW1
491	191	TCPROFIL EXEC	PROFILE EXEC	DTCVSW2
491	191	TCPROFIL EXEC	PROFILE EXEC	DTCVSW3
491	191	TCPROFIL EXEC	PROFILE EXEC	DTCVSW4
491	191	TCPROFIL EXEC	PROFILE EXEC	SNMPSUBA
491	191	TCPROFIL EXEC	PROFILE EXEC	LDAPSRV
491	191	TCPROFIL EXEC	PROFILE EXEC	SSLDCSSM
491	___ (3*)	TCPROFIL EXEC	PROFILE EXEC	SSL*nnnnn*
491	191	TCPROFIL EXEC	PROFILE EXEC	DTCSMAPI

Notes:

1. Source minidisks owned by the 6VMTCP40 user ID.
2. Production minidisk, owned by the listed TCP/IP server user ID
3. SFS-resident; consult the notes that precede this figure for more information.

Figure 15 on page 50 lists the various TCP/IP for z/VM ***sample*** configuration files that have been provided to assist you with customization of TCP/IP services for your installation. The *sample* file locations shown are those established by the TCP/IP for z/VM product packaging build lists, where as *configured* locations are those established through *optional* use of the **PRODUTL** command, with **tcpconfig** specified as the catalog section operand. For reference, source and production file naming information provided as well.

Note: Unless noted otherwise, the minidisks listed in the *Sample Location* and *Configured Location* columns in Figure 15 on page 50 are TCP/IP for z/VM *production* minidisks owned by the TCPMAINT user ID.

Figure 15 (Page 1 of 2). TCP/IP for z/VM Sample and Configuration Files

Sample Location (1*)	Configured Location (1*, 2*)	Sample File Name / Type	Configured File Name / Type	Usage
591	198	TCPRUNXT SAMPEXEC	TCPRUNXT EXEC	TCP/IP Servers
591	198	PROFILE STCPIP	PROFILE TCPIP	TCPIP
591	198	SCEXIT SAMPEXEC	SCEXIT EXEC	TCPIP
591	198	SCEXIT SAMPASM	SCEXIT ASSEMBLE	TCPIP
591	198	PMEXIT SAMPEXEC	PMEXIT EXEC	TCPIP
591	198	PMEXIT SAMPASM	PMEXIT ASSEMBLE	TCPIP
591	198	CHKIPADR SAMPEXEC	CHKIPADR EXEC	FTPSERVE
591	198	FTPEXIT SAMPEXEC	FTPEXIT EXEC	FTPSERVE
591	198	FTPEXIT SAMPASM	FTPEXIT ASSEMBLE	FTPSERVE
591	198	SRVRFTP SCONFIG	SRVRFTP CONFIG	FTPSERVE
591	198	IMAP SCONFIG	IMAP CONFIG	IMAP
591	198	TCPVMIPC SAMPNAME	$SERVER$ NAMES	IMAP
591	198	IMAPAUTH SAMPEXEC	IMAPAUTH EXEC	IMAPAUTH
591	198	LDAP-DS SCONFIG	DS CONF	LDAPSRV
591	198	LDAP-DS SAMPENVR	DS ENVVVAR	LDAPSRV
591	198	MPROUTE SCONFIG	MPROUTE CONFIG	MPRoute
591	198	RSCSTCP SCONFIG	RSCSTCP CONFIG	RSCS
591	198	RSCSLPD SCONFIG	RSCSLPD CONFIG	RSCS (LPD)
591	198	RSCSLPR SCONFIG	RSCSLPR CONFIG	RSCS (LPD)
591	198	RSCSLPRP SCONFIG	RSCSLPRP CONFIG	RSCS (LPD)
591	198	RSCSUFT SCONFIG	RSCSUFT CONFIG	RSCS (UFT)
591	198	SMTP SCONFIG	SMTP CONFIG	SMTP
591	198	SMTPCMDX SAMPEXEC	SMTPCMDX EXEC	SMTP
591	198	SMTPCMDX SAMPASM	SMTPCMDX ASSEMBLE	SMTP
591	198	SMTPVERX SAMPEXEC	SMTPVERX EXEC	SMTP
591	198	SMTPVERX SAMPASM	SMTPVERX ASSEMBLE	SMTP
591	198	SMTPFWDX SAMPEXEC	SMTPFWDX EXEC	SMTP
591	198	SMTPFWDX SAMPASM	SMTPFWDX ASSEMBLE	SMTP

Notes:

1. Minidisks owned by the TCPMAINT user ID.
2. Location as ***optionally*** placed into production by using the **PRODUTL** command.
3. A pre-configured copy of this file is installed on the TCPMAINT 591 minidisk. Any modifications required must be implemented in a 198-resident copy of this file.
4. This file is provided for exclusive use by this server, and should ***not*** altered in any manner.

Figure 15 (Page 2 of 2). TCP/IP for z/VM Sample and Configuration Files

Sample Location (1*)	**Configured Location** (1*, 2*)	**Sample File Name / Type**	**Configured File Name / Type**	**Usage**
591	198	SMTPMEMO SAMPLE	SECURITY MEMO	SMTP
591	198	SMTPSECT SAMPTABL	SMTP SECTABLE	SMTP
591	198	MIB_DESC SDATA	MIB_DESC DATA	SNMPQE
591	198	MIB_EXIT SDATA	MIB_EXIT DATA	SNMPSUBA
591	198	SNMPMIBX SAMPASM	SNMPMIBX ASSEMBLE	SNMPSUBA
591	198	UFTD SCONFIG	UFTD CONFIG	UFTD
591	198	UFTCMDX SAMPEXEC	UFTCMDX EXEC	UFTD
591	198	UFTNSLKX SAMPEXEC	UFTNSLKX EXEC	UFTD
591	198	VMNFS SCONFIG	VMNFS CONFIG	VMNFS
591	198	VMNFSCMS SAMPEXEC	VMNFSCMS EXEC	VMNFS
591	198	VMNFSSMG SAMPEXEC	VMNFSSMG EXEC	VMNFS
591	198	VMNFSMON SAMPEXEC	VMNFSMON EXEC	VMNFS
592	592	TCPIP SDATA	TCPIP DATA	All Services
592	592	ETCHOSTS SAMPLE	ETC HOSTS	All Services
592	592	ETC SAMPSERV	ETC SERVICES	All Services
592	198	HOSTS SLOCAL	HOSTS LOCAL	All Services
592	592	LCL2ETC SAMPEXEC	LCL2ETC EXEC	TCP/IP Admin.
592	592	RTD2MPR SAMPEXEC	RTD2MPR EXEC	TCP/IP Admin.
592	592	MIBX2DSC SAMPEXEC	MIBX2DSC EXEC	TCP/IP Admin.
592	592	IPFORMAT SCONFIG	IPFORMAT CONFIG	TCP/IP Admin.
592	592	PKTTRACE SAMPEXEC	PKTTRACE EXEC	TCP/IP Admin.
592	592	FTP SDATA	FTP DATA	FTP Client
592	592	GDXAPLCS SAMPMAP	GDXAPLCS MAP	GDDMXD/VM
591	198	DTCVSW1 STCPIP	DTCVSW1 TCPIP (3*)	DTCVSW1
591	198	DTCVSW2 STCPIP	DTCVSW2 TCPIP (3*)	DTCVSW2
591	198	DTCVSW3 STCPIP	DTCVSW3 TCPIP (3*)	DTCVSW3
591	198	DTCVSW4 STCPIP	DTCVSW4 TCPIP (3*)	DTCVSW4
591	____	DTCSMAPI STCPIP (4*)	_____ _____	DTCSMAPI

Notes:

1. Minidisks owned by the TCPMAINT user ID.
2. Location as ***optionally*** placed into production by using the **PRODUTL** command.
3. A pre-configured copy of this file is installed on the TCPMAINT 591 minidisk. Any modifications required must be implemented in a 198-resident copy of this file.
4. This file is provided for exclusive use by this server, and should ***not*** altered in any manner.

6.2.3 TCP/IP for z/VM CATALOG Files

For the most part, a TCP/IP for z/VM **catalog** file is one that is referenced by the PRODUTL command, to determine if any TCP/IP for z/VM sample configuration file samples have been updated by service actions.

Certain sections and entries within this file also can be used to create a starter set of TCP/IP configuration files (as described in 6.2.2.1, "Create a Starter Set of TCP/IP Configuration Files (Optional)" on page 44). For TCP/IP for z/VM, the TCPCONFIG section of the 6VMTCP40 CATALOG file is such a section. For reference, the files identified within this section are listed in Figure 15 on page 50).

See *z/VM: VMSES/E Introduction and Reference*, Chapter 20, for detailed information about the PRODUTL command, as well as information about the structure, content, and customization requirements and considerations for TCP/IP for z/VM catalog files.

6.2.3.1 Catalog Files Supplied with TCP/IP for z/VM

The catalog files provided for with TCP/IP for z/VM are listed in Figure 16.

Figure 16. TCP/IP for z/VM Catalog Files

Catalog File Name / Type	Associated Files
6VMTCP40 CATALOG	Various TCP/IP for z/VM Files

The catalog sections listed and described here are defined in the catalog file supplied with TCP/IP for z/VM:

Section	Description
TCPCONFIG	**Optionally** used to create suitably named configuration files for customizing TCP/IP and TCP/IP services for your installation. For reference, the files processed using the this section are listed in Figure 15 on page 50.
TCPNOTIFY	Used to process product files for which notification of any service updates to these files is of importance. For reference, the files processed using the this section are listed in Figure 13 on page 48.
TCPSAMPLE	Used to process customizable TCP/IP sample files. For reference, the files processed using this section are listed in Figure 15 on page 50.
TCPSVMCMS	Used to process non-customizable TCP/IP for z/VM run-time files that must reside on individual **CMS-based** server virtual machine (SVM) minidisks. For reference, the files processed

using the TCPSVMCMS section are listed in Figure 14 on page 48.

6.2.4 Customization Notes

1. It is advised that any TCP/IP for z/VM CATALOG file changes that are required for your environment be made via a VMSES/E local modification, to allow for the reporting of service-related changes during VMSES/E processing. For more information about creating a local modification for a TCP/IP for z/VM CATALOG file, consult the local modification process described in *z/VM: Service Guide* (GC24-6247).

   When changes are made, ensure the only files identified for PRODUTL processing are those associated with the servers defined for your environment.

2. The source and target minidisk/directory variable names used within the CATALOG file correspond to those used within the TCP/IP for z/VM ($)PPF file (or an override variation of that file). If any changes are made to the Variable Declarations (:DCL.) section of the TCP/IP for z/VM PPF file via a PPF override, you might need to incorporate similar changes within TCP/IP for z/VM CATALOG files (through separate VMSES/E local modifications) to allow for the correct resolution of PPF :DCL. variable names.

3. Any :DCL. wildcard values (%*) that might be present in a TCP/IP CATALOG file are unique to that file — these values are *not* supported (or present) within a VMSES/E PPF file. Such values should be used only to define a file exclusion entry that is to be referenced during a wildcard file copy operation.

4. If new sample and configuration files are supplied as part of service for TCP/IP for z/VM, the 6VMTCP40 CATALOG file will be updated to reflect the new files.

TCP/IP for z/VM is now installed and built on your system.

7.0 Service Instructions

Note — z/VM Automated Service Procedure

The z/VM automated service procedure (use of the z/VM **SERVICE** and **PUT2PROD** commands) is ***required*** for applying service to TCP/IP for z/VM.

7.1 Install TCP/IP for z/VM Preventive or Corrective Service

Use the service instructions documented in *z/VM: Service Guide* to receive, apply, build and place TCP/IP for z/VM service into production.

For information about testing TCP/IP for z/VM service prior to placing it into production, see the appropriate appendix of *z/VM: Service Guide*.

7.2 Additional TCP/IP for z/VM Service Procedures (Optional)

In most instances, the procedures and information presented in this section will not be required when TCP/IP for z/VM service has been installed. However, these procedures might be required if:

- specific messages are received from the z/VM **PUT2PROD** command when the z/VM automated service procedure is used.
- new TCP/IP for z/VM functions and customizable files are provided through service updates (for which case, notification of any newly added files does not occur).

7.2.1 Message VMFPRD3043W Notifications

Note

If message **VMFPRD3043W** is reported during the z/VM automated service procedure for any TCP/IP for z/VM files, you need to review and take action for one or both of the situations described here.

1. If this message is reported for any of the ***non-sample*** files listed in Figure 13 on page 48, you must take further action to ensure the subject files are properly placed into production. For more information, see Appendix E, “Managing TCP/IP Files with Unique Service Requirements” on page 74.
2. If this message is reported for any of the ***sample*** files listed in Figure 15 on page 50, you might need to update your TCP/IP for z/VM configuration. For more information, see 7.2.2, “Update your TCP/IP for z/VM Configuration” on page 55.

© Copyright IBM Corp. 1990, 2016

7.2.2 Update your TCP/IP for z/VM Configuration

If any TCP/IP for z/VM *sample* configuration files have been updated through service (as reported by message **VMFPRD3043W**) review the updated content of all pertinent files, and determine whether changes are required to any customized, production-use counterparts that are used for your installation.

When necessary, an updated sample file can be compared with its base-level counterpart (on the **6VMTCP40 2B2** Base Code minidisk) to identify specific changes that might not be apparent in a customized, production-use file.

For information about specific service-related changes, you might consult APAR-specific documentation or an updated publication (if applicable). If necessary, See *TCP/IP Planning and Customization* (SC24-6238) for detailed information about the content and use of these files, and how to configure specific TCP/IP servers for your environment.

7.2.3 Re-Initialize TCP/IP Services

Once you have completed any necessary configuration changes, the appropriate TCP/IP servers must be initialized. For more information, see the section that discusses “Starting and Stopping TCP/IP Servers” in the chapter titled “General TCP/IP Server Configuration,” of *TCP/IP Planning and Customization*.

In addition, the TCPMSMGR command is available to manage the startup and shutdown of the TCP/IP servers used by your installation. For more information about the TCPMSMGR command, see Appendix A, “TCP/IP Utilities” on page 57.

7.2.3.1 Copy Serviced TCP/IP Client Code to the z/VM Product Code Disk (Optional)

If you previously copied TCP/IP for z/VM client code to the z/VM product code disk, you should replace the appropriate files with their serviced counterparts. See Appendix D, “Copying TCP/IP for z/VM Client Code to the Y-Disk” on page 71 for additional information and instructions concerning this process.

Note: For a single system image (SSI) environment, this action must be completed ***for each member system*** that has been defined.

You have finished servicing TCP/IP for z/VM.

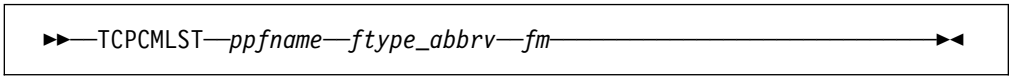
Appendix A. TCP/IP Utilities

A.1 TCPCMLST Command

A.1.1 Purpose

Use the TCPCMLST command to generate a file that lists PTF-numbered parts for which VMSES/E COMMIT processing might be applicable. The generated file (*ppfname* $REMLIST) can be used as input to the VMSES/E **VMFREM** command, which commits specific service levels for your maintenance environment.

Note: The TCPCMLST command is intended for use by the MAINT640 user ID, and should only be used when you commit service levels for TCP/IP for z/VM files.



A.1.2 Operands

ppfname The name of the usable form product parameter file used for installing and maintaining TCP/IP for z/VM; the file type must be **PPF**.

ftype_abbrv The 3-character abbreviation used for PTF-numbered files that correspond to the actual (or, *base*) CMS file types used for TCP/IP for z/VM files. For example, **MOD** is the part-type abbreviation used for TCP/IP parts that have a base file type of **MODULE**. The mapping of file type abbreviations and their corresponding base file types can be found in the VM SYSABRVT file.

fm The file mode of the minidisk or directory on which PTF-numbered parts of concern are maintained. By convention, this is the TCP/IP for z/VM **DELTA** minidisk (**6VMTCP40 2D2**, by default) or an equivalent SFS directory.

A.1.3 Usage Notes

1. A minidisk or directory must be accessed at file mode A with Read/Write (R/W) status, to allow for the creation of files by TCPCMLST.
2. TCPCMLST creates the files listed in Figure 17 (dependent upon current maintenance circumstances):

© Copyright IBM Corp. 1990, 2016

Figure 17. TCPCMLST - Generated Files

File Name / File Type	Content
ppfname $REMLIST	Lists PTFs that are candidates for commit processing. This file is created when PTF-numbered parts exist that correspond to the selected *ftype_abbrv* abbreviation).
ppfname $CMLSTLG	Lists PTFs identified for commit processing through prior TCPCMLST invocations. This file is produced (or updated) when a *ppfname* $REMLIST file already exists and PTF commit candidates are identified by TCPCMLST.
ppfname $BASLIST	Lists base-level parts that can be removed *after* commit processing has been completed for PTFs listed in the *ppfname* $REMLIST file. The base-level parts listed correspond to one (or more) of the listed PTF-numbered parts.
ppfname $CMBASLG	Lists base-level parts identified for removal through prior TCPCMLST invocations. This file is produced (or updated) when a *ppfname* $BASLIST file already exists and TCPCMLST is invoked and base-level removal candidates are identified along with PTF commit candidates.

3. If TCPCMLST is invoked with *ppfname* specified as a question mark (**?**), the command syntax is displayed.

A.1.4 Return Codes

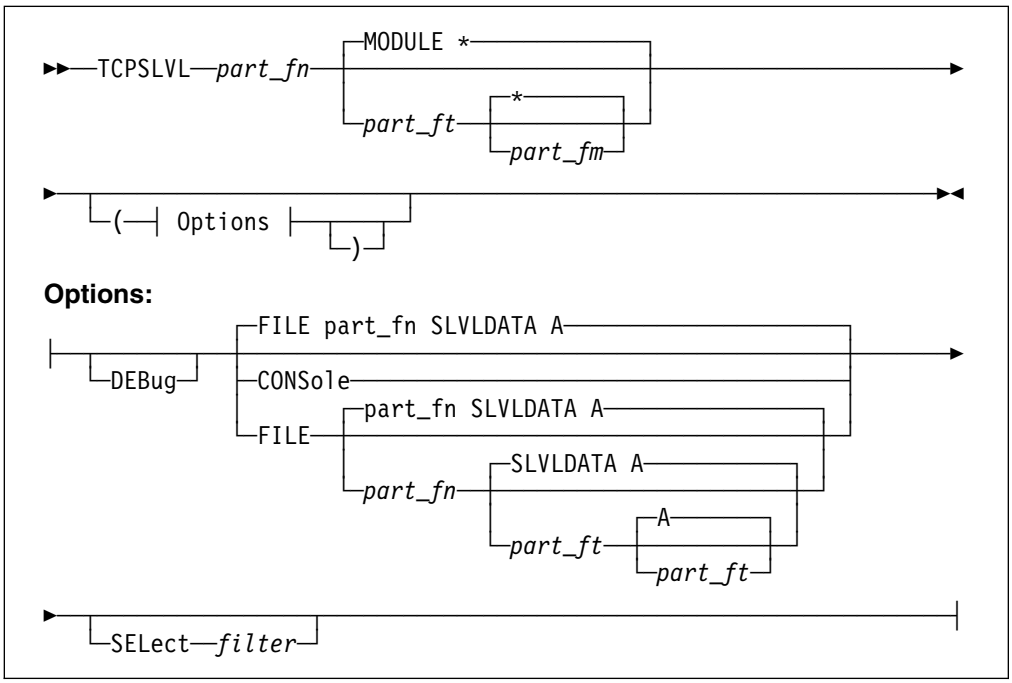
Return Code	Description
0	Successful execution; no processing errors were encountered.
1	Incorrect invocation. TCPCMLST was invoked with an incorrect number of operands. A message that identifies the missing operand is displayed, in addition to the command syntax.
2	Internal error. If return code 2 is returned, processing status is unknown. Contact the TCP/IP for z/VM support group for problem determination and assistance in addressing this type of error.
8	Errors encountered; processing has not completed successfully.

A.2 TCPSLVL Command

A.2.1 Purpose

Use the TCPSLVL command to display service information that is intrinsic to a TCP/IP executable MODULE file. The information presented is obtained from data that is embedded within the various TEXT decks (files) that comprise a given MODULE.

Note: The TCPSLVL command is intended for use as a diagnostic aid, in consultation with the IBM TCP/IP support group.



A.2.2 Operands

part_fn The file name of the TCP/IP executable file from which service information is to be obtained.

part_ft The file type of the TCP/IP file from which service information is to be obtained. The default is MODULE (since internal service information is available for only TCP/IP MODULE files.

part_fm The file mode of the minidisk or directory on which the file of interest resides. The default is an asterisk (*), which means the first file present in the current search order that matches the provided *part_fn* and *part_fn* is to be evaluated.

A.2.3 Options

CONSole
Causes command results to be displayed at the console.

DEBUG
Causes supplementary messages and data to be reported for diagnostic purposes.

SELect *filter*
Specifies a character string that is used to limit response information to entries that match the value of *filter*.

FILE *fn ft fm*
Directs command results to be placed in a designated CMS file. By default, results are placed in a file named to match the part of interest (*part_fn*) with a file type of SLVLDATA, at file mode A.

A.2.4 Usage Notes

1. When TCPSLVL examines the MODULE you specify, it produces an output line for each TEXT deck in which maintenance data is present. Each line begins with the keyword **SLVL**, followed by the name of a TEXT deck, and its corresponding service indicator. This indicator might reflect either an Authorized Program Analysis Report (APAR) number or an IBM development tracking number. This information, taken as a whole, then can provide an overall (or perhaps, "rule of thumb") indication of the service that is incorporated within a given module.
2. The TCPSLVL command and the information it provides are intended to supplement the information and files that are maintained or used by VMSES/E and its various utilities. TCPSLVL data should be used, at most, only to form generalizations about the service content of TCP/IP modules.

A.2.5 Examples

- This TCPSLVL command that follows checks the service content of the NETSTAT MODULE that resides at file mode "P":

  ```
  tcpslvl netstat module p
  ```

  For this command, results would be placed in the file LPR SLVLDATA A, which might then contain this information:

```
SLVL  CMNETST   ZVM640
SLVL  CMTCPPR   MT02782
SLVL  CMERUPT   ZVM640
SLVL  CMRESOL   ZVM640
SLVL  CMPRCOM   ZVM640
SLVL  CMUNTOK   ZVM640
SLVL  CMHOSTN   ZVM640
SLVL  CMXTRPT   PQ68463
```

In this example, an APAR level number is cited for the CMXTRPT TEXT file, while an internal IBM development tracking number is cited for the CMTCPPR TEXT part. For the remaining TEXT components, a level-specific value (ZVM640), which reflects more generalized update activity associated with development of the current z/VM deliverable, is cited.

- This next example adds the **SELECT** option to the previous command, to limit results to entries associated with APAR updates — specifically those that begin with the string `PQ`:

  `tcpslvl netstat module p ( cons sel pq`

  Based on the results shown for the previous example, the results displayed at the console for this command would be:

  ```
  SLVL  CMXTRPT   PQ68463
  ```

A.2.6 Return Codes

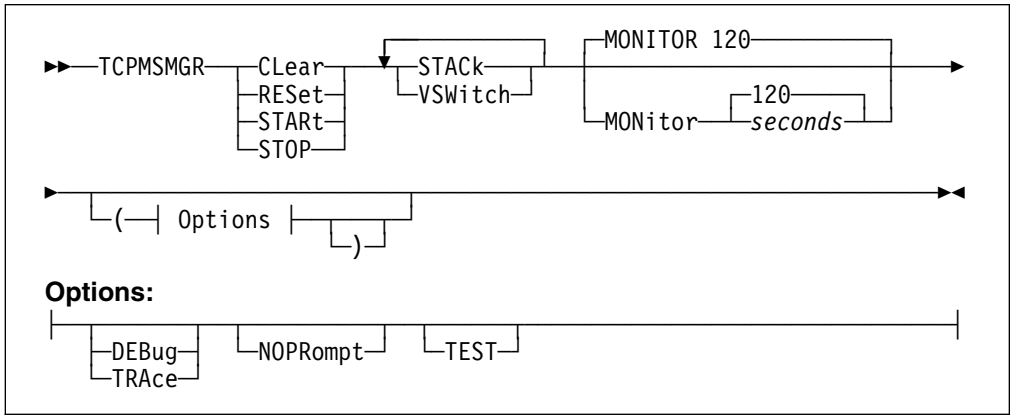
Return Code	Description
0	Successful execution; no processing errors were encountered.
1	Incorrect command invocation, or “help” was requested. TCPSLVL was invoked with an incorrect number of operands, or was invoked with a question mark (?) as the first (or only) operand. In response, the command syntax is displayed.
nn	Processing error. A nonzero return code (other than 1) indicates an problem was encountered when the file was evaluated. Such a return code will be presented when the specified file cannot be located, or when an error occurs when file contents are examined.

A.3 TCPMSMGR Command

A.3.1 Purpose

Use the TCPMSMGR command to shutdown (stop) or initialize (start) the set of **TCP/IP stack** servers, **VSWITCH controller** virtual machines, or both, that are defined for your installation. The virtual machines that are to be stopped or started using this command are identified based on `:stack` class definitions that are present within available DTCPARMS files.

Note: The TCPMSMGR command has been provided as an aid for stopping and starting the indicated groups of servers as part of the z/VM service procedures. However, it can be used in a stand-alone manner (provided the appropriate operational environment is established).



A.3.2 Operands

CLear
RESet

Causes saved GLOBALV values used by the program to be cleared. Variables for STACK and VSWITCH processing are reset independent of one another using this operand. Thus, a STACK or a VSWITCH operand **must also be specified** when the CLEAR operand is used. RESET is synonymous with CLEAR.

If *test mode* values are to be cleared, include the TEST option as part of the command.

STARt

Initiates the start-up of TCP/IP stack or VSWITCH controller servers that were previously stopped via this program. Such servers are identified by saved GLOBALV values, as set through use of the STOP command function.

STOP
Initiates a shutdown of active TCP/IP stack or VSWITCH controller servers, as defined by applicable DTCPARMS files.

STACk
Directs TCPMSMGR START or STOP operations to affect the set of TCP/IP stack servers that are defined for the system, or signifies that GLOBALV variables which identify such servers should be cleared (for a CLEAR operation).

VSWitch
Directs TCPMSMGR START or STOP operations to affect the set of VSWITCH controllers that are defined for the system, or signifies that GLOBALV variables which identify such servers should be cleared (for a CLEAR operation).

MONitor *seconds*
Specifies the time (duration) for which a server should be monitored for reaching a logoff state, once it has successfully received a shutdown command. The default is 120 seconds, with minimum and maximum values of 10 and 360 seconds, respectively.

If the specified value is not a multiple of the internally defined monitoring interval of 10 seconds, the supplied value is rounded to the nearest such value. This operand is ignored for START and CLEAR operations.

A.3.3 Options

DEBUG
TRACE
Causes supplementary messages to be issued, to provide information for diagnostic purposes. Some supplementary messages (prefaced with a header of the form: `DTCMSM---->`) are also issued when this option is used. The DEBUG and TRACE options are synonymous.

NOPRompt
Prevents the issuance of confirmation prompts. An ***affirmative response*** (**1**) is assumed for prompts that are bypassed through use of this option.

TEST
Instructs TCPMSMGR to operate in *test* mode. Test mode allows one to see how the various servers identified for a START or STOP operation will be dealt with by TCPMSMGR, without taking direct action against those servers.

Note that because no such action is taken, successful command operations are assumed. Thus, any error handling that might be required for a non-test operation is likely not be evident.

A.3.4 Usage Notes

1. This command is intended for use by an appropriate TCP/IP or system administrative user ID (such as **TCPMAINT** or **MAINT**) that is authorized to use privileged TCP/IP functions. (That is, a user ID that is included in appropriate **OBEY** statement lists, as defined within the TCP/IP server configuration files that pertain to your installation). In lieu of such authorization, a privilege class sufficient to use the CP FORCE command is necessary.
2. A privilege class sufficient to use the CP QUERY CONTROLLER ALL command is necessary to use the TCPMSMGR command.
3. When the **TEST** option is used, the server monitoring time is forced to a period of **three** seconds, with a one second interval applied. This is done to portray the fact that such delays would occur during normal operations, even though no actions are taken under test mode to stop or start a given server virtual machine.

A.3.5 Return Codes

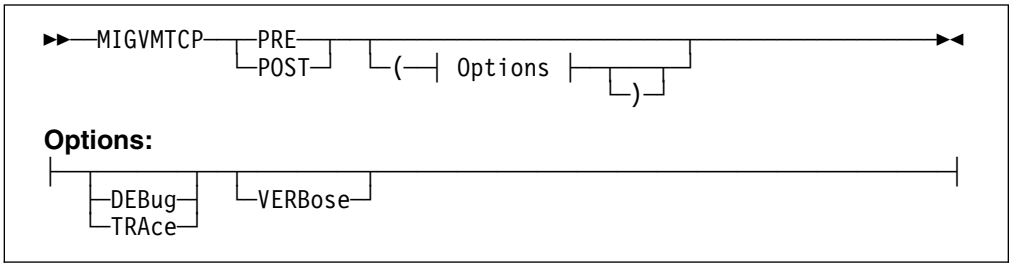
Return Code	Description
0	Successful execution; no processing errors were encountered.
1	Incorrect invocation. TCPMSMGR was invoked with an incorrect number of operands, or one or more operands that are not recognized.
2	Internal error. If this return code is produced, processing status is indeterminate. Contact the TCP/IP for z/VM support group for problem determination and assistance in addressing this type of error.
3	TCP/IP for z/VM configuration error encountered; processing is cancelled upon the identification and reporting of such a problem.
4	Errors encountered, with warnings issued. The errors encountered might have caused processing to complete with only partial success. Review the messages produced by the command for information about any problems that were encountered.
8	Errors encountered; processing has not completed successfully. Review the messages produced by the command for information regarding the problems encountered.

A.4 MIGVMTCP Command

A.4.1 Purpose

The MIGVMTCP command is a VMSES/E MIGRATE command exit that performs a collective evaluation of customized TCP/IP for z/VM files that are in use on a production z/VM system. This evaluation attempts to identify configuration files that are associated with IBM-supplied sample file counterparts, so that the VMSES/E migration procedures can properly manage such customized files as they are migrated to a new z/VM system (which might also include the reporting of customization changes that might be required, due content changes in IBM sample counterparts).

Note: The MIGVMTCP command has been provided for use by VMSES/E MIGRATE command, and is designed to operate on a z/VM system that is the intended target of a migration operation. The MIGVMTCP command **is not intended for use in a stand-alone manner**.



A.4.2 Operands

PRE Instructs the MIGVMTCP command to perform preparation operations that pertain to the migration of TCP/IP for z/VM. When this operand is used, the MIGVMTCP command analyzes the various configured files and attempts to associate these files with IBM-supplied sample file counterparts. In addition, selected TCP/IP server minidisks (those for server virtual machines defined in the relevant system TCP/IP PPF file) are evaluated, again to discern server-specific configuration files from those that are not pertinent to the migration procedure. The results of this evaluation then are used to update various VMSES/E tables that are referenced by the VMSES/E MIGRATE command.

POST Instructs the MIGVMTCP command to perform follow-on operations that pertain to the migration of TCP/IP for z/VM. At present, no specific actions are performed when this operand is used.

A.4.3 Options

DEBUG
TRACE

Instructs the MIGVMTCP command to log internal data and logic information in a file (migvmtcp $DEBUG), for diagnostic purposes. Some supplementary messages (prefaced with a header of the form: `DTCMIG---->`) are also issued when this option is used. The DEBUG and TRACE options are synonymous.

VERBose

Causes supplementary messages to be issued to provide information for diagnostic purposes. Messages produced from using this option are prefaced with a header of the form:

- `DTCMIG....:`
- `DTCMIG....*>`

A.4.4 Usage Notes

1. The DEBUG, TRACE, and VERBOSE command options are intended for diagnostic use, in consultation with the IBM TCP/IP support group

A.4.5 The MIGVMTCP $MSGLOG File

Pertinent informational, warning and error messages that are issued to the console by MIGVMTCP are also recorded in a message log file, MIGVMTCP $MSGLOG. This log file is written to the minidisk or directory accessed at file mode A, and can be viewed using the VMSES/E **VMFVIEW** command.

The MIGVMTCP $MSGLOG is cumulative, with the most recent entries appended at the **top** of the file. Separator headers that include date and time stamps are inserted in the log with each MIGVMTCP invocation so newer log entries can be distinguished from older ones.

Notes:

1. Messages are not logged until MIGVMTCP has completed an initial validation of supplied operands.
2. Diagnostic and other incidental messages are not recorded in the MIGVMTCP $MSGLOG file.

A.4.6 Return Codes

Return Code	Description
0	Successful execution; no processing errors were encountered.

4	Errors encountered, with warnings issued. The errors encountered might have caused processing to complete with only partial success. Review the messages produced by the command for information about any problems that were encountered.
8	Errors encountered; processing has not completed successfully. Review the messages produced by the command for information regarding the problems encountered.
9	TCP/IP for z/VM configuration error encountered; processing is cancelled upon the identification and reporting of such a problem.
10	Incorrect invocation. MIGVMTCP was invoked with an incorrect number of operands, or one or more operands that are not recognized.
11	Internal error. If this return code is produced, processing status is indeterminate. Contact the TCP/IP for z/VM support group for problem determination and assistance in addressing this type of error.

Appendix B. TCP/IP for z/VM Local Modifications

This appendix provides information to assist you with making local modifications to various (but not all) types of TCP/IP for z/VM components.

The information herein is intended only to supplement the local modification process described in *z/VM: Service Guide* (GC24-6247). This publication includes detailed information about installing and maintaining local modifications for your installation.

Note: TCP/IP source files are distributed as part of the z/VM version 6 release 4 System deliverable. These files reside on the TCP/IP for z/VM **SOURCE** minidisk (**6VMTCP40 2B3**, by default), or an equivalent SFS directory.

B.1 VMNFS Local Modification Considerations

Local modifications to the TCP/IP for z/VM NFS server module (VMNFS). would be required for the NFS server to:

- use of a file handle encryption subroutine different from that in NFSFHCIP ASSEMBLE
- validate SMSG requests in a manner different from its current implementation (affects NFSSMSG C)
- report failed minidisk link attempts in a manner different from its current implementation (affects NFSBADPW C).

Certain modifications might also require changes to the TCPBLC91 EXEC, which is the build list used to build the VMNFS module.

© Copyright IBM Corp. 1990, 2016

Appendix C. TCP/IP for z/VM Build Lists

This appendix provides a complete list of the VMSES/E build lists used to maintain TCP/IP for z/VM. This information has been provided to help you determine which build list to use with VMSES/E commands when you need to build or service specific TCP/IP objects, and to assist you with making local modifications. For more information about build list content and formats, see the *z/VM: VMSES/E Introduction and Reference* (GC24-6243).

The build lists identified in the tables that follow can be found on the 6VMTCP40 2B2 (BASE1) minidisk. However, before using the information within a given build list, the 6VMTCP40 2D2 (DELTA) minidisk should be checked for a more current, serviced counterpart; this will ensure the most current build list file is referenced.

Also, note that the minidisks shown under the "Build String" headings are 6VMTCP40 minidisk defaults. If a PPF override has been used in your environment to change Build String minidisks or SFS directories, use your values when you determine which files are affected by a build list.

C.1 TCP/IP for z/VM Build Lists

Figure 18 lists the VMSES/E build lists used for TCP/IP for z/VM, and provides general information about the objects (files) managed by each:

Figure 18 (Page 1 of 2). VMSES/E Build Lists - TCP/IP for z/VM

Build List Name	VMSES/E Part Handler	Build String (Minidisk)	Build List Description / Affected Objects
TCPBL491	VMFBDCOM	BUILD1 (491)	Full-replacement objects built to the 491 minidisk
TCPBL492	VMFBDCOM	BUILD3 (492)	Full-replacement objects built to the 492 minidisk
TCPBLM91	VMFBDMOD	BUILD1 (491)	MODULE objects built to the 491 minidisk
TCPBLM92	VMFBDMOD	BUILD3 (492)	MODULE objects built to the 492 minidisk
TCPBLC91 (1*)	VMFBDMOD	BUILD1 (491)	C-based MODULE objects built to the 491 minidisk
TCPBLC92 (1*)	VMFBDMOD	BUILD3 (492)	C-based MODULE objects built to the 492 minidisk
TCPBLP91 (1*)	VMFBDTLB	BUILD1 (491)	VMFBDPMD-dependent MODULE objects built to the 491 minidisk
TCPBLP92 (1*)	VMFBDTLB	BUILD3 (492)	VMFBDPMD-dependent MODULE objects built to the 492 minidisk
TCPBLHLP	VMFBDCOM	BUILD8 (29D)	TCP/IP CMS Help Files for z/VM 19D Help minidisk

Notes:

1. Language Environment for z/VM support must be available when building objects identified in this build list.

© Copyright IBM Corp. 1990, 2016

Figure 18 (Page 2 of 2). VMSES/E Build Lists - TCP/IP for z/VM

Build List Name	VMSES/E Part Handler	Build String (Minidisk)	Build List Description / Affected Objects
TCPBLLC1	VMFBDCOM	BUILD1 (491)	LDAP server-only message catalog build list
TCPBLLC2	VMFBDCOM	BUILD3 (492)	LDAP server and client message catalog build list
TCPBLLBF	VMFBDBFS	None (BFS)	Facilitates processing of BFS-resident files
TCPBLALL	VMFBDMLB	BUILD3 (492)	ALLMACRO MACLIB build list
TCPBLCSL	VMFBDCLB	BUILD1 (491)	TCPCSLIB CSLIB build list
TCPBLCOM	VMFBDTLB	BUILD3 (492)	COMMTXT TXTLIB build list
TCPBLGDD	VMFBDTLB	BUILD3 (492)	GDDMXD TXTLIB build list
TCPBLXAW	VMFBDTLB	BUILD3 (492)	XAWLIB TXTLIB build list
TCPBLDPI	VMFBDTLB	BUILD3 (492)	DPILIB TXTLIB build list
TCPBLRPC	VMFBDTLB	BUILD3 (492)	RPCLIB TXTLIB build list
TCPBLRPT	VMFBDPMD	BUILD3 (492)	VMRPC TXTLIB build list
TCPBLOLD	VMFBDTLB	BUILD3 (492)	OLDXLIB TXTLIB build list
TCPBLXTL	VMFBDTLB	BUILD3 (492)	XTLIB TXTLIB build list
TCPBLX11	VMFBDTLB	BUILD3 (492)	X11LIB TXTLIB build list
TCPBLSNM	VMFBDLLB	BUILD1 (491)	SNMPLIB LOADLIB build list

Notes:

1. Language Environment for z/VM support must be available when building objects identified in this build list.

Appendix D. Copying TCP/IP for z/VM Client Code to the Y-Disk

To simplify access to TCP/IP client functions for your user community, you might find it desirable to copy all, or a subset of, TCP/IP for z/VM client code to the z/VM Product Code minidisk (typically the MAINT 19E minidisk, or the **Y-disk**). Doing so will avoid the need for users to additionally link and access the TCPMAINT 592 minidisk.

As well, applications that use certain programming interfaces might require TCP/IP-specific information to be available for proper operation. For example, information defined in the TCPIP DATA file is referenced by:

- the C run-time library sockets support to correctly identify the TCP/IP virtual machine. See the *XL C/C++ for z/VM Run-Time Library Reference* (SC09-7624) for more information.
- the VMTCPDT routine, which resides in the VMMTLIB TXTLIB that is associated with the VMLIB Callable Services Library (CSL). See the *z/VM: CMS Callable Services Reference* (SC24-6165) for more information about the VMTCPDT CSL routine.
- various functions provided as part of the CMS REXX Socket library. See the *z/VM: REXX/VM Reference* (SC24-6221) for more information.

To copy TCP/IP for z/VM client files to the Product Code minidisk, use the following procedure **after** you have installed TCP/IP for z/VM.

Warning - Cross-Component File Overlap Considerations

Before you copy *any* TCP/IP for z/VM client files to the Y-disk (or a similar *common use* minidisk), you should first determine whether any conflicts exist between the TCP/IP client files you choose to copy, and those present on the target (Y-disk) minidisk. If any file conflicts are found, these should be addressed and resolved with respect to your installation environment before you continue with the procedure that follows.

Notes:

1. **You will need to repeat this procedure:**
   - each time you apply service to TCP/IP for z/VM
   - for each member system that is defined as part of an SSI cluster.
2. Use discretion when wildcards (*) are used for both the *fn* (file name) and *ft* (file type) parameters of the VMFCOPY commands shown in this section, since files that exist on the Y-disk can be replaced with similarly-named TCP/IP counterpart files. The overlay of certain files might be warranted in some cases, and might be undesirable for others.

© Copyright IBM Corp. 1990, 2016

An example of this latter case is cited here. Both TCP/IP for z/VM and the Language Environment for z/VM have several **H** files that are identically named, but differ in content. These files are:

```
FCNTL    H    IF       H    IN       H    INET     H
IOCTL    H    NETDB    H    RESOURCE H    SOCKET   H
STRINGS  H    TTYDEV   H    TYPES    H    UIO      H
```

An overlay of Language Environment for z/VM **H** files (those already present on the Y-disk) by their TCP/IP counterparts might create problems when applications are developed or rebuilt that expect (and rely upon) the content of Language Environment for z/VM files.

3. Before copying TCP/IP for z/VM files to another minidisk, ensure adequate storage space is available to maintain the files you have selected.

   1 Log on the z/VM product maintenance user ID, **MAINT640**.

   2 Process TCP/IP for z/VM files used by or available to TCP/IP clients.

link tcpmaint 592 592 rr
access 592 e
access 19e f

Note: If the Y-disk is not defined as the 19E minidisk in your environment, substitute the appropriate device number for this minidisk.

vmfcopy *fn ft* **e = = f2 (olddate replace sprodid 6vmtcp40%tcpip prodid 6vmtcp40%tcpip**

The VMFCOPY command will update the VMSES/E PARTCAT file on the Y-disk.

Wildcards (*) can be substituted for *fn* (file name) and *ft* (file type), but should be used with discretion.

   3 (Optional) Erase any TCP/IP for z/VM files that you do not want to remain on the Y-disk — for example, any MAP files that correspond to TCP/IP for z/VM modules re-built during service. Refer to the VMSES/E PARTCAT file on Y-disk to determine which files are associated with TCP/IP for z/VM.

   Note: Additional information about managing TCP/IP for z/VM client files, as well as their association with specific TCP/IP functions, is available on-line via the TCP/IP for z/VM home page on the World Wide Web. The URL for this home page is:

   ```
   www.vm.ibm.com/related/tcpip/
   ```

vmferase file *filename filetype* **f**

See the *z/VM: VMSES/E Introduction and Reference* for more information about the VMFERASE command and options that might help you remove specific files.

4 Re-save the CMS saved system, to return the Y-disk to shared status. See the “Placing (Serviced) Components into Production” section of the *z/VM: Service Guide* for detailed information about how to save the CMS saved system.

Appendix E. Managing TCP/IP Files with Unique Service Requirements

When to Use This Procedure

The steps outlined in this appendix must be completed if message **VMFPRD3043W** is reported by the PRODUTL command — through its direct use, or as part of the z/VM automated service procedure — when ***specific*** TCP/IP for z/VM files are processed.

This appendix provides information to assist you with managing certain TCP/IP files that require some manner of unique processing to fully place those files into production on your system.

Files that warrant such action are the:

- TCPROFIL EXEC

E.1.1 TCP/IP Server Profile Processing Requirements

The following server profiles are provided with TCP/IP for z/VM:

- the **CMS** server profile (**PROFILE EXEC**), which is common to all TCP/IP *CMS-based* servers — inclusive of VSWITCH controller virtual machines. This file is supplied (and serviced) as the file: TCPROFIL EXEC

If any of the above-listed server profiles are updated by service, the subject file must be copied to the 191 minidisks of the pertinent TCP/IP servers used by your installation. To accomplish this, write access to each such minidisk is necessary; however, this type of access is not possible while the servers are in operation. Thus, each affected server used by your installation must be stopped, with the server profile then copied to the appropriate minidisks, and the servers restarted.

Because write access to the various TCP/IP server 191 minidisks is generally not possible when z/VM service is installed, the z/VM automated service procedure does not attempt to place any updated TCP/IP server profiles into production.

For the rare occasion when this type of processing is required, the procedure that follows can be used to effect the necessary updates.

Note: You will need to repeat this procedure for each member system that is defined as part of an SSI cluster.

E.1.1.1 Copy Server Profile Files Into Production

1 Log on the z/VM product maintenance user ID, **MAINT640**.

The PROFILE EXEC supplied with the z/VM version 6 release 4 System deliverable for this user ID contains ACCESS commands for VMSES/E

© Copyright IBM Corp. 1990, 2016

minidisks that are necessary to run the commands cited in later steps. The minidisks required are the VMSES/E code minidisk (MAINT640 5E5, by default) and the VMSES/E Software Inventory minidisk (MAINT640 51D, by default).

2 Issue the CMS QUERY DISK command to verify the VMSES/E code and Software Inventory minidisks are correctly linked and accessed.

query disk

Verify the MAINT640 5E5 minidisk is accessed as file mode **B**.

Verify the MAINT640 51D minidisk is accessed as file mode **D**, and is linked **R/W**.

Note: If another user has the MAINT640 51D minidisk linked in write (R/W) mode, you'll obtain only read (R/O) access to this minidisk. If this occurs, have that user re-link the 51D disk in read-only (RR) mode, after which you need issue the appropriate LINK and ACCESS commands for the 51D minidisk. Do not continue with these procedures until a R/W link is established to the 51D minidisk.

3 If necessary, establish the appropriate access to the VMSES/E minidisks.

a Establish read access to the VMSES/E code minidisk. (to allow use of the PRODUTL command).

link maint640 5e5 5e5 rr
access 5e5 b

b Establish write access to the Software Inventory minidisk.

link maint640 51d 51d mr
access 51d d

4 Establish the appropriate working environment, to ensure the appropriate TCP/IP for z/VM files are available.

vmfsetup servp2p {tcpipp2p | tcpipsfsp2p}

Use **tcpipp2p** if the TCP/IP for z/VM default minidisk environment has been maintained; use **tcpipsfsp2p** if the service minidisks were moved to Shared File System directories.

The 6VMTCP40 CATALOG file and TCPMSMGR command (used in later steps), which reside on the 491 minidisk, are made accessible this command.

5 Shutdown the appropriate set of servers — the TCP/IP and VSWITCH controller servers defined for your installation.

Note - Server Shutdown Considerations

Before you shutdown any TCP/IP or VSWITCH controller servers, ensure that applicable conditions or guidelines for your installation have been followed. The shutdown of such servers can impact TCP/IP connectivity for:

- traditional CMS users and applications
- remote users and applications
- virtual machines (including Linux guests) that rely upon CP virtual switch connectivity support.

The TCPMSMGR command is used in the next step to manage the shutdown (and later, the re-initialization) of the TCP/IP protocol *stack* servers and VSWITCH controller virtual machines that are used by your installation.

If other procedures are required by your installation for such operations, use those procedures instead of the TCPMSMGR command.

For additional information about shutting down TCP/IP servers, see the section that discusses “Starting and Stopping TCP/IP Servers” in the chapter titled “General TCP/IP Server Configuration,” of *TCP/IP Planning and Customization*.

For more information about the TCPMSMGR command, and its operands and capabilities, see Appendix A, “TCP/IP Utilities” on page 57.

Verifying Your Environment

When you perform this step, it is suggested that you first invoke TCPMSMGR as illustrated, but with the **TEST** option also specified. This will help verify that certain command authorization requirements have been met, and that the appropriate set of servers will be affected by TCPMSMGR command operations.

With the **TEST** option in effect, **no servers are shutdown**.

Resolve any reported problems, then invoke TCPMSMGR (without the TEST option) as illustrated.

tcpmsmgr stop stack vswitch

where the **stack** and **vswitch** operands signify that respective shutdown operations are to be performed for TCP/IP protocol *stack* servers and VSWITCH controller virtual machines.

Notes:

a. If servers in either of the listed **stack** or **vswitch** groups need to remain operational at this time, **do not continue with this procedure**, because write access to minidisks associated with any operational severs will not be possible.

b. For most TCP/IP configurations, the shutdown of a TCP/IP protocol *stack* server causes similar actions to be performed for subordinate protocol servers (such as an FTP server). However, there are instances when a subordinate protocol server might need to be stopped through some overt action.

At this time, stop any such servers used by your installation to which such considerations apply.

6 Detach previously acquired TCP/IP minidisks.

vmfsetup detach

This step is necessary to allow the various TCP/IP server minidisks to be acquired with Read/Write status, in the next step.

7 Re-establish access to required TCP/IP minidisks, in R/W mode.

vmfsetup servp2p {tcpipp2p | tcpipsfsp2p}

Use **tcpipp2p** if the TCP/IP for z/VM default minidisk environment has been maintained; use **tcpipsfsp2p** if the service minidisks were moved to Shared File System directories.

8 Copy the serviced TCP/IP server profile into production using the PRODUTL command. The command cited below processes files that are listed in the TCPSVMCMS section of the 6VMTCP40 CATALOG file. See Appendix A, "TCP/IP Utilities" on page 57 for information about this command and TCP/IP for z/VM catalog files.

Verifying Your Environment

When you perform this step, it is suggested that you first invoke PRODUTL as illustrated, but with the **TEST** option also specified. This will verify that all resources can be accessed and that the appropriate files will be processed.

With the **TEST** option in effect, **no files are copied into production**.

Resolve any reported problems, then invoke PRODUTL (without the TEST option) as illustrated.

produtl servp2p {tcpipp2p | tcpipsfsp2p} 6vmtcp40 *ctlg_section*

Use **tcpipp2p** if the TCP/IP for z/VM default minidisk environment has been maintained; use **tcpipsfsp2p** if the service minidisks were moved to Shared File System directories.

If the **TCPROFIL EXEC** file has been serviced, specify *ctlg_section* as **tcpsvmcms**.

9 Review the PRODUTL message log (PRODUTL $MSGLOG). If necessary, correct any problems before you proceed with the next step.

vmfview produtl

10 Detach previously acquired TCP/IP minidisks.

vmfsetup detach

This step is necessary to allow the various TCP/IP servers to obtain their respective A-disks with Read/Write status, when they are re-initialized in step 12.

11 Acquire the TCP/IP minidisks necessary to run the TCPMSMGR command.

link 6vmtcp40 491 491 rr
link 6vmtcp40 492 492 rr

access 491 *fm1*
access 492 *fm2*

where *fm1* and *fm2* are available file modes.

12 (Re)Initialize TCP/IP and VSWITCH controller servers.

Note - TCP/IP and VSWITCH Controller Startup Considerations

Before you initialize any TCP/IP or VSWITCH controller servers, ensure that applicable conditions or guidelines for your installation have been followed. The shutdown of such servers can impact TCP/IP connectivity for:

- traditional CMS users and applications
- remote users and applications
- virtual machines (including Linux guests) that rely upon CP virtual switch connectivity support.

The TCPMSMGR command is used in the next step to manage the (re)initialization of the TCP/IP protocol *stack* servers and VSWITCH controller virtual machines that are used by your installation.

If other procedures are required by your installation for such operations, use those procedures instead of the TCPMSMGR command.

For additional information about starting up TCP/IP servers, see the section that discusses “Starting and Stopping TCP/IP Servers” in the chapter titled “General TCP/IP Server Configuration,” of *TCP/IP Planning and Customization*.

For more information about the TCPMSMGR command, and its operands and capabilities, see Appendix A, “TCP/IP Utilities” on page 57.

Verifying Your Environment

When you perform this step, it is suggested that you first invoke TCPMSMGR as illustrated, but with the **TEST** option also specified. This will help verify that certain command authorization requirements have been met, and that the appropriate set of servers will be affected by TCPMSMGR command operations.

With the **TEST** option in effect, **no servers are initialized**.

Resolve any reported problems, then invoke TCPMSMGR (without the TEST option) as illustrated.

tcpmsmgr start stack vswitch

where the **stack** and **vswitch** operands signify that respective startup operations are to be performed for TCP/IP protocol *stack* servers and VSWITCH controller virtual machines.

Note: For most TCP/IP configurations, the initialization of a TCP/IP protocol *stack* server causes similar actions to be performed for subordinate protocol servers (such as an FTP server). However, there are instances when a subordinate protocol server might need to be started through some overt action.

At this time, start any such servers used by your installation to which such considerations apply.

13 Log off the **MAINT640** user ID, after server initialization operations are complete.

Notices

This information was developed for products and services offered in the U.S.A. IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

```
IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.
```

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

```
Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan
```

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes to the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

© Copyright IBM Corp. 1990, 2016

IBM Corporation
TCP/IP for VM Development
Dept. G79G
1701 North Street
Endicott, NY 13760

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities on non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to IBM programming interfaces. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Sample programs are provided “AS IS,” without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Privacy Policy Consideration

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If the Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see the IBM Online Privacy Policy at http://www.ibm.com/privacy and the IBM Online Privacy Statement at http://www.ibm.com/privacy/details, in particular the section entitled “Cookies, Web Beacons and Other Technologies,” and the IBM Software Products and Software-as-a-Service Privacy Statement at http://www.ibm.com/software/info/product-privacy.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at IBM copyright and trademark information - United States:

www.ibm.com/legal/us/en/copytrade.shtml

Reader's Comments

TCP/IP for z/VM level 640

You can use this form to comment about this document, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes is appropriate, without incurring any obligation to you. If you prefer to provide feedback electronically, please use the appropriate "Contact z/VM" form that is provided as part of the z/VM home page on the World Wide Web. The URL for this page is:

`www.vm.ibm.com`

For each of the topics below please indicate your satisfaction level by circling your choice from the rating scale. If a statement does not apply, please circle N.

RATING SCALE

very satisfied	←			very dissatisfied	not applicable
1	2	3	4	5	N

	Satisfaction					
Ease of product installation	1	2	3	4	5	N
Time required to install the product	1	2	3	4	5	N
Contents of program directory	1	2	3	4	5	N
Readability and organization of program directory tasks	1	2	3	4	5	N
Necessity of all installation tasks	1	2	3	4	5	N
Accuracy of the definition of the installation tasks	1	2	3	4	5	N
Technical level of the installation tasks	1	2	3	4	5	N
Installation verification procedure	1	2	3	4	5	N
Ease of customizing the product	1	2	3	4	5	N
Ease of migrating the product from a previous release	1	2	3	4	5	N
Ease of putting the system into production after installation	1	2	3	4	5	N
Ease of installing service	1	2	3	4	5	N

- Did you order this product as an independent product or as part of a package?
  - □ Independent
  - □ Package

    What type of package was ordered?

    - □ CustomPac
    - □ System Delivery Offering (SDO)
    - □ Other - Please specify type: _____

© Copyright IBM Corp. 1990, 2016

- Is this the first time your organization has installed this product?
  - □ Yes
  - □ No
- Were the people who did the installation experienced with the installation of VM products using VMSES/E?
  - □ Yes

    How many years of experience do they have? _____
  - □ No
- How long did it take to install this product? _____
- If you have any comments to make about your ratings above, or any other aspect of the product installation, please list them below:

  _____

  _____

  _____

  _____

  _____

  _____

  _____

  _____

Please provide the following contact information:

_____

Name and Job Title

_____

Organization

_____

_____

Address

_____

Telephone

Thank you for your participation.

Please send the completed form to the following address, or give to your IBM representative who will forward it to the TCP/IP for z/VM Development group:

IBM Corporation
TCP/IP for VM Development
Dept. G37G
1701 North Street
Endicott, NY 13760

Program Number: 5741-A07

Printed in USA

GI13-3474-00