

Z/VM One Touch — VMOT Installation and Administration **Guide and Reference**



Table of Contents

Guide and Reference.....	1
Table of Contents.....	2
Introduction.....	4
Installation Overview.....	4
Configuration.....	4
Software Installation.....	4
Enablement.....	4
Administration Overview.....	4
IP Address administration. Prerequisites.....	4
Prerequisites.....	5
Software.....	5
DASD Space.....	5
Installation.....	6
DownLoading.....	6
FTP to a VM userid.....	6
Command sequence.....	6
Configuration.....	9
DASD Space and Group.....	9
Factors affecting space requirements.....	9
DASD Group.....	9
Sample Directory entries and VM:Secure statements.....	9
Software Installation.....	10
Optional installation of VMARC.....	10
Prepare MAINT 1111 and unpack archive.....	10
Run installation exec, LXINS.....	10
Installation example.....	11
Removal.....	12
Multiple Installations.....	12
TCP/IP VM configuration files.....	13
Secondary TCP/IP VM.....	13
Enabling TCP/IP VM configuration changes.....	13
Autologging at VM IPL.....	14
Groups and Major Groups.....	15
Rules and Definitions.....	15
Userid and Major Group Administration.....	15
VLMADMIN — the Initial Userid.....	15
Reaching the Userid, Group and Major Group Administration Panel.....	16
Administration Authority Levels — Full and Major Group.....	16
Major Group Administration.....	17
Userid Administration.....	17
Co-ordination Requirements.....	19
Co-ordination with TCP/IP VM Administrator.....	19
Co-ordination with LAN Administrator and VM System Programmer.....	19
Reaching the Manage IP Addresses Administration Panel.....	19
IP Range Selection.....	20

Reconfiguring TCP/IP VM.....	20
; Generated on dd Mmm yyyy at hh:mm:ss	21
Color Scheme.....	23
IP Address property descriptions	23
Changing IP Address Properties	27
Index	28

Introduction

This manual describes the prerequisites and tasks required to install and administer **Z/VM One Touch**; generally known as **VMOT**, the term that will be used in this and other product publications.

Usage of **VMOT** is discussed in the *User Guide and Reference*.

Installation Overview

Installation consists of downloading, configuration, software installation and enablement.

Configuration

Configuration includes:

- DASD space planning
- Setting pools in the directory to accommodate the required space.

Software Installation

The **VMOT** software installation consists of:

1. downloading the software files
2. optional installation of VMARC
3. unpacking the archive files
4. running the installation exec, **LXINS**.

Enablement

For PPP connections via IUCV or Virtual CTCs to TCP/IP VM, a TCP/IP VM service machine, either the primary TCP/IP or a secondary, needs to be enabled to communicate with the IP address pool set up for the Linux machines managed by **VMOT**.

Direct connections via real CTCs or dedicated adapters such as CLAW and OSA require configuration of these devices.

The **VMOT** server needs to be started.

Administration Overview

Administration consists of:

- Userid, Major Group and Group administration

IP Address administration.

Prerequisites

Software

These are the earliest software levels **VMOT** has run on. All later releases will operate correctly with **VMOT**.

- VM/ESA V2R4.0 and later
- TCP/IP FL320
 - TCPIP must be running during software installation
 - FTPSERVE must also be active
 - MAINT should be in OBEYFILE
 - Add PROXYARP to the TCP/IP configuration unless the Linux IP addresses are to be sub-netted.
- Either VM:Secure or DIRMAINT V1R5.0 must be running during software installation
 - DASD Group LINUX on 3390 defined in DIRMAINT's EXTENT CONTROL file with sufficient space to accommodate VMOT files and Linux images.
- CMS Utilities Feature
- CMS Shared File System on MAINT 0193
- VMARC MODULE — VM Archive

DASD Space

All space is specified in 3390 DASD Cylinders¹. The space required for MAINT and other userids are shown in the following table. The **xx** preceding most of the userids stands for the **VMOT** prefix, default **LX**. You may change the amount of space to suit your installation.

Userid	Quantity in 3390 cylinders	Remarks
MAINT	50	Installation files defined on 1111 or another address during installation
xxSFS LXSFS	5233	SFS FILEPOOL
xxMAINT LXMAINT	30	VMOT Files
xxMASTER LXMASTER	30	Common 0191 for several USERids
	5343	VMOT Subtotal
xxMASTER LXMASTER	3500	Master copy of Linux Images. Depending on the packages you decide to install, the size of Linux images can vary

¹ A 3390 cylinder holds 720 Kb. when formatted in 4096 byte blocks, the usual block size used by both VM/CMS and Linux.

Userid	Quantity in 3390 cylinders	Remarks
		enormously. Read/Write images will require individual space for every Linux image created. Read-Only images can be shared at a very considerable saving of space.
	8400	VMOT + Images

Installation

Installation consists of configuration, software installation and enablement, once the VMOT archive file has been downloaded.

DownLoading

The following example shows how to FTP the VMOT files to a VM userid. You may also use a PC as an intermediate host, especially if you need to get around a firewall, but you will eventually have to get the files to a VM userid. For instructions on using a PC as an intermediate host, see the *Linux for S/390* redbook, SG24-4987 at: <http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg244987.html?Open>

FTP to a VM userid

Command sequence

The prompts are shown in **boldface**; commands and responses are shown in fixed pitch; comments are shown in this font after an em dash —.

VMLINK TCPMAINT 0592 — for access to TCP/IP commands, i.e. ftp
ftp VMOT. Download. IP. Address.

USER (identify yourself to the host):

ftpuser — or other userid specified by VMOT support

331 Send password please.

Password:

ftpuser — or other password specified by VMOT support

Command:

binary fixed 80

Command:

get lx.vma lx.vma

Command:

get read.me read.me

Command: — if vmarc module is not available on your system

get vmarc.dmp vmarc.dmp

Command:
qui t

Command sequence example with all responses

Please note that the IP address, FTP userid and password specified by VMOT support will likely be different from those used in this example.

```
VMLINK TCPMAINT 0592
ftp 24.100.203.157
VM TCP/IP FTP Level 320
Connecting to 24.100.203.157, port 21
220-FTPSERVE IBM VM Level 320 at vmrvm1.P/390.com...,
220 Connection will close if idle for more than 5 minutes.
USER (identify yourself to the host):
ftpuser
>>>USER ftpuser
331 Send password please.
Password:
ftpuser
>>>PASS *****
230-FTPUSER logged in; working directory = FTPUSER 191
(ReadOnly)
230 write access currently unavailable
Command:
binary fixed 80
>>>TYPE i
200 Representation type is IMAGE.
Command:
get lx.vma lx.vma
>>>PORT xxx,xxx,xxx,xxx,xxx,xxx
200 Port request OK.
>>>RETR lx.vma
150 Sending file 'lx.vma'
286080 bytes transferred.
588480 bytes transferred.
821760 bytes transferred.
1078640 bytes transferred.
250 Transfer completed successfully.
1162800 bytes transferred in 43.642 seconds. Transfer rate
26.64 Kbytes/sec.
Command:
get read.me read.me
>>>PORT xxx,xxx,xxx,xxx,xxx,xxx
200 Port request OK.
>>>RETR read.me
150 Sending file 'read.me'
250 Transfer completed successfully.
11600 bytes transferred in 0.580 seconds. Transfer rate
20.00 Kbytes/sec.
Command:
```

VMOT Installation and Administration Guide

```
qui t  
>>>QUI T  
221 Qui t command recei ved. Goodbye.
```

Configuration

DASD Space and Group

Configuration includes ensuring sufficient DASD space as specified in on page 5.

Factors affecting space requirements

DASD space requirements will depend on how many separate Linux images you choose to support and whether the individual Linux machines/userids defined to VM use a shared or unshared copy of a Linux kernel.

Depending on the packages you decide to install, the size of Linux images can vary enormously. Read/Write images will require individual space for every Linux image created. Read-Only images can be shared at a very considerable saving of space.

VMOT log files are maintained in a Shared File System, SFS, filepool. The log activity and how often you purge the logs directly affect your space usage in this filepool.

DASD Group

You also need to add a **LINUX** DASD group in DIRMAINT's EXTENT CONTROL file.

Sample Directory entries and VM:Secure statements

After expanding the archive files on MAINT 1111, you can review the DASD allocations in the sample directory files. These files can be modified to suit your installation's requirements. If you do, we recommend keeping a copy of the original files for later diagnosis or restoration if you encounter problems.

Note that you should use `CASE M` if you modify any of these files with XEDIT.

XXJOB-XX	SAMPLE	Batch Job
XXMASTER	SAMPLE	Container for Linux Masters
XXMAINT	SAMPLE	Maintenance USERid for VMOT
XXPROF	SAMPLE	Profile for several CP DIRECTORY Entries
XXSCHED	SAMPLE	Batch Job Scheduler
XXSFS	SAMPLE	CMS SFS FILEPOOL Server
XXSYSLOG	SAMPLE	Log Recorder
XXTCPIP	SAMPLE	Sample for TCPIP/VM
XXO	SAMPLE	HTTP Server

Software Installation

The **VMOT** software installation consists of unpacking the archive files with **VMARC** and running the installation exec, **LXINS**.

Optional installation of VMARC

To install VMARC:

1. Locate the VMARC DMP file received from an FTP site.
2. `cp spool punch *`
3. `punch vmarc dmp (noh — with response similar to:`

```
RDR FILE ssss SENT FROM uuuuuuuu PUN WAS ssss RECS  
rrrr CPY 001 A NOHOLD NOKEEP
```

1. `receive ssss = = fm — with response similar to:`

```
DMSDSK1079R Receive VMARC MODULE fm as VMARC MODULE fm?  
DMSDSK1079R Reply 0 (NO), 1 (YES), 2 (QUIT), or 3 (RENAME)
```

1. 1 for Yes to obtain:

```
VMARC MODULE fm created from VMARC MODULE fm
```

```
File VMARC MODULE fm received from uuuuuuuu at nnnnnnnn sent as  
VMARC MODULE fm
```

Prepare MAINT 1111 and unpack archive

1. Add DASD Group LINUX for 3390 to DIRMAINT's EXTENT CONTROL file if not already done
2. LOGON to MAINT
3. Depending on your Directory Maintenance product, either:
 - `DIRMAINT AMDISK 1111 3390 AUTOG 0050 LINUX M` and wait for messages from DIRMAINT stating that the AMDISK request is successfully completed.
 - `VMSECURE ADDMDISK MAINT 1111 LINUX 0050 3390 * * M (NOFORMAT`
4. `CP LINK * 1111 1111 M`
5. `FORMAT 1111 L`
 - Reply with "Yes"
 - You may specify a volume label, say **LXMNT**
 - Press ENTER and wait for `FORMAT` to complete.
6. `COPY LX VMA A = = L` to keep this file with other **VMOT** installation files.
7. `VMARC UNPACK LX VMA L = = L`
8. `VMARC UNPACK M VMA L = = L`

Run installation exec, LXINS

Note: **LXINS** automatically spools its virtual console to MAINT's virtual reader for later reference.

If not specified, the default prefix, **LX**, will be used as the first two characters of the VM userids created by the installation exec. If this prefix conflicts with similarly named userids, the installation exec will notify you that the prefix is already in use and will halt. In this case, you will need to try a different prefix until you find one that does not conflict. To specify a different prefix, type: **LXINS prefix**, where **prefix** is any two characters acceptable in a VM userid.

After **LXINS** determines that there are no conflicts with the prefix, it will ask for the HTTP port VMOT will use for the web interface. **LXINS** will then perform the installation process without further need for intervention.

Installation example

The **LXINS** command does not show because **CP SP CON *** (**STA** is issued after the **LXINS** command is issued).

```

22: 45: 46
22: 45: 46 Step 1.  Checking the CP DIRECTory for conflicts...
22: 46: 00
22: 46: 00 Step 2.  Checking DIRMAINT for DASD Group "LINUX"...
22: 47: 39
22: 47: 39 Step 3.  What HTTP Port would you like to use for the Client
Interface?
50
22: 48: 44
22: 48: 44 Step 4.  Creating Service Virtual Machines...
22: 48: 44
22: 48: 44 ADDing LXPROF to the CP DIRECTory...
22: 49: 39 ADDing LXMAINT to the CP DIRECTory...
22: 50: 34 ADDing LXMASTER to the CP DIRECTory...
22: 51: 36 ADDing LXSFS to the CP DIRECTory...
22: 53: 39 Generating FILEPOOL LXSFS:... (go get a coffee)
22: 58: 39 Still waiting for FILEPOOL LXSFS:...
23: 08: 41 Still waiting for FILEPOOL LXSFS:...
23: 18: 43 Still waiting for FILEPOOL LXSFS:...
23: 22: 56 ADDing LX0 to the CP DIRECTory...
23: 23: 19 ADDing LX1 to the CP DIRECTory...
23: 23: 56 ADDing LX2 to the CP DIRECTory...
23: 24: 32 ADDing LX3 to the CP DIRECTory...
23: 25: 08 ADDing LX4 to the CP DIRECTory...
23: 25: 45 ADDing LX5 to the CP DIRECTory...
23: 26: 21 ADDing LX6 to the CP DIRECTory...
23: 26: 57 ADDing LX7 to the CP DIRECTory...
23: 27: 34 ADDing LX8 to the CP DIRECTory...
23: 28: 11 ADDing LX9 to the CP DIRECTory...
23: 28: 48 ADDing LXSCHED to the CP DIRECTory...
23: 29: 11 ADDing LXSYSLOG to the CP DIRECTory...
23: 29: 34 ADDing LXJOB-01 to the CP DIRECTory...
23: 29: 57 ADDing LXJOB-02 to the CP DIRECTory...
23: 30: 21 ADDing LXJOB-03 to the CP DIRECTory...
23: 30: 44 ADDing LXJOB-04 to the CP DIRECTory...
23: 31: 07 ADDing LXJOB-05 to the CP DIRECTory...
23: 31: 30 ADDing LXJOB-06 to the CP DIRECTory...
23: 31: 53 ADDing LXJOB-07 to the CP DIRECTory...
23: 32: 16 ADDing LXJOB-08 to the CP DIRECTory...
23: 32: 41 ADDing LXJOB-09 to the CP DIRECTory...
23: 33: 08 ADDing LXJOB-10 to the CP DIRECTory...
23: 33: 31 ADDing LXJOB-11 to the CP DIRECTory...
23: 33: 54 ADDing LXJOB-12 to the CP DIRECTory...
23: 34: 17 ADDing LXJOB-13 to the CP DIRECTory...

```

VMOT Installation and Administration Guide

```
23: 34: 40 ADDi ng LXJOB-14 to the CP DIRECTory...
23: 35: 03 ADDi ng LXJOB-15 to the CP DIRECTory...
23: 35: 26 ADDi ng LXJOB-16 to the CP DIRECTory...
23: 35: 48 ADDi ng LXJOB-17 to the CP DIRECTory...
23: 36: 11 ADDi ng LXJOB-18 to the CP DIRECTory...
23: 36: 34 ADDi ng LXJOB-19 to the CP DIRECTory...
23: 36: 57 ADDi ng LXJOB-20 to the CP DIRECTory...
23: 37: 20
23: 37: 20 Step 5.  Installing Source Code...
23: 38: 44
23: 38: 44 Step 6.  Installing Data Files...
23: 38: 44
23: 38: 44 Step 7.  Installing Help Information...
23: 38: 51
23: 38: 51 Step 8.  GENERating VMRHTTP MODULE Z1...
23: 38: 55 GENMOD VMRHTTP, rc: 0
DMSCPY721I Copy VMRHTTP MODULE A1 to VMRHTTP MODULE Z1 (old file)
DMSCPY721I Copy VMRHTTP LOADMAP A5 to VMRHTTP LOADMAP Z5 (old file)
23: 38: 56
23: 38: 56 Step 9.  Starting the HTTP Engine...
AUTO LOGON   ***           LX0           USERS = 14
23: 38: 56
23: 38: 56 Installation completed successfully!
23: 38: 56
```

Removal

To remove **VMOT**, enter **LXINS prefix (REMOVE**

The prefix does not have to be specified if it was the default, **LX**.

LXINS may detect conflicts after removal until all DIRMAINT operations have completed. If this happens, wait a few more minutes and try again.

Multiple Installations

By using different prefixes, multiple VMOTs may be installed. Each will require a different HTTP port.

Enablement

A TCP/IP VM service machine, either the primary TCP/IP or a secondary, needs changes to its configuration files to enable communications via virtual CTC or IUCV connections with the IP addresses set up for the Linux machines managed by **VMOT** — and the **VMOT** server needs to be running.

VMOT can generate TCP/IP VM configuration statements for newly added IP Addresses using Virtual CTC or IUCV.

TCP/IP VM configuration files

Sample TCP/IP VM configuration files are created by **LXINS** in the **xxSFS:xx.PROD.DATA** (default **LXSFS:LX.PROD.DATA**) directory which is accessible to **xxMAINT** (default **LXMAINT**).

- TCPIP OBEY
- TCPIP DEVICE
- TCPIP HOME
- TCPIP GATE
- TCPIP START

Configuration files for Virtual CTC and IUCV may be generated directly from **VMOT** in IP Address Range Administration. See Reconfiguring TCP/IP VM on page 20 for information on doing this.

Secondary TCP/IP VM

Instead of modifying your primary TCP/IP VM, you may choose to define a secondary TCP/IP VM to connect to the Linux images. You will need to configure the secondary and primary TCP/IP VMs to connect to each other. This process is analogous to the TCP/IP definitions required to have a Linux image connect to TCP/IP and is discussed in Chapter 6. Linux for S/390 connectivity to VM, OS/390, VSE in the Linux for S/390 Redbook, SG24-4987:

<http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg244987.html?Open>

Enabling TCP/IP VM configuration changes

You may either:

- restart your TCP/IP VM with:
 - CP FORCE TCPI P
 - CP XAUTOLOG TCPI P SYNCH

or use the OBEYFILE command to enable these parameters. To make OBEYFILE changes permanent, you need to integrate these files in your TCP/IP configuration and schedule a TCP/IP restart at a convenient time for your installation.

Startup

1. CP XAUTOLOG **xx0** SYNCH where xx is the prefix you selected. LXINS automatically starts this userid when installation has been completed.
2. In Netscape or Internet Explorer, specify your Home IP Address with Port 50 (or the port specified in step 3 of **LXINS EXEC**²) to obtain the **VMOT LOGON** Window.

Examples:

- o <http://xxx.xxx.xxx.xxx:httpPort>
- o <http://24.43.137.81:50>

1. LOGON the Administrator with Userid and Password both: **vladmin**

1. For security, we recommend you immediately change the LOGON Password for VLMADMIN or anybody who knows your IP Address can gain **VMOT** Administrator privileges. See on page 17 for instructions on how to do this.

Autologging at VM IPL

Add "CP XAUTOLOG **xx0** SYNCH" to the PROFILE EXEC of AUTOLOG1. See the READ ME file for sample Rexx code to autolog the SFS server first, test results and then autolog the web server that can be added to AUTOLOG1 or AUTOLOG2 depending on whether DIRMAINT or VM:Secure is used.

² What HTTP Port would you like to use for the Client Interface?
httpPort

Administration

VMOT administration consists of:

- Userid, Major Group and Group administration. VMOT userids are independent of userids on your VM system.
- IP Address Administration.

Groups and Major Groups

Groups and Major Groups are used to organise Linux Images in a hierarchy that can simplify management of large numbers of Linux Images. For example, a college can set up a Major Group for a semester of a single course and have each student able to set up images in his default group. Students wanting to share images for a project can be enrolled in a project group where each student in the group can control that group's images. Students outside the project group or the course Major Group have no access to that project's images.

At the end of the term, all the Major Group's Linux images can be deleted with one command by the Major Group administrator, normally the instructor.

Alternatively, each department can have its own Major Group and Groups can be set up for each course, section and term.

Rules and Definitions

- Major Groups are collections of Groups.
- The same Group name may be used in more than one Major Group.
- Every Linux Image belongs to a single Major Group.Group combination.
- Each Userid belongs to one Major Group and is assigned its Default Group (the same identifier as the userid) and any number of other groups assigned by the Major Group Administrator.
- A Userid may create, view and control Linux Images belonging to his Major Group and one of his authorised Groups.
- Group and Major Group identifiers may be a maximum of 16 characters. Valid characters are A-Z, a-z, 0-9, @, #, \$, _ (underscore). Lowercase letters are converted to uppercase.

Userid and Major Group Administration

Userids and Major Groups are managed in the **Manage USERids and Groups** panel.

This panel is offered to userids with either Full or Major Group Administration Authority. Major Group Administrators are restricted to operations within their Major Group.

VLMADMIN — the Initial Userid

After installation, there is only one userid, VLMADMIN, with password: VLMADMIN. Since this password is commonly known, you should logon to VLMADMIN and change its password to something you can remember immediately after installation.

Alternatively you can create another userid with Full Authority and delete the VLMADMIN userid, preferably after verifying that you can logon to it.

Recovery of Administration Capability

If you delete all userids with Administration Authority, you will not be able to carry out Administration Functions. To retrieve this authority, you will need to create a new VLMADMIN USER file in the **datadir** directory shown in the CONFIG SETTINGS file.

Procedure

1. Logon to the VM userid, xxMAINT - where xx is the prefix you used to install **VMOT**
2. Xedit VLMADMIN USER **datadir**
3. Add a line containing: VLMADMIN VLMADMIN ADMINISTRATOR L
4. FILE to save changes.

Reaching the Userid, Group and Major Group Administration Panel

Once logged on to a userid with Administration authority, click on the hyperlink: [Manage USERids and Groups](#) which follows the list of hyperlinks to standard user functions.

The Administration option lines appear after the standard user functions when the userid has administration authority. You will then be shown the selected Administration panel which consists of a number of subpanels which are discussed in sequence. Scroll down to see the various subpanels.



After any Administration function in this panel has been requested, this panel will reappear with a message giving the results of the last attempted function. In the case of certain failures, one or more return codes will be shown which should be communicated to **VMOT** support. If you are familiar with CMS you may examine LINUX CGI from xxMAINT and attempt diagnosis on your own.

Administration Authority Levels — Full and Major Group

Full Authority allows administration of Major Groups and any userid.

Major Group Authority allows administration of userids within the Major Group.

Major Group Administration

Major Group functions are offered to userids with Full Authority. These users may Create, Delete and Reassign Major Groups.

To Create a Major Group, enter the new Major Group name and click the **Add New Major Group** button.

To Delete a Major Group, select the Major Group from the pull-down list and click the **Delete Major Group** button. Before deletion, the Major Group must have all userids and images either deleted or reassigned.

To Reassign a Major Group, select the from and to Major Groups and click on Reassign Major Group. All Userids and Linux Images will be reassigned. If the same Major Group is selected in both boxes, no reassignment will be done.

Userid Administration

Userids may be Created, Changed, Deleted, Disabled, Reenabled, and Enrolled or Removed from Groups.

Creation

Fill in the Userid and Password boxes and click the **Add New Userid** button.

Full Authority users may also select the Major Group and Administration Authority; Major Group Authority users are not shown these options.

The screenshot shows a dark blue interface with yellow text. At the top, the title "USERid Change, Delete, Enable, Disable, Groups" is displayed in yellow. Below the title, there are several form fields and buttons:

- Major Group and USERid:** A dropdown menu showing "ADMINISTRATOR.LOST".
- New Password:** An empty text input field.
- New Major Group:** A dropdown menu showing "(no change)".
- New Administrative Authority:** A dropdown menu showing "(no change)".
- Action Buttons:** Four buttons arranged in a 2x2 grid: "Change USERid", "Enable USERid", "Delete USERid", and "Disable USERid".
- Group:** An empty text input field.
- Group Management Buttons:** Two buttons stacked vertically: "Add Group to USERid" and "Delete Group from USERid".

Change

Select the Userid; Full Authority users will see all userids prefaced with Major Group. Major Group Authority users may only change the password. Full Authority users may also change Major Group and Administration Authority.

Delete, Disable and Enable

Select the userid and click the appropriate action button. Disabled userids remain in the system, but they are not available for logon until enabled. A userid may be deleted only after all its images are deleted.

Add Group

Select a userid, enter a Group Name and click **Add Group to Userid**.

Delete Group

Select a userid, enter a Group Name and click Delete Group from Userid.

IP Address Administration

IP Addresses used by Linux Images created by **VMOT** are managed in the Manage IP Addresses Administration panel. This panel is offered to userids with either Full or Major Group Administration Authority.

Co-ordination Requirements

IP Addresses must be co-ordinated with network administrators. IP Addresses that use real devices must also be co-ordinated with the VM System Programmer.

Co-ordination with TCP/IP VM Administrator

IP Addresses that connect to **TCP/IP VM** must have their parameters co-ordinated with the TCP/IP VM Administrator. These IP Addresses use either Virtual CTC (CTC) or Inter-User Communication Vehicle (IUCV) Connection Types.

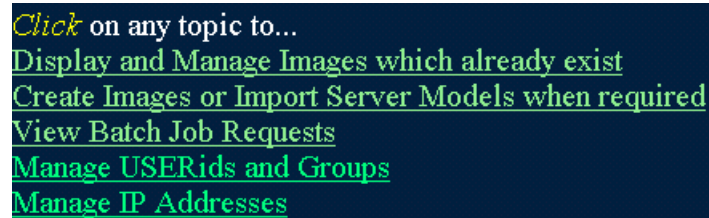
TCP/IP VM configuration statements can be generated by **VMOT** and sent directly to TCPMAINT's or other userid's virtual reader for use by the TCP/IP VM Administrator.

Co-ordination with LAN Administrator and VM System Programmer

IP Addresses that connect directly to the network via real CTCs, OSA or CLAW devices need to be co-ordinated with both parties.

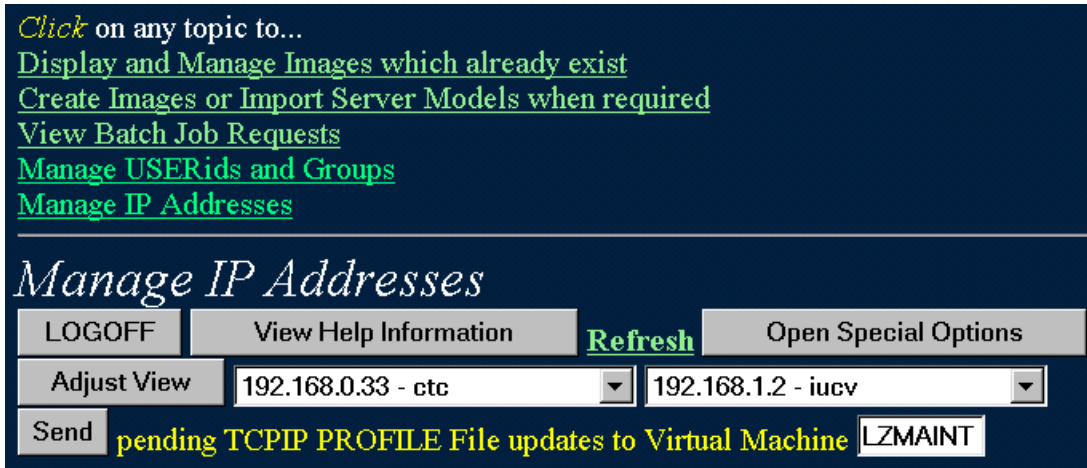
Reaching the Manage IP Addresses Administration Panel

Once logged on to a userid with Administration authority, click on the hyperlink: [Manage IP Addresses](#) which follows the list of hyperlinks to standard user functions.



Click on any topic to...
[Display and Manage Images which already exist](#)
[Create Images or Import Server Models when required](#)
[View Batch Job Requests](#)
[Manage USERids and Groups](#)
[Manage IP Addresses](#)

Links to Administration panels appear after the standard user functions when the userid has administration authority. You will then be shown the Manage IP Addresses Administration panel which consists of a number of subpanels which are discussed in sequence. Scroll down to see the various subpanels.



Note: When selecting this panel the first time after installation, you will be taken directly to Add IP Addresses.

After any IP Address Administration function has been requested, this panel will reappear with a message giving the results of the last attempted function. In the case of certain failures, one or more return codes will be shown which should be communicated to **VMOT** support. If you are familiar with CMS you may examine LINUX CGI from xxMAINT and attempt diagnosis on your own.

IP Range Selection

The IP Address pull-downs following the **Adjust View** button select the **first** and **last** IP Addresses the buttons in this subpanel will affect. Only IP Addresses within the selected Major Group will be operated upon.

Reconfiguring TCP/IP VM

Clicking on the **Send** button produces TCP/IP VM configuration statements for any Virtual CTC and IUCV connection types within the selection range that are shown in red and punches these statements to the virtual reader of the selected VM userid (typically xxMAINT where xx is the **VMOT** prefix). A separate TCPIP file is punched for each TCP/IP VM userid found.

The sample generated files follow.

Note that these files are divided in **three** sections. **Each section should be placed in the corresponding section of the existing TCPIP configuration file.** Your TCP/IP VM administrator should be familiar with this task.

To make these configuratons effective, TCP/IP generally should be restarted. Your TCP/IP VM Administrator may also copy these definitions to an OBEY file and update TCP/IP VM dynamically.

Sample TCPIP NEW File

```

; Generated on dd Mmm yyyy at hh:mm:ss
;
; =====
;
; New PROFILE TCPIP records for the "TCPIP" Service Virtual Machine
;
; Insert these new Device and Links in an appropriate location...
Device CTC-cccc CTC cccc
Link CTC-cccc CTC 1 CTC-cccc
Device IUCV2 iiiiii 0 0 iiiiii A
Link IUCV2 iiiiii 0 iiiiii
;
; Include the following in the current "Home" Addresses...
hhh.hhh.hhh.hhh CTC-cccc
hhh.hhh.hhh.hhh iiiiii
;
; Include the following in the current "GateWays"...
ggg.ggg.ggg.ggg = CTC-cccc 1492 Host
ggg.ggg.ggg.ggg = iiiiii 1492 Host
;
; Include the following in the "Start" Commands...
Start CTC-cccc
Start iiiiii
;
; =====
;
; New records for the "TCPIP" Service Virtual Machine in the CP DIRECTory
;
; Add these SPECIALs to USER TCPIP...
SPECIAL cccc CTCA

SPECIAL cccc CTCA

```

IP Address Range display

The IP Addresses are displayed according to the last selection made.

A sample listing follows:

<u>Address</u>	<u>Image Name</u>	<u>Connection Device</u>	<u>Gateway Name</u>	<u>Peer Address</u>	<u>MTU</u>	<u>Subnet Mask</u>	<u>DNS Addr</u>
<u>192.168.0.33</u>	<i>(none)</i>	ctc - B890	TCPIP	192.168.0.3	1492	255.255.255.0	0.0.0
<u>192.168.0.34</u>	<i>(none)</i>	ctc - B892	TCPIP	192.168.0.3	1492	255.255.255.0	0.0.0
<u>192.168.0.35</u>	<i>(none)</i>	ctc - B894	TCPIP	192.168.0.3	1492	255.255.255.0	0.0.0
<u>192.168.0.36</u>	<i>(none)</i>	ctc - B896	TCPIP	192.168.0.3	1492	255.255.255.0	0.0.0
192.168.0.211	SUSE-211	ctc - 2500	TCPIP	192.168.0.3	1492	255.255.255.0	209.
192.168.0.212	SUSE-212	ctc - 2502	TCPIP	192.168.0.3	1492	255.255.255.0	209.
192.168.0.213	SUSE-213	ctc - 2504	TCPIP	192.168.0.3	1492	255.255.255.0	209.
<u>192.168.0.214</u>	IUCV-214	iucv	TCPIP	192.168.0.3	3942	255.255.255.240	209.
<u>192.168.0.215</u>	IUCV-215	iucv	TCPIP	192.168.0.3	3942	255.255.255.240	209.

Depending on the resolution of your monitor, you may need to scroll horizontally and vertically to see all the parameters, viz:

Image Name	Connection Device	Gateway Name	Peer Address	MTU	Subnet Mask	DNS Address	Host Name
<i>(none)</i>	ctc - B890	TCPIP	192.168.0.3	1492	255.255.255.0	0.0.0.0	vmr.com
<i>(none)</i>	ctc - B892	TCPIP	192.168.0.3	1492	255.255.255.0	0.0.0.0	vmr.com
<i>(none)</i>	ctc - B894	TCPIP	192.168.0.3	1492	255.255.255.0	0.0.0.0	vmr.com
<i>(none)</i>	ctc - B896	TCPIP	192.168.0.3	1492	255.255.255.0	0.0.0.0	vmr.com
SUSE-211	ctc - 2500	TCPIP	192.168.0.3	1492	255.255.255.0	209.167.83.9	vmr.com
SUSE-212	ctc - 2502	TCPIP	192.168.0.3	1492	255.255.255.0	209.167.83.9	vmr.com
SUSE-213	ctc - 2504	TCPIP	192.168.0.3	1492	255.255.255.0	209.167.83.9	vmr.com
IUCV-214	iucv	TCPIP	192.168.0.3	3942	255.255.255.240	209.167.83.8	vmr.com
IUCV-215	iucv	TCPIP	192.168.0.3	3942	255.255.255.240	209.167.83.9	vmr.com

Color Scheme

The status of an IP Address is indicated by the color of its display.

Allocated to a Linux Image
Virtual CTC or IUCV not yet configured to TCP/IP VM
Available for allocation to a Linux image

IP Address property descriptions

This manual can only give a cursory explanation of the purpose of these properties. Please review the manuals documenting whichever connection type you use for detailed guidance on determination of suitable choices for these properties.

IP Address

This is the IP number for the Linux Image. If it is underlined, the properties can be changed by clicking on it. Then follow the instructions given in on page 27.

Image Name

This is either the Linux Image Name that owns the IP Address or *(none)*. Note that IUCV connections must have a predetermined Image Name.

Connection Device

Note that your Linux system must have the appropriate kernel support, including drivers, for the selected Connection Type. Also kernel parameters and configuration files may have to be specified. If the kernel parameters are modified after the Linux Image is created, you will need to run `silos`, `zilos` or `zipls`³ to rebuild the Linux boot sector.

VMOT currently is able to automatically configure IUCV, Virtual and Real CTC connection types.

Currently available connection types are:

iucv — Inter-User Communication Vehicle

IUCV is a VM facility that allows direct communication between different VM userids. This option connects via IUCV to a TCP/IP VM Userid.

ctc — Virtual Channel-to-Channel

CTC connects via a CTC link to a TCP/IP VM Userid.

eth — Real Channel-to-Channel

RCTC is a connection to a real CTC in the S/390 or zSeries hardware which likely connects to another LPAR.

Device

This is the lower number of the even/odd device address pair for the real devices defined for the adapter or the virtual CTC connection to TCP/IP VM.

When multiple IP Addresses are defined, the device address is incremented by two for each new pair.

Host Gateway Name

Hardware adapters such as CLAW may require this name. PPP connections to TCP/IP VM via VCTC or IUCV require the name of the TCP/IP VM userid they connect to.

Note that an IUCV connection will require an `IUCV=TCP/IP VM userid kernel` parameter. If the kernel parameter is changed after the Linux Image is created, `silos` must be run to enable the new kernel parameter.

Peer Address — also Gateway Address

This is the IP Address of the adapter, external device or TCP/IP VM userid the Linux Image connects to.

Note: Peer address is the term normally used for a PPP link while Gateway is used for a LAN connection.

Gateway Address or, Reserved Name: (*ONLY for IUCV*)

Note: Gateway is a miscaption for Broadcast Address.

The Broadcast IP Address is required by hardware adapters connected to a LAN.

³ `silos`, `zilos` and `zipls` are Linux commands that build a Linux boot file. See Linux/390 reference material for information on these commands.

For IUCV connections, it is the Linux Image Name reserved for this connection to TCP/IP VM. When **Create Image** is performed for an IUCV connection, this name is used for the Image Name.

Maximum Transmission Unit

This is the maximum size TCP/IP packet sent or received by the Linux Image. The default supplied, 1492, is normal for VCTC connections. Larger values may be appropriate for other connection types.

Subnet Mask

The default supplied, 255.255.255.255 is appropriate for PPP connections to TCP/IP VM. Adapter connections will often require a different value.

Domain Name Server (DNS) IP Address

This address is used for resolution of names to IP Addresses.

Host Name — DNS Default Domain Suffix

This name is used as a suffix when generating a host name for Linux images. The prefix is the name you give the Linux image when you create it. For example, if your domain suffix is myLinuxFarm.mycompany.com and you create a Linux image with the name myLinux, the domain name for the new Linux image will be myLinux.myLinuxFarm.mycompany.com

Adding and Deleting IP Address Ranges

The values entered on this subpanel must be determined in collaboration with your TCP/IP VM or Network Administrator.

Three steps are required:

1. Click on the Open Special Options button.
2. Fill in or select the input fields.
3. Click on the Insert or Remove button.

Click on the Close Special Options button to return to the IP Address List.

See on page 23 for a description of the input fields.

Insert IP Addresses starting at

using...

Device Type:

Device Unit Address: *(NOT used for iucv)*

Gateway Name: *(or a TCPIP Virtual Machine USERid)*

MTU:

Subnet Mask:

Peer Address:

Gateway Address: *or Reserved Name (ONLY used for iucv)*

DNS Address:

Host Name:

Remove

Changing IP Address Properties

The values entered on this subpanel must be determined in collaboration with your TCP/IP VM or Network Administrator.

Changes can only be applied to unassigned IP Addresses. Once an IP Address has been assigned to a Linux Image, you must Delete the Linux Image before you can make any changes to the IP Address Properties.

See on page 23 for a description of the input fields.

Manage IP Addresses

LOGOFF
View Help Information
Cancel
Refresh

Press Save to update your changes for **192.168.0.211** when you are done.

Definition	New Value	Current Setting
Device Type:	<input type="text" value="(no change)"/>	ctc
Device Unit Address: (<i>NOT</i> used for iucv)	<input type="text" value="2500"/>	2500
Gateway Name: (<i>or</i> a TCPIP Virtual Machine USERid)	<input type="text" value="TCPIP"/>	TCPIP
MTU:	<input type="text" value="1492"/>	1492
Subnet Mask:	<input type="text" value="255.255.255.0"/>	255.255.255.0
Peer Address:	<input type="text" value="192.168.0.3"/>	192.168.0.3

Gateway Address or, Reserved Name: (<i>ONLY</i> for iucv)	<input type="text" value=""/>	<i>(nothing)</i>
DNS Address:	<input type="text" value="209.167.83.9"/>	209.167.83.9
Host Name:	<input type="text" value="vmr.com"/>	vmr.com

Index

11116, 10, 11
33906

A

adapter25
adapters
 Broadcast IP25
Add Group19
Add New Major Group18
Add New Userid19
Administration16
Administration authority17
Administration Authority16
Administration Authority Levels
 Full17
Administration Capability
 Recovery17
Administration panel16
Administration panels20
Administrator15
archive5, 7, 11
AUTOLOG115

B

Batch Job10
Batch Job Scheduler10

C

Change Userid19
CLAW5, 25
collaboration
 TCP/IP VM27, 28
Configuration5, 10
Co-ordination Requirements20
Create Image
 IUCV:Reserved Image Name26

D

DASD Group10
 LINUX10
DASD Group LINUX11
DASD space5
DASD Space6, 10
datadir17
 CONFIG SETTINGS17
dedicated adapters
 CLAW5
Default Group16
default prefix12
Delete Group19
Delete Major Group18
Device Address25
Direct connections5
directory
 sample files10
Directory10
DIRMAINT11, 15
DNS26
DNS Default Domain Suffix26
Domain Name Server IP Address26
domain suffix26
DownLoading7

E

Enablement5, 14
 EXTENT CONTROL10
 EXTENT CONTROL file11

F

filepool10
 FILEPOOL6
 filepools5
 FORCE14
 FTP7
 Command sequence7
 Full Authority19

G

group5
 Group
 Administration panel17
 Group and Major Group
 identifiers16
 Rules and Definitions16
 Groups16

H

hierarchy16
 Host Gateway25
 host name26
 HTTP port12, 13
 HTTP Port15
 HTTP Server10

I

installation
 tasks5
 Installation
 multiple13
 Installation example12
 installation exec11
 installation exec
 LXINS5
 IP address14
 4.IP Address15
 Add27
 administration5
 Administration20
 Connection Type25
 connection type:IUCV25
 Connection Type:kernel support25
 connection type:VCTC25
 co-ordination:CLAW20
 co-ordination:OSA20
 Co-ordination:TCP/IP VM Administrator20
 multiple25
 pull-down21
 Range display23
 TCP/IP VM:IUCV20
 TCP/IP VM:TCPMAINT20
 TCP/IP VM:virtual CTC20
 IP address pool5
 IP Address Range14
 IP Address Range Administration20
 IP Range
 Selection21
 IP Range Administration Panel20

VMOT Installation and Administration Guide

IUCV5, 14, 21, 25

reserved Image Name26

IUCV=TCP/IP VM userid25

IUCV Link

Image Name25

K

kernel parameter25

L

Linux boot sector25

LINUX CGI21

Linux Images

Read-Only7

Linux Master

Container10

log10

LOGON15

Log Recorder10

LXINS5, 11, 12, 13, 14, 15

LXMAINT14

LXMASTER6

LXSFS6

LXSFS\

LX.PROD.DATA14

LX VMA11

M

MAINT6, 10, 11

MAINT 111111

Maintenance USERid10

Major Group5, 21

Major Group

Administration16, 18

Administration panel17

Delete18

Major Group Administrator16

Major Groups16

Manage IP Address Ranges20

Master copy7

Maximum Transmission Unit26

N

Network Administrator

collaboration27, 28

O

OBEY file21

OBEYFILE14

OSA5

P

PPP5

prefix6

Prerequisites

software6

R

RCTC25

Read/Write10

READ ME15

Reassign Major Group18

redbook7

Removal13

S

Set IP Parameters for Add or Change27, 28

SFS10
 SFS FILEPOOL6
 SFS FILEPOOL Server10
 Shared File System10
 silo25
 space requirements
 factors10
 space usage10
 Startup15
 Subnet Mask26
T
 TCP/IP VM5, 14, 25
 administrator21
 collaboration27, 28
 configuration files14
 Configuration files14
 configuration statements20
 Enabling configuration changes14
 Reconfiguring21
 Secondary14
 service machine5, 14
 userid21, 25
 Userid25
 TCP/IP VM userid25
 TCPIP/VM10
 TCPIP DEVICE14
 TCPIP GATE14
 TCPIP HOME14
 TCPIP OBEY14
 TCPIP START14
 TCPMAINT21
U
 User Guide and Reference5
 userid5
 Administration Authority20
 Userid6, 15, 16, 17, 18, 19, 25
 Administration16
 Creation19
 Delete19
 Initial16
V
 VCTC21, 25
 virtual console11
 virtual CTC14, 25
 Virtual CTC5
 VLMADMIN15, 16
 VLMADMIN USER17
 VM\
 Secure10, 15
 VMARC5, 11
 VMARC DMP11
 VMARC MODULE11
 VMSECURE11
X
 XAUTOLOG14, 15
 Xedit17
 XEDIT10
 xxMAINT6, 14, 17, 21
 xxSFS6
 xxSFS\
 xx.PROD.DATA14

VMOT Installation and Administration Guide

Z

zilo25

zipl25