

MAINVIEW[®] for IP User Guide

Version 2.1

August 15, 2002



Copyright 2000–2002 BMC Software, Inc., as an unpublished work. All rights reserved.

BMC Software, the BMC Software logos, and all other BMC Software product or service names are registered trademarks or trademarks of BMC Software, Inc. IBM is a registered trademark of International Business Machines Corp. All other registered trademarks or trademarks belong to their respective companies.

THE USE AND CONTENTS OF THIS DOCUMENTATION ARE GOVERNED BY THE SOFTWARE LICENSE AGREEMENT ENCLOSED AT THE BACK OF THIS DOCUMENTATION.

Restricted Rights Legend

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Section 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC Software, Inc., 2101 CityWest Blvd., Houston, TX 77042-2827, USA. Any contract notices should be sent to this address.

Contacting BMC Software

You can access the BMC Software Web site at <http://www.bmc.com>. From this Web site, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

United States and Canada

Address BMC Software, Inc.
2101 CityWest Blvd.
Houston TX 77042-2827

Telephone 713 918 8800 or
800 841 2031

Fax 713 918 8000

Outside United States and Canada

Telephone (01) 713 918 8800

Fax (01) 713 918 8000

Customer Support

You can obtain technical support by using the Support page on the BMC Software Web site or by contacting Customer Support by telephone or e-mail. To expedite your inquiry, please see “Before Contacting BMC Software.”

Support Web Site

You can obtain technical support from BMC Software 24 hours a day, 7 days a week at <http://www.bmc.com/support.html>. From this Web site, you can

- read overviews about support services and programs that BMC Software offers
- find the most current information about BMC Software products
- search a database for problems similar to yours and possible solutions
- order or download product documentation
- report a problem or ask a question
- subscribe to receive e-mail notices when new product versions are released
- find worldwide BMC Software support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

Support by Telephone or E-mail

In the United States and Canada, if you need technical support and do not have access to the Web, call 800 537 1813. Outside the United States and Canada, please contact your local support center for assistance. To find telephone and e-mail contact information for the BMC Software support center that services your location, refer to the Contact Customer Support section of the Support page on the BMC Software Web site at www.bmc.com/support.html.

Before Contacting BMC Software

Before you contact BMC Software, have the following information available so that Customer Support can begin working on your problem immediately:

- product information
 - product name
 - product version (release number)
 - license number and password (trial or permanent)
- operating system and environment information
 - machine type
 - operating system type, version, and service pack or other maintenance level such as PUT or PTF
 - system hardware configuration
 - serial numbers
 - related software (database, application, and communication) including type, version, and service pack or maintenance level
- sequence of events leading to the problem
- commands and options that you used
- messages received (and the time and date that you received them)
 - product error messages
 - messages from the operating system, such as `file system full`
 - messages from related software

Contents

About This Book	xi
Summary of Changes	xvii
Chapter 1	Introduction
Overview	1-2
Features and Functions	1-3
Sample SAS Programs	1-4
Chapter 2	Using MAINVIEW for IP
Overview	2-3
Easy Menus	2-3
Accessing MAINVIEW for IP	2-4
Navigating in MAINVIEW for IP	2-7
Working with MAINVIEW for IP	2-8
MAINVIEW for IP Views	2-8
Availability	2-9
Configuration	2-10
Connections	2-11
Connections Information	2-11
Dropping a Connection by Using a Line Command	2-12
Pinging a Device by Using a Line Command	2-14
Performing a Traceroute on a Device by Using a Line Command ..	2-16
Diagnostics	2-18
Pinging a Device	2-20
Performing a Traceroute on a Device	2-22
Accessing More Traceroute Information	2-25
Starting a Packet Trace	2-26
Stopping a Packet Trace	2-28
Displaying a Packet Trace	2-29
Accessing More Packet Trace Information	2-31
Viewing Packet Details	2-32
Clearing Packet Trace Entries	2-33
Dynamic Virtual IP Addresses	2-34
FTP Servers	2-35

	Interfaces	2-36
	IP Resource Links	2-37
	Hyperlinks	2-37
	Activating the Web Server Hyperlink	2-38
	Routers	2-40
	SNMP Information	2-40
	Defining SNMP Parameters	2-41
	Service Levels	2-43
	Storage	2-44
	Traffic/Response Times	2-45
	Tools and Menus	2-46
	Historical Data Sets	2-46
	Select View	2-46
	Return	2-46
	Exiting from MAINVIEW for IP	2-46
Chapter 3	Displaying Historical Data	
	Overview	3-2
	Data Availability	3-3
	TIME Command	3-4
	Viewing Historical Data in the JOBNAME Response Times View	3-5
	Displaying the Intvl Time Field	3-10
	Moving between Timeframes	3-11
	Time and Duration Fields	3-12
Chapter 4	Setting Alarms	
	MAINVIEW Alarm Manager	4-2
	Alarm Setting Checklist	4-2
	Sample Alarms	4-5
	Alarm Definitions	4-6
Chapter 5	MAINVIEW for IP Messages	
	Interpreting Messages	5-2
	Message Format	5-2
	Message Identifiers	5-3
	Message Levels	5-3
	Description Format	5-4
	Contacting BMC Software Customer Support	5-4
	Gathering Problem Report Documentation	5-5
	MAINVIEW for IP Messages	5-8
Appendix A	Operator Commands	
	Conventions	A-2
	Commands	A-2
	DNR—Domain Name Resolution Function	A-2
	XSUPP—Exit Suppression	A-2

Index

Figures

Figure 2-1	MAINVIEW Selection Menu	2-4
Figure 2-2	Session Control Parameters Panel	2-5
Figure 2-3	EZIP Menu (Page One)	2-6
Figure 2-4	EZIP Menu (Page Two)	2-7
Figure 2-5	PING Information View	2-15
Figure 2-6	TRACE Information View	2-17
Figure 2-7	Ping Information Detail View	2-20
Figure 2-8	Traceroute Information Detail View	2-23
Figure 2-9	Traceroute Details	2-25
Figure 2-10	Packet Tracing View	2-26
Figure 2-11	Packet Tracing Filters View	2-29
Figure 2-12	Packet Tracing Details View	2-30
Figure 2-13	More Packet Tracing Details View	2-31
Figure 2-14	More Packet Details View	2-32
Figure 2-15	Cache Info (WebSphere) View	2-38
Figure 2-16	WASPERF Summary View	2-39
Figure 2-17	SNMP Define View	2-42
Figure 3-1	DSLISIT View	3-3
Figure 3-2	TCPCONS with an Open Window	3-6
Figure 3-3	SET TIME FRAME Dialog	3-7
Figure 3-4	JOBRESP in Two Timeframes	3-8
Figure 3-5	Example of TIME PREV to Cycle through Timeframes	3-12
Figure 5-1	Parts of a Message	5-2

Tables

Table 1-1	Features and Functions	1-3
Table 1-2	SMF Information	1-4
Table 2-1	MAINVIEW for IP Easy Menus	2-3
Table 2-2	Availability Views	2-9
Table 2-3	Configuration Views	2-10
Table 2-4	Connection Views	2-11
Table 2-5	Diagnostic Views	2-19
Table 2-6	Dynamic VIPA Views	2-34
Table 2-7	FTP Servers Views	2-35
Table 2-8	Interface Views	2-36
Table 2-9	IP Resource Links	2-37
Table 2-10	Router Views	2-40
Table 2-11	Service Level Views	2-43
Table 2-12	Storage Views	2-44
Table 2-13	Traffic/Response Time Views	2-45
Table 4-1	Alarm Setting Checklist	4-3
Table 4-2	MAINVIEW for IP Sample Alarms	4-5
Table 5-1	Message Identifiers	5-3
Table 5-2	Message Severity Codes	5-3

About This Book

This book contains detailed information about MAINVIEW® for IP and is intended for network administrators, system administrators, and system programmers.

To use this book, you should be familiar with the following items:

- Multiple Virtual Storage (MVS) systems, job control language (JCL), and the Interactive System Productivity Facility (ISPF)
- your client and host operating systems

For example, you should know how to respond to ISPF panels and how to perform common actions in a window environment (such as choosing menu items and resizing windows).

How This Book Is Organized

This book is organized as follows:

Chapter/Appendix	Description
Chapter 1, "Introduction"	provides an introduction to the features and functions of MAINVIEW for IP
Chapter 2, "Using MAINVIEW for IP"	explains the MAINVIEW for IP views that are displayed on the MAINVIEW console, and provides instructions for using the views
Chapter 3, "Displaying Historical Data"	provides instructions for using the TIME command to display historical data Note: For instructions on how to generate historical performance reports, see <i>Using MAINVIEW</i> .
Chapter 4, "Setting Alarms"	provides a list of sample alarms and a checklist with the steps that are required to set an alarm in MAINVIEW for IP
Chapter 5, "MAINVIEW for IP Messages"	explains the messages that can be displayed within the MAINVIEW for IP environment
Appendix A, "Operator Commands"	lists operator commands available for MAINVIEW for IP

In addition, an index appears at the end of the book.

Related Documentation

BMC Software products are supported by several types of documentation:

- online and printed books
- online Help
- release notes and other notices

In addition to this book and the online Help, you can find useful information in the following publications:

Category	Document	Description
installation documents	<i>Implementing Security for MAINVIEW Products</i>	describes how to implement MAINVIEW security with your external security manager to protect MAINVIEW product resources from user access
	<i>MAINVIEW Common Customization Guide</i>	provides instructions for manually customizing the MAINVIEW environment for your products
	<i>MAINVIEW Installation Requirements Guide</i>	provides product-specific information such as software and storage requirements, product libraries, and FMIDs
	<i>OS/390 and z/OS Installer Guide</i>	provides instructions for using the installation system, and describes the Product Authorization utility and AutoCustomization
	<i>MAINVIEW for IP Customization Guide</i>	provides instructions for customizing and implementing MAINVIEW for IP
core documents	<i>MAINVIEW Administration Guide</i>	provides information about MAINVIEW operations, targets, single-system image contexts, MAINVIEW Alarm Manager, data sets, view customization, and diagnostic facilities
	<i>MAINVIEW Alarm Manager User Guide</i>	describes how to create and install alarm definitions that indicate when exceptions occur in a sysplex
	<i>MAINVIEW Alternate Access Implementation and User Guide</i>	explains how to configure, start, and stop VTAM and EXCP AutoLogon sessions to access MAINVIEW products without an active TSO subsystem
	<i>MAINVIEW Quick Reference</i>	provides a quick reference for MAINVIEW terminal sessions, logs, data sets, targets, contexts, windows mode, and full-screen mode and describes the functions, syntax, and parameters of the commands that are used to manage the MAINVIEW window environment
	<i>Using MAINVIEW</i>	provides information about working with MAINVIEW products in windows mode and full-screen mode
supplemental documents	release notes, flashes, technical bulletins	provide current information about MAINVIEW for IP

Online and Printed Books

The books that accompany BMC Software products are available in online format and printed format. If you are a Windows or Unix user, you can view online books with Acrobat Reader from Adobe Systems. The reader is provided at no cost, as explained in “To Access Online Books.” You can also obtain additional printed books from BMC Software, as explained in “To Request Additional Printed Books.”

To Access Online Books

Online books are formatted as Portable Document Format (PDF) files. You can view them, print them, or copy them to your computer by using Acrobat Reader 3.0 or later. You can access online books from the documentation compact disc (CD) that accompanies your product or from the World Wide Web.

In some cases, installation of Acrobat Reader and downloading the online books is an optional part of the product-installation process. For information about downloading the free reader from the Web, go to the Adobe Systems site at <http://www.adobe.com>.

To view any online book that BMC Software offers, visit the support page of the BMC Software Web site at <http://www.bmc.com/support.html>. Log on and select a product to access the related documentation. (To log on, first-time users can request a user name and password by registering at the support page or by contacting a BMC Software sales representative.)

To Request Additional Printed Books

BMC Software provides printed books with your product order. To request additional books, go to <http://www.bmc.com/support.html>.

Online Help

MAINVIEW for IP includes online Help. In the MAINVIEW for IP ISPF interface, you can access Help by pressing **F1** from any ISPF panel.

Release Notes and Other Notices

Printed release notes accompany each BMC Software product. Release notes provide current information such as

- updates to the installation instructions
- last-minute product information

In addition, BMC Software sometimes provides updated product information between releases (in the form of a flash or a technical bulletin, for example). The latest versions of the release notes and other notices are available on the Web at <http://www.bmc.com/support.html>.

Conventions

This book uses the following general conventions:

Item	Example
information that you are instructed to type	Type SEARCH DB in the designated field.
specific (standard) keyboard key names	Press Enter .
field names, text on a panel	Type the appropriate entry in the Command field.
directories, file names, Web addresses	The BMC Software home page is at www.bmc.com .
nonspecific key names, option names	Use the HELP function key. KEEPDICTIONARY option
MVS calls, commands, control statements, keywords, parameters, reserved words	Use the SEARCH command to find a particular object.
code examples, syntax statements, system messages, screen text	//STEPLIB DD The table <i>table_name</i> is not available.
emphasized words, new terms, variables	The instructions that you give to the software are called <i>commands</i> . In this message, the variable <i>file_name</i> represents the file that caused the error.

This book uses the following types of special text:

Note: Notes contain important information that you should consider.

Warning! Warnings alert you to situations that could cause problems, such as loss of data, if you do not follow instructions carefully.

Tip: Tips contain useful information that may improve product performance or that may make procedures easier to follow.

Summary of Changes

This summary of changes includes changes to the functionality of the product, enhancements to the product, and any major changes to the documentation. The summary of changes is listed by release date.

Revision bars are used in the manual to note changes that clarify or correct existing information or that provide new information related to product changes. Revision bars are not used to note editorial and formatting changes or typographical errors that have been corrected unless these updates significantly affect the use of the information.

Version 2.1.00

August 15, 2002

The following features have been added to MAINVIEW for IP:

- support for z/OS 1.3
- Define Simple Network Management Protocol (SNMP) Routers view
- File Transfer Protocol (FTP) exit
- FTP Servers views
- Open Systems Adapter (OSA) configuration view
- OSA performance views
- OSA utilization view
- packet tracing
- socket tracing
- sample Statistical Analysis System (SAS) program for viewing OSA device information recorded to system management facility (SMF)

The following changes have been made to MAINVIEW for IP and to this book:

- A list of operator commands has been added to the user guide.
- The IP addresses that are displayed are no longer padded with leading zeroes.

-
- Comments were added to the sample SAS reports to describe each field in the reports.
 - The SNMPSYSD view has been enhanced to display more information about Simple Network Management Protocol (SNMP) system routers.

Version 2.0.00

March 28, 2002

The following features have been added to MAINVIEW for IP:

- support for z/OS 1.2
- Communications Storage Manager statistics view
- Virtual Telecommunications Access Method buffer statistics view
- Common Storage Area statistics view
- DR command to terminate connections
- Connection Routing Table detail view
- Distribution Port Table detail view
- Service Level Agreement Policy view
- Cache Information view
- historical data sets
- MAINVIEW[®] for UNIX System Services hyperlink
- MAINVIEW[®] for WebSphere Application Server hyperlink
- sample MAINVIEW Alarm Manager alarms with default thresholds
- system overview view
- error message BMC259510E
- sample SAS programs for viewing service level agreement policy information and Web cache analysis information recorded to system management facility

The following changes have been made to MAINVIEW for IP and to this book (formerly the *MAINVIEW for IP Reference Manual*):

- The MAINVIEW Selection Menu and the EZIP Menu were redesigned.
- Installation and customization instructions were moved to the *MAINVIEW for IP Customization Guide*.
- The VIPA Destination Port Table view has been renamed the Distribution Port Table view.

Chapter 1 Introduction

This chapter introduces and describes the features and functions of MAINVIEW for IP.

This chapter contains the following sections:

Overview	1-2
Features and Functions	1-3
Sample SAS Programs	1-4

Overview

MAINVIEW for IP provides a way to monitor OS/390 and z/OS mission-critical application performance. MAINVIEW for IP collects application performance data from the Transmission Control Protocol/Internet Protocol (TCP/IP) stack. This data is displayed on the MAINVIEW console.

Note: You cannot manipulate the collected data; you can only view the data.

For information about using these features and functions, see Chapter 2, “Using MAINVIEW for IP.”

Features and Functions

MAINVIEW for IP provides monitoring and management of TCP/IP stacks. Table 1-1 describes the features and functions of MAINVIEW for IP.

Table 1-1 Features and Functions

Feature	Description
actions	lets you initiate specific actions in a view, such as dropping a connection, pinging a device, or performing a Traceroute
availability	provides information about the availability of application and stack connections
configuration	provides configuration information by TCP, UDP, IP, SMF, and port
connections	provides information about the devices that are connected to an application by domain name, IP address, and remote port number
diagnostics	provides information about a ping or a Traceroute that you requested; lets you perform packet tracing and socket tracing
dynamic VIPA	provides information about dynamic Virtual IP Addresses (DVIPA)
FTP statistics	provides file transfer protocol (FTP) information
historical data	provides information about previous performance to compare with current performance
interfaces	provides information about network devices, network links, and Open Systems Adapter (OSA) cards
IP resource links	provide hyperlinks to views in MAINVIEW® for UNIX System Services and to MAINVIEW® for WebSphere Application Server
routers	lets you specify every IP node that you want to monitor; provides information about TCP, UDP, IP, system, and interface router performance; and provides information about network routes
service levels	provides information about application access availability, and about your Web servers to help ensure that you are meeting your service level agreements
storage	provides statistics about Communication Storage Manager (CSM), Virtual Telecommunications Access Method (VTAM), and Common Storage Area (CSA) buffer pools and storage usage
threshold/alarm conditions	sample alarms and threshold conditions use color or highlighting to add visual indicators to display data that instantly shows when resources are reaching a critical state
traffic/response times	provides information about the amount of data that is being sent and received as well as compression rates, and provides information about host and network response times by station (IP address or domain name), port, or subnet

Sample SAS Programs

BMC Software provides sample Statistical Analysis System (SAS) programs in *hilevel.BBSAMP*. You can use these programs to view the information that is recorded to system management facility (SMF). The default startup parameters for SMF recording are provided in *hilevel.BBSAMP(TACPRM)*. For more information about the TACPRM data set member and SMF recording startup parameters, see the *MAINVIEW for IP Customization Guide*.

For information about SMF records, setting up the SMF data set, and specifying the SMF record type numbers, see the *IBM System Management Facilities* documentation.

Table 1-2 describes the SAS program members that are available in *hilevel.BBSAMP*.

Table 1-2 SMF Information

Member	Description
SMF252A	service level agreement policy information
SMF252C	connections and response times information
SMF252D	device information
SMF252F	configuration information
SMF252H	Web cache analysis information
SMF252I	SNMP IP information
SMF252N	SNMP interface information
SMF252P	port information
SMF252R	router information
SMF252S	SNMP system information
SMF252T	SNMP TCP information
SMF252U	SNMP UDP information
SMF252V	Virtual IP Address (VIP) information

Chapter 2 Using MAINVIEW for IP

This chapter helps you interpret the views that are provided with MAINVIEW for IP. These views display application performance data that is collected by MAINVIEW for IP.

This chapter contains the following sections:

Overview	2-3
Easy Menus	2-3
Accessing MAINVIEW for IP	2-4
Navigating in MAINVIEW for IP	2-7
Working with MAINVIEW for IP	2-8
MAINVIEW for IP Views	2-8
Availability	2-9
Configuration	2-10
Connections	2-11
Connections Information	2-11
Dropping a Connection by Using a Line Command	2-12
Pinging a Device by Using a Line Command	2-14
Performing a Traceroute on a Device by Using a Line Command	2-16
Diagnostics	2-18
Pinging a Device	2-20
Performing a Traceroute on a Device	2-22
Accessing More Traceroute Information	2-25
Starting a Packet Trace	2-26
Stopping a Packet Trace	2-28
Displaying a Packet Trace	2-29
Accessing More Packet Trace Information	2-31
Viewing Packet Details	2-32
Clearing Packet Trace Entries	2-33
Dynamic Virtual IP Addresses	2-34
FTP Servers	2-35
Interfaces	2-36

IP Resource Links	2-37
Hyperlinks	2-37
Activating the Web Server Hyperlink	2-38
Routers	2-40
SNMP Information	2-40
Defining SNMP Parameters	2-41
Service Levels	2-43
Storage	2-44
Traffic/Response Times	2-45
Tools and Menus	2-46
Historical Data Sets	2-46
Select View	2-46
Return	2-46
Exiting from MAINVIEW for IP	2-46

Overview

MAINVIEW windows mode technology provides views that summarize data which is pulled from multiple subsystems. Within MAINVIEW for IP, you can display detailed and summary views of collected data. To display a list of all MAINVIEW for IP views, select **Select View** (Tools and Menus) on the EZIP Menu. For more information about the Select View feature, see the *Using MAINVIEW* manual.

Note: The online Help contains information about MAINVIEW for IP views and the fields in them. To access Help, position the cursor over the applicable field and press the Help key (usually **PF1**).

MAINVIEW for IP views summarize application performance data that is collected by MAINVIEW for IP. You can monitor applications by job name, IP address, and port. You can analyze which enterprise resources have priority access to critical data.

Easy Menus

MAINVIEW for IP offers a series of easy menus that provide a quick, convenient way to use the product with little introduction and without having to remember view names. Easy menus allow navigation to the parts of MAINVIEW for IP, based on a feature that you want to monitor rather than on a specific view.

EZIP is the primary easy menu for MAINVIEW for IP. The selections on this menu let you access other high-level easy menus, such as EZIPRESP, to locate information quickly. Table 2-1 describes the easy menus that are provided in MAINVIEW for IP.

Table 2-1 MAINVIEW for IP Easy Menus

Menu	Description
EZIPCONF	configuration details
EZIPCONS	connection details
EZIPOSA	Open Systems Adapter (OSA) card details
EZIPRESP	response time details
EZIPSNMP	Simple Network Management Protocol and router details
EZIPSUBN	subnet response time summary details
EZIPVIPA	dynamic Virtual IP Address details

Accessing MAINVIEW for IP

MAINVIEW for IP can be accessed from the MAINVIEW Selection Menu (Figure 2-1).

Figure 2-1 MAINVIEW Selection Menu

```

----- MAINVIEW Selection Menu -----
OPTION  ===>                                DATE   -- 01/10/03
                                           TIME   -- 16:45:41
      0   Parameters and Options             USERID -- BMVDID3
      E   Alerts and Alarms                 MODE    -- ISPF 4.8
      P   PLEX Management (PLEXMGR)
      U   Utilities, Tools, and Messages

Solutions for:
      A   Automated Operations
      C   CICS
      D   DB2
      I   IMS
      L   Linux
      N   Network Management
      S   Storage Management
      T   Application Management and Performance Tuning
      W   WebSphere and MQSeries
      Z   OS/390, z/OS, and USS

Enter X to Terminate

                                Copyright BMC Software, Inc. 2001
    
```

To access MAINVIEW for IP, perform the following steps from the MAINVIEW Selection Menu:

Step 1 Type **N** on the command line to select **Network Management**, and press **Enter**.

The Network Management Solutions menu is displayed.

Step 2 Type **1** to select MAINVIEW for IP, and press **Enter**.

The Session Control Parameters panel (Figure 2-2) is displayed.

Figure 2-2 Session Control Parameters Panel

```
BMC Software  ----- SESSION CONTROL PARAMETERS -----  
COMMAND ===>  
  
Subsystem ID  ===> BBIP (Coordinating Address Space subsystem ID)  
  
XDM mode     ===> NO      (Execute session in diagnostic mode, Yes/No)  
  
Press ENTER to confirm use of session parameters entered above.
```

Step 3 Type the subsystem ID **BBIP** for the coordinating address space (CAS), and press **Enter**.

The EZIP Menu (Figure 2-3) is displayed.

Figure 2-3 EZIP Menu (Page One)

```

08JUL2002 12:30:48 ----- INFORMATION DISPLAY -----
COMMAND ==>>                                SCROLL ==>> PAGE
CURR WIN ==>> 1                            ALT WIN ==>>
>W1 =EZIP=====MCBSYS1=*=====08JUL2002==12:24:10====MVIP====D====1

      Availability                Routers                Diagnostics
      . TCP/IP Stacks             . Define              . Ping Information
      . Applications              . TCP                 . Tracerte Information
      . Traffic/Response Times   . UDP                 . Packet Tracing
      . by Job                   . IP                 . Socket Tracing
      . by Port                  . System
      . by Connection            . Interface
      . Connections              . Network Routes
      . TCP                      . Interfaces
      . UDP                      . Network Devices
      . All                      . Network Links
      . Configuration            > OSA Cards
      . Storage                  . General Information
      . SLA Policy Information
      . Cache Info (WebSphere)
  
```

To see the second page of the EZIP Menu (Figure 2-4 on page 2-7), scroll down by pressing **F8**.

Figure 2-4 EZIP Menu (Page Two)

```

08JUL2002 12:31:03 ----- INFORMATION DISPLAY -----
COMMAND ==>
CURR WIN ==> 1          ALT WIN ==>
>W1 =EZIP=====MCBSYS1=*=====08JUL2002==12:24:10====MVIP====D====1
      . CSM Buffer Pools      > Response Times
      . VTAM Buffer Pools    > Subnet Response Times
      . CSA Information
      . IP                      Tools and Menus
      . SMF                    FTP Servers
      . Port                   . Historical Data Sets
      . File Information       . Select View
      . Userid Information     . Return....
      . IPaddr Information

```

To display a list of all MAINVIEW for IP easy menus and views, select **Select View** (Tools and Menus) from the EZIP Menu.

Navigating in MAINVIEW for IP

Select the menu or view that you want to display by performing one of the following tasks:

- Place the cursor on the menu item you want to view, and press **Enter**.
- Type the name of the easy menu or view on the command line (for example, EZIPSNMP), and press **Enter**.

As part of the MAINVIEW environment, MAINVIEW for IP functions as an extension of the standard ISPF panel interface. For a description of the common window interface, and for details on how to use the features and services that are available within the MAINVIEW environment, see the *Using MAINVIEW* manual.

Working with MAINVIEW for IP

You can display MAINVIEW for IP views and manage the panels in which the views are displayed in the same way you do any MAINVIEW product. You can display multiple panels of different sizes simultaneously and you can direct actions from one panel to another, all on one terminal.

MAINVIEW for IP Views

MAINVIEW for IP views display information that helps you monitor and manage your network. To access detailed or summary information about application availability, traffic, sessions (or connections), configuration, routers, service levels, and so on, use the EZIP Menu (Figure 2-3 on page 2-6).

In several views, you can perform a “drill-down” function. Drill-down functions let you view more detailed information about an item.

You can drill down for more information in any view where a field name is highlighted. Some highlighted field names are hyperlinks to other applications or resources. For sample instructions on how to perform a drill-down function, see “Accessing More Traceroute Information” on page 2-25. For a description of the hyperlinks that are available in MAINVIEW for IP, see “IP Resource Links” on page 2-37.

Sample alarms and threshold conditions are provided in many MAINVIEW for IP views. You can use color or highlighting to add visual indicators to view data that instantly show when resources are reaching a critical state. For more information about this feature, see Chapter 4, “Setting Alarms.”

Availability

The availability feature provides statistical information for each application and Transmission Control Protocol/Internet Protocol (TCP/IP) stack that is detected on an OS/390 or z/OS platform. By using the Applications view, you can monitor the application status for any address space that is associated with a TCP/IP stack. By using the TCP/IP Stacks view, you can quickly determine the status of a TCP/IP stack.

Table 2-2 describes the views that provide detailed information about application or TCP/IP stack availability.

Table 2-2 **Availability Views**

View	Description
TACAPPL	displays throughput information for each remote application
TACTCSB	displays statistical information for each TCP/IP stack that is detected on an OS/390 or z/OS platform

Configuration

The configuration feature provides configuration information for the PROFILE data set for each TCP/IP stack on your system. For realtime data about the programs that make up your system, subsystem, or network, access the TCP, UDP, IP, SMF, or PORT configuration views. These views let you see configuration information without searching through several data sets.

Table 2-3 describes the views that provide detailed or summary information about your system configurations.

Table 2-3 Configuration Views

View	Description
TCPCONF	displays configuration information for each TCP/IP stack on your system
UDPCONF	displays configuration information for each User Datagram Protocol (UDP) on your system
IPCONF	displays configuration information for each IP stack on your system
SMFCONF	displays configuration information for each system management facility (SMF) that is defined on your system Note: For information about viewing the SMF logs in your system, see "Sample SAS Programs" on page 1-4.
TACPORT	displays configuration information for each port on your system

Connections

The connections feature provides realtime data about all TCP and UDP connections on your system. A connection is a path between two protocol applications that provides reliable data stream delivery service. You can use the connections views to see what information is being accessed and to assess application performance.

Table 2-4 describes the views that provide detailed information about all TCP and UDP connections on your system.

Table 2-4 Connection Views

View	Description
TCPCONS	displays TCP connection information for each remote IP address on your system
UDPCONS	displays UDP connection information for each remote IP address on your system
ALLCONS	displays all TCP and UDP connections for each remote IP address on your system

Connections Information

The connections information views display information about all TCP and UDP connections. The views let you quickly see realtime data about the IP stack. You can use these views to see what information is being accessed and to assess application performance. You can also use these views to perform the following line commands:

- drop
- ping
- Traceroute

Dropping a Connection by Using a Line Command

Summary: In this task, you will drop a connection by using the **DR** line command.

Before You Begin

Users who connect to your MVS system through TN3270 or FTP sessions can encounter various problems. For example, they may experience a connection that is hung. You can determine information about a problem connection by using the ping and Traceroute commands. To resolve the problem, you may decide that you need to terminate the connection that is hung. MAINVIEW for IP provides a line command that lets you quickly terminate (or drop) a connection.

Warning! Performing this line command terminates a connection immediately. Anyone who can access the monitor has authority to drop connections. Before you perform this line command, ensure that you have notified the person whose connection you are terminating.

To Perform the DR Line Command from a Connections View

Step 1 From the EZIP Menu (Figure 2-3 on page 2-6), select one of the following types of connections from the Connections section:

- TCP
- UDP
- All

Step 2 Press **Enter**.

Step 3 Navigate the cursor so that it is in the **CMD** field to the left of the connection that you want to terminate.

Step 4 Type **DR** in the **CMD** field, and press **Enter**.

Write-to-operator (WTO) message BMC256615I is displayed to confirm that the DR line command has been performed. A return code of 0 indicates that the connection was terminated successfully.

Pinging a Device by Using a Line Command

Summary: In this task, you will ping a device by using the **P** line command.

Before You Begin

A ping is a diagnostic echo packet that measures and displays the round-trip time and percentage of returned packets. For more information about pings, see “Diagnostics” on page 2-18.

You can ping a device by using one of the following methods:

- Select an IP address that is displayed in the **Ping IPAddr** field of the PCONS view. For more information, see “Pinging a Device” on page 2-20.
- Type a ping command on the command line. For more information, see “Pinging a Device” on page 2-20.
- Perform the **P** line command from a Connections view.

To Perform the P Line Command from a Connections View

Step 1 From the EZIP Menu (Figure 2-3 on page 2-6), select one of the following types of connections from the Connections section:

- TCP
- UDP
- All

Step 2 Press **Enter**.

Step 3 Type **P** in the **CMD** field, and press **Enter**.

The PING view (Figure 2-5) is displayed.

Figure 2-5 PING Information View

```

08JUL2002 16:49:49 ----- INFORMATION DISPLAY -----
COMMAND ==>
CURR WIN ==> 1          ALT WIN ==>
W1 =PING=====MCBSYS1=*=====08JUL2002==16:49:49===MVIP====D===1

Ping Information....

Ping IP addr.....          172.19.1.242
Domain Name.....          cager.bmc.com

Ping Response Times.

Ping Response (sec)..          0.0034

Ping Status.....

Ping Flags (hex).....          4
Ping Status.....          Successful

```

Performing a Traceroute on a Device by Using a Line Command

Summary: In this task, you will perform a Traceroute on a device by using the **TR** line command.

Before You Begin

A Traceroute is a series of pings that progresses outward in incremental hops from the MAINVIEW for IP client to the final destination for which the TRACE was requested. By default, each hop is sent three requests; the response time is determined from these requests.

You can perform a Traceroute on a device by using one of the following methods:

- Select an IP address that is displayed in the **Tracerte IPAddr** field. For more information, see “Performing a Traceroute on a Device” on page 2-22.
- Type a Traceroute command on the command line. For more information, see “Performing a Traceroute on a Device” on page 2-22.
- Perform the **TR** line command from a Connections view.

To Perform the TR Line Command from a Connections View

Step 1 From the EZIP Menu (Figure 2-3 on page 2-6), select one of the following types of connections from the Connections section:

- TCP
- UDP
- All

Step 2 Press **Enter**.

Step 3 Type **TR** in the **CMD** field, and press **Enter**.

The TRACE view (Figure 2-6) is displayed.

Figure 2-6 TRACE Information View

```

09JUL2002 11:02:13 ----- INFORMATION DISPLAY -----
COMMAND ==>
CURR WIN ==> 1          ALT WIN ==>
>W1 =TRACE=====MCBSYS1==*=====09JUL2002==11:02:12====MVIP====D====7
Cur Hop          Hop          Min  Max  Avg  Total Hop  Tracerte
Hop DNS          IPaddr      Rsp  Rsp  Rsp  Hops  Delay  Status
1  gatel9ha1.bmc.com  172.19.2.251    1   1   1    7    1  In progre
2  * NO RESPONSE *   0.0.0.0         0   0   0    0    0
3  fp-us-houl.bmc.com 172.17.19.15    3   8   6    3    0
4  fw-us-houl4.bmc.com 172.17.19.5     1   8   3    0    0
5  Internet-7206.bmc.com 198.207.223.253 3  427 218    2    0
6  * NO RESPONSE *   0.0.0.0         0   0   0    0    0
7  * NO RESPONSE *   0.0.0.0         0   0   0    0    0
    
```

Step 4 If the status in the **Tracerte Status** field is In progress, refresh the data on the TRACE view by pressing **Enter**.

Note: To see the **Tracerte Status** field, scroll right by pressing **F11**.

Diagnostics

MAINVIEW for IP lets you perform actions that provide you with diagnostic information.

- The Ping Information view lets you perform a ping, then displays information about the ping that you have performed. A ping is a diagnostic echo packet that measures and displays the round-trip time of returned packets.

Pings help you determine the following information:

- network connectivity (whether the IP address is considered valid)
 - destination host status (whether the destination host is operational)
 - network loading and speed (how long it takes the replies to return)
 - network errors (percentage of packets that are lost)
- The Traceroute Information view lets you perform a Traceroute, then displays information about the Traceroute that you have performed. Traceroute information helps you pinpoint delays in your network.

A Traceroute is a series of pings that progress outward in incremental hops from the MAINVIEW for IP product address space (PAS) to the final destination for which the TRACE was requested. By default, each hop is sent three requests; the time taken to respond is determined from these requests.

- The Packet Tracing views let you quickly start, stop, or display a trace on a packet. The Packet Tracing views provide all the TCP/IP header and packet data to help you diagnose a problem on your network.
- The Socket Tracing views let you start, stop, or display a trace on a socket. The Socket Tracing views provide detailed information about a socket call, including all socket parameters and return codes.

Note: If you are tracing a packet or a socket and you cancel the product address space (PAS), you may receive an abend.

Table 2-5 describes the views that provide detailed information about pings, packet traces, socket traces, and Traceroutes.

Table 2-5 Diagnostic Views

View	Description
PCONS	lets you perform a ping, then displays information about the ping that you have performed
PKTTRACD	displays details about a packet that has been traced
PKTTRACF	lets you specify the filtering parameters for displaying packet traces
PKTTRACS	lets you start, stop, or display a trace on a packet
SKTTRACD	displays details about a socket that has been traced
SKTTRACF	lets you specify the filtering parameters for displaying socket traces
SKTTRACS	lets you start, stop, or display a trace on a socket
TCONS	lets you perform a Traceroute, then displays information about the Traceroute that you have performed

Pinging a Device

Summary: In this task, you will ping a device.

Before You Begin

You can ping a device by using one of the following methods:

- Select an IP address that is displayed in the **Ping IPAddr** field.
- Type a ping command on a command line.
- Perform the **P** line command from a Connections view. For more information, see “Pinging a Device by Using a Line Command” on page 2-14.

To Select an IP Address that is Displayed in the Ping IPAddr Field

Step 1 From the EZIP Menu (Figure 2-3 on page 2-6), select **Ping Information** from the Diagnostics section, and press **Enter**.

The Ping Information view (PCONS) (Figure 2-7) is displayed.

Figure 2-7 Ping Information Detail View

```

08JUL2002 16:56:23 ----- INFORMATION DISPLAY -----
COMMAND ==>>>                                SCROLL ==>> PAGE
CURR WIN ==>> 1          ALT WIN ==>>
W1 =PCONS=====MCBSYS1==*=====08JUL2002==16:56:23====MVIP====D====8
Domain                Ping                Conn
Name                  IPAddr           Status
cager.bmc.com         172.19.1.242     Establish
esajgig.bmc.com       172.19.84.46     Establish
localhost.bmc.com    127.0.0.1        Establish
BWHITING-5.bmc.com   172.19.133.246   Establish
DWHATLY2.bmc.com     172.25.121.159   Establish
JOTT-NT4.bmc.com     172.25.121.183   Establish
MKARIER2.bmc.com     172.25.121.163   Establish
MNGO.bmc.com         172.25.107.28    Establish

```

- Step 2** Select the IP address of the device that you want to ping from the **Ping IPAddr** field, and press **Enter**.

The PING view (Figure 2-5 on page 2-15) is displayed.

To Type a Ping Command on a Command Line

- Step 1** Type one of the following commands on a command line:

- PING *IPAddr* *
- PING * *domainname*
- PING *domainname*

The asterisk (*) represents an unknown IP address or an unknown domain name. *IPAddr* is the IP address of the device that you want to ping. *domainname* is the domain name of the device that you want to ping.

- Step 2** Press **Enter**.

The PING view (Figure 2-5 on page 2-15) is displayed.

Performing a Traceroute on a Device

Summary: In this task, you will perform a Traceroute on a device.

Before You Begin

You can perform a Traceroute on a device by using one of the following methods:

- Select an IP address that is displayed in the **Tracerte IPAddr** field.
- Type a Traceroute command on a command line.
- Perform the **TR** line command from a Connections view. For more information, see “Performing a Traceroute on a Device by Using a Line Command” on page 2-16.

Note: The data that is displayed on the Tracerte Information view may not be complete data or realtime data. The Traceroute task is asynchronous; because a Traceroute may take several minutes to complete, MAINVIEW for IP may display data while the Traceroute is running. Data that is displayed may not be complete, or some hop data that is displayed may not be fresh. To determine the status of the Traceroute request, see the **Tracerte Status** field.

To Select an IP Address that is Displayed in the Tracerte IPAddr Field

- Step 1** From the EZIP Menu (Figure 2-3 on page 2-6), select **Tracerte Information** from the Diagnostics section, and press **Enter**.

The Traceroute Information view (TCONS) (Figure 2-8) is displayed.

Figure 2-8 Traceroute Information Detail View

```

08JUL2002 16:56:44 ----- INFORMATION DISPLAY -----
COMMAND ==>>
CURR WIN ==>> 1          ALT WIN ==>>
W1 =TCONS=====MCBSYS1==*=====08JUL2002==16:56:44====MVIP=====D====8
Domain                Tracerte                Conn
Name                  IPAddr                  Status
cager.bmc.com         172.19.1.242            Establish
esajgig.bmc.com       172.19.84.46            Establish
localhost.bmc.com     127.0.0.1               Establish
BWHITING-5.bmc.com    172.19.133.246          Establish
DWHATLY2.bmc.com      172.25.121.159          Establish
JOTT-NT4.bmc.com      172.25.121.183          Establish
MKARIER2.bmc.com      172.25.121.163          Establish
MNGO.bmc.com          172.25.107.28           Establish

```

- Step 2** Select the IP address of the device that you want to trace from the **Tracerte IPAddr** field, and press **Enter**.

The TRACE view (Figure 2-6 on page 2-17) is displayed, showing information about the number of hops that were required to trace the IP address, and the time (in milliseconds) that was required to perform each hop.

- Step 3** To refresh the data on the TRACE view, press **Enter**.

To access more information about the Traceroute, see “Accessing More Traceroute Information” on page 2-25.

To Type a Traceroute Command on a Command Line

Step 1 Type one of the following commands on a command line:

- `TRACE IPAddr *`
- `TRACE * domainname`
- `TRACE domainname`

The asterisk (*) represents an unknown IP address or an unknown domain name. *IPAddr* is the IP address of the device that you want to trace. *domainname* is the domain name of the device that you want to trace.

Step 2 Press **Enter**.

The TRACE view (Figure 2-6 on page 2-17) is displayed. To access more information about the Traceroute, see “Accessing More Traceroute Information” on page 2-25.

Accessing More Traceroute Information

Summary: In this task, you will drill down in the TRACE view to access more information about a specific hop on a Traceroute.

To drill down to more information about a Traceroute, perform the following steps:

Step 1 From the TRACE view (Figure 2-6 on page 2-17), position the cursor over the hop in the **Current Hop** field for which you want to see more information.

Tip: To see ping information for the hop, position the cursor over the **Hop IPaddr** field and press **Enter**. The PING view (Figure 2-5 on page 2-15) is displayed.

Step 2 Press **Enter**.

More Traceroute information (TRACEDET) (Figure 2-9) is displayed.

Figure 2-9 Traceroute Details

```

09JUL2002 11:02:53 ----- INFORMATION DISPLAY -----
COMMAND ==>>                                SCROLL ==>> PAGE
CURR WIN ==>> 1          ALT WIN ==>>
W1 =TRACE====TRACEDET=MCBSYS1==*=====09JUL2002==11:02:48====MVIP=====D=====1

  Tracerte Information....

Tracerte IP addr.....          WWW.BMC.COM
Domain Name.....              *
Total Hops.....
Hop Delay (ms).....           2

  Tracerte Hop Analysis...

Hop Sequence Number.....      5
Hop IP addr.....              198.207.223.253
Hop Domain Name.....          Internet-7206.bmc.com

  Tracerte Response Times.

Min Response (ms).....        3
Max Response (ms).....        427
Avg Response (ms).....        218

```

Starting a Packet Trace

Summary: In this task, you will start a packet trace.

Note: If you are tracing a packet (or a socket) and you cancel the product address space (PAS), you might encounter an abend. BMC Software recommends that you shut down the PAS normally *or* stop the trace.

To start tracing a packet, perform the following steps:

Step 1 From the EZIP Menu (Figure 2-3 on page 2-6), select **Packet Tracing** from the Diagnostics section, and press **Enter**.

The Packet Tracing view (PKTTRACS) (Figure 2-10) is displayed.

Figure 2-10 Packet Tracing View

```

03JUN2002 15:13:38 ----- INFORMATION DISPLAY -----
COMMAND ==>
CURR WIN ==> 1          ALT WIN ==>
W1 =PKTTRACS=====MCBSYS1==*=====03JUN2002==15:13:38====MVIP====D====1
Command Stack  Trace      Protocol IP          Src  Dest
----- Name      Status   Type      Address          Port  Port
          TCPIP    NOT ACTIVE

```

Step 2 To trace all packets, type **STA** or **START** in the **Command** field and press **Enter**.

Tip: Before pressing **Enter**, you can limit the parameters of the packet trace by typing an entry in one or more of the following fields:
Protocol Type, IP Address, Src Port, or Dest Port.

Message TACI9210E is displayed to indicate that the trace has been activated.

Step 3 Press **Enter** to return to the PKTTRACS view.

ACTIVE is displayed in the **Trace Status** field.

Stopping a Packet Trace

Summary: In this task, you will stop a packet trace.

To stop tracing a packet, perform the following steps:

Step 1 On the PKTTRACS view (Figure 2-10 on page 2-26), verify that **ACTIVE** is displayed in the **Trace Status** field.

Step 2 In the **Command** field, type **STO** or **STOP**, and press **Enter**.

Message TACI9211E is displayed to indicate that the trace has been terminated.

Step 3 Press **Enter** to return to the PKTTRACS view.

NOT ACTIVE is displayed in the **Trace Status** field.

Displaying a Packet Trace

Summary: In this task, you will display a packet trace.

To display a packet that has been traced, perform the following steps:

Step 1 From the PKTTRACS view (Figure 2-10 on page 2-26), type **D** in the **Command** field and press **Enter**.

The Packet Tracing Filters (PKTTRACF) view (Figure 2-11) is displayed.

Figure 2-11 Packet Tracing Filters View

```

06JUN2002 12:16:38 ----- INFORMATION DISPLAY -----
COMMAND ==>>                                SCROLL ==>> PAGE
CURR WIN ==>> 1          ALT WIN ==>>
>W1 =PKTTRACF=====MCBSYS1==*=====06JUN2002==12:16:38====MVIP====D====1
Command Stack  Local/ Start Date  Start Time  Stop Date  Stop Time
----- Name   GMT    mm/dd/yy   hh:mm:ss.xxxx  mm/dd/yy   hh:mm:ss.xxxx
          TCPIP  GMT
  
```

Step 2 To display information about the first 5000 traced packets, type **D** in the **Command** field and press **Enter**.

Tip: To display information about a packet that was traced at a particular time or on a particular date, type an entry in one or more of the following field: **Start Date**, **Start Time**, **Stop Date**, or **Stop Time**.

To display the information in Greenwich Mean Time, type **GMT** in the **Local/GMT** field. To display the information in local time, type **Local** in the **Local/GMT** field.

The Packet Tracing Details (PKTTRACD) view (Figure 2-12) is displayed.

Figure 2-12 Packet Tracing Details View

```

09JUL2002 11:07:00 ----- INFORMATION DISPLAY -----
COMMAND ==>
CURR WIN ==> 1          ALT WIN ==>
+W1 =PKTTRACD=====MCBSYS1=*=====09JUL2002==11:06:59====MVIP====D=2134

```

Date	Time	Pkt Len	Source IPAddr	Src Port	Dest IPAddr	Dest Port	Prot Type
07/09/02	16:04:41.7410	40	10.10.10.10	2301	255.255.255.255	2301	UDP
07/09/02	16:04:41.7767	40	172.19.133.195	2301	255.255.255.255	2301	UDP
07/09/02	16:04:41.7985	104	172.17.4.19	1051	255.255.255.255	14000	UDP
07/09/02	16:04:41.8062	104	172.17.4.19	1033	255.255.255.255	14000	UDP
07/09/02	16:04:41.8257	567	172.19.84.46	30080	172.19.133.246	3644	TCP
07/09/02	16:04:41.8360	78	172.17.3.140	137	172.17.255.255	137	UDP
07/09/02	16:04:41.9010	583	172.19.202.250	138	172.19.255.255	138	UDP
07/09/02	16:04:41.9100	583	172.19.202.250	138	172.19.255.255	138	UDP
07/09/02	16:04:41.9199	565	172.19.202.250	138	172.19.255.255	138	UDP
07/09/02	16:04:41.9335	583	172.19.202.250	138	172.19.255.255	138	UDP
07/09/02	16:04:41.9625	583	172.19.202.250	138	172.19.255.255	138	UDP
07/09/02	16:04:41.9700	40	172.19.133.246	3644	172.19.84.46	30080	TCP
07/09/02	16:04:41.9724	583	172.19.202.250	138	172.19.255.255	138	UDP
07/09/02	16:04:41.9790	78	172.19.136.221	137	172.19.255.255	137	UDP
07/09/02	16:04:41.9801	583	172.19.202.250	138	172.19.255.255	138	UDP
07/09/02	16:04:41.9847	52	172.19.16.86	7474	172.19.255.255	7474	UDP
07/09/02	16:04:41.9908	419	172.19.202.250	138	172.19.255.255	138	UDP
07/09/02	16:04:42.0218	229	172.19.0.66	138	172.19.255.255	138	UDP

Accessing More Packet Trace Information

Summary: In this task, you will drill down in the PKTTRACD view to access more information about a specific packet that has been traced.

To drill down to more information about a packet that has been traced, perform the following steps:

Step 1 From the PKTTRACD view (Figure 2-12 on page 2-30), position the cursor over the date of the packet for which you want to see more information.

Step 2 Press **Enter**.

The Packet Tracing Details (PKTTRACd) view (Figure 2-13) is displayed.

Figure 2-13 More Packet Tracing Details View

```

09JUL2002 11:08:29 ----- INFORMATION DISPLAY -----
COMMAND ==>                                SCROLL ==> PAGE
CURR WIN ==> 1          ALT WIN ==>
W1 =PKTTRACD=PKTTRACd=MCBSYS1==*=====09JUL2002==11:06:59====MVIP====D====1

Link Name..... GIG1
Device Type..... Ipaenet
Date..... 07/09/02
Time..... 16:04:41.825747

** IP Header **
Source IPAddr.... 172.19.84.46
Dest IPAddr..... 172.19.133.246
IP Version..... 4
Packet Len..... 567
TOS..... 0
Ident Nbr..... 601
Frag Offset..... 0
Time to Live..... 60
Checksum..... 4475
Header Len..... 20
  Offset.... ----- IP Header -----
00000000.... 45000237 06010000 3C064475 AC13542E
00000010.... AC1385F6

```

To see more pages of the PKTTRACd view, scroll down by pressing **F8**.

Viewing Packet Details

Summary: In this task, you will drill down in the PKTTRACd view to access more information about a specific packet that has been traced.

To drill down to more information about a packet that has been traced, perform the following steps:

Step 1 From the PKTTRACd view (Figure 2-13 on page 2-31), position the cursor over the item (**IP Header**, **Protocol Hdr**, or **Packet Data**) for which you want to see more information.

Step 2 Press **Enter**.

More packet details (Figure 2-14) are displayed.

Figure 2-14 More Packet Details View

```

09JUL2002 11:09:50 ----- INFORMATION DISPLAY -----
COMMAND ==>>
CURR WIN ==>> 1          ALT WIN ==>>
W1 =PKTTRACD=PKTTRACd=MCBSYS1==*=====09JUL2002==11:06:59====MVIP====D====1

Len      527

----- Data -----      ---- EBCDIC ----      ---- ASCII ----
000  48545450 2F312E31 20323030 204F4B0D  ...&.....|..  HTTP/1.1 200 OK.
010  0A536572 7665723A 20576562 53706865  .....      .Server: WebSphe
020  72652041 70706C69 63617469 6F6E2053  .....%../?>.. re Application S
030  65727665 722F342E 300D0A43 6F6E7465  .....?>..   erver/4.0..Conte
040  6E742D54 7970653A 20746578 742F6874  >.....      nt-Type: text/ht
050  6D6C0D0A 436F6E74 656E742D 4C616E67  _%...?>...</>. ml..Content-Lang
060  75616765 3A20656E 0D0A5472 616E7366  ./.....>.../>.. uage: en..Transf
070  65722D45 6E636F64 696E673A 20636875  ....>?..>..... er-Encoding: chu
080  6E6B6564 0D0A0D0A 3134390D 0A3C4854  >.....      nked....149..<HT
090  4D4C3E0A 3C484541 443E0A3C 5449544C  (<.....<   ML>.<HEAD>.<TITL
0A0  453E0A41 20736572 766C6574 20696E63  .....%.....>. E>.A servlet inc
0B0  6C756465 6420696E 20616E6F 74686572  %.....>./?.... luded in another
0C0  20736572 766C6574 0A3C2F54 49544C45  ....%.....<.   servlet.</TITLE
0D0  3E0A3C48 4541443E 0A0A3C42 4F445920  .....|...   >.<HEAD>..<BODY
0E0  4247434F 4C4F523D 23303046 30303E0A  ...|<|.....   BGCOLOR=#00F00>..
0F0  0A3C424F 44593E0A 41747465 6D707469  ...|....._...   .<BODY>..Attempti

```

To see more pages of the PKTTRACd view, scroll down by pressing **F8**.

Clearing Packet Trace Entries

Summary: In this task, you will clear (or delete) the packet trace entries.

Packet trace entries are stored in a table. To clear packet trace table entries, perform the following steps:

Step 1 On the PKTTRACS view (Figure 2-10 on page 2-26), verify that `NOT ACTIVE` is displayed in the **Trace Status** field.

Step 2 In the **Command** field, type **DEL** or **DELETE**, and press **Enter**.

Message TACI9215E is displayed to indicate that the trace table entries have been cleared.

Step 3 Press **Enter** to return to the PKTTRACS view.

Dynamic Virtual IP Addresses

A virtual IP address (VIPA) refers to an Internet address on an OS/390 or z/OS host that is not associated with a physical adapter. A Dynamic VIPA (DVIPA) is a virtual Internet address that can move dynamically to other TCP/IP stack members in a sysplex.

A VIPA is configured on a TCP/IP stack. When you configure multiple paths to a stack by using VIPA *and* conventional IP addresses, you can eliminate hardware and transmission media as single points of failure for many connections. If a TCP/IP or its hosting operating system suffers an outage (for example, a power failure), you can move the VIPA to another TCP/IP stack. DVIPA automatically moves a VIPA to other TCP/IP stack members in a sysplex.

MAINVIEW for IP provides the Dynamic VIPA views that let you monitor the DVIPAs on your OS/390 or z/OS host. These views display details about DVIPA configuration, DVIPA routing connection tables, and DVIPA destination port tables. You can use these views to identify the distribution of your TCP/IP resources that are attached to OS/390 or z/OS TCP/IP stacks.

Table 2-6 describes the views that provide detailed or summary information about your DVIPAs.

Table 2-6 Dynamic VIPA Views

View	Description
VIPACFG	provides access to the VIPACFG Menu
VIPACFG1	displays VIPA backup information
VIPACFG2	displays VIPA definition information
VIPACFG3	displays VIPA range information
VIPACFG4	displays VIPA distribution information
VIPACFG5	displays VIPA service level agreement policy information
VIPACONN	displays all current connections that are being distributed by the distributing stack
VIPADYN	displays general information about DVIPA
VIPAPORT	displays which target stacks are available with the server applications ready

FTP Servers

File Transfer Protocol (FTP) is a method for exchanging files between computers on the Internet. FTP can be used to transfer Web page files to a computer that acts as a server for everyone on the Internet. FTP can also be used to download programs and other files to your computer from other servers.

MAINVIEW for IP provides the FTP Servers views that let you monitor traffic on your FTP servers. These views display details about FTP files, IP addresses, and user IDs.

Table 2-7 describes the views that provide detailed or summary information about FTP.

Table 2-7 **FTP Servers Views**

View	Description
TACFTPF	displays FTP file information
TACFTPI	displays FTP IP address information
TACFTPU	displays FTP user ID information

Interfaces

MAINVIEW for IP lets you see information about interfaces on your network.

- The Network Devices view displays information about network devices that are defined to the TCP/IP stack. You can quickly see the device name, type, status, link count, and whether the device is multicast capable.
- The Network Links view displays information about network links. You can use the network links view to see data traffic counts and the status of the link. This information lets you see suspicious performance information and helps you identify performance problems.
- The OSA Cards menu provides quick access to views that display information about Open Systems Adapter (OSA) devices. These views let you see OSA configuration information, utilization statistics, network device details, network link details, and Ethernet-like statistics.

Note: Before using the OSA Cards menu, ensure that you have completed the required customization tasks and that your operating system meets the minimum requirements. Customization tasks and minimum requirements are described in the *MAINVIEW for IP Customization Guide*.

Table 2-8 describes the views that provide detailed information about your network interfaces.

Table 2-8 **Interface Views**

View	Description
TACDEVS	displays information about network devices that are defined to the IP stack
TACLNKS	displays information about network links
TACOSA3	displays Ethernet-like statistics
TACOSAC	displays OSA configuration information
TACOSAD	displays OSA device information
TACOSAL	displays OSA link information
TACOSAU	displays OSA utilization information

IP Resource Links

MAINVIEW for IP provides access to MAINVIEW for UNIX System Services and MAINVIEW for WebSphere Application Server through hyperlinks. Table 2-9 shows where to find the hyperlink and describes the information that can be accessed when the hyperlink is activated.

Table 2-9 IP Resource Links

MAINVIEW for IP View	Field Name	Resource Link	Resource Link Description
JOBRESPS	USS Resource	MAINVIEW for UNIX System Services	summary of resource usage for a specific UNIX System Services address space based on processes that are running in that address space
TACCACHE	Web Server	MAINVIEW for WebSphere Application Server	summary of WebSphere Application Server performance statistics

Hyperlinks

A hyperlink is one or more commands that are associated with a particular field and the conditions under which those commands are issued. When you activate a hyperlink, the underlying command is issued against the resource where the cursor is positioned. Hyperlinks to other related views are displayed in different colors or are highlighted for a monochrome monitor.

When you activate a hyperlink that goes to another view or form, the output replaces the view in the current window by default or the output is displayed in an alternate window.

For sample instructions on how to activate a hyperlink, see “Activating the Web Server Hyperlink” on page 2-38. For more information about hyperlinks, see *Using MAINVIEW*.

Activating the Web Server Hyperlink

Summary: In this task, you will activate the hyperlink that accesses WebSphere Application Server performance statistics.

Before You Begin

To activate the hyperlink for a resource, the resource must be installed at your site. To access WebSphere Application Server performance statistics, MAINVIEW for WebSphere Application Server must be installed at your site.

To Activate the Web Server Hyperlink

Step 1 Access the Cache Information view (TACCACHE) (Figure 2-15).

Figure 2-15 Cache Info (WebSphere) View

```

13FEB2002 10:48:38 ----- INFORMATION DISPLAY -----
COMMAND ==>
CURR WIN ==> 1          ALT WIN ==>
W1 =TACCACHE=====BJWESAJ==*=====13FEB2002==10:48:38====MVIP====D====2
Cache  Web      Listen Max    Curr  Number Conns  Cache  Cache
Client Server  Port   Size   Size  Conns  Timeout Hits  Misses
IMVWEBQA IMVWEBQA 11180 25000  7  23269    0    0    15
IMWEBSRV IMWEBSRV   80  25000  0    2     0    0    2
    
```

Step 2 Position the cursor over the name of a client that is displayed in the **Web Server** field for which you want to see performance information.

Tip: To see more cache information for the client, position the cursor over the client name in the **Cache Client** field and press **Enter**. The Cache detail view (TACCACHD) is displayed.

Step 3 Press **Enter**.

The MAINVIEW for WebSphere Application Server WASPERF summary view (Figure 2-16) is displayed.

Figure 2-16 WASPERF Summary View

```

13FEB2002 10:49:53 ----- INFORMATION DISPLAY -----
COMMAND ==>>
CURR WIN ==>> 1          ALT WIN ==>>
>W1 =WASPERF=====BJWESAJ==*=====13FEB2002==10:49:52====MVWEB====D====2
Requested      File  Cumulative Average  HTTPServ HTTPServ Client
File           Hits  Seconds  Seconds  Jobname  ASID   Request
TestMenu.html  1    0.999955  0.999955  IMVWEBQA  F2    GET /TestMe
TestMenu.html  1    1.999975  1.999975  IMVWEBQA  34    GET /TestMe

```

Routers

MAINVIEW for IP provides the information that you need to monitor the network control path.

- The Define view lets you add or change SNMP parameters dynamically. The SNMP Data views display TCP, UDP, IP, system, and interface router information. You can use these views to see detailed and summary information about router performance.
- The Network Routes Information view displays information about network routes that are defined on a TCP/IP stack.

Table 2-10 describes the views that provide detailed or summary information about network routes and router performance.

Table 2-10 Router Views

View	Description
SNMPDEF	lets you specify every IP node that you want to monitor
SNMPIF	displays SNMP information by interface host name
SNMPIP	displays SNMP information by IP host name
SNMPSYS	displays SNMP information by system host name
SNMPTCP	displays SNMP information by TCP host name
SNMPUDP	displays SNMP information by UDP host name
TACROUT	displays information about network routes that are defined on an IP stack

SNMP Information

SNMP views display data that was collected in the last interval. To access realtime data, you can drill down.

If you added or changed the SNMP parameters by using the SNMPDEF view, and you select an SNMP Data view, the fields are refreshed with new data. For instructions on how to define SNMP parameters, see “Defining SNMP Parameters” on page 2-41.

Defining SNMP Parameters

Summary: In this task, you will specify the IP nodes that you want monitored through MAINVIEW for IP.

Before You Begin

By using the Define view, you can update SNMP parameters dynamically for each IP node that you want monitored through MAINVIEW for IP.

Note: Information in the SNMP parameter file is case sensitive. If the Define view does not implement your request dynamically, verify that you entered the information correctly.

A sample SNMP parameter file is provided with the distribution tape in member *hilevel.BBSAMP(TACSNM)*. For more information about the parameter file and its syntax rules, see the *MAINVIEW for IP Customization Guide*.

To Define SNMP Parameters

- Step 1** From the EZIP Menu (Figure 2-3 on page 2-6), select **Define** from the Routers section, and press **Enter**.

The Define view (SNMPDEF) (Figure 2-17) is displayed.

Figure 2-17 SNMP Define View

```

08JUL2002 12:34:30 ----- INFORMATION DISPLAY -----
COMMAND ==>>                                SCROLL ==>> PAGE
CURR WIN ==>> 1          ALT WIN ==>>
>W1 =SNMPDEF=====MCBSYS1==*=====08JUL2002==12:34:30====MVIP====D====4
Cmd Host                                IP                                Community
--- Name                                Address                             Name
$DEFAULT                                000.000.000.000 public
ipor12p.houlab.bmc.com                  192.168.1.253 public
ipor321.houlab.bmc.com                  192.168.3.253 IPO
UNKNOWN                                  192.168.2.253 public

```

- Step 2** To add an IP address to the list of nodes that are monitored, type **ADD** in the **Cmd** field.

Tip: To delete an IP address from the list, type **DEL** in the **Cmd** field.

- Step 3** Move the cursor to the **IP Address** field and type the IP address of the node that you want to monitor.

Tip: If you know the host name but not the IP address, you can type the host name in the **Host Name** field. When defining the SNMP parameters, you can add or delete the host name *or* the IP address.

- Step 4** Press **Enter**.

Service Levels

MAINVIEW for IP provides the information that you need to ensure that you are meeting your service level agreements (SLA). An SLA is an essential tool for building accountability into the provider/customer relationship and for measuring the provider's performance. An SLA policy often lists services (and service levels) that users should expect, describes user responsibilities in addressing problems, and defines problem resolution paths.

When you need information about your Web servers, access the Cache Information view. This view displays the network status of the local host and provides statistics about Fast Response Cache Accelerator. The statistics are displayed for each listening socket that is configured for Cache Accelerator support.

To analyze application access availability, to monitor service level events, and to ensure that you are meeting your SLA, access the Service Level Agreement Policy view.

Table 2-11 describes the views that provide detailed information about your service levels.

Table 2-11 Service Level Views

View	Description
TACCACHE	displays Fast Response Cache Accelerator statistics, provides information for Web cache analysis, and provides a hyperlink to MAINVIEW for WebSphere Application Server
TACSLAP	displays SLA policy statistics
EZIPRESP	provides menu access to response time information
EZIPSUBN	provides menu access subnet response time summary information

Storage

For realtime statistics about your buffer pools and storage usage, access the Communication Storage Manager (CSM) Buffer Pools view, the Virtual Telecommunications Access Method (VTAM) Buffer Pools view, or the Common Storage Area (CSA) Information view. These views let you monitor and manage the storage allocations that are required to run your system at optimum levels.

Table 2-12 describes the views that provide detailed information about your buffer pools and storage usage.

Table 2-12 Storage Views

View	Description
CSM	displays storage allocation and CSM buffer pool information
VTMBUFF	displays VTAM buffer pool statistics
VTMBUFQ	displays quick view of VTAM buffer pool statistics
CSAU	displays CSA usage and limit information

Traffic/Response Times

MAINVIEW for IP provides the information that you need to monitor the amount of data which is transmitted by your applications and through your network.

MAINVIEW for IP also provides response time statistics by job name, port, and connections. By using the Response Times information views, you can access the information that you need to identify delays in your network. Response times are reported in milliseconds.

When you need throughput information about remote applications, connections with applications, or traffic counts, access the Application information and detail views.

When you need summary throughput information for a network by class subnet (A, B, or C), access the Class Subnet Byte Count Summary views. These views display throughput count information such as bytes in, bytes out, retransmissions, duplicate acknowledgements, inbound datagrams and outbound datagrams.

When you need summary response time statistics for a network by class subnet (A, B, or C), access the Class Subnet Response Time Summary views. These views display response time information such as bytes in, bytes out, and round-trip time.

Table 2-13 describes the views that provide detailed or summary information about traffic and response times on your system.

Table 2-13 Traffic/Response Time Views

View	Description
CONNRESP	displays connection response times
JOBRESP	displays jobname response times
JOBRESPTS	displays application response time summary and provides a hyperlink to MAINVIEW for UNIX System Services
PORTRSPP	displays port response times
PORTRSPS	displays port response time summary
CLSxCONS	displays subnet byte count summaries x is class A, B, or C.
CLSxRESP	displays subnet response time summaries x is class A, B, or C.

Tools and Menus

The Tools and Menus section on the EZIP Menu (Figure 2-4 on page 2-7) provides you with the following options:

- historical data sets
- select view
- return

Historical Data Sets

MAINVIEW for IP lets you recreate the operating environment as it existed during a previous time period. This option, historical data sets, stores information on your operating environment at the end of each interval so that you can compare the current performance with a previous performance. This comparison lets you determine whether your system is working normally or whether there is a problem.

For more information about using the historical data sets feature, see Chapter 3, “Displaying Historical Data.”

Select View

To display a list of view names and descriptions of the views that are available in MAINVIEW for IP, access the Select View option.

Return

You can use the Return option to display the previous view.

Exiting from MAINVIEW for IP

When you are finished working with MAINVIEW for IP, you can return to the MAINVIEW Selections Menu by issuing one of the following commands from the command list:

- Quit
- RETURN

Chapter 3 Displaying Historical Data

This chapter provides information about the historical data feature. Historical data lets you look at system data as it existed an hour ago, yesterday, last week, last month, or last year.

Note: For instructions on how to generate historical performance reports, see *Using MAINVIEW*.

This chapter contains the following sections:

Overview	3-2
Data Availability	3-3
TIME Command	3-4
Viewing Historical Data in the JOBNAME Response Times View	3-5
Displaying the Intvl Time Field	3-10
Moving between Timeframes.	3-11
Time and Duration Fields	3-12

Overview

Historical data lets you recreate the operating environment as it existed during a previous timeframe so that you can compare the current performance with a previous performance. This comparison lets you determine whether your system is working normally or whether there is a problem.

Historical data consists of your data from a specified recent interval and its preceding intervals. Using the TIME command, you can specify intervals from any timeframe for which data exists on your system. You can also use certain fields to determine when the data was collected and to hyperlink to particular timeframes.

For information about the historical database and how it operates in the MAINVIEW environment, see the *MAINVIEW Administration Guide*.

Note: For instructions on how to generate historical performance reports, see *Using MAINVIEW*.

Data Availability

When you need historical data, you must ensure that the data is available in one of the historical data sets that has been allocated.

To determine whether data has been recorded to historical data sets, and to view a list of allocated historical data sets, type **DSL** on the command line. **DSL** (Figure 3-1) is displayed.

Figure 3-1 DSL View

```

28NOV2001 15:16:17 ----- INFORMATION DISPLAY -----
COMMAND ==>                                     SCROLL ==> PAGE
CURR WIN ==> 1           ALT WIN ==>
>W1 =DSL-----VXGSI=====28NOV2001==15:16:17====MVIP====D====3
C DDNAME   From Date  Time  To Date   Time  Rec Status Pending  Data set name
-----
HISTDS00 14NOV2001  15:43 28NOV2001 15:16 Yes Active ***** TAC20.SYSN.HIS
HISTDS02                                     Yes Closed ***** TAC20.SYSN.HIS
HISTDS01                                     Yes Closed ***** TAC20.SYSN.HIS

```

BMC Software recommends that you check **DSL** before using the **TIME** command. When you specify the **TIME** command for an unavailable date and time, an error message is displayed.

Data from recording intervals between **From Date** and **To Date** may not be available for any of the following reasons:

- Data was not collected.
- Data is offline.
- Data was overwritten by new data.
- The data set has an error.

If you do not see the date and/or time that you want on the DSLIST view, the data set that you need may have been archived on tape or in an offline data set, or the data may have been purged. To determine whether the data was archived or purged, see your product administrator. (If you are the administrator, see the *MAINVIEW Administration Guide*).

TIME Command

You can use the TIME command to specify the intervals of historical data that you want to display. The TIME command lets you display data as it existed at the end of one interval. To see data that spans a greater timeframe, use the TIME duration parameter with the date and time parameters.

For detailed information about using the TIME command, the syntax of the command, and examples of different uses of the TIME command, see *Using MAINVIEW*.

Viewing Historical Data in the JOBNAME Response Times View

Summary: In this task, you will use the TIME command to view historical data for the TCPCONS Response Times view.

Before You Begin

Before viewing historical data, you must perform the following tasks:

- Specify the timeframe for which you want to collect data.
- Ensure that yesterday's date and time are contained in one of the allocated historical data sets by displaying the DSLIST.

For instructions on specifying the timeframe or on displaying the DSLIST, see *Using MAINVIEW*.

To View Historical Data

Step 1 Display the TCPCONS view in Window 1.

Step 2 Open a second window:

2.A On the command line, type **HS**.

2.B Position the cursor partway down the screen, where you want the next view to appear, and press **Enter**.

The screen splits horizontally, as shown in Figure 3-2.

Figure 3-2 TCPCONS with an Open Window

```

28NOV2001 15:24:20 ----- INFORMATION DISPLAY -----
COMMAND ==>>
CURR WIN ==>> 2          ALT WIN ==>>
>W1 -TCPCONS-----VXGSYSI--*-----28NOV2001--15:23:33---MVIP----U---58
CMD Remote          Interval  Intvl Remote Local          Local Bytes  By
--- IPAddr         Date----- Time- Port  IPAddr          Port  In    Ou
172.25.89.4        28NOV2001  15:23  1282 172.17.4.115    23    2624
172.25.10.40       28NOV2001  15:23  1237 172.17.4.115    23    6481  1
172.19.135.111     28NOV2001  15:23  3174 172.19.2.45     5568   430
172.19.135.111     28NOV2001  15:23  3222 172.19.2.45     900   212589  4
172.19.135.111     28NOV2001  15:23  3225 172.19.2.45     5568   868
172.19.135.111     28NOV2001  15:23  3224 172.19.2.45     5553  12924
172.19.135.111     28NOV2001  15:23  3170 172.19.2.45     900    88
172.19.135.111     28NOV2001  15:23  2327 172.19.2.45     23    71502 18
T2 =====

```

In the window information line, the current time is displayed as 15:23.

- Step 3** Display TCPCONS in Window 2 by typing **TCPCONS** on the command line, and pressing **Enter**.
- Step 4** On the command line, type **TIME** to set the timeframe for Window 2.

The SET TIME FRAME dialog box (Figure 3-3) is displayed.

Figure 3-3 SET TIME FRAME Dialog

```

----- SET TIME FRAME -----
COMMAND ==>

Requested Time Frame:
End Date ==> *           (*, =, or ddmmmyyyy)
End Time ==> *           (*, =, or hh:mm)
Duration ==> 1I         (*, =, NEXT, PREV, TODAY, MONTH,
                        nnnnI, nnnnM, nnnnH, nnnD, or nnW)
DOW Mask ==> EVERYDAY   (EVERYDAY, WEEKDAYS, WEEKENDS)
TOD Mask ==> ALLDAY     (ALLDAY, PRIMESHIFT, SWINGSHIFT,
                        GRAVEYARDSHIFT)

Data in the Requested Time Frame:
Interval ==> 1M         (Length, in minutes, of one interval)
End Date ==> 28NOV2001  (End date of data)
End Time ==> 15:24      (End time of data)
Duration ==> 1M         (Minutes spanned by data)
DOW Mask ==> EVERYDAY   (Day-of-week mask)
TOD Mask ==> ALLDAY     (Time-of-day mask)

Type END to set the window's requested time frame
Type CANCEL to quit without setting

```

Step 5 Type 2D in the **Requested Time Frame: Duration** field to display the historical data for a two-day timeframe.

Step 6 To save your changes and return to the view (Figure 3-4), press **PF3**.

The interval information is displayed in Window 2. You can customize the order in which the data is displayed by using the **CUST** command. In this example, the data is displayed by remote IP addresses in descending order.

Figure 3-4 JOBRESP in Two Timeframes

```

28NOV2001 15:27:19 ----- INFORMATION DISPLAY -----
COMMAND ==>> SCROLL ==>> PAGE
CURR WIN ==>> 2 ALT WIN ==>>
>W1 -TCPCONS-----VXGSYSI--*-----28NOV2001--15:26:36---MVIP---U---60
CMD Remote Interval Intvl Remote Local Local Bytes By
--- IPAddr Date----- Time- Port IPAddr Port In Ou
172.25.89.4 28NOV2001 15:26 1282 172.17.4.115 23 2630
172.25.10.40 28NOV2001 15:26 1237 172.17.4.115 23 6487 1
172.19.135.111 28NOV2001 15:26 3224 172.19.2.45 5553 12924
172.19.135.111 28NOV2001 15:26 3173 172.19.2.45 5553 258
172.19.135.111 28NOV2001 15:26 3222 172.19.2.45 900 212589 4
172.19.135.111 28NOV2001 15:26 3170 172.19.2.45 900 88
172.19.135.111 28NOV2001 15:26 2327 172.19.2.45 23 72433 18
172.19.135.111 28NOV2001 15:26 3174 172.19.2.45 5568 430
>H2 =TCPCONS=====VXGSYSI==*=====28NOV2001==15:27=275M==MVIP=====U=6060
CMD Remote Interval Intvl Remote Local Local Bytes By
--- IPAddr Date----- Time- Port IPAddr Port In Ou
172.25.89.4 28NOV2001 13:15 1282 172.17.4.11 23 2630
172.25.89.4 28NOV2001 11:04 1282 172.17.4.115 23 2630
172.25.89.4 28NOV2001 15:23 1282 172.17.4.115 23 2630
172.25.89.4 28NOV2001 10:58 1282 172.17.4.115 23 2630
172.25.89.4 28NOV2001 15:27 1282 172.17.4.115 23 2630
172.25.89.4 28NOV2001 12:59 1282 172.17.4.115 23 2630
172.25.89.4 28NOV2001 11:24 1282 172.17.4.115 23 2630

```

This view displays two versions of TCPCONS: one as the system exists and one as it existed at a date and time in the past. With the two timeframes displayed in the same screen, you can easily compare them to determine whether a perceived problem is a regular occurrence or whether it is an abnormality.

Note: The window status indicator for Window 2 has changed from >W2 to >H2. *H* indicates historical data.

Step 7 Press **Enter**.

The data in Window 1 is updated; the data in Window 2 is not. Historical data cannot be updated because it represents the system at a fixed point in time.

Note: When you have used the TIME command or the SET TIME FRAME dialog box for a window, all views sent to that window reflect the system as it existed at the date and time that you specified. The views reflect the system for the date and time that you specified until you issue another TIME command, until the window is closed, or until you press **PF3**.

For more examples of using the TIME command, see *Using MAINVIEW*.

Displaying the Intvl Time Field

Summary: In this task, you will display the **Intvl Time** field in every view.

To automatically display the **Intvl Time** field in every view, perform the following steps:

- Step 1** Select one of the following access methods:
- From the MAINVIEW Selection Menu, select option **0**, Parameters and Options. Then select the Windows Mode option.
 - From the MAINVIEW for IP EZIP Menu, type **MVP** on the command line.
- Step 2** From the MAINVIEW Parameter Editors Menu, select option **2**, Display.
- Step 3** Move the cursor to the **Show Time** field, and type **Y**.
- Step 4** To save your updates, press **End**.
- Step 5** To hide the field from views when you do not want it displayed, on the command line, type **EXclude TIME**. To redisplay the field, type **INclude TIME**.
- Tip:** To see the date that the data was gathered, use the **INclude DATE** command to reveal the **Intvl Date** field. This tip is most useful if your timeframe spans more than a 24-hour period.

Moving between Timeframes

Summary: This task describes a scenario of a situation that requires you to move between timeframes. In this task, you will use the scenario to learn how to move between timeframes quickly.

Before You Begin

Imagine that you are studying the **JOBRESP** view and you notice slow response times for a particular jobname. Alerted to a possible problem, you determine that it would be helpful to display what the system was doing in the previous interval.

To effectively compare intervals and associated system performances, you must be able to move quickly between intervals to determine how long an abnormal activity lasted or what intervals it affected. Use the **NEXT** and **PREV** parameters to move quickly between timeframes.

NEXT and **PREV** use the duration that was last specified to move the timeframe forward (**NEXT**) or backward (**PREV**) by the same amount.

To Move between Timeframes

- Step 1** Horizontally split the screen approximately half way down by typing **HS** on the command line, moving the cursor approximately halfway down the screen, and pressing **Enter**.
- Step 2** In Window 2, display **JOBRESP** by typing **JOBRESP** on the command line and pressing **Enter**.
- Step 3** On the command line, type **TIME = = PREV** and press **Enter**.

Note: Insert a space between each parameter.

An example of the screen that is displayed is shown in Figure 3-5.

Figure 3-5 Example of TIME PREV to Cycle through Timeframes

```

28NOV2001 15:48:45 ----- INFORMATION DISPLAY -----
COMMAND ==>
CURR WIN ==> 2          ALT WIN ==>
>W1 -JOBRESP-----VXGYSYSI--*-----28NOV2001--15:47:47---MVIP-----U---25
Job      Interval  Intvl Total  Active Total      Total      Total      High
Name     Date-----  Time- Conns  Conns  Bytesin  Bytesout  Resp      Resp
RDAAZSV4 28NOV2001 15:47      3      2          90817    2391633    57      41
TN3270E 28NOV2001 15:47      3      3          1102235  259540    11      8
IMVWEBQA 28NOV2001 15:47      6      3          455      4384      268     148
TN3270   28NOV2001 15:47      2      1          212866   416430    99      99
DBE4DIST 28NOV2001 15:47      2          4          212866   416430    436     225
RIHWXCW 28NOV2001 15:47      6          4          212866   416430    436     225
SYSMGT01 28NOV2001 15:47      1          4          212866   416430    436     225
>H2 =JOBRESP=====VXGYSYSI==*=====28NOV2001==15:46:52====MVIP=====U====25
Job      Interval  Intvl Total  Active Total      Total      Total      High
Name     Date-----  Time- Conns  Conns  Bytesin  Bytesout  Resp      Resp
RDAAZSV4 28NOV2001 15:46      3      2          91121    2404651    6       3
TN3270E 28NOV2001 15:46      3      3          1125241  265990    232     112
IMVWEBQA 28NOV2001 15:46      6      3          455      4384      99      99
TN3270   28NOV2001 15:46      2      1          212866   416430    436     225
DBE4DIST 28NOV2001 15:46      2          4          212866   416430    436     225
RIHWXCW 28NOV2001 15:46      6          4          212866   416430    436     225
SYSMGT01 28NOV2001 15:46      1          4          212866   416430    436     225
$$KMISAR 28NOV2001 15:46      1

```

In this example, the current time was compared to a previous time. You can also compare two historical times and can continue to type NEXT and PREV to move through different timeframes.

Note: If you are looking at the current time, you cannot look at the NEXT time because no data has been created yet.

You might want to define a PF key to TIME == PREV or TIME == NEXT so that you can step through subsequent intervals in historical mode with a single key and access the time information more quickly

Time and Duration Fields

Sometimes the time and duration fields on the window information line do not always contain the values that you expect. The reason for this discrepancy is because these fields reflect the actual data that is displayed, which may not be the same as the data you requested with the TIME command.

For example, it is 9:00 A.M. and you want to look at JOBRESPTS to determine the highest response times that occurred between 5:00 A.M. and 8:00 A.M. this morning. You display the JOBRESPTS view and type the following command:

```
TIME * 8:00 3h
```

You expect the resulting window information line to look like this:

```
>W1 =JOBRESPTS=====SJSC=====14MAR2002==8:00=180M====MVIP=====59=====
```

The last interval in the duration that you requested is 8:00; the 3-hour period that you are interested in is equivalent to 180 minutes.

The resulting window information line may actually look like this:

```
>W1 =JOBRESPTS=====SJSC=====14MAR2002==7:15=115M====MVIP=====59=====
```

Data is not always available for the intervals that you request. Sometimes the product address space (PAS) is shut down in the middle of a recording interval, creating gaps in the data that is recorded to the historical data set. The data that appears on the window information line represents the data that is *actually displayed*.

In our example, 7:15 A.M. was the last interval within the timeframe for which data was recorded. No data was recorded at 7:30 A.M., 7:45 A.M., or 8:00 A.M., so the window information shows 7:15 A.M. instead of 8:00 A.M.

Other gaps may have occurred in the record between 5:15 A.M. and 7:15 A.M. If so, the gaps were too short to significantly affect the data that is displayed. MAINVIEW makes adjustments so that you get the most accurate possible perspective of the data that is actually displayed in the view.

Note: The time field always contains the end of the last interval for which data was available, and the number of intervals for which data was actually available (normalized over the timeframe that you requested).

Chapter 4 Setting Alarms

MAINVIEW Alarm Manager works with MAINVIEW for IP, and other MAINVIEW products, to provide alarms. These alarms display messages that can alert you when system resources are overused.

This chapter provides a list of sample alarms and a checklist with the steps that are required to set an alarm in MAINVIEW for IP.

This chapter contains the following sections:

MAINVIEW Alarm Manager	4-2
Alarm Setting Checklist	4-2
Sample Alarms	4-5

MAINVIEW Alarm Manager

MAINVIEW[®] Alarm Manager is a tool that, with other MAINVIEW products, notifies you when an exception condition occurs. MAINVIEW Alarm Manager can monitor multiple systems simultaneously. You can display a single view that shows exceptions for all MAINVIEW performance monitors within your MVS enterprise.

Any data element on any MAINVIEW product can be used to generate alarms that produce the following results:

- create MVS console or subsystem messages
- display messages in a MAINVIEW Alarm Manager view that let you hyperlink to the MAINVIEW product which produced the exception
- trigger an automated alert or action from MAINVIEW[®] AutoOPERATOR[™] for quick problem resolution

MAINVIEW Alarm Manager generates alarms when thresholds from specific MAINVIEW product views are exceeded. Alarms can be based on summarized data from multiple systems and subsystems that use MAINVIEW's single system image (SSI) capabilities.

Using MAINVIEW Alarm Manager, you can create and modify alarm definitions that display meaningful messages for your site's requirements. Alarms can be set for any (or all) severity levels, from informational to critical.

Sample alarms and threshold conditions are provided in many MAINVIEW for IP views. You can use color or highlighting to add visual indicators to display data that instantly shows when resources are reaching a critical state. For more information about thresholds, see *Using MAINVIEW*. For more information about MAINVIEW Alarm Manager, see the MAINVIEW Alarm Manager *User Guide*.

Alarm Setting Checklist

Table 4-1 contains the steps that you must perform to set an alarm for MAINVIEW for IP. This checklist provides a summary of the steps that you must perform and where to find detailed instructions if you need them.

As an example, the alarm that you set up by using the following checklist is triggered when the threshold value for the average response time on the JOBRESP view exceeds 50 or 75 milliseconds.

Table 4-1 Alarm Setting Checklist (Part 1 of 2)

Step	Task	Description	Reference
1	allocate a new GROUP BBVDEF data set similar to USER BBVDEF	If you do not have the user view definition (USER BBVDEF) data set allocated, you are asked whether a clist should create one. Indicate Yes to create the USER BBVDEF data set.	MAINVIEW Alarm Manager <i>User Guide</i>
2	issue tso isrddn , and examine the BBVDEF concatenation	In the MAINVIEW for IP monitor, issue tso isrddn from the command line. This information is required for Step 9.	MAINVIEW Alarm Manager <i>User Guide</i>
3	set an alarm threshold	The alarm threshold is set in the JOBRESP view.	MAINVIEW Alarm Manager <i>User Guide</i>
4	issue cust	In the MAINVIEW for IP monitor, issue cust from the command line.	MAINVIEW Alarm Manager <i>User Guide</i>
5	issue threshold command, and determine where threshold value should be set	Enter t (for <i>threshold</i>) on the View Customization command line, and select the column where the threshold value should be set. In this example, the Avg Resp field is in column i .	MAINVIEW Alarm Manager <i>User Guide</i>
6	set condition and attribute values	These are examples of condition and attribute values: Condition Attr 1st => =50 =>9 reverse red 2nd => >75 => 2 yellow	MAINVIEW Alarm Manager <i>User Guide</i>
7	check field entries	Field entries that match threshold values are highlighted in the attribute color.	MAINVIEW Alarm Manager <i>User Guide</i>
8	display the Exit Views Customization panel	To display the Exit Views Customization panel, press PF3 .	MAINVIEW Alarm Manager <i>User Guide</i>
9	save changes to the Exit Views Customization panel	To display the Save View Definition panel and save your changes, indicate Yes . The view is saved in the first data set of BBVDEF concatenation.	MAINVIEW Alarm Manager <i>User Guide</i>
10	copy the USER BBVDEF data set	When the new view is saved in USER BBVDEF, copy it into the GROUP BBVDEF data set.	MAINVIEW Alarm Manager <i>User Guide</i>
11	add the GROUP BBVDEF data set	The GROUP BBVDEF data set must be added in front of BBVDEF concatenation. You must add the data set to the MAINVIEW Alarm Manager PAS and the MAINVIEW for IP PAS.	MAINVIEW Alarm Manager <i>User Guide</i>
12	start the MAINVIEW Alarm Manager PAS	Use the sample JCL in <i>hilevel.UBBSAMP(MVALPAS)</i> to start the MAINVIEW Alarm Manager PAS.	MAINVIEW Alarm Manager <i>User Guide</i>

Table 4-1 Alarm Setting Checklist (Part 2 of 2)

Step	Task	Description	Reference
13	perform a recycle	The MAINVIEW for IP PAS must be recycled.	<i>Using MAINVIEW</i>
14	issue the Setalarm 00 command	Within the new view, issue Setalarm 00 from the command line.	MAINVIEW Alarm Manager <i>User Guide</i>
15	go to the MAINVIEW Alarm Manager Easy Menu (MVALARM)	In the split screen, MVALARM is displayed. Select Current Alarms , and install the alarm.	MAINVIEW Alarm Manager <i>User Guide</i>
16	save the alarm	When you install the alarm, save your selection.	MAINVIEW Alarm Manager <i>User Guide</i>
17	verify the installation of Alarm 00	To verify the installation of Alarm 00, select List Alarm Groups and check the status.	MAINVIEW Alarm Manager <i>User Guide</i>

Sample Alarms

MAINVIEW Alarm Manager is capable of monitoring multiple systems simultaneously; MAINVIEW Alarm Manager installed on one system can administer your entire sysplex.

Table 4-2 describes sample alarms that are provided with MAINVIEW for IP. You can customize these sample alarms to meet your specific monitoring needs.

Table 4-2 MAINVIEW for IP Sample Alarms

Alarm Name	Description
CONNRESP	response time for the connection has exceeded a specified number of milliseconds
JOBRA	average response time for the job has exceeded a specified number of milliseconds
JOBRDA	average response time for the job has exceeded a specified number of milliseconds
JOBRDH	highest response time for the job has exceeded a specified number of milliseconds
JOBRH	highest response time for the job has exceeded a specified number of milliseconds
JOBRSA	average response time for the job has exceeded a specified number of milliseconds
JOBRSH	highest response time for the job has exceeded a specified number of milliseconds
PORTRA	average response time for the port has exceeded a specified number of milliseconds
PORTRDA	average response time for the port has exceeded a specified number of milliseconds
PORTRDH	highest response time for the port has exceeded a specified number of milliseconds
PORTRH	highest response time for the port has exceeded a specified number of milliseconds
PORTRSA	average response time for the port has exceeded a specified number of milliseconds
PORTRSH	highest response time for the port has exceeded a specified number of milliseconds

Alarm Definitions

Alarm definitions consist of the following parameters:

- threshold and filter criteria
- view, product, and context for which the criteria are established
- message IDs and message text
- monitoring frequency and time periods
- hyperlinks to views, extended help, or MAINVIEW AutoOPERATOR commands

Note: Sample alarm definitions are shipped with `CONTEXT='SAMPCTXT'`. For the sample to work on your system, change `CONTEXT='VALUE'`. *VALUE* is variable for a value that is valid at your site.

Alarm definitions are stored in a parameter library member that is read by MAINVIEW Alarm Manager at MVALARM PAS initialization.

Threshold conditions are defined as one of the following priority levels:

- Critical
- Information
- Major
- Minor
- Warning

Chapter 5 **MAINVIEW for IP Messages**

This chapter provides information about the messages that are issued by MAINVIEW for IP.

This chapter contains the following sections:

Interpreting Messages	5-2
Message Format	5-2
Message Identifiers	5-3
Message Levels	5-3
Description Format	5-4
Contacting BMC Software Customer Support	5-4
Gathering Problem Report Documentation	5-5
MAINVIEW for IP Messages.	5-8

Interpreting Messages

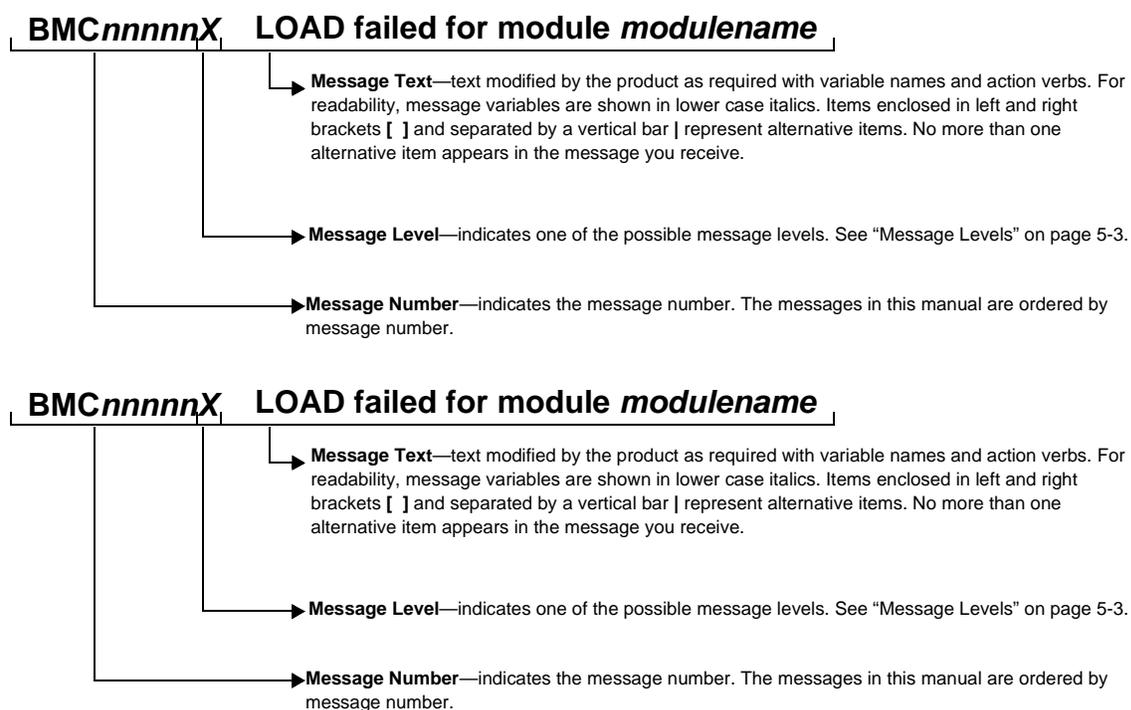
This section provides general information about the messages that are issued by MAINVIEW for IP. This section describes the following items:

- parts of a message
- description format
- message levels
- information that you should have available when contacting BMC Software Customer Support

Message Format

Figure 5-1 describes the parts of a message.

Figure 5-1 Parts of a Message



Message text that is italicized and in lowercase characters (*example*) indicates variable text that will be determined when the message is issued.

Message text that is enclosed in left and right brackets and is separated by vertical lines ([ON | OFF]) indicates actual values, one of which will be included at that point in the message.

Message Identifiers

All messages consist of a message identifier and message text of the following format:

BMCnnnnnX Message Text

Table 5-1 describes the message identifiers.

Table 5-1 Message Identifiers

Field	Description
BMC	The prefix identifies the owner of the message. All BMC Software messages begin with <i>BMC</i> .
<i>nnnnn</i>	This two-digit to five-digit number identifies the message.
<i>X</i>	This identifier is the severity code. The severity code indicates the amount of action required by the user and the nature of the message. For an explanation of the severity codes, see Table 5-2.

Message Levels

A severity code indicates the nature of the message and the amount of action that is required by the user. Table 5-2 describes the levels of message severity.

Table 5-2 Message Severity Codes

Code	Description
A (action)	Immediate action is required.
E (error)	The function that you requested was not completed. Action is required.
I (information)	Information only. No action is required.
R (reply)	You must reply to the message before the system can continue.
S (severe)	A severe error occurred. Action is required.
W (warning)	The system is still operating and no immediate action is required. When time is available, further investigation is needed.

Note: All messages with severity code *E* are sent to the system console. Some messages with severity code *A* or *I* are also sent to the system console.

Description Format

The following information is provided for each message:

- *Explanation* explains why the product issued the message.
- *System Action* explains the product action as a result of encountering the situation.
- *User Response* explains the action that you should perform in this situation.

The text that is associated with each message is a short phrase or sentence describing a condition that has occurred or that requests a user response. For example:

```
BMC7005I No active Applids BSOP
```

Contacting BMC Software Customer Support

Some message descriptions instruct you to contact your BMC Software customer support representative. The customer support representative can help you resolve the problem quickly if you can answer the following questions before calling:

- What kind of problem do you have?
- Can you repeat the problem or preceding conditions?
- Do you have supporting dumps or other diagnostic information?
- What has changed in your environment:
 - Have you recently installed a new product on your system?
 - Have you recently modified an application program?
 - Have you recently installed a BMC Software product or product maintenance tape?

Gathering Problem Report Documentation

If you encounter a problem with MAINVIEW for IP, BMC Software customer support representatives may ask you to send documentation of the problem in the form of one or more dumps.

Use the following SYSIN parameters for debugging each collection point:

```

DBGBUF5
DBGCACH
DBGCONF
DBGCONS
DBGDEVS
DBGKILL
DBGOBEY
DBGPING
DBGPORT
DBGROUT
DGBSLAP
DBGSNMP
DBGTRCE
DBGVIPA
DBGOSAD

```

To Gather Problem Report Documentation

- Step 1** Add the debug parameters to the SYSIN file. The file must have the following DD statements:

```

/*
/*  DEBUG DATASETS.
/*
//UCONFDBG DD  SYSOUT=*
//UPORTDBG DD  SYSOUT=*
//UROUTDBG DD  SYSOUT=*
//UTRCEDBG DD  SYSOUT=*
//UPINGDBG DD  SYSOUT=*
//UDEVSDBG DD  SYSOUT=*
//UCONSDBG DD  SYSOUT=*
//UVIPADBG DD  SYSOUT=*
//USNMPDBG DD  SYSOUT=*
//UKILLDBG DD  SYSOUT=*
//UOBEYDBG DD  SYSOUT=*
//USLAPDBG DD  SYSOUT=*
//UCACHDBG DD  SYSOUT=*
//UBUFSDBG DD  SYSOUT=*
//UOSADDBG DD  SYSOUT=*

```

- Step 2** Restart the MAINVIEW for IP product address space (PAS).
- Step 3** Recreate the problem.

- Step 4** Send the JES2 job log that contains the debugging information to your MAINVIEW for IP customer support representative.
- Step 5** Type the command `/mvip options` on the console, print the output, and send it to your MAINVIEW for IP customer support representative.
- Step 6** Create an SVC dump of the PAS experiencing the problem by using the MVS command `DUMP COMM`. Supply the job name of the appropriate address space.
- Step 7** Reply to the prompt with the following command:
- ```
SDATA=(NUC,LPA,CSA,LSQA,SQA,PSA,TRT,RGN,SUM)
```
- Step 8** Check for log message IEA911 to confirm that the dump is a complete dump, not a partial dump.
- Step 9** Send the dump to your MAINVIEW for IP customer support representative by using one of the following methods:
- Copy the dump to a tape.
  - FTP the dump.

If you copy the dump to a tape, ship the tape to your MAINVIEW for IP customer support representative. Include the following items:

- description of the problem
- user action that preceded the problem
- version number of MAINVIEW for IP
- case number

If you FTP the dump, select one of the following methods:

- TSO command line interface
- sample batch job

### To Use a TSO Command Line Interface

**Note:** Use `TRSMAN` to compress the dump before uploading the information to **FTP.BMC.COM**.

- Step 1** Use TSO to access **FTP.BMC.COM**.
- Step 2** At the prompt, enter **ANONYMOUS** as your ID.
- Step 3** Enter **Your\_Email@company.com** as the password.

- Step 4** Enter **CD INCOMING**.
- Step 5** Enter **BINARY**.
- Step 6** Enter **PUT 'MVS.DATASET.NAME.TRS' cnnnnnn\_dump1.trs**.
- Step 7** Enter **QUIT**.
- Step 8** Notify your MAINVIEW for IP customer support representative that the dump has been uploaded.

### To Run a Sample Batch Job

**Note:** Use TRSMMAIN to compress the dump before uploading the information to **FTP.BMC.COM**.

- Step 1** Run the following batch job:

---

```
//BATCHFTP JOB
//FTP EXEC PGM=FTP,REGION=4096K
//SYSPRINT DD SYSOUT=*
//OUTPUT DD SYSOUT=*
//INPUT DD *
ftp.bmc.com
anonymous
YOUR_EMAIL@COMPANY.COM
bin
cd /incoming
put 'MVS.DATASET.NAME.TRS' cNNNNNN_dump1.trs
quit
/*
```

---

- Step 2** Notify your MAINVIEW for IP customer support representative that the dump has been uploaded.

## MAINVIEW for IP Messages

MAINVIEW for IP messages may be displayed on the MAINVIEW monitor. The message information includes an explanation of the message, the system action, and the suggested user response.

**BMC11234E FTP EXIT processing failed—increase FTPXBUF value.**

*Explanation:* The number of allocated FTPX control blocks has been exhausted.

*System Action:* File Transfer Protocol (FTP) data collection is not performed, and information for the file transfer is not recorded.

*User Response:* Allocate more FTPX control blocks. The control blocks will be available after the next logging interval, allowing data collection and recording to resume.

**BMC256503E PLEASE SPECIFY THE CORRECT OPTIONS IN THE SYSIN DATASET AND RESTART MAINVIEW/IP.subsysid**

*Explanation:* An invalid SYSIN DD statement was specified.

*System Action:* MAINVIEW for IP terminates.

*User Response:* Specify the correct options in the SYSIN data set, and restart MAINVIEW for IP subsysid. Contact BMC Software Customer Support for assistance.

**BMC256506I SSCT (address) FOR SUBSYSTEM OBTAINED and QUEUED.subsysid**

*Explanation:* The subsystem dispatcher had to construct and insert an SSCT (Subsystem Control Table) into the SSCT queue. The subsystem was not previously active, and the entry was not defined in any IEFSSN members of SYS1.PARMLIB.

*System Action:* Processing continues.

*User Response:* This message is for your information only. No action is required.

**BMC256507I MAINVIEW/IP SUBSYSTEM HAS GENERATED SSCT (address), TSVT (address).subsysid**

*Explanation:* The MAINVIEW for IP service tables were successfully created and initialized.

*System Action:* Processing continues.

*User Response:* This message is for your information only. No action is required.

- 
- BMC256509S**      **ABEND *nnnnn* OCCURRED DURING SUBSYSTEM ADDRESS SPACE INITIALIZATION.*subsysid***
- Explanation:*      The subsystem dispatcher ESTAE routine received control during address space initialization. The *subsysid* indicates the name of the subsystem.
- System Action:*      The subsystem terminates. The address space terminates.
- User Response:*      Contact BMC Software Customer Support.
- BMC256518S**      **XST (*address*) CONNECTION FAILURE, R15 (*retrncode*), SSOBRETN (*address*).*subsysid***
- Explanation:*      The BMCP initialization has failed with the indicated return code.
- System Action:*      The subsystem terminates.
- User Response:*      Contact BMC Software Customer Support.
- BMC256520S**      **SERVICE MODULE VALUES NOT CONSISTENT WITH EXISTING SSVT (*address*).*subsysid***
- Explanation:*      An inconsistency in the subsystem vector table (SSVT) values was detected during installation. One or more subsystem modules are at maintenance levels that are incompatible with the existing SSVT.
- System Action:*      The subsystem address space terminates.
- User Response:*      Ensure that the installation and refresh processes were performed correctly. Contact BMC Software Customer Support.
- BMC256521S**      **SUBSYSTEM DOWN-LEVELING ATTEMPTED, *old level*, *new level* SSVT (*address*).*subsysid***
- Explanation:*      The product tried to initialize at a lower level than was previously active. The installed product was created by a set of modules from a more current (or later) maintenance level. This message provides the version and modification levels of the current modules and those being initialized.
- System Action:*      The subsystem initialization process stops, and initialization does not occur.
- User Response:*      Restart the more current version of the subsystem modules, and restart the address space.

- BMC256522S**      **MAINVIEW/IP SUBSYSTEM ADDRESS SPACE (*nnnn*) is CURRENTLY ACTIVE.*subsysid***
- Explanation:*      An attempt was made to start the subsystem. The subsystem that was just started has detected an active subsystem in address space *nnnn*.
- System Action:*      The subsystem that was just started terminates.
- User Response:*      None.
- 
- BMC256524S**      **SERVICE MODULE FVT OFFSET/SIZE (*nnnn/nnnn*) NOT CONSISTENT WITH THE SSVT (*nnnn/nnnn*).*subsysid***
- Explanation:*      An inconsistency in the subsystem vector table (SSVT) values was detected during initialization.
- System Action:*      The subsystem address space terminates.
- User Response:*      Ensure that the installation and refresh processes were performed correctly. Contact BMC Software Customer Support.
- 
- BMC256526S**      **SERVICE MODULE FVT OFFSET/SIZE (*nnnn/nnnn*) NOT CONSISTENT WITH THE SSVT (*nnnn/nnnn*).*subsysid***
- Explanation:*      An inconsistency in the subsystem vector table (SSVT) values was detected during initialization.
- System Action:*      The subsystem address space terminates.
- User Response:*      Ensure that the installation and refresh processes were performed correctly. Contact BMC Software Customer Support.
- 
- BMC256528S**      **SERVICE MODULE FVT OFFSET/SIZE (*nnnn/nnnn*) NOT CONSISTENT WITH THE SSVT (*nnnn/nnnn*).*subsysid***
- Explanation:*      An inconsistency in the subsystem vector table (SSVT) values was detected during initialization.
- System Action:*      The subsystem address space terminates.
- User Response:*      Ensure that the installation and refresh processes were performed correctly. Contact BMC Software Customer Support.
- 
- BMC256529S**      **ABEND *nnnnn* OCCURRED DURING MAINVIEW/IP SUBSYSTEM INITIALIZATION.*subsysid***
- Explanation:*      An abend occurred during the initialization phase of the subsystem.
- System Action:*      Subsystem initialization terminates.
- User Response:*      Contact BMC Software Customer Support.

- 
- BMC256530S**      **MSTR SUBSYSTEM VERIFICATION REQUEST FAILED, R15 (*retrncode*), SSOBRETN (*address*).*subsysid***
- Explanation:*      An unrecoverable error occurred during a subsystem verify request to the master MVS subsystem.
- System Action:*    The subsystem address space terminates.
- User Response:*    Contact BMC Software Customer Support.
- 
- BMC256532S**      **INVALID SUBSYSTEM AFFINITY INDEX (*hhhh*) RETURNED BY SUBSYSTEM VERIFY.*subsysid***
- Explanation:*      An illogical subsystem affinity index (in hexadecimal notation) was returned by the master MVS subsystem for the subsystem.
- System Action:*    The subsystem address space terminates.
- User Response:*    Contact BMC Software Customer Support.
- 
- BMC256534S**      **SSCT ADDRESS NOT PROVIDED FOR SUBSYSTEM INITIALIZATION**
- Explanation:*      The required MAINVIEW for IP subsystem table (SSCT) was not found.
- System Action:*    The subsystem terminates.
- User Response:*    Notify your system programmer of the error. Ensure that the installation and refresh processes were performed correctly. Contact BMC Software Customer Support.
- 
- BMC256538S**      **MAINVIEW/IP SUBSYSTEM INITIALIZATION PROCESS TERMINATED.*subsysid***
- Explanation:*      The initialization process is being terminated because of one or more previous errors.
- System Action:*    The subsystem address space terminates.
- User Response:*    Verify the message log for previous messages pertaining to this error. Notify the system programmer of the error.

**BMC256621W****TERMINATING SUBSYSTEM ASID (nnnn) INCONSISTENT WITH DISPATCHER ASID (nnnn).subsysid**

*Explanation:* This message is issued during end-of-task and/or end-of-memory processing. The subsystem address space being terminated does not match the subsystem address space previously in control of the SSVT. This condition usually arises only when a storage overlay occurs. This message should not be issued again.

*System Action:* Processing continues. The subsystem address space is flagged as terminated.

*User Response:* None.

**BMC256615I****User \*\*\*\*\* has dropped Connection \*\*\*\*\*X \*\*\*\*\*..\*\*\*\*\* with id \*\*\*\*\* RC(zzzzzzzz)**

*Explanation:* A write-to-operator (WTO) is displayed when you perform the DR (drop connection) line command. *User* is the TSO USERID, *Connection* is the IP address and port number of the terminated connection, *ID* is the connection ID from TACCONS view, and *RC* is the return code. A return code of 0 indicates that the connection was terminated successfully.

*System Action:* The connection is terminated.

*User Response:* This message is for your information only. No action is required.

**BMC256732E****ERROR OPENING SYSIN DATASET—SUBSYSTEM TERMINATING**

*Explanation:* The data set name (DSN) could not be opened.

*System Action:* The subsystem address space terminates.

*User Response:* Access *hilevel.BBSAMP(TACPAS)*, correct the SYSIN DSN, and restart the product address space (PAS).

**BMC256733E****INVALID INITIALIZATION STATEMENT \*\*\*\*\***

*Explanation:* The initialization statement for the statement that is indicated in the error message is invalid.

*System Action:* The subsystem address space terminates.

*User Response:* Correct the SYSIN data set name (DSN), and restart the product address space (PAS).

- BMC256734E NO DELIMITER OR CONTINUATION FOUND BEFORE COL 71—SUBSYSTEM TERMINATING**
- Explanation:* The delimiter or continuation character preceding column 71 is missing.
- System Action:* The subsystem address space terminates.
- User Response:* Add the delimiter or continuation character, and restart the product address space (PAS).
- BMC256735E INCOMPLETE END OF INITIALIZATION STATEMENT STATEMENTS—SUBSYSTEM TERMINATING**
- Explanation:* The end of the initialization statements is incomplete.
- System Action:* The subsystem address space terminates.
- User Response:* Complete the end statement, and restart the product address space (PAS).
- BMC256736E DYNALLOC ALLOCATE FAILED, R15(\*\*\*\*\*) REASON(\*\*\*\*\*)**
- Explanation:* The DYNALLOC dynamic allocation macro could not be processed. The return code and reason code are displayed.
- System Action:* The SNMPPARMS are not processed.
- User Response:* Contact BMC Software Customer Support for assistance.
- BMC256737E DYNALLOC UNALLOCATE FAILED, R15(\*\*\*\*\*) REASON(\*\*\*\*\*)**
- Explanation:* The DYNALLOC dynamic unallocation macro could not be processed. The return code and reason code are displayed.
- System Action:* The SNMPPARMS are not processed.
- User Response:* Contact BMC Software Customer Support for assistance.
- BMC256738E ERROR OPENING SNMPPARM DATASET—SUBSYSTEM TERMINATING**
- Explanation:* The data set name (DSN) could not be opened.
- System Action:* The subsystem address space terminates.
- User Response:* Access *hilevel.BBSAMP(TACPAS)*, correct the SNMPPARM DSN, and restart the product address space (PAS).

**BMC256739E      INVALID SNMPPARM INITIALIZATION STATEMENT \*\*\*\*\***

*Explanation:*     The initialization statement for the statement that is indicated in the error message is invalid.

*System Action:*   The subsystem address space terminates.

*User Response:*   Correct the SNMPPARM data set name (DSN), and restart the product address space (PAS).

**BMC256740E      NO DELIMITER OR CONTINUATION FOUND BEFORE COL 71 in  
SNMPPARM—SUBSYSTEM TERMINATING**

*Explanation:*     The delimiter or continuation character preceding column 71 in the SNMPPARM is missing.

*System Action:*   The subsystem address space terminates.

*User Response:*   Add the delimiter or continuation character, and restart the product address space (PAS).

**BMC256741E      INCOMPLETE END OF SNMPPARM INITIALIZATION STATEMENT  
STATEMENTS—SUBSYSTEM TERMINATING**

*Explanation:*     The end of the SNMPPARM initialization statements is incomplete.

*System Action:*   The subsystem address space terminates.

*User Response:*   Complete the end statement, and restart the product address space (PAS).

**BMC256800I      SNMP Parameters have been refreshed**

*Explanation:*     A user successfully performed the REFRESH command.

*System Action:*   The system reads and processes the SNMPPARM data set.

*User Response:*   This message is for your information only. No action is required.

**BMC256800I      SNMP Parameters have not been refreshed**

*Explanation:*     A user tried to perform the REFRESH command.

*System Action:*   The system is unable to read the SNMPPARM data set. The SNMPPARM data set is not processed.

*User Response:*   Retry the REFRESH command. If processing fails again, contact BMC Software Customer Support.

- 
- BMC256849E**      **MAINVIEW/IP SUBSYSTEM FOUND NO ACTIVE TCPIP STACKS TO MONITOR. *subsysid***
- Explanation:*      The MAINVIEW for IP subsystem detected no active or available Transmission Control Protocol/Internet Protocol (TCP/IP) stacks.
- System Action:*      Processing continues. MAINVIEW for IP monitoring is not available for TCP/IP.
- User Response:*      Notify the system programmer of the error.
- 
- BMC256850E**      **MAINVIEW/IP SUBSYSTEM *name* CANNOT FIND TSCB CONTROL BLOCK - TERMINATING.*subsysid***
- Explanation:*      The MAINVIEW for IP subsystem service module, *name* could not find the required TSCB control block to determine the availability of Transmission Control Protocol/Internet Protocol (TCP/IP).
- System Action:*      The called service terminates.
- User Response:*      Ensure that the TCP/IP stack is active.
- 
- BMC256851E**      **MAINVIEW/IP SUBSYSTEM *name* UPDATE FAILED WITH R15 (*retrncode*) - TERMINATING.*subsysid***
- Explanation:*      The subsystem UPDATE process for *name* failed.
- System Action:*      The UPDATE service request terminates.
- User Response:*      Notify the system programmer of the error. Contact BMC Software Customer Support for assistance.
- 
- BMC256852E**      **MAINVIEW/IP SUBSYSTEM *name* LOAD UPDATE MODULE FAILED - TERMINATING.*subsysid***
- Explanation:*      The subsystem LOAD process for an UPDATE service request failed for *name*.
- System Action:*      The process terminates.
- User Response:*      Notify the system programmer of the error. Contact BMC Software Customer Support for assistance.
- 
- BMC256900I**      **MAINVIEW/IP SUCCESSFULLY STARTED**
- Explanation:*      The product has been started successfully.
- System Action:*      None.
- User Response:*      This message is for your information only. No action is required.

**BMC256901W**

**TIER \*\*\* HAS *nnn* DAYS LEFT IN ITS GRACE PERIOD**

*Explanation:* The MAINVIEW for IP TIER is running on a trial authorization that will expire in *nnn* days.

*System Action:* Processing continues.

*User Response:* Contact your BMC Software sales representative to purchase a license and receive a permanent authorization.

**BMC256903E**

**TRIAL LICENSE HAS EXPIRED, CONTACT BMC SOFTWARE**

*Explanation:* The MAINVIEW for IP authorization process detected that the trial license has expired.

*System Action:* MAINVIEW for IP functions are inactivated.

*User Response:* Contact your BMC Software sales representative to purchase a license and receive a permanent authorization.

**BMC256904E**

**MAINVIEW/IP NOT LICENSED FOR PROCESSOR, RC=\*\*, REASON=\*\*\*\***

*Explanation:* An attempt was made to start MAINVIEW for IP on a CPU for which it is not licensed. The return code and reason code represent specific reasons for the security violation.

*System Action:* No functions are performed by the indicated CPU.

*User Response:* Contact your BMC Software sales representative to obtain a product password.

**BMC256905W**

**MAINVIEW/IP NOT LICENSED FOR PROCESSOR, RC=\*\*, REASON=\*\*\*\***

*Explanation:* An attempt was made to start MAINVIEW for IP on a CPU for which it is not licensed. The return code and reason code represent specific reasons for the security violation.

*System Action:* No functions are performed by the indicated CPU.

*User Response:* Contact your BMC Software sales representative to obtain a product password.

**BMC256906E**

**MAINVIEW/IP NOT LICENSED FOR PROCESSOR, RC=\*\*, REASON=\*\*\*\***

*Explanation:* An attempt was made to start MAINVIEW for IP on a CPU for which it is not licensed. The return code and reason code represent specific reasons for the security violation.

*System Action:* No functions are performed by the indicated CPU.

*User Response:* Contact your BMC Software sales representative to obtain a product password.

**BMC256907E****RACF-PROTECTED WHILE SETTING GRACE PERIOD**

*Explanation:* The data set containing the authorization table is Resource Access Control Facility (RACF)-protected and allows read-only access.

*System Action:* Processing continues.

*User Response:* Contact your RACF administrator to obtain access permission to this data set.

**BMC256908W****GRACE PERIOD HAS *nnn* DAYS LEFT**

*Explanation:* MAINVIEW for IP is running a trial authorization that will expire in *nnn* days.

*System Action:* Processing continues.

*User Response:* Contact your BMC Software sales representative to purchase a license and receive a permanent authorization.

**BMC256909W****TEMPORARY WILL EXPIRE IN *nnn* DAYS**

*Explanation:* MAINVIEW for IP is running on a temporary authorization that will expire in *nnn* days.

*System Action:* Processing continues.

*User Response:* Contact your BMC Software sales representative to purchase a license and receive a permanent authorization.

**BMC256910E****PHASE1 SECURITY NEVER EXECUTED**

*Explanation:* The first phase of the MAINVIEW for IP security process has not executed.

*System Action:* No functions are performed under MAINVIEW for IP.

*User Response:* Contact BMC Software Customer Support.

**BMC256911E****PHASE1 SECURITY DID NOT COMPLETE SUCCESSFULLY**

*Explanation:* The MAINVIEW for IP authorization process detected an error during security processes.

*System Action:* No functions are performed under MAINVIEW for IP.

*User Response:* Contact BMC Software Customer Support.

**BMC256912E SECURITY WORKAREA IS CORRUPTED**

*Explanation:* The MAINVIEW for IP authorization process detected a corrupted security database.

*System Action:* No functions are performed under MAINVIEW for IP.

*User Response:* Contact BMC Software Customer Support.

**BMC256913E PHASE1 SECURITY NEVER EXECUTED**

*Explanation:* The first phase of the MAINVIEW for IP security authorization process detected an invalid license. *RTNCD* represents the return code from security phase 1 processing.

*System Action:* No functions are performed under MAINVIEW for IP.

*User Response:* Contact your BMC Software sales representative to purchase a license and receive a permanent password.

**BMC256914E PHASE FAIL PASSWORDS NOT SUPPORTED, CONTACT BMC SOFTWARE**

*Explanation:* MAINVIEW for IP security authorization process detected an invalid password.

*System Action:* No functions are performed under MAINVIEW for IP.

*User Response:* Contact BMC Software Customer Support.

**BMC256999E RTNCD= \*\*\*\* REASON= \*\*\*\* TIER= \*\*\*\* TMPDAYS=nnn PRMDAYS=nnn GRACE=nnn**

*Explanation:* This message displays the status from the security authorization routine. It provides license information and is issued during the MAINVIEW for IP initialization process.

*System Action:* Processing continues.

*User Response:* None.

**BMC259510E****Error Initializing Library: *nn***

*Explanation:* The system encountered a problem when collecting Simple Network Management Protocol (SNMP) data from one of the specified IP nodes. *nn* is one of the following values:

- 1 (SNMP Bad Parameters)
- 3 (SNMP Already Initialized)
- 5 (SNMP System Error)
- 6 (SNMP Transport Error)

*System Action:* The SNMP request fails. The system continues collecting SNMP data.

*User Response:* Contact BMC Software Customer Support.



---

---

# Appendix A Operator Commands

This appendix describes operator commands that you can use to control operation of MAINVIEW for IP.

This appendix contains the following sections:

|                                           |     |
|-------------------------------------------|-----|
| Conventions .....                         | A-2 |
| Commands .....                            | A-2 |
| DNR—Domain Name Resolution Function ..... | A-2 |
| XSUPP—Exit Suppression .....              | A-2 |

## Conventions

You typically issue these operator commands from the MVS system console. The syntax uses the following conventions:

- Items in italics are variables for which you must supply a value. For example, in `HALT subsysid`, you must supply the correct subsystem ID name.
- When two or more items are separated by a vertical line, you must select only one item. For example, in `Z | HALT subsysid,CANCEL`, you use Z or HALT but not both.

## Commands

This section lists descriptions of the operator commands alphabetically to help you find them more easily.

### DNR—Domain Name Resolution Function

Use this command to enable or disable the domain name resolution (DNR) function. The DNR function resolves an IP address to a domain name, and provides the IP address of a domain name. DNR can be entered as an operator command from the MVS console in the format `mvip DNR ON | OFF`.

### XSUPP—Exit Suppression

MAINVIEW for IP collects file transfer protocol (FTP) statistics by using an exit point (defined by IBM) and an exit that is provided by BMC Software. The exit point is activated by requesting system management facility (SMF) logging in the FTP server. SMF logging writes type 118 records that can be suppressed by the exit.

To suppress SMF records after MAINVIEW for IP has collected the data, perform the XSUPP command by entering `mvip XSUPP ON`.

XSUPP can be entered as an operator command from the MVS console in the format `mvip XUPP ON | OFF`.

---

# Index

## A

- abend 2-18, 2-26
- actions
  - drop connections 2-12
  - ping 2-14
  - Traceroute 2-16
- activating hyperlinks 2-38
- Alarm Manager, MAINVIEW 4-2
- alarms
  - definition 2-8
  - features 4-2
  - sample 4-5
  - setting 4-2
- ALLCONS view 2-11
- Application view 2-9
- applications
  - availability 1-3, 2-9
  - connections 1-3, 2-11
  - monitoring performance 1-2, 2-11
  - throughput 1-3, 2-9, 2-45
- availability
  - applications 2-9
  - historical data 3-3
  - TCP/IP stacks 2-9

## B

- batch jobs, sample 5-7
- BBSAMP members
  - MVALPAS 4-3
  - sample SAS programs 1-4
  - TACSNM 2-41
- BBVDEF data sets 4-2, 4-3
- BMC Software, contacting 5-4
- buffer pools 2-44

## C

- cache 2-43
- Cache Info view 2-38
- canned alarms. *See* sample alarms
- CAS (coordinating address space) 2-5
- checklists, setting alarms 4-2
- CLSxCONS views 2-45
- CLSxRESP views 2-45
- codes, message severity levels 5-3
- commands
  - D 2-29
  - DR 2-12
  - DSLIS 3-3
  - DUMP COMM 5-5
  - operator A-2
  - P 2-14
  - ping 2-11, 2-20
  - quit 2-46
  - RETURN 2-46
  - SDATA 5-6
  - setalarm 4-3
  - STA 2-26
  - STO 2-28
  - TIME 2-46, 3-2, 3-4
  - TR 2-22
  - Traceroute 2-11, 2-16
  - tsoisrddn 4-2
- Common Storage Area. *See* CSA
- Communication Storage Manager. *See* CSM

---

- configurations 2-10
- connections, information views 2-11
- CONNRESP view 2-45
- coordinating address space. *See* CAS
- CSA (Common Storage Area) 2-44
- CSAU view 2-44
- CSM (Communication Storage Manager) 2-44
- CSM view 2-44
- customer support 5-4

## D

- data definition statements 5-5
- data set members
  - MVALPAS 4-3
  - TACSNM 2-41
- data sets
  - BBVDEF 4-2, 4-3
  - PROFILE 2-10
- debugging 5-5
- devices
  - clearing packet trace entries 2-33
  - displaying packet traces 2-29
  - dropping connections 2-12
  - OSA cards 2-36
  - performing packet traces 2-26
  - performing Traceroutes 2-16, 2-22
  - pinging 2-14, 2-20
  - stopping packet traces 2-28
- diagnostic features 2-18
- displaying views 2-8
- DNR (domain name resolution) command A-2
- documentation
  - problem reports 5-5
- domain name resolution function A-2
- drill-down function
  - definition 2-8
  - using 2-25, 2-31
- dropping connections 2-12
- DSLIS command 3-3
- DUMP COMM command 5-5
- dumps
  - compress 5-6, 5-7
  - debugging collection points 5-5
  - problem reporting 5-5
  - sending 5-6
- DVIPA (Dynamic Virtual IP Address) 2-34

## E

- easy menus. *See* EZ menus
- electronic documentation, online Help 2-3
- error messages
  - description format 5-4
  - MAINVIEW for IP 5-8
- exceptions, setting alarms for 4-2
- exit suppression A-2
- EZ menus
  - EZIP Menu 2-3, 2-5, 2-8
  - overview 2-3

## F

- features of MAINVIEW for IP 1-3
- File Transfer Protocol. *See* FTP
- FTP (File Transfer Protocol)
  - sending dumps 5-6
  - servers 2-35

## H

- Help key 2-3
- highlighting 2-8
- historical data
  - allocated data sets 3-3
  - definition 2-46
  - displaying Intvl Time field 3-10
  - displaying with TIME command 3-5
  - moving between timeframes 3-11
  - overview 3-2
  - reasons for unavailability 3-3
  - reports 3-2
  - window status indicator 3-8
- hyperlinks
  - activating 2-38
  - definition 2-37
  - MAINVIEW for UNIX System Services 2-37
  - MAINVIEW for WebSphere Application Server 2-37, 2-43

---

## I

input parameters, updating SNMP parameters 2-41  
interfaces 2-36  
interval recorder. *See* historical data  
IP (Internet Protocol)  
    *See also* TCP  
    availability 2-9  
    configuration 2-10  
    MAINVIEW for IP overview 1-2  
    resource links 2-37  
IP addresses, updating SNMP parameters 2-41  
IP stacks, realtime data 2-11  
IPCONF view 2-10

## J

JOBRESP view 2-45  
JOBRESPTS view 2-45

## L

line commands  
    D 2-29  
    DR 2-12  
    in Connections views 2-11  
    P 2-14  
    ping 2-20  
    STA 2-26  
    STO 2-28  
    TR 2-22  
    Traceroute 2-16  
links. *See* hyperlinks

## M

MAINVIEW Alarm Manager 4-2  
MAINVIEW for UNIX System Services link 2-37  
MAINVIEW for WebSphere Application Server 2-37, 2-43  
MAINVIEW Selection Menu 2-4  
managing views 2-8

menus

    EZIP Menu 2-3, 2-5  
    MAINVIEW Selection Menu 2-4  
    overview 2-3

messages

    format 5-2, 5-4  
    generating alarms 4-2  
    interpreting 5-2  
    MAINVIEW for IP 5-8  
    severity levels 5-3

Multiple Virtual Storage. *See* MVS  
MVALPAS data set member 4-3  
MVS (Multiple Virtual Storage) A-2

## N

navigation 2-3, 2-7  
network connections 2-11  
network devices 2-36  
network links 2-36  
network routers 2-40  
nodes. *See* IP addresses

## O

online Help 2-3  
Open Systems Adapter. *See* OSA  
operator commands A-2  
OSA (Open Systems Adapter) 2-36  
overview, MAINVIEW for IP 1-2

## P

packet tracing  
    accessing packet details 2-31  
    clearing entries 2-33  
    diagnostic feature 2-18  
    displaying 2-29  
    drill-down function 2-31, 2-32  
    limiting trace parameters 2-27  
    PKTTRACD view 2-30  
    PKTTRACd view 2-31, 2-32  
    PKTTRACF view 2-29  
    PKTTRACS view 2-26

---

packet tracing (*continued*)  
    starting 2-26  
    stopping 2-28  
    viewing packet details 2-32

panels  
    Session Control Parameters 2-4  
    using and managing 2-8

parameters  
    historical data 3-4  
    Session Control Parameters panel 2-4  
    SYSIN 5-5  
    updating SNMP parameters 2-41

parms. *See* parameters

PAS (product address space) 2-18

PCONS view 2-19, 2-20

performance, applications 1-2, 2-11

ping  
    command 2-11  
    definition 2-14  
    diagnostic feature 2-18  
    performing 2-20

Ping Information view 2-20

PING view 2-15

PKTTRACD view 2-19, 2-30, 2-31

PKTTRACd view 2-31, 2-32

PKTTRACF view 2-19, 2-29

PKTTRACS view 2-19, 2-26

PORTRSPP view 2-45

PORTRSPS view 2-45

ports, configuration 2-10

prepackaged alarms. *See* sample alarms

primary menu 2-5

problem reports, documentation 5-5

problems, reporting 5-5

product address space. *See* PAS

product features 1-3

product overview 1-2

product support 5-4

PROFILE data sets 2-10

program members, SAS 1-4

protocols  
    FTP 2-35, 5-6  
    SNMP 1-3  
    TCP/IP 1-2, 2-9, 2-10  
    UDP 2-10

## Q

Quit command 2-46

## R

remote applications 2-9

reports  
    historical performance 3-2  
    problem documentation 5-5

resource links. *See* hyperlinks

response times  
    product overview 1-3  
    statistics 2-45

RETURN command 2-46

routers 2-40

## S

sample alarms 4-5

sample batch job 5-7

SAS (Statistical Analysis System) programs 1-4

SDATA command 5-6

Select View option 2-3

Selection Menu, MAINVIEW 2-4

service level agreements. *See* SLA

Session Control Parameters panel 2-4

setalarm command 4-3

severity codes 5-3

Simple Network Management Protocol. *See* SNMP

SKTTRACD view 2-19

SKTTRACF view 2-19

SKTTRACS view 2-19

SLA (service level agreement) 2-43

SMF (system management facility),  
    configuration 2-10

SMFCONF view 2-10

SNMP (Simple Network Management Protocol)  
    2-40  
        defining monitored nodes 2-42

SNMPDEF view 2-40, 2-41, 2-42

SNMPIF view 2-40

SNMPIP view 2-40

SNMPSYS view 2-40

SNMPTCP view 2-40

---

SNMPUDP view 2-40  
socket tracing 2-18  
SSID (subsystem ID), session parameters 2-5  
stacks  
    *See also* IP stacks  
    availability 2-9  
    connections 2-11  
    product overview 1-2  
    TCP/IP 2-9  
startup parameters 2-41  
Statistical Analysis System. *See* SAS  
storage usage 2-44  
support, customer 5-4  
SVC dumps 5-5  
SYSIN parameters 5-5  
system management facility. *See* SMF

## T

TACAPPL view 2-9  
TACCACHD view 2-39  
TACCACHE view 2-38, 2-43  
TACDEVS view 2-36  
TACFTPF view 2-35  
TACFTPJ view 2-35  
TACFTPU view 2-35  
TACLNKS view 2-36  
TACOSA3 view 2-36  
TACOSAC view 2-36  
TACOSAD view 2-36  
TACOSAL view 2-36  
TACOSAU view 2-36  
TACPORT view 2-10  
TACROUT view 2-40  
TACSLAP view 2-43  
TACTCSB view 2-9  
TCONS view 2-19, 2-23  
TCP (Transmission Control Protocol)  
    *See also* TCP  
    configuration 2-10  
    connections 2-11  
    product overview 1-2  
    stacks view 2-9  
TCP/IP Stacks view 2-9  
TCPCONF view 2-10  
TCPCONS view 2-11  
technical support 5-4

terminating connections 2-12  
threshold conditions 2-8  
thresholds 4-2  
throughput  
    application information view 2-9  
    product overview 1-3  
    statistics 2-45  
TIME command  
    definition 2-46  
    NEXT and PREV parameters 3-11  
    overview 3-2  
    using 3-4  
timeframes, moving between 3-11  
TRACE view 2-17  
TRACEDET view 2-25  
Traceroute  
    accessing details 2-25  
    command 2-11  
    diagnostic feature 2-18  
    performing 2-22  
    TR line command 2-16  
Traceroute Information view 2-23  
traffic. *See* throughput  
Transmission Control Protocol/Internet Protocol.  
    *See* TCP and IP  
TRSMAN 5-6, 5-7  
TSO command line 5-6  
tsoisrddn command 4-2

## U

UDP (User Datagram Protocol)  
    configuration 2-10  
    connections 2-11  
UDPCONF view 2-10  
UDPCONS view 2-11  
User Datagram Protocol. *See* UDP  
USS (UNIX System Services). *See* MAINVIEW  
    for UNIX System Services

## V

views  
    accessing EZIP Menu 2-8  
    Application 2-9  
    displaying list 2-3

---

views (*continued*)

drilling down 2-8, 2-25, 2-31

PCONS 2-20

PING 2-15

PKTTRACD 2-30

PKTTRACd 2-31, 2-32

PKTTRACF 2-29

PKTTRACS 2-26

SNMPDEF 2-42

TACCACHD 2-39

TACCACHE 2-38

TCONS 2-23

TRACE 2-17

TRACEDT 2-25

using and managing panels 2-8

WASPERF 2-39

VIPA (Virtual IP Address). *See* DVIPA

Virtual Telecommunications Access Method.

*See* VTAM

VTAM (Virtual Telecommunications Access

Method) 2-44

VTMBUFF view 2-44

VTMBUFQ view 2-44

## W

WAS (WebSphere Application Server). *See*

MAINVIEW for WebSphere Application  
Server

WASPERF view 2-39

Web cache analysis 2-38, 2-43

write-to-operator. *See* WTO

WTO (write-to-operator) 2-13

## X

XSUPP (Exit Suppression) command A-2

# END USER LICENSE AGREEMENT NOTICE

**BY OPENING THE PACKAGE, INSTALLING, PRESSING "AGREE" OR "YES" OR USING THE PRODUCT, THE ENTITY OR INDIVIDUAL ENTERING INTO THIS AGREEMENT AGREES TO BE BOUND BY THE FOLLOWING TERMS. IF YOU DO NOT AGREE WITH ANY OF THESE TERMS, DO NOT INSTALL OR USE THE PRODUCT, PROMPTLY RETURN THE PRODUCT TO BMC OR YOUR BMC RESELLER, AND IF YOU ACQUIRED THE LICENSE WITHIN 30 DAYS OF THE DATE OF YOUR ORDER CONTACT BMC OR YOUR BMC RESELLER FOR A REFUND OF LICENSE FEES PAID. IF YOU REJECT THIS AGREEMENT, YOU WILL NOT ACQUIRE ANY LICENSE TO USE THE PRODUCT.**

This Agreement ("**Agreement**") is between the entity or individual entering into this Agreement ("**You**") and BMC Software Distribution, Inc., a Delaware corporation located at 2101 CityWest Blvd., Houston, Texas, 77042, USA or its affiliated local licensing entity ("**BMC**"). "**You**" includes you and your Affiliates. "**Affiliate**" is defined as an entity which controls, is controlled by or shares common control with a party. THIS AGREEMENT WILL APPLY TO THE PRODUCT, UNLESS (1) YOU AGREED TO A WEB BASED LICENSE AGREEMENT WITH BMC WHEN ORDERING THE PRODUCT, IN WHICH CASE THAT WEB BASED LICENSE AGREEMENT GOVERNS THE USE OF THE PRODUCT, OR (2) IF YOU DID NOT AGREE TO A WEB BASED LICENSE AGREEMENT WITH BMC WHEN ORDERING THE PRODUCT AND YOU HAVE A WRITTEN LICENSE AGREEMENT WITH BMC, THEN THAT WRITTEN AGREEMENT GOVERNS THE USE OF THE PRODUCT. THE ELECTRONIC AGREEMENT PROVIDED WITH THE PRODUCT AS PART OF THE INSTALLATION OF THE PRODUCT WILL NOT APPLY. In addition to the restrictions imposed under this Agreement, any other usage restrictions contained in the Product installation instructions or release notes shall apply to Your use of the Product.

**PRODUCT AND CAPACITY.** "**Software**" means the object code version of the computer programs provided, via delivery or electronic transmission, to You. Software includes computer files, enhancements, maintenance modifications, upgrades, updates, bug fixes, and error corrections.

**"Documentation"** means all written or graphical material provided by BMC in any medium, including any technical specifications, relating to the functionality or operation of the Software.

**"Product"** means the Software and Documentation.

**"License Capacity"** means the licensed capacity for the Software with the pricing and other license defining terms, including capacity restrictions, such as tier limit, total allowed users, gigabyte limit, quantity of Software, and/or other capacity limitations regarding the Software. For licenses based on the power of a computer, You agree to use BMC's current computer classification scheme, which is available at <http://www.bmc.com> or can be provided to You upon request.

**ACCEPTANCE.** The Product is deemed accepted by You, on the date that You received the Product from BMC.

**LICENSE.** Subject to the terms of this Agreement, as well as Your payment of applicable fees, BMC grants You a non-exclusive, non-transferable, perpetual (unless a term license is provided on an order) license for each copy of the Software, up to the License Capacity, to do the following:

- (a) install the Software on Your owned or leased hardware located at a facility owned or controlled by You in the country where You acquired the license;
- (b) operate the Software solely for processing Your own data in Your business operations; and
- (c) make one copy of the Software for backup and archival purposes only (collectively a "**License**").

If the Software is designed by BMC to permit you to modify such Software, then you agree to only use such modifications or new software programs for Your internal purposes or otherwise consistent with the License. BMC grants You a license to use the Documentation solely for Your internal use in Your operations.

**LICENSE UPGRADES.** You may expand the scope of the License Capacity only pursuant to a separate agreement with BMC for such expanded usage and Your payment of applicable fees. There is no additional warranty period or free support period for license upgrades.

**RESTRICTIONS:** You agree to **NOT**:

- (a) disassemble, reverse engineer, decompile or otherwise attempt to derive any Software from executable code;
- (b) distribute or provide the Software to any third party (including without limitation, use in a service bureau, outsourcing environment, or processing the data of third parties, or for rental, lease, or sublicense); or
- (c) provide a third party with the results of any functional evaluation or benchmarking or performance tests, without BMC's prior written approval, unless prohibited by local law.

**TRIAL LICENSE.** If, as part of the ordering process, the Product is provided on a trial basis, then these terms apply: (i) this license consists solely of a non-exclusive, non-transferable evaluation license to operate the Software for the period of time specified from BMC or, if not specified, a 30 day time period ("**Trial Period**") only for evaluating whether You desire to acquire a capacity-based license to the Product for a fee; and (ii) Your use of the Product is on an AS IS basis without any warranty, and **BMC, ITS AFFILIATES AND RESELLERS, AND LICENSORS DISCLAIM ANY AND ALL WARRANTIES (INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT) AND HAVE NO LIABILITY WHATSOEVER RESULTING FROM THE USE OF THIS PRODUCT UNDER THIS TRIAL LICENSE ("Trial License").** BMC may terminate for its convenience a Trial License upon notice to You. When the Trial Period ends, Your right to use this Product automatically expires. If You want to continue Your use of the Product beyond the Trial Period, contact BMC to acquire a capacity-based license to the Product for a fee.

**TERMINATION.** This Agreement shall immediately terminate if You breach any of its terms. Upon termination, for any reason, You must uninstall the Software, and either certify the destruction of the Product or return it to BMC.

**OWNERSHIP OF THE PRODUCT.** BMC or its Affiliates or licensors retain all right, title and interest to and in the BMC Product and all intellectual property, informational, industrial property and proprietary rights therein. BMC neither grants nor otherwise transfers any rights of ownership in the BMC Product to You. BMC Products are protected by applicable copyright, trade secret, and industrial and intellectual property laws. BMC reserves any rights not expressly granted to You herein.

**CONFIDENTIAL AND PROPRIETARY INFORMATION.** The BMC Products are and contain valuable confidential information of BMC (“**Confidential Information**”). Confidential Information means non-public technical and non-technical information relating to the BMC Products and Support, including, without limitation, trade secret and proprietary information, and the structure and organization of the Software. You may not disclose the Confidential Information to third parties. You agree to use all reasonable efforts to prevent the unauthorized use, copying, publication or dissemination of the Product.

**WARRANTY.** Except for a Trial License, BMC warrants that the Software will perform in substantial accordance with the Documentation for a period of one year from the date of the order. This warranty shall not apply to any problems caused by software or hardware not supplied by BMC or to any misuse of the Software.

**EXCLUSIVE REMEDY.** BMC’s entire liability, and Your exclusive remedy, for any defect in the Software during the warranty period or breach of the warranty above shall be limited to the following: BMC shall use reasonable efforts to remedy defects covered by the warranty or replace the defective Software within a reasonable period of time, or if BMC cannot remedy or replace such defective copy of the Software, then BMC shall refund the amount paid by You for the License for that Software. BMC’s obligations in this section are conditioned upon Your providing BMC prompt access to the affected Software and full cooperation in resolving the claim.

**DISCLAIMER. EXCEPT FOR THE EXPRESS WARRANTIES ABOVE, THE PRODUCT IS PROVIDED “AS IS.” BMC, ITS AFFILIATES AND LICENSORS SPECIFICALLY DISCLAIM ALL OTHER WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. BMC DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT ALL DEFECTS CAN BE CORRECTED.**

**DISCLAIMER OF DAMAGES. IN NO EVENT IS BMC, ITS AFFILIATES OR LICENSORS LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES RELATING TO OR ARISING OUT OF THIS AGREEMENT, SUPPORT, AND/OR THE PRODUCT (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, LOST COMPUTER USAGE TIME, AND DAMAGE OR LOSS OF USE OF DATA), EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND IRRESPECTIVE OF ANY NEGLIGENCE OF BMC OR WHETHER SUCH DAMAGES RESULT FROM A CLAIM ARISING UNDER TORT OR CONTRACT LAW.**

**LIMITS ON LIABILITY. BMC’S AGGREGATE LIABILITY FOR DAMAGES IS LIMITED TO THE AMOUNT PAID BY YOU FOR THE LICENSE TO THE PRODUCT.**

**SUPPORT.** If Your order includes support for the Software, then BMC agrees to provide support (24 hours a day/7 days a week) (“**Support**”). You will be automatically re-enrolled in Support on an annual basis unless BMC receives notice of termination from You as provided below. There is a free support period during the one year warranty period.

(a) **Support Terms.** BMC agrees to make commercially reasonable efforts to provide the following Support: (i) For malfunctions of supported versions of the Software, BMC provides bug fixes, patches or workarounds in order to cause that copy of the Software to operate in substantial conformity with its then-current operating specifications; and (ii) BMC provides new releases or versions, so long as such new releases or versions are furnished by BMC to all other enrolled Support customers without additional charge. BMC may refuse to provide Support for any versions or releases of the Software other than the most recent version or release of such Software made available by BMC. Either party may terminate Your enrollment in Support upon providing notice to the other at least 30 days prior to the next applicable Support anniversary date. If You re-enroll in Support, BMC may charge You a reinstatement fee of 1.5 times what You would have paid if You were enrolled in Support during that time period.

(b) **Fees.** The annual fee for Support is 20% of the Software’s list price less the applicable discount or a flat capacity based annual fee. BMC may change its prices for the Software and/or Support upon at least 30 days notice prior to Your support anniversary date.

**VERIFICATION.** If requested by BMC, You agree to deliver to BMC periodic written reports, whether generated manually or electronically, detailing Your use of the Software in accordance with this Agreement, including, without limitation, the License Capacity. BMC may, at its expense, audit Your use of the Software to confirm Your compliance with the Agreement. If an audit reveals that You have underpaid fees, You agree to pay such underpaid fees. If the underpaid fees exceed 5% of the fees paid, then You agree to also pay BMC’s reasonable costs of conducting the audit.

**EXPORT CONTROLS.** You agree not to import, export, re-export, or transfer, directly or indirectly, any part of the Product or any underlying information or technology except in full compliance with all United States, foreign and other applicable laws and regulations.

**GOVERNING LAW.** This Agreement is governed by the substantive laws in force, without regard to conflict of laws principles: (a) in the State of New York, if you acquired the License in the United States, Puerto Rico, or any country in Central or South America; (b) in the Province of Ontario, if you acquired the License in Canada (subsections (a) and (b) collectively referred to as the “**Americas Region**”); (c) in Singapore, if you acquired the License in Japan, South Korea, Peoples Republic of China, Special Administrative Region of Hong Kong, Republic of China, Philippines, Indonesia, Malaysia, Singapore, India, Australia, New Zealand, or Thailand (collectively, “**Asia Pacific Region**”); or (d) in the Netherlands, if you acquired the License in any other country not described above. The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed in its entirety.

**ARBITRATION. ANY DISPUTE BETWEEN YOU AND BMC ARISING OUT OF THIS AGREEMENT OR THE BREACH OR ALLEGED BREACH, SHALL BE DETERMINED BY BINDING ARBITRATION CONDUCTED IN ENGLISH. IF THE DISPUTE IS INITIATED IN THE AMERICAS REGION, THE ARBITRATION SHALL BE HELD IN NEW YORK, U.S.A., UNDER THE CURRENT COMMERCIAL OR INTERNATIONAL, AS APPLICABLE, RULES OF THE AMERICAN ARBITRATION ASSOCIATION. IF THE DISPUTE IS INITIATED IN A COUNTRY IN THE ASIA PACIFIC REGION, THE ARBITRATION SHALL BE HELD IN SINGAPORE, SINGAPORE UNDER THE CURRENT UNCITRAL ARBITRATION RULES. IF THE DISPUTE IS INITIATED IN A COUNTRY OUTSIDE OF THE AMERICAS REGION OR ASIA PACIFIC REGION, THE ARBITRATION SHALL BE HELD IN AMSTERDAM, NETHERLANDS UNDER THE CURRENT UNCITRAL ARBITRATION RULES. THE COSTS OF THE ARBITRATION SHALL BE BORNE EQUALLY PENDING THE ARBITRATOR’S AWARD. THE AWARD RENDERED SHALL BE FINAL AND BINDING UPON THE PARTIES AND SHALL NOT BE SUBJECT TO APPEAL TO ANY COURT, AND MAY BE ENFORCED IN ANY COURT OF COMPETENT JURISDICTION. NOTHING IN THIS AGREEMENT SHALL BE DEEMED AS PREVENTING EITHER PARTY FROM SEEKING INJUNCTIVE RELIEF FROM ANY COURT HAVING JURISDICTION OVER THE PARTIES AND THE SUBJECT MATTER OF THE DISPUTE AS NECESSARY TO PROTECT EITHER PARTY’S CONFIDENTIAL INFORMATION, OWNERSHIP, OR ANY OTHER**

**PROPRIETARY RIGHTS. ALL ARBITRATION PROCEEDINGS SHALL BE CONDUCTED IN CONFIDENCE, AND THE PARTY PREVAILING IN ARBITRATION SHALL BE ENTITLED TO RECOVER ITS REASONABLE ATTORNEYS' FEES AND NECESSARY COSTS INCURRED RELATED THERETO FROM THE OTHER PARTY.**

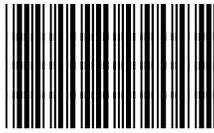
**U.S. GOVERNMENT RESTRICTED RIGHTS.** The Software under this Agreement is "commercial computer software" as that term is described in 48 C.F.R. 252.227-7014(a)(1). If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of this Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulations ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of this Agreement as specified in 48 C.F.R. 227.7202 of the DOD FAR Supplement and its successors.

**MISCELLANEOUS TERMS.** You agree to pay BMC all amounts owed no later than 30 days from the date of the applicable invoice, unless otherwise provided on the order for the License to the Products. You will pay, or reimburse BMC, for taxes of any kind, including sales, use, duty, tariffs, customs, withholding, property, value-added (VAT), and other similar federal, state or local taxes (other than taxes based on BMC's net income) imposed in connection with the Product and/or the Support. This Agreement constitutes the entire agreement between You and BMC and supersedes any prior or contemporaneous negotiations or agreements, whether oral, written or displayed electronically, concerning the Product and related subject matter. No modification or waiver of any provision hereof will be effective unless made in a writing signed by both BMC and You. You may not assign or transfer this Agreement or a License to a third party without BMC's prior written consent. Should any provision of this Agreement be invalid or unenforceable, the remainder of the provisions will remain in effect. The parties have agreed that this Agreement and the documents related thereto be drawn up in the English language. Les parties exigent que la présente convention ainsi que les documents qui s'y rattachent soient rédigés en anglais.

SW EULA Int 030102



# Notes



\*19382\*