Contacting BMC Software

Several methods are available for contacting BMC Software.

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

**United States and Canada**

**Address**

BMC SOFTWARE INC
2103 CITYWEST BLVD
HOUSTON TX 77042-2827 USA

**Telephone**

1 713 918 8800
or
1 800 841 2031

**Fax**

1 713 918 8000

**Outside United States and Canada**

**Telephone**

+01 713 918 8800

**Fax**

+01 713 918 8000

© Copyright 2003-2016 BMC Software, Inc.

BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners.

Cisco and Explorer are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

CICS, DB2, HiperSockets, IBM, IBM z, IMS, MQSeries, MVS, System z, VTAM, WebSphere, z/OS, and z/VM are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Linux is the registered trademark of Linus Torvalds.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

UNIX is the registered trademark of The Open Group in the US and other countries.

The information included in this documentation is the proprietary and confidential information of BMC Software, Inc., its affiliates, or licensors. Your use of this information is subject to the terms and conditions of the applicable End User License agreement for the product and to the proprietary and restricted rights notices included in the product 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 UNPUBLISHED—RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES.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.
Customer support

Support website
You can obtain technical support from BMC 24 hours a day, 7 days a week at [http://www.bmc.com/support](http://www.bmc.com/support). From this website, you can:

- Read overviews about support services and programs that BMC offers
- Find the most current information about BMC products
- Search a database for problems similar to yours and possible solutions
- Order or download product documentation
- Download products and maintenance
- Report a problem or ask a question
- Subscribe to receive proactive e-mail alerts
- Find worldwide BMC 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 1 800 537 1813 or send an e-mail message to customer_support@bmc.com. (In the subject line, enter **SupID:** yourSupportContractID, such as SupID:12345). Outside the United States and Canada, contact your local support center for assistance.

Before contacting BMC
Have the following information available so that Customer Support can begin working on your issue 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
  - Messages from related software
License key and password information

If you have questions about your license key or password, contact Customer Support through one of the following methods:

- Send an e-mail message to customer_support@bmc.com. (In the Subject line, enter SupID:yourSupportContractID, such as SupID:12345.)
- In the United States and Canada, call 1 800 537 1813. Outside the United States and Canada, contact your local support center for assistance.
Contents

About this book ................................................................. 9
Related publications .............................................................. 9
Conventions ......................................................................... 10
Syntax statements .................................................................. 10

Chapter 1 Overview of MainView for IP .......................... 13
Features and functions ............................................................ 13

Chapter 2 Navigation in MainView for IP .................. 17
Overview of navigating in MainView for IP ......................... 17
Accessing MainView for IP ...................................................... 17
Easy menus (EZ) in Mainview for IP ...................................... 19
Selecting menus in MainView for IP ....................................... 20
Views in MainView for IP ......................................................... 20
Setting the context for a view using the CONtext command ................................................. 21
Alias Target ................................................................. 23

Chapter 3 Using the views of MainView for IP .............. 25
Overview of using MainView for IP views ......................... 25
IPv6 addressing support in MainView for IP ....................... 26
Availability options in MainView for IP ............................... 28
TCP/IP monitor views .......................................................... 29
Availability monitor ............................................................. 29
Availability ping in MainView for IP ...................................... 33
Monitoring MainView .......................................................... 36
Traffic and response times information in MainView for IP ...................................................... 37
Connections views in MainView for IP ............................... 38
Sample connection views in MainView for IP ................. 39
Dropping a connection by using a line command in MainView IP ................................................. 40
Pinging a device by using a line command in MainView IP ......................................................... 42
Performing a traceroute on a device by using a line command ................................................. 44
Performing a packet trace by using a line command ................................................................. 46
Connection errors views in MainView for IP ......................... 47
VTAM Session Data views in MainView for IP ..................... 47
VTAM Resource views in MainView for IP ......................... 49
Monitor and Auto Activate VTAM Resources ...................................................... 50
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Historical data display in MainView for IP</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td>Overview of the historical data display</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td>Data availability</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>TIME command in MainView for IP</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>Viewing JOBNAME response times in MainView for IP</td>
<td>99</td>
</tr>
<tr>
<td></td>
<td>Displaying Intvl Time field</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>Moving between time frames in MainView for IP</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>Time and duration fields</td>
<td>104</td>
</tr>
<tr>
<td>5</td>
<td>MainView for IP alarm settings manager</td>
<td>107</td>
</tr>
<tr>
<td></td>
<td>MainView Alarm Manager</td>
<td>107</td>
</tr>
<tr>
<td></td>
<td>Setting alarms</td>
<td>108</td>
</tr>
<tr>
<td></td>
<td>Sample alarms shipped with MainView for IP</td>
<td>110</td>
</tr>
<tr>
<td></td>
<td>Alarm definitions in MainView for IP</td>
<td>110</td>
</tr>
<tr>
<td>A</td>
<td>Operator commands in MainView for IP</td>
<td>113</td>
</tr>
<tr>
<td></td>
<td>Commands in MainView for IP</td>
<td>113</td>
</tr>
<tr>
<td></td>
<td>DUMP - Dump for MainView for IP address and data space</td>
<td>113</td>
</tr>
<tr>
<td></td>
<td>OPTIONS - Display MainView for IP options status</td>
<td>113</td>
</tr>
<tr>
<td>B</td>
<td>Troubleshooting MainView for IP</td>
<td>115</td>
</tr>
<tr>
<td></td>
<td>Message format</td>
<td>115</td>
</tr>
<tr>
<td></td>
<td>Contacting BMC Software customer support</td>
<td>116</td>
</tr>
<tr>
<td></td>
<td>Gathering problem report documentation</td>
<td>117</td>
</tr>
<tr>
<td></td>
<td>Selecting debug data collection points</td>
<td>119</td>
</tr>
</tbody>
</table>
About this book

This book contains detailed product information 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).

Like most BMC documentation, this book is available in printed and online formats. To request printed books or to view online books and notices (such as release notes and technical bulletins), see the support website at http://www.bmc.com/support.

**Note**

Online books are formatted as PDF or HTML files. To view, print, or copy PDF books, use the free Adobe Reader from Adobe Systems. If your product installation does not install the reader, you can obtain the reader at http://www.adobe.com.

The software also offers online Help. To access Help, press F1 within any product or click the **Help** button in graphical user interfaces (GUIs).

Related publications

From the BMC Support Central website, you can use the following methods to access related publications that support your product or solution:

View Quick Course videos (short overviews of selected product concepts, tasks, or features), which are available from the following locations:

— Documentation Center (primary center and secured center)

— Support Central (at http://www.bmc.com/support/mainframe-demonstrations)

— BMC Mainframe YouTube channel (https://www.youtube.com/user/BMCSoftwareMainframe)


Products with online interfaces also offer online Help via the F1 key or, for graphical user interfaces (GUIs), via a Help button.

Tip
If you prefer hardcopy documentation, you can order it from your BMC sales representative or from Support Central. Also, from Support Central you can subscribe to receive proactive e-mail alerts when BMC issues notices.

Conventions
This document uses the following special conventions:

■ All syntax, operating system terms, and literal examples are presented in this typeface.

■ Variable text in path names, system messages, or syntax is displayed in italic text: testsys/instance/fileName

■ Menu sequences use a symbol to convey the sequence. For example, Actions => Create Test instructs you to choose the Create Test command from the Actions menu.

Syntax statements
This topic explains conventions for showing syntax statements.
A sample statement follows:

```
COMMAND KEYWORD1 [KEYWORD2 | KEYWORD3] KEYWORD4={YES | NO} fileName...
```

The following table explains conventions for syntax statements and provides examples:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Items in italic type represent variables that you must replace with a name</td>
<td>alias</td>
</tr>
<tr>
<td>or value. If a variable is represented by two or more words, initial</td>
<td>databaseDirectory</td>
</tr>
<tr>
<td>capitals distinguish the second and subsequent words.</td>
<td>serverHostName</td>
</tr>
<tr>
<td>Brackets indicate optional items. Do not type the brackets when you</td>
<td>[tableName, columnName, field]</td>
</tr>
<tr>
<td>enter the option. A comma means that you can choose one or more of the</td>
<td>[-full, -incremental, -level]</td>
</tr>
<tr>
<td>listed options. You must use a comma to separate the options if you</td>
<td></td>
</tr>
<tr>
<td>choose more than one option.</td>
<td></td>
</tr>
<tr>
<td>Braces indicate that at least one of the enclosed items is required.</td>
<td>{DBDName</td>
</tr>
<tr>
<td>Do not type the braces when you enter the item.</td>
<td>UNLOAD device={disk</td>
</tr>
<tr>
<td>A vertical bar means that you can choose only one of the listed items.</td>
<td>{-a</td>
</tr>
<tr>
<td>In the example, you would choose either commit or cancel.</td>
<td>{commit</td>
</tr>
<tr>
<td>An ellipsis indicates that you can repeat the previous item or items as</td>
<td>columnName...</td>
</tr>
<tr>
<td>many times as necessary.</td>
<td></td>
</tr>
</tbody>
</table>
Overview of MainView for IP

MainView for IP provides utilities that enable you to monitor IBM z/OS mission-critical application performance. This chapter describes the features and functions available in MainView for IP.

MainView for IP collects data from the Transmission Control Protocol/Internet Protocol (TCP/IP) stack and displays it through the MainView console as configurable views. You can monitor applications by job name, IP address, and port, and analyze which enterprise resources have priority access to critical data. You can also configure data collection in MainView for IP to allow filtering, which enables you to view this information (but not to change it).

Features and functions

This topic describes the features and functions provided by MainView for IP that enable monitoring and management of TCP/IP stacks through customizable views.

Table 1 on page 13 describes the monitoring and management features and the functions that are available in MainView for IP.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Initiates specific actions in a view, such as dropping a connection, pinging a device, or performing a traceroute</td>
</tr>
<tr>
<td>Activity</td>
<td>Displays information about the availability and activity of application and stack connections</td>
</tr>
<tr>
<td>Availability monitoring</td>
<td>Provides a single view from which you can monitor critical resources, such as applications, devices, links, and other resources</td>
</tr>
<tr>
<td>Availability ping</td>
<td>Allows you to ping an IP network device automatically to determine its availability and provide device response times</td>
</tr>
<tr>
<td>Cisco MIB support</td>
<td>Provides detailed Cisco data to keep your critical routers running at their peak</td>
</tr>
<tr>
<td>Configuration</td>
<td>Displays configuration information by TCP, UDP, IP, SMF, and port</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connections</td>
<td>Displays information about the devices that are connected to an application by domain name, IP address, and remote port number</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Displays information about a ping or a traceroute that you requested; performs packet tracing and socket tracing</td>
</tr>
<tr>
<td>Dynamic VIPA</td>
<td>Displays information about dynamic Virtual IP Addresses (DVIPA)</td>
</tr>
<tr>
<td>Enterprise extender</td>
<td>Displays information for Enterprise Extenders (EEs) shipped through the UDP protocol and information for Rapid Transfer Protocol (RTP) pipes that are used by Enterprise Extenders</td>
</tr>
<tr>
<td>FTP statistics</td>
<td>Displays File Transfer Protocol (FTP) information</td>
</tr>
<tr>
<td>HiperSockets</td>
<td>Displays detailed views for applications that use hipersockets, such as devices, links, routes, sessions, and channel data</td>
</tr>
<tr>
<td>Historical data</td>
<td>Displays information about previous performance (to compare with current performance)</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Displays information about network devices, network links, and Open Systems Adapter (OSA) cards</td>
</tr>
<tr>
<td>IPv6</td>
<td>Displays IP addresses along 16-bit boundaries, with each 16-bit block converted to a 4-digit hexadecimal number separated by colons An IP address is 128 bits or 16 bytes long. In contrast to IPv6, IPv4 displays IP addresses in dotted decimal format. The IPv6 feature is available in every view that contains an IP address field.</td>
</tr>
<tr>
<td>IP pacing</td>
<td>Delays (or &quot;paces&quot;) outbound data from any TCP/IP application to provide more processing time to business-critical applications and displays information about applications that have been paced</td>
</tr>
<tr>
<td>IP resource links</td>
<td>Links to views in MainView for z/OS, MainView for UNIX System Services, MainView for VTAM, and MainView for WebSphere Application Server</td>
</tr>
<tr>
<td>IPSec</td>
<td>Displays IP Security and defensive filtering configuration information for the TCPIP stack</td>
</tr>
<tr>
<td>Name Resolver</td>
<td>Displays the Name Resolver configuration information</td>
</tr>
<tr>
<td>Open Systems Adapter</td>
<td>Gathers data about Open Systems Adapter (OSA) devices You can view OSA configuration information, utilization statistics, network device details, network link details, and ethernet-like statistics.</td>
</tr>
<tr>
<td>Packet and socket tracing</td>
<td>Provides sophisticated packet and socket tracing capabilities that can be started and stopped dynamically You can filter by protocol type, IP address, source port, and destination port. You can view packet header information in both a formatted and unformatted display. You can also view a subset of the actual packet data in hexadecimal dump format.</td>
</tr>
<tr>
<td>Routes and OSPF</td>
<td>Provides information about all Routes as well as statistics and parameters related to OSPF</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Shared Memory Communications over RDMA (SMC-R)</td>
<td>Displays configuration and statistics for Shared Memory Communications over RDMA.</td>
</tr>
<tr>
<td>SNMP data collection</td>
<td>Displays performance information about TCP, UDP, IP, system, interface router, OSPF, CISCO router, and network routes for every IP node that you specify</td>
</tr>
<tr>
<td>Security</td>
<td>Displays information about the Intrusion Detection Services (IDS), which enables detecting attacks and applying defensive mechanisms on the z/OS server</td>
</tr>
<tr>
<td>Service levels</td>
<td>Displays information about application availability and your web servers to help ensure that you are meeting your service level agreements</td>
</tr>
<tr>
<td>Storage</td>
<td>Displays statistics from the following areas about buffer pools and storage usage:</td>
</tr>
<tr>
<td></td>
<td>■ Communications storage manager (CSM)</td>
</tr>
<tr>
<td></td>
<td>■ Virtual Telecommunications Access Method (VTAM)</td>
</tr>
<tr>
<td></td>
<td>■ TCP/IP private and common storage</td>
</tr>
<tr>
<td></td>
<td>■ Common storage area (CSA)</td>
</tr>
<tr>
<td>Threshold/alarm conditions</td>
<td>Lets you add visual indicaters that use color or highlighting to instantly show when resources are reaching a critical state</td>
</tr>
<tr>
<td>Traffic/response times</td>
<td>Displays information about the amount of data that is being sent and received (and connection detail), and displays information about host and network response times by station (IP address or domain name), port, subnet, or TN3270 session</td>
</tr>
<tr>
<td>VTAM session data collection</td>
<td>Collects and displays VTAM session information, and session awareness (SAW) data. Also collects VTAM PIUs</td>
</tr>
<tr>
<td>VTAM PPO data</td>
<td>Collects and displays VTAM messages collected through the VTAM Primary Program Operator</td>
</tr>
<tr>
<td>VTAM Resources</td>
<td>Collects and displays VTAM resources, and allows actions to be performed against each VTAM resource</td>
</tr>
</tbody>
</table>
Navigation in MainView for IP

MainView windows-mode technology provides views that summarize data from multiple subsystems. This section provides guidelines about navigating within the MainView for IP views.

Overview of navigating in MainView for IP

This chapter describes the ways that you can navigate between the detailed and summary views of collected data within the MainView for IP product.

Accessing MainView for IP

The following procedures show how to display a list of detail and summary views and how to access MainView for IP from the MainView selection menu.

Note

- When MainView Explorer is installed on your system you can access MainView for IP through a browser.
- For information about using MainView Explorer to access MainView products, see the MainView User Guide.

To display list of detailed and summary views in MainView for IP

1. On the command line enter VIEWS
2. Press ENTER

To access MainView for IP

1. On the option line in the Figure 1 on page 18, type N to select Network Management, and press Enter.
Figure 1 on page 18 shows the MainView Selection menu from where you access MainView for IP.

Figure 1: MainView Selection Menu

<table>
<thead>
<tr>
<th>OPTION</th>
<th>MAINVIEW Selection Menu</th>
<th>DATE</th>
<th>-- 2011/12/07</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>TIME</td>
<td>-- 04:07:03</td>
</tr>
<tr>
<td>0</td>
<td>Parameters and Options</td>
<td>USERID</td>
<td>-- BMCUID1</td>
</tr>
<tr>
<td>E</td>
<td>Alerts and Alarms</td>
<td>MODE</td>
<td>-- ISPF 6.3</td>
</tr>
<tr>
<td>P</td>
<td>PLEX Management (PLEXMGR)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>U</td>
<td>Utilities, Tools, and Messages</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Copyright BMC Software, Inc.

2 Type 1 to select MainView for IP, and then press Enter.

The Session Control Parameters panel is displayed as shown here:

<table>
<thead>
<tr>
<th>BMC SOFTWARE</th>
<th>SESSION CONTROL PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMAND</td>
<td>---------------------------</td>
</tr>
</tbody>
</table>

Subsystem ID    ===> BBIP (CAS Subsystem ID, ? for list of active SSIDs)
XDM mode        ===> NO     (Execute session in diagnostic mode, Yes/No)

Press ENTER to confirm use of session parameters entered above.

3 In the Subsystem ID field, type BBIP, and then press Enter.

The EZIP menu is displayed as shown here:
Easy menus (EZ) in Mainview for IP

Easy (EZ) menus allow navigation to the views of MainView for IP, based on the component that you want to monitor rather than on a specific view. EZIP is the primary easy menu for MainView for IP.

You can use the selections on this menu to access other high-level easy menus, such as EZRESP, to locate information quickly. Table 2 on page 19 describes the easy menus that are provided in MainView for IP.

Table 2: MainView for IP easy menus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EZAVAIL</td>
<td>Availability monitoring details</td>
</tr>
<tr>
<td>EZCONF</td>
<td>TCP/IP Configuration details</td>
</tr>
<tr>
<td>EZCONS</td>
<td>Connection details</td>
</tr>
<tr>
<td>EZFTP</td>
<td>FTP statistics</td>
</tr>
<tr>
<td>EZHS</td>
<td>HiperSockets details</td>
</tr>
<tr>
<td>EZIDS</td>
<td>Intrusion Detection details</td>
</tr>
<tr>
<td>EZIPSEC</td>
<td>IP Security details</td>
</tr>
<tr>
<td>EZMVENV</td>
<td>Environment settings</td>
</tr>
<tr>
<td>EZOSA</td>
<td>Open Systems Adapter card details</td>
</tr>
<tr>
<td>EZPARMS</td>
<td>Parameter details</td>
</tr>
</tbody>
</table>
### Selecting menus in MainView for IP

You can select the menu or view that you want to display by performing one of the following actions:

- Place the cursor on the menu or view name and press **Enter**.
- Type the name of the easy menu or view (for example, **EZNMP**) on the **COMMAND** line, 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 about how to use the features and services that are available within the MainView environment, see the *MainView User Guide*.

### Views in 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 with any MainView product.

You can also display multiple panels of different sizes simultaneously, and you can direct actions from one panel to another panel, all on one terminal.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EZRESP</td>
<td>Response-time details</td>
</tr>
<tr>
<td>EZROUT</td>
<td>Route details</td>
</tr>
<tr>
<td>EZSMCR</td>
<td>Shared Memory Communications over RDMA</td>
</tr>
<tr>
<td>EZNMP</td>
<td>Simple Network Management Protocol and router details</td>
</tr>
<tr>
<td>EZSTAT</td>
<td>Stack Statistics</td>
</tr>
<tr>
<td>EZSTOR</td>
<td>Storage details</td>
</tr>
<tr>
<td>EZTOPU</td>
<td>Top Users</td>
</tr>
<tr>
<td>EZTTL</td>
<td>Transport Layer Security details</td>
</tr>
<tr>
<td>EZVIPA</td>
<td>Dynamic Virtual IP Address details</td>
</tr>
<tr>
<td>EZVTAMP</td>
<td>Virtual Telecommunications Access Method PPO messages</td>
</tr>
<tr>
<td>EZVTAMS</td>
<td>Virtual Telecommunication Access Method session details</td>
</tr>
<tr>
<td>EZVTAMR</td>
<td>Virtual Telecommunication Access Method resource details</td>
</tr>
</tbody>
</table>
Setting the context for a view using the CONtext command

You can use the **CONtext** command to display data for a target, an SSI context, or a dynamic context. With the **CONtext** command, you can switch from one target to another within a MainView product, or switch to another MainView product.

In MainView for IP, the targets are defined as TCP/IP stacks. MainView for IP detects all TCP/IP stacks and defines a single target for each. MainView for IP displays statistics for only the current target that is set by the **CONtext** command:

```
CON {SSIname | target} product;view
```

where:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSIname</td>
<td>target</td>
</tr>
<tr>
<td>product</td>
<td></td>
</tr>
<tr>
<td>;</td>
<td></td>
</tr>
<tr>
<td>view</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

MainView for IP has some views that display statistics that are not TCP/IP stack specific. For these views, statistics are displayed for the whole system, not for a specific TCP/IP stack.

**Example**

To switch from MainView for IP to the MVMQS CHATTR view for GRT2 target (queue manager), this command is used:

```
CON GRT2 MVMQS;CHATTR
```

Table 3: Product values for transfer to windows mode

<table>
<thead>
<tr>
<th>Product value</th>
<th>To access this product</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMF</td>
<td>CMF MONITOR Online</td>
</tr>
<tr>
<td>MVALARM</td>
<td>MainView Alarm Management</td>
</tr>
<tr>
<td>MVCICS</td>
<td>MainView for CICS</td>
</tr>
<tr>
<td>MVCSMON</td>
<td>COMMON STORAGE MONITOR (CSMON)</td>
</tr>
<tr>
<td>MVDAC</td>
<td>DATA ACCELERATOR Compression</td>
</tr>
<tr>
<td>MVDB2</td>
<td>MainView for DB2</td>
</tr>
<tr>
<td>MVIMS</td>
<td>MainView for IMS Online and MainView for DBCTL</td>
</tr>
<tr>
<td>Product value</td>
<td>To access this product</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>MVIP</td>
<td>MainView for IP</td>
</tr>
<tr>
<td>MVLNX</td>
<td>MainView for Linux - Servers</td>
</tr>
<tr>
<td>MVMQS</td>
<td>MainView for WebSphere MQ and MainView for WebSphere MQ Integrator</td>
</tr>
<tr>
<td>MVMVS</td>
<td>MainView for z/OS</td>
</tr>
<tr>
<td>MVSP</td>
<td>MainView SYSPROG Services</td>
</tr>
<tr>
<td>MVSRM</td>
<td>MainView Storage Resource Manager (SRM)</td>
</tr>
<tr>
<td>MVTA</td>
<td>MainView Transaction Analyzer</td>
</tr>
<tr>
<td>MVUSS</td>
<td>MainView for UNIX System Services</td>
</tr>
<tr>
<td>MVVP</td>
<td>MainView VistaPoint</td>
</tr>
<tr>
<td>MVVTAM</td>
<td>MainView for VTAM</td>
</tr>
<tr>
<td>MVWEB</td>
<td>MainView for WebSphere Application Server</td>
</tr>
<tr>
<td>PLEXMGR</td>
<td>Plex Manager</td>
</tr>
</tbody>
</table>

**Example**

- You can display statistics for a specific stack on the current system, by issuing this command:
  
  CON xxx1

  If you then want to switch from one stack to the another stack, issue this command:

  CON xxx2

- For displaying statistics for a specific TCPIP stack (TCPIP3) on another LPAR (SYSM), issue the following command:

  CON TCPIP3 MVIP * SYSM

- If you want to display statistics for all TCPIP stacks on the system, issue this command:

  CON ALL

When the MainView for IP product is first entered, the panel shown in Figure 2 on page 23 is displayed. In this panel you specify which context is used by default. You can also specify the initial screen to go to (if not specified, the default value is
the EZIP menu). For bypassing this panel, you can specify NO for Confirm, and the product will automatically display the initial screen with the specified context.

**Figure 2: Context Confirmation panel**

<table>
<thead>
<tr>
<th>Command</th>
<th>Context Confirmation --- MAINVIEW for IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm parameters for this session of MAINVIEW for IP</td>
<td></td>
</tr>
<tr>
<td>Context ====&gt; ALL (Default context)</td>
<td></td>
</tr>
<tr>
<td>Screen ====&gt; (Initial screen)</td>
<td></td>
</tr>
<tr>
<td>Confirm ====&gt; NO Yes/No (Present this panel at MVIP start)</td>
<td></td>
</tr>
</tbody>
</table>

**Context**

BMC MAINVIEW for IP lets you display only data for a specific TCPIP stack. Specify the TCPIP stack as the single context.

**Screen**

At startup, the screen listed above will be presented. If set to blank, the default EZIP view will display.

**Confirm**

Designates whether to display this panel every time MVIP is started. Note: If NO, changes can only be made using parameters editor (MVPARMS)

Press ENTER to continue or press HELP for additional information.

---

**Alias Target**

You can specify an alias target for any TCP/IP stack. The alias target is specified on the **MVIPALSD** view, accessible from the **MVIPCNFD** view. The alias target allows you to customize the target instead of using the TCP/IP stack name.

---

**Note**

This is very useful when dealing with multiple LPARs all using the same TCP/IP stack name.
Using the views of MainView for IP

This chapter helps you interpret the views that are provided with the MainView for IP product.

Overview of using MainView for IP views

MainView for IP views display information that help you monitor and manage your network by summarizing application performance data. You can then analyze the data (but not change it).

Using the EZIP Menu you access information about the MainView for IP views, including the following:

■ Application availability
■ Traffic
■ Sessions (or connections)
■ Configuration
■ Routers
■ Service levels

In several views, you can use drill-down functions to view more detailed information about an item. You can drill-down in any view where a field name is highlighted. Some highlighted field names are hyperlinks to other applications or resources.

Sample instructions using drill-down functions (traceroute information), or hyperlinks (IP resource links), sample alarms and threshold conditions are provided in many MainView for IP views. You can use color or highlighting to add visual indicators to show when resources are reaching a critical state.
IPv6 addressing support in MainView for IP

IP version 6 (IPv6) is a version of the Internet Protocol, designed as the successor of IP version 4 (IPv4).

The biggest change in IPv6 is its expanded addressing capability. The IP address in IPv4 is 32 bits or 4 bytes long. The IP address in IPv6 is 128 bits or 16 bytes long. MainView for IP supports IPv6 by providing expanded IP addresses.

IPv4 addresses are represented in dotted decimal format. The 32 bit address is divided at 8 bit boundaries. Each of the 4 sets of 8 bits is converted to its decimal (base 10) equivalent, and the sets are separated from each other by a period (or stop).

For IPv6, the 128 bit address is divided at 16 bit boundaries. Each 16 bit block is converted to a 4 digit hexadecimal number (base 16, 0-F), and the blocks are separated from each other by a colon. Here are two examples of IPv4 and IPv6 uncompressed and compressed addresses.

**Example**

If the uncompressed IPv4 address is:
0000.0000.0000.0000.0000.0000.172.25.121.130

The compressed form is:
::172.25.121.130

**Example**

If the uncompressed IPv6 address is:
2001:0:0:0:0:5BFF:FE3A:2203

The compressed format will be: 2001::5BFF:FE3A:2203

To simplify IPv6 addresses, any consecutive sequence of 16-bit blocks that is set to 0 in the colon hexadecimal format is compressed to "::" (two colons) as shown in the following example:

**Example**

An IPv6 address of 2001:0:0:0:5BFF:FE3A:2203 is compressed to 2001::5BFF:FE3A:2203, and an IPv6 address of 2001:0:0:0:0:0:2203 is compressed to 2001::2203.

The loop back address of 0:0:0:0:0:0:1 in IPv6 (127.0.0.1 in IPv4) is compressed to two colons and 1 (::1).

An unspecified address of 0:0:0:0:0:0:0 is compressed to two colons (::).
The following guidelines apply:

- Zero compression can be used only once in an IPv6 address.
- Only one null string can be replaced with a double colon, which can then be filled out to retrieve the original long form address.
- If there are two null strings, only one can be compressed. If both were compressed, it would be impossible to determine the length of each string, and the address would be ambiguous.

Another form, which is sometimes more convenient in dealing with a mixed environment of IPv4 and IPv6 nodes, is:

```
x:x:x:x:d.d.d
```

The value of \( x \) represents the hexadecimal values of the six high-order 16-bit pieces of the address, and \( d \) represents the decimal values of the four low-order 8-bit pieces of the address.

**Example**

```
0:0:0:0:0:0:172.25.121.130, which can be compressed to ::172.25.121.130.
```

### Long and short IPv6 addresses compatibility in MainView for IP

MainView for IP is a TCP/IP monitor and displays IP addresses on many different views.

Typically, an IPv4 address displays only 15 characters on a 3270 view. An IPv6 address can display up to 39 characters. MainView for IP accommodates customers who are running IPv4 networks, IPv6 networks, or a combination of both.

MainView for IP can display full IPv6 addresses without impacting those networks that are still running IPv4 networks. However, on MainView tabular views where records are displayed on one line is IP addresses must fit within the viewable 80 columns. The MainView detailed views are not affected because the fields can be expanded without impacting other fields in the record.

To accommodate IPv4, IPv6 and mixed networks, MainView for IP will continue to use 16 character fields for both IPv4 and IPv6 addresses. However, for IPv6 addresses that extend beyond 16 characters, only the first 7 characters and the last 7 characters are displayed. Two periods ‘..’ in the middle of the IP address indicate that the IPv6 address has been truncated or shortened.
**Example**

2001:FFA:3E8:2050:1042:2::4103 is displayed in MainView for IP as 2001:FF..2::4103

**Note**

You can change the default of the IPv6 address field through the IPv6 Short Format parameter on the MVIP Parms Configuration (MVIPCONF) view. For more information, see the *MainView for IP Customization Guide*.

In Figure 3 on page 28, the IPv6 address (2002:0:0:1::3306) is the last entry in the panel.

### Figure 3: Example of a MainView for IP window interface with an IPv6 address

<table>
<thead>
<tr>
<th>06OCT2009 03:37:52</th>
<th>MAINVIEW WINDOW INTERFACE (V6.0.00)</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMAND ====&gt;</td>
<td>SCROLL ===&gt; PAGE</td>
</tr>
<tr>
<td>CURR WIN ====&gt; 1</td>
<td>ALT WIN ===&gt;</td>
</tr>
<tr>
<td>CMD Remote</td>
<td>Remote Local</td>
</tr>
<tr>
<td>-- IPAddr</td>
<td>Local Bytes Bytes Conn DNS</td>
</tr>
<tr>
<td>172.22.33.48</td>
<td>1379 172.17.4.175 23 3 3 Establish dd0</td>
</tr>
<tr>
<td>172.22.33.84</td>
<td>4304 172.17.4.175 23 0 0 Establish AUS</td>
</tr>
<tr>
<td>172.22.34.119</td>
<td>1209 172.17.4.175 23 0 0 Establish AUS</td>
</tr>
<tr>
<td>172.24.33.211</td>
<td>48759 172.17.4.175 21 0 0 Closed phx</td>
</tr>
<tr>
<td>172.24.33.211</td>
<td>48838 172.17.4.175 21 0 0 Closed phx</td>
</tr>
<tr>
<td>172.24.33.211</td>
<td>49255 172.17.4.175 21 0 0 Timewait phx</td>
</tr>
<tr>
<td>172.24.33.213</td>
<td>32990 172.17.4.175 7104 60618 123K Establish phx</td>
</tr>
<tr>
<td>172.24.33.213</td>
<td>34017 172.17.4.175 7104 572 1249 Closed phx</td>
</tr>
<tr>
<td>172.24.33.213</td>
<td>34412 172.17.4.175 7104 955 1946 Closed phx</td>
</tr>
<tr>
<td>172.24.33.213</td>
<td>34987 172.17.4.175 7104 0 0 Establish phx</td>
</tr>
<tr>
<td>172.24.8.87</td>
<td>60330 172.17.4.175 2740 0 54 Establish phx</td>
</tr>
<tr>
<td>172.24.8.87</td>
<td>60331 172.17.4.175 2741 605 0 Establish phx</td>
</tr>
<tr>
<td>172.28.34.138</td>
<td>2068 172.17.4.175 23 0 0 Establish UNK</td>
</tr>
<tr>
<td>192.168.7.5</td>
<td>1573 172.17.4.175 6119 0 0 Establish mvs</td>
</tr>
<tr>
<td>192.168.7.5</td>
<td>61015 172.17.4.175 6117 242 4 Establish mvs</td>
</tr>
<tr>
<td>2002:0:0:1::3306</td>
<td>1027 2002:0:0:2::3304 21 29 221 Establish mvs</td>
</tr>
</tbody>
</table>

You can see the full IPv6 address in MainView for IP, by placing your cursor on the compressed IP address on the tabular view and pressing Enter. The hyperlink will display the full IPv6 address, either in a multi-platform dialog (MPD) or a detailed view for the record.

As you migrate from IPv4 to IPv6, the fields will not change on the MainView for IP views to accommodate the longer IPv6 addresses. However, you can view the partial IPv6 address through the tabular views, or display the full IPv6 address either through the detailed view or from a MainView MPD.

### Availability options in MainView for IP

This topic describes the options available in MainView for IP to monitor component availability.

Table 4 on page 29 describes functions that enable you to establish and monitor component availability on your system.
Table 4: Availability options

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/IP monitor</td>
<td>Allows you to monitor the status and activity of your TCP/IP stacks</td>
</tr>
<tr>
<td>Availability monitor</td>
<td>Allows you to establish and monitor critical resources, such as applications, devices, links, ports, and other resources</td>
</tr>
<tr>
<td>Availability ping</td>
<td>Allows you to automatically ping an IP network device to determine its availability and provide device response times</td>
</tr>
</tbody>
</table>

TCP/IP monitor views

The TCP/IP monitor views provide detailed information about TCP/IP stack activity.

Table 5: TCP/IP monitor views

<table>
<thead>
<tr>
<th>View name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>STACKIP</td>
<td>IP statistics</td>
</tr>
<tr>
<td>STACKICM</td>
<td>Internet Control Message Protocol (ICMP) statistics</td>
</tr>
<tr>
<td>STACKTCP</td>
<td>TCP statistics</td>
</tr>
<tr>
<td>STACKUDP</td>
<td>User Datagram Protocol (UDP) statistics</td>
</tr>
<tr>
<td>STACKCPU</td>
<td>CPU and paging statistics</td>
</tr>
<tr>
<td>STACKS</td>
<td>Statistical information for each TCP/IP stack that is detected on a z/OS platform</td>
</tr>
</tbody>
</table>

Availability monitor

Availability monitoring provides a single view (AMON) from which you can establish and monitor critical resources, such as applications, devices, links, ports, and other resources.

Monitored resources can be TCP applications (job name or IP address/port), Enterprise Extender links, RTP PU’s, or any device or link defined to the TCPIP stack.

The status of the resource and the number of connections (if relevant) are displayed for each resource. You can see detailed information by hyperlinking on each resource.
You can establish the critical resources that are to be monitored. The AMON view always shows the current status of the application and allows you to set alarms on these applications and connections.

You can add, update, and delete resources through the MainView monitor. The resource table is updated to a file and is saved if the MainView for IP is recycled.

**Configuring availability monitoring in MainView for IP**

Use the availability monitoring wizard to add resources to monitor.

**To configure availability monitoring**

Use the following procedure to access the wizard that will step you through the process of entering the required information.

1. From the EZIP menu, select **Availability** from the TCP/IP Activity section, and then press **Enter**.

2. From the EZAVAIL panel, select **Availability Monitor** from the Detail Views menu section, and then press **Enter**.

   The AMON view is displayed. The first time you enter the AMON view, no resources are defined and only a $DEFAULT entry is shown (Figure 4 on page 30).

**Figure 4: AMON view**

<table>
<thead>
<tr>
<th>Command line, type Add and then press Enter.</th>
</tr>
</thead>
</table>

   Note

   To delete an existing entry, type **DEL** in the **Cmd** field next to the resource you want to delete.
The Specify Resource Type screen is displayed, as shown in Figure 5 on page 31.

**Figure 5: Specify Resource Type screen**

4 Type the required information in the fields provided based on the prompts on the screen.

5 When you have finished adding the required information, type one of the following entries on the COMMAND line:
   - **END** to add an Availability Monitor resource
   - **CANCEL** to NOT add an Availability Monitor resource

---

**Note**

For more information, you can press the Help key (F1).

**Availability monitor view**

The **AMON** view displays resources that are being monitored along with the current state and number of connections.

The following Table 6 on page 32 shows the monitoring resource values.
### Table 6: Monitoring resource values

<table>
<thead>
<tr>
<th>Resource</th>
<th>State field values</th>
<th>Nbr Conn field values</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP applications (TYPE=PORT or APPL)</td>
<td>■ Established (if at least one established connection for this port is present)</td>
<td>Number of active TCP connections to this port</td>
</tr>
<tr>
<td></td>
<td>■ Listen (if no connections are present but the port is in Listen mode)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Not Active (if there are no connections)</td>
<td></td>
</tr>
<tr>
<td>Devices and links</td>
<td>■ Ready (if the device or link is active)</td>
<td>Always blank</td>
</tr>
<tr>
<td>RTP PUs</td>
<td>■ Connected (RTP PU is active)</td>
<td>Number of LU-LU sessions over the RTP pipe</td>
</tr>
<tr>
<td>EE connections</td>
<td>■ Active</td>
<td>Number of LU-LU sessions over the EE connection</td>
</tr>
<tr>
<td></td>
<td>■ Not Active</td>
<td></td>
</tr>
<tr>
<td>VTAM Resources</td>
<td>VTAM state</td>
<td>Number of LU-LU sessions for the VTAM resource.</td>
</tr>
</tbody>
</table>

a MainView for IP attempts to match both the local and remote IP address and port. Therefore, you could actually monitor a remote client or server that is connecting to an IP address on the LPAR that MainView for IP is monitoring. A wildcard (*) is allowed for the port for a remote client (IP address).

- Alarms are set on the **State** field or the **Nbr Conn** (number of connections) field.
- The records are written to history.

From the availability monitor view (AMON), you can hyperlink to each resource and get more detailed information, as described in Figure 6 on page 32:

**Figure 6: Availability monitor (AMON) view with defined resources**

<table>
<thead>
<tr>
<th>Cad Resource</th>
<th>Resource Name</th>
<th>Type</th>
<th>State</th>
<th>Stack</th>
<th>Nbr VTAM Conn</th>
<th>Name</th>
<th>Nbr VTAM Conn</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.0.0.1.3000</td>
<td>TCP</td>
<td>PORT</td>
<td>Not Active</td>
<td>TCP/IP</td>
<td>0</td>
<td>9</td>
<td>TCP/IP</td>
</tr>
<tr>
<td>TEST</td>
<td>RTP</td>
<td>Not Active</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TEST</td>
<td>LINK</td>
<td>Not Active</td>
<td></td>
<td></td>
<td>TCP/IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TEST</td>
<td>DEVS</td>
<td>Not Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following view always shows the current status of the application and allows you to set alarms on these applications and connections.
The Table 7 on page 33 shows Hyperlinked views by resource type:

**Table 7: Hyperlinked views by resource type**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Hyperlink view</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP applications and ports</td>
<td>TCPCONS (only the TCP connections for that applications name, IP address, or port)</td>
</tr>
<tr>
<td>Devices and links</td>
<td>DEVSD or LINKSD</td>
</tr>
<tr>
<td>RTP nodes</td>
<td>RTPSD</td>
</tr>
<tr>
<td>EE nodes</td>
<td>EED</td>
</tr>
<tr>
<td>VTAM Resources</td>
<td>'Specific VTAM resource detailed view</td>
</tr>
</tbody>
</table>

**Auto Activate VTAM Resources**

 Certain VTAM Resources always need to be active. If one of the resources goes inactive, it will automatically be reactivated. You can monitor the VTAM resources through the AMON view. The view displays the current status of the resource. In addition, you have the option to have the VTAM resource auto activated if it is found to be inactive after being checked at the specified interval.

Using the ADD on the AMON view will give you the VTAM resources. From this view, you have a detailed view of all the resources and if they are active or not.

**Availability ping in MainView for IP**

In MainView for IP you can automatically ping (APNG) an IP network device to determine its availability and provide device response times.

With the availability ping view, you can do the following:

- Monitor important devices
- Provide early detection of network outages
- Monitor ping response times to predict network problems
- Trend ping response times to determine periods of the day where problems can exist

The APINGD view provides the detailed view of the entries that are pinged for availability performance.
Note
You can specify whether the availability ping is enabled or disabled at startup by setting the Availability Ping parameter on the MVIP Parms Configuration (MVIPCONF) view. The Availability Ping parameter is set to ON by default. For more information, see the MainView for IP Customization Guide.

Starting the availability ping command in MainView IP

When defining the availability ping, you can control the ping by specifying the size and frequency of the ping, and the time frame when APNG is necessary.

To start the availability ping command

1. From the EZIP menu, select Availability from the TCP/IP Activity section, and then press Enter.

2. From the EZAVAIL panel, select Availability Ping from the Detail View section and press Enter.

The APING panel is displayed, as shown in Figure 7 on page 34:

Figure 7: Availability ping view

<table>
<thead>
<tr>
<th>CMD Target</th>
<th>--- aPng ---</th>
<th>Resp. times(avg)</th>
<th>DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>Idle 30</td>
<td>56 1</td>
<td>DEFAULT A</td>
</tr>
<tr>
<td>1.2.3.4</td>
<td>Idle 30</td>
<td>56 1</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>172.18.242.150</td>
<td>Idle 30</td>
<td>56 1</td>
<td>dsmith-G7</td>
</tr>
<tr>
<td>172.18.243.9</td>
<td>Idle 45</td>
<td>56 1</td>
<td>ssmith-RT</td>
</tr>
</tbody>
</table>

Note
To see more fields, press F11 to scroll to the right.

Adding an IP address to the availability ping configuration in MainView IP

Use the following procedure to add an IP network device to be pinged for availability and response-time information.

To add an IP address to the availability ping configuration

1. From the EZIP menu, select Availability from the TCP/IP Activity section, and then press Enter.
2 From the EZAVAIL panel, select **Availability Ping** from the Detail View section and press **Enter**.

3 Type **A** in the **CMD** field next to any IP address, and press **Enter**. The Add APing Entries pop-up window is displayed.

4 Complete the following fields as needed:
   - In the **IP Address** field, type the IP address
   - In the **TCP/IP Stack** field, type the TCP/IP stack name
   - In the **Interval** field, type the interval
   - In **Buffer Size**, type the buffer size
   - In **Retry Count**, type the number of retries
   - In the **Start Time** field, type the time that you want the delay to start
   - In the **Stop Time** field, type the time that you want the delay to stop
   - In the **DNS Name** field, type the name of the DNS
   - In the **Mon-Fri** field, type Yes to restrict to ping to Monday thru Friday. If entering Yes ensure that the Sat and Sun fields are marked as **No**
   - In the **Sat** field, type **No** to prevent pings on Saturday
   - In the **Sun** field, type **No** to prevent pings on Sunday

   **Tip**
   Press the spacebar to delete any characters that are not part of the IP address that you are adding.

   For information about the other fields in this view, press **F1** for Help.

5 Press **F3** or type **END** to complete the task.

   Message TACI5810E is displayed stating that the aPng record was added for the IP address that you entered.
Adding a domain name to the availability ping configuration in MainView IP

Use the following task to add a Domain Name (DNS) to ping a IP network device to determine its availability and device response times.

**To add a domain name to the availability ping configuration**

1. From the EZIP menu, select **Availability** from the TCP/IP Activity section, and then press **Enter**.

2. From the EZAVAIL panel, select **Availability Ping** from the Detail View section and press **Enter**.

3. In the **CMD** field type **A** and press **Enter**.

4. Use the **Tab** key to move to the **DNS Name** field, and type the domain name that you want to add.

5. Press **F3** or type **END** to complete the task.

   Message TACI5810E is displayed stating that the aPng record was added for the IP address that you entered.

**Monitoring MainView**

MainView for IP monitors its tasks and the percentage of CPU that each task is using:

- The MVIPPERF view shows the CPU used and the percentage of processing that is done on IBM System z Integrated Information Processors (zIIPs).

- The MVIPSELD view shows the counts for each MainView for IP data selector.

MainView for IP will offload processing to the zIIP processors if zIIP is enabled for the product on the MVIPCNFD view. The zIIP percentage may also be set on this configuration view. By default, MainView for IP will have zIIP enabled at 100%.

---

**Note**

MainView for IP can offload processing to zIIPs if zIIP is enabled for the product on the MVIPCNFD configuration view. Also, you can use that view to control the percentage of processing that the product can offload to zIIPs. By default, MainView for IP enables zIIP processing and sets the percentage to 100%.
MainView for IP can offload the following tasks to the zIIPs:

- Availability Ping
- SNMP
- OSA data collection (interval and real-time data)

Table 8 on page 37 shows the PASPARM views by type.

**Table 8: PASPARM views by parameter type**

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVIPCNFD</td>
<td>Displays configuration parameters for MainView for IP</td>
</tr>
<tr>
<td>MVIPSELD</td>
<td>Displays the counts for each data selector</td>
</tr>
<tr>
<td>MVIPPERF</td>
<td>Displays the total percent of zIIP offloaded, and the percentage for each task</td>
</tr>
<tr>
<td>PASPARM</td>
<td>Displays the actively installed parameter members and the data sets in which they reside</td>
</tr>
</tbody>
</table>

**Traffic and response times information in MainView for IP**

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

MainView for IP also provides response-time statistics by job name, port, and connections. You can access the information needed to identify delays in your network by using the response times information views described in Table 9 on page 37.

**Table 9: Accessing response-time statistics**

<table>
<thead>
<tr>
<th>View</th>
<th>Displayed information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONNRSPZ</td>
<td>Throughput information about remote applications, connections with applications, or traffic counts</td>
</tr>
<tr>
<td>TNPERRF</td>
<td>Response-time statistics for TN3270 connections, access the TN3270 Server Performance Data view. This view displays statistics such as life-of-connection response-time averages, IP response-time, SNA response-time, and total round-trip response-time</td>
</tr>
<tr>
<td>CLS x CONZ</td>
<td>Summary throughput information for a network by class subnet (A, B, or C). These views display throughput count information such as bytes in, bytes out, re-transmissions, duplicate acknowledgments, inbound datagrams, and outbound datagrams</td>
</tr>
</tbody>
</table>
### Connections views in MainView for IP

The connections views provide real-time 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.

The connections views display all connections for each view, along with real-time data associated with each connection.

- Local and remote ports
- Local and remote IP addresses
- Byte count information
- Response times
- Job and application names
- Changing TCP/IP parameters dynamically

You can display more information by drilling down to the detailed view. All closed connections are displayed until the interval ends. You can issue commands to accomplish the following tasks:

- Traceroute the remote IP address (TR)
- Ping the remote IP address (P)
- Drop the connection (DR)

---

<table>
<thead>
<tr>
<th>View</th>
<th>Displayed information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLS x RSPZ</td>
<td>Summary response-time statistics for a network by class subnet (A, B, or C). These views display response-time information such as bytes in, bytes out, and round-trip time</td>
</tr>
<tr>
<td>JOBRSPZ</td>
<td>Application response-time summary and provides a hyperlink to MainView for UNIX System Services</td>
</tr>
<tr>
<td>PORTRSPZ</td>
<td>Port response time summary</td>
</tr>
<tr>
<td>TNRSPZ</td>
<td>TN3270 connection response-time summary</td>
</tr>
</tbody>
</table>

**Note**

Response times are reported in hundredths of seconds.
Packet trace the remote IP address (PKT)

Table 10 on page 39 describes the views that provide detailed information about all TCP and UDP connections on your system. You can use the views to quickly see real-time data about the IP stack.

Table 10: Connections views

<table>
<thead>
<tr>
<th>View</th>
<th>Display</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTCONS</td>
<td>All active TCP and UDP connections</td>
</tr>
<tr>
<td>ALLCONS</td>
<td>All TCP and UDP connections for each remote IP address on your system</td>
</tr>
<tr>
<td>LSTCONS</td>
<td>All active TCP listeners on your system</td>
</tr>
<tr>
<td>TCPCONS</td>
<td>All TCP connections, active and inactive, that occurred since the last interval</td>
</tr>
<tr>
<td>TNCONS</td>
<td>All TN3270 connections, active and inactive, that occurred since the last interval</td>
</tr>
<tr>
<td>UDPCONS</td>
<td>UDP connection information for each remote IP address on your system</td>
</tr>
<tr>
<td>TTLSCNN</td>
<td>AT-TLS connections</td>
</tr>
<tr>
<td>TOPUSERS</td>
<td>Top application and connection bandwidth users by percentage</td>
</tr>
</tbody>
</table>

Sample connection views in MainView for IP

Connection views display all active TCP and UDP connections. This topic shows some examples of ACTCONS, TCPCONS, and TNCONS views.

The ACTCONS view displays all active TCP and UDP connections (Figure 8 on page 39):

Figure 8: ACTCONS view

```
06OCT2009 09:20:09 ------ MAINVIEW WINDOW INTERFACE (V6.0.00) ------
COMMAND ===> SCROLL ===> PAGE
CURR WIN ===> 1       ALT WIN ===> >W1=ACTCONS=-=-TCPIP=-*-06OCT2009=09:18:46=-MVIP=-D=128
CMD Remote           Remote Local            Local  Intvl   Intvl   Conn
--- IPAddr           Port   IPAddr           Port   BytesIn BytesOt Status
172.17.4.175      24581 172.17.4.175      36253    2976   15315 Establish
172.17.4.175      36253 172.17.4.175      24581   15315    2976 Establish
172.17.4.175      36253 172.17.4.175      36339   12116     408 Establish
172.17.4.175      36253 172.17.4.175      36340     408   12116 Establish
172.18.1.75      175 172.17.4.175       1107      88       0 Establish
172.18.2.42.166  1171 172.17.4.175      36339     573   26605 Establish
172.18.2.42.166  1170 172.17.4.175      36340     54    6993 Establish
172.18.2.42.198  1268 172.17.4.175      1077   3318   33843 Establish
172.18.2.42.202  1324 172.17.4.175      36339     0   15315 Establish
172.18.2.42.35  1167 172.17.4.175      36339     0   15315 Establish
172.18.2.42.36  1171 172.17.4.175      36339     0   15315 Establish
```

Chapter 3 Using the views of MainView for IP 39
The TCPCONS view displays all active and inactive TCP connections that occurred since the last intervals (Figure 9 on page 40).

**Figure 9: TCPCONS view**

<table>
<thead>
<tr>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>06OCT2009 09:43:31</td>
<td>MAINVIEW WINDOW INTERFACE (V6.0.00)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>06OCT2009 09:59:42</td>
<td>MAINVIEW WINDOW INTERFACE (V6.0.00)</td>
</tr>
</tbody>
</table>

The TNCONS view displays all active and inactive TN3270 connections that occurred since the last interval (Figure 10 on page 40).

**Figure 10: TNCONS view**

<table>
<thead>
<tr>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>06OCT2009 09:59:42</td>
<td>MAINVIEW WINDOW INTERFACE (V6.0.00)</td>
</tr>
</tbody>
</table>

**Dropping a connection by using a line command in MainView**

Use the following procedure to drop a connection by using the DR line command.

Users who connect to your MVS system through TN3270 or FTP sessions can encounter various problems, such as 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 might decide to terminate the connection that is hung. MainView for IP provides a line command to quickly terminate (or drop) a connection.

**WARNING**

Performing this line command terminates a connection immediately. If you determine that a connection should be dropped, be sure to notify the owner of that connection. Anyone who can access the monitor has authority to drop connections.

**To issue the DR line command from a connections view**

1. From the EZIP menu, select Connections from the TCP/IP Activity section.

2. From the EZCONS menu, select one of the following types of connections from the Connections section and press Enter.
   - All
   - Listen
   - Active
   - TCP
   - UDP
   - TN3270
   - AT-TLS

   The panel for the selection is displayed with a list of IP addresses. For example, if you selected All, the ALLCONS panel is displayed.

3. In the Command field, type DR next to the connection that you want to terminate, and then press Enter.

   Write-to-operator (WTO) message BMC256615I confirms 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 in MainView IP

A ping is a diagnostic echo packet that measures and displays the round-trip time and percentage of returned packets (EE and RTP information). Use these procedures to ping a device by using the P line command.

Use one of the following procedures to ping a device:

- Select an IP address that is displayed in the Ping IPAddr field of the PCONS view
- Type a ping command on the COMMAND line
- Issue the P line command from a Ping Information view
- Issue the P line command from a Connections view

To issue the P line command from a connections view

1. From the EZIP menu, select Connections from the TCP/IP Activity section.
2. From the EZCONS menu, select one of the following types of connections from the Connections section and press Enter:
   - All
   - Listen
   - Active
   - TCP
   - UDP
   - TN3270
   - AT-TLS

   The panel for the selection is displayed with a list of IP addresses. For example, if you selected All, the ALLCONS panel is displayed.
3. Type P in the CMD field beside the connection address that you want to ping.
The Ping Connection pop-up is displayed.

**Figure 11: Ping Pop-up dialogue**

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>SCROLL</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address:</td>
<td>10.0.0.01</td>
<td></td>
</tr>
<tr>
<td>Stack Name:</td>
<td>TCPIP</td>
<td></td>
</tr>
<tr>
<td>Ping Count:</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Ping Buffer Size:</td>
<td>256</td>
<td></td>
</tr>
<tr>
<td>END to Ping Connection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CANCEL to NOT Ping Connection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HELP to view related help</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 Edit the fields as needed and press F3.

- **Stack Name**
- **Ping Count** - default value is 1.
- **Ping Buffer size** - default value is 256.

**Figure 12 on page 43** shows the PINGD view.

**Figure 12: PING information view**

<table>
<thead>
<tr>
<th>Domain Name............</th>
<th>localhost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping IPAddr............</td>
<td>10.0.0.01</td>
</tr>
<tr>
<td>Ping Count.............</td>
<td>1</td>
</tr>
<tr>
<td>Ping Status............</td>
<td>Successful</td>
</tr>
</tbody>
</table>

Ping Response Times.

<table>
<thead>
<tr>
<th>Ping Resp 1 (sec)</th>
<th>0.0002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping Resp 2 (sec)</td>
<td></td>
</tr>
<tr>
<td>Ping Resp 3 (sec)</td>
<td></td>
</tr>
<tr>
<td>Ping Resp 4 (sec)</td>
<td></td>
</tr>
<tr>
<td>Ping Resp 5 (sec)</td>
<td></td>
</tr>
<tr>
<td>Ping Resp 6 (sec)</td>
<td></td>
</tr>
<tr>
<td>Ping Resp 7 (sec)</td>
<td></td>
</tr>
<tr>
<td>Ping Resp 8 (sec)</td>
<td></td>
</tr>
<tr>
<td>Ping Resp 9 (sec)</td>
<td></td>
</tr>
<tr>
<td>Ping Resp 10 (sec)</td>
<td></td>
</tr>
<tr>
<td>Ping Resp 11 (sec)</td>
<td></td>
</tr>
<tr>
<td>Ping Resp 12 (sec)</td>
<td></td>
</tr>
<tr>
<td>Ping Resp 13 (sec)</td>
<td></td>
</tr>
</tbody>
</table>
Performing a traceroute on a device by using a line command

A traceroute is a series of pings that progress outward in incremental hops from the MainView for IP client to the final trace target destination. By default, each hop is sent three requests; the response time is determined from these requests.

Use one of the following procedures to perform a traceroute on a device by using the TR line command.

- Select an IP address that is displayed in the **Tracerte IPAddr** field
- Type a **TRACEROUTE** command on the **COMMAND** line
- Issue the **TR** line command from a **Tracerte Information** view

**To issue the TR line command from a connections view**

1. From the EZIP menu, select **CONNECTIONS** from the TCP/IP Activity section.
2. From the EZCONS menu, select one of the following types of connections from the **CONNECTIONS** section then press **Enter**:  
   - All  
   - Listen  
   - Active  
   - TCP  
   - UDP  
   - TN3270  
   - AT-TLS

   The panel for the selection is displayed with a list of IP addresses. For example, if you selected All, the ALLCONS panel is displayed.

3. In the **CMD** field, type **TR** beside the IP address to be traced, and then press **Enter**.
The TraceRte Connection pop-up is displayed (Figure 13 on page 45).

**Figure 13: TraceRte Connection Pop-up window**

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>06:29:56</td>
<td>TraceRte Connection window displayed.</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.18.242.84</td>
</tr>
<tr>
<td>Stack Name</td>
<td>TCPIP</td>
</tr>
<tr>
<td>TraceRte Port</td>
<td>33434</td>
</tr>
<tr>
<td>Max Hops</td>
<td>32</td>
</tr>
<tr>
<td>Max Wait</td>
<td>5</td>
</tr>
</tbody>
</table>

4 Edit the fields as needed and press `F3`:

- **For Stack name**, specify the TCPIP Stack to use when issuing the PING command
- **For TraceRte port**, specify the port to be used for the traceRoute
- **For Max Hops**, specify the maximum number of hops on the traceRoute (valid values are 1-64, the default is 32)
- **For Max Wait**, specify the maximum wait on each hop of the traceRoute (valid values are 1-255, the default is 5 seconds)

**Figure 12 on page 43 shows the Trace view.**

**Figure 14: Trace view**

<table>
<thead>
<tr>
<th>Cur Hop DNS</th>
<th>Hop DNS</th>
<th>Hop IPAddr</th>
<th>Hop Rsp</th>
<th>Hop Rsp</th>
<th>Hop Rsp</th>
<th>Hop Rsp</th>
<th>Hop Delay</th>
<th>Total Hop</th>
<th>Tracerte Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>sw-prod-core-usa-phx</td>
<td>sw-prod-core-usa-phx</td>
<td>172.24.51.252</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Complete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rtr-twtc-ppp-usa-phx</td>
<td>rtr-twtc-ppp-usa-phx</td>
<td>172.24.1.38</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Complete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rtr-twtc-ppp-usa-hou</td>
<td>rtr-twtc-ppp-usa-hou</td>
<td>172.21.1.2</td>
<td>27</td>
<td>28</td>
<td>27</td>
<td>27</td>
<td>Complete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sw-dist-usa-hou-b4rdf</td>
<td>sw-dist-usa-hou-b4rdf</td>
<td>172.18.245.57</td>
<td>27</td>
<td>28</td>
<td>27</td>
<td>27</td>
<td>Complete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sw-dist-usa-hou-b1mdf</td>
<td>sw-dist-usa-hou-b1mdf</td>
<td>172.18.254.173</td>
<td>27</td>
<td>30</td>
<td>28</td>
<td>28</td>
<td>Complete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sw-edge-usa-hou-b1f4s</td>
<td>sw-edge-usa-hou-b1f4s</td>
<td>172.18.254.102</td>
<td>28</td>
<td>28</td>
<td>28</td>
<td>28</td>
<td>Complete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bmc-74bm2f1.bmc.com</td>
<td>bmc-74bm2f1.bmc.com</td>
<td>172.18.242.84</td>
<td>27</td>
<td>28</td>
<td>27</td>
<td>27</td>
<td>Complete</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5 If the status in the Tracerte Status field is **In progress**, refresh the data by pressing Enter.
Performing a packet trace by using a line command

Use the following procedure to start a packet trace by using the line command. The packet trace can be started for a specific IP address, source port, destination port, protocol type, and packet length.

**Note**
If you are tracing a packet, and you cancel the PAS, you might encounter an abend. BMC recommends that you shut down the PAS normally or stop the trace. You can also perform a packet trace by issuing the STA line command from the Packet Trace view.

**To perform a packet trace by using a line command**

1. From the EZIP menu, select **CONNECTIONS** from the TCP/IP Activity section.

2. From the EZCONS menu, select one of the following types of connections from the **CONNECTIONS** section and then press **ENTER**:
   - All
   - Listen
   - Active
   - TCP
   - UDP
   - TN3270

3. In the **COMMAND** field, type **PKT**, and then press Enter.
   
   The Start Packet Trace pop-up window is displayed showing details of the specific connection.

4. Type any additional information that you want in this window, such as an identifier for the packet trace in the **Trace Identifier** field.

5. Press **F3**, or type **END** to start the packet trace.
   
   The PKTTRACS view is displayed so you can verify that the trace has been activated. **ACTIVE** is displayed in the **Trace Status** field.

   Other status types include:
■ STOP/NWRAP indicates that the packet trace has been stopped because the trace table has wrapped and you specified no wrap for Packet Trace (Pkttrace Wrap).

■ STOP/ABEND indicates that the abend limit has been exceeded in the Packet Trace routine and that Packet Tracking has been stopped.

6 Press F3 to return to the CONNECTIONS view.

Connection errors views in MainView for IP

The connection errors views provide real-time data on network errors such as duplicate acks and retransmits. These views can also be used to identify problems by using historical trends.

The connection errors can be displayed by job name, port, and IP address. The CONNECTION views also display duplicate acks and retransmits.

Table 11 on page 47 describes the connection error views.

<table>
<thead>
<tr>
<th>View</th>
<th>Display</th>
</tr>
</thead>
<tbody>
<tr>
<td>JOBACKZ</td>
<td>Duplicate acks by job name</td>
</tr>
<tr>
<td>PORTACKZ</td>
<td>Duplicate acks by port number</td>
</tr>
<tr>
<td>IPACKZ</td>
<td>Duplicate acks by IP address</td>
</tr>
<tr>
<td>JOBRETZ</td>
<td>Retransmits by job name</td>
</tr>
<tr>
<td>PORTRETZ</td>
<td>Retransmits by port number</td>
</tr>
<tr>
<td>IPRETZ</td>
<td>Retransmits by IP address</td>
</tr>
</tbody>
</table>

VTAM Session Data views in MainView for IP

The VTAM session menu displays a list of views from which you can display VTAM session data and VTAM PIU trace data.

VTAM PIU traces are for a specific VTAM LU.

From the VTAM session views, you can issue commands to accomplish the following tasks:
- Display the PIUs traced for the current session (DT)
- Update the PIU trace settings for the current session (U)
- Start a PIU trace for the Secondary LU name (STA)
- Stop a PIU trace for the Secondary LU name (STO)

Table 12 on page 48 lists all of the Views and their descriptions.

**Note**
You can access the views by typing their name on the command line and pressing enter.

You can define filters that limit the VTAM session data and PIU trace data collected. You can apply filters globally to all VTAM data collected, specific sets of logical units (LU), or an individual LU. For more information on filtering VTAM session data and PIU trace data, see the *MainView for IP Customization Guide*.

### Table 12: VTAM Session data views

<table>
<thead>
<tr>
<th>View name</th>
<th>View description</th>
<th>View name</th>
</tr>
</thead>
<tbody>
<tr>
<td>All VTAM Sessions</td>
<td>Displays all VTAM sessions</td>
<td>ALLSESS</td>
</tr>
<tr>
<td>Active VTAM Sessions</td>
<td>Displays all active VTAM sessions</td>
<td>ACTSESS</td>
</tr>
<tr>
<td>Closed VTAM Sessions</td>
<td>Displays all closed VTAM sessions for the current interval</td>
<td>CLSSESS</td>
</tr>
<tr>
<td>VTAM Session Failures</td>
<td>Displays all VTAM session failures for the current interval</td>
<td>FAILSESS</td>
</tr>
<tr>
<td>LU-LU Sessions</td>
<td>Displays all VTAM LU-LU sessions</td>
<td>LULUSESS</td>
</tr>
<tr>
<td>CP-CP Sessions</td>
<td>Displays all VTAM CP-CP sessions</td>
<td>CPCPSESS</td>
</tr>
<tr>
<td>SSCP-LU Sessions</td>
<td>Displays all VTAM SSCP-LU sessions</td>
<td>SSLUSESS</td>
</tr>
<tr>
<td>SSCP-PU Sessions</td>
<td>Displays all VTAM SSCP-PU sessions</td>
<td>SSPUSESS</td>
</tr>
<tr>
<td>SSCP-SSCP Sessions</td>
<td>Displays all VTAM SSCP-SSCP sessions</td>
<td>SSCPSESS</td>
</tr>
<tr>
<td>Primary Logical Units (PLU)</td>
<td>Displays a summary of all the PLU sessions</td>
<td>VTAMLPLUZ</td>
</tr>
<tr>
<td>Secondary Logical Units (SLU)</td>
<td>Displays a summary of all the SLU sessions</td>
<td>VTAMSLUZ</td>
</tr>
<tr>
<td>Explicit Routes (ERs)</td>
<td>Displays a summary of all current Explicit routes</td>
<td>VTAMERZ</td>
</tr>
<tr>
<td>Virtual Routes (VRs)</td>
<td>Displays a summary of all current Virtual routes</td>
<td>VTAMVRZ</td>
</tr>
</tbody>
</table>
VTAM Resource views in MainView for IP

The VTAM Resource menu displays a list of views from which you can display VTAM resources and perform actions against them. These resources include:

- Formatted VTAM Resources
- Major Nodes
- Applications
- CDRSCs
- CDRMs
- Lines
- Clusters
- Terminals
- RTP PUs
- TRL Major Nodes

From the VTAM resource views, you can issue commands to accomplish the following tasks:

- Display the VTAM resource (D)
- Display everything for the VTAM resource (DE)
- Activate the VTAM resource (A)
- Inactivate the VTAM resource (I)
- Inactivate force of the VTAM resource (F)

Table 13: VTAM Resource views

<table>
<thead>
<tr>
<th>View name</th>
<th>View description</th>
<th>View name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major Nodes</td>
<td>Displays all VTAM major nodes</td>
<td>MAJNODES</td>
</tr>
<tr>
<td>Applications</td>
<td>Displays all VTAM applications</td>
<td>VTMAPPLS</td>
</tr>
<tr>
<td>View name</td>
<td>View description</td>
<td>View name</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Cross Domain Resource Managers</td>
<td>Displays all VTAM CDRMs</td>
<td>VTMCDRMS</td>
</tr>
<tr>
<td>Cross Domain Resources</td>
<td>Displays all VTAM CDRSCs</td>
<td>VTMCDRSC</td>
</tr>
<tr>
<td>Lines</td>
<td>Displays all VTAM lines</td>
<td>VTMLINES</td>
</tr>
<tr>
<td>Clusters</td>
<td>Displays all VTAM clusters</td>
<td>VTMCLSTR</td>
</tr>
<tr>
<td>Terminals</td>
<td>Displays all VTAM terminals</td>
<td>VTMTERMS</td>
</tr>
<tr>
<td>RTP PUs</td>
<td>Displays all VTAM RTP PUs</td>
<td>VTMRTPS</td>
</tr>
<tr>
<td>TRL Major Nodes</td>
<td>Displays all VTAM TRLs</td>
<td>VTMTRL</td>
</tr>
</tbody>
</table>

**Monitor and Auto Activate VTAM Resources**

MainView for IP allows you to monitor any VTAM resource on the AMON view. The AMON view displays the current status of the VTAM resource. Additionally, you can optionally have the VTAM resource auto activated if found to be inactive after being checked at the specified interval. The AMON view now includes VTAM resources. The ADD command on the AMON view has another option for VTAM resources. Additionally, you can specify to auto-activate the VTAM resource, and specify the interval periods to check if the VTAM resource is active.

Hyperlinks on the AMON view for VTAM resources drill down to the detailed view for that resource type.

**VTAM message views in MainView for IP**

The VTAM PPO Messages menu displays a list of views from which you can display VTAM messages.

*Table 12 on page 48* lists all of the Views and their descriptions.
You can access the views by typing their name on the command line and pressing enter.

You can define filters that limit the messages collected. You can apply filters to all messages, specific sets of messages, or an individual message. For more information on filtering messages, see the *MainView for IP Customization Guide*.

### Table 14: VTAM message views

<table>
<thead>
<tr>
<th>View name</th>
<th>View description</th>
<th>View name</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTAM Messages Log</td>
<td>Displays all messages collected through VTAM PPO interface</td>
<td>VTAMMSG</td>
</tr>
<tr>
<td>VTAM Message Statistics</td>
<td>Displays statistics about the VTAM messages collected</td>
<td>PPOSTATS</td>
</tr>
<tr>
<td>VTAM Resources</td>
<td>Displays all the VTAM Resources</td>
<td>EZVTAMR</td>
</tr>
</tbody>
</table>

### Configuration views in MainView for IP

For real-time configuration data about the programs that make up your system, subsystem, or network, access the TCP, UDP, IP, SMF, or PORT configuration views. With these views, you can see and modify configuration information without searching through several data sets.

The configuration views provide configuration information which you can modify the parameters for the PROFILE data set for each TCP/IP stack on your system. For each TCP/IP stack on your system, the configuration views provide configuration information for the PROFILE data set. You can dynamically modify some of the parameters for these views by typing over the corresponding fields in the view. The data set can then be updated via the OBEYFILE command.

*Table 15 on page 51* describes views that provide information about your system configurations.

### Table 15: Configuration views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTCONF</td>
<td>Displays information about the jobs that are started by the Autolog task when TCP/IP is started</td>
</tr>
<tr>
<td>DATCONF</td>
<td>Displays the active data traces and settings</td>
</tr>
<tr>
<td>GLBCONF</td>
<td>Displays the global configuration information defined in the GLOBALCONFIG profile statement</td>
</tr>
</tbody>
</table>
EE and RTP information in MainView for IP

In MainView for IP, you can view statistics and performance data related to the status and health of your SNA/IP network connections. The Enterprise Extender (EE) connection data view displays information about all EE connections.

The High Performance Routine (HPR) connection data views display information about the specific HPR connections RTP physical units. The IBM SNA NMI is used to retrieve the EE and RTP statistics. For information about enabling the IBM SNA NMI, see the MainView for IP Customization Guide.

Table 16 on page 52 describes views that provide detailed information about EE connections and RTP statistics.

**Table 16: EE and RTP information views**

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EE</td>
<td>Displays information about the Enterprise Extender connection</td>
</tr>
<tr>
<td>RTPS</td>
<td>Displays information for the connections between the RTP endpoints</td>
</tr>
<tr>
<td>RTPSD</td>
<td>Displays more detailed information for the RTP endpoints that includes status, path, switch, congestion, and throughput information</td>
</tr>
</tbody>
</table>

**Note**

APPN/HPR uses RTP as part of the routing protocol.
Accessing EE and RTP information in MainView IP

In this task, you will display the EE and RTP views.

You can access EE and RTP information by using either of the following procedures:

- “To use the EE traffic command” on page 53
- “To use the EE RTP Info command” on page 54

Before you begin

Before using the EE and RTP views, ensure that your operating system meets the minimum requirements. You must have EE defined on your TCP/IP system. For more information about how to install and configure EE, see the IBM documentation included with the Enterprise Extender.

To use the EE traffic command

1. From the EZIP menu, select EE Connections from the Communications Server section, and then press Enter.

   The EE Connections view (EE) is displayed (Figure 15 on page 53).

   Figure 15: EE Connections detail view

   This screen displays the VTAM and TCP/IP data that is transmitted on the local ports and the number of bytes in and out.

2. To see the detail of a physical unit, select the PU Name to display, and press Enter.
The detail view is displayed (Figure 16 on page 54).

**Figure 16: Physical unit detail**

<table>
<thead>
<tr>
<th>Connection Info........</th>
<th>Port Priority = HIGH.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local IPAddr...........</td>
<td>172.19.84.16 NLPs Sent.........</td>
</tr>
<tr>
<td>Remote IPAddr...........</td>
<td>172.19.84.12 Bytes Sent........</td>
</tr>
<tr>
<td>Line Name..............</td>
<td>09/01/07 04:14 NLPs Retransmitted......</td>
</tr>
<tr>
<td>PU Name..............</td>
<td>LOO000000 Bytes Received......</td>
</tr>
<tr>
<td>RTP Pipes..............</td>
<td>4 Bytes Sent..............</td>
</tr>
<tr>
<td>LU-LU Sessions........</td>
<td>14 Port Priority = MEDIUM</td>
</tr>
<tr>
<td>Signal Retrans 1 Time....</td>
<td>0 NLPs Sent...............</td>
</tr>
<tr>
<td>Signal Retrans Max......</td>
<td>0 Bytes Sent..............</td>
</tr>
<tr>
<td>Redial Count...........</td>
<td>3 NLPs Retransmitted......</td>
</tr>
<tr>
<td>Redial Delay...........</td>
<td>30 Bytes Received...........</td>
</tr>
<tr>
<td>KEEPACT..............</td>
<td>YES Bytes Received..........</td>
</tr>
<tr>
<td>Port Priority = SIGNAL.</td>
<td></td>
</tr>
<tr>
<td>NLPs Sent..............</td>
<td>33 NLPs Sent...............</td>
</tr>
<tr>
<td>Bytes Sent..............</td>
<td>99 Bytes Sent..............</td>
</tr>
<tr>
<td>NLPs Retransmitted.......</td>
<td>0 Bytes Sent..............</td>
</tr>
<tr>
<td>NLPs Received...........</td>
<td>33 NLPs Received...........</td>
</tr>
<tr>
<td>Bytes Received...........</td>
<td>99 Bytes Received..........</td>
</tr>
<tr>
<td>Port Priority = NETWORK</td>
<td></td>
</tr>
<tr>
<td>NLPs Sent..............</td>
<td>111K NLPs Sent...............</td>
</tr>
<tr>
<td>Bytes Sent..............</td>
<td>17.8M Bytes Sent..............</td>
</tr>
<tr>
<td>NLPs Retransmitted.......</td>
<td>0 NLPs Retransmitted......</td>
</tr>
<tr>
<td>NLPs Received...........</td>
<td>110K NLPs Received...........</td>
</tr>
<tr>
<td>Bytes Received...........</td>
<td>15.4M Bytes Received..........</td>
</tr>
</tbody>
</table>

To use the EE RTP Info command

1. From the EZIP menu, select **EE RTP Information** from the Communications Server section, and then press **Enter**.

   **Note**

   This command can take several minutes, depending on the number of sessions you have running.

The EE RTP Information view (RTPS) is displayed (Figure 17 on page 54).

**Figure 17: EE RTP information view**

<table>
<thead>
<tr>
<th>PU Name</th>
<th>Mode</th>
<th>SWITCH</th>
<th>CONGEST</th>
<th>STALL</th>
<th>State</th>
<th>LU-LU</th>
<th>NLPs</th>
<th>Wait-to-Wait-SESS</th>
<th>Retrans</th>
<th>SendQ</th>
<th>Ack</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNR000002</td>
<td>GREEN</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>CONNECTED</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CNR000003</td>
<td>GREEN</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>CONNECTED</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CNR000004</td>
<td>GREEN</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>CONNECTED</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
This panel displays the RTP PUNAME, CPNAME, class of service name, and path switch information that occurs, as well as if the pipe is congested or a number of sessions are using the pipe simultaneously. The panel also displays the status of the pipe, and some throughput information (for example, the allowed, initial, and actual flow rates).

To see the detail of a physical unit, place the cursor on the PU Name in the PU Name field, and press Enter.

The detail view is displayed (Figure 18 on page 55).

**Figure 18: Physical unit detail**

<table>
<thead>
<tr>
<th>20JAN2010 11:17:00</th>
<th>MAINVIEW WINDOW INTERFACE (V6.0.00)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMAND ====&gt;</td>
<td>SCROLL ===&gt; PAGE</td>
<td></td>
</tr>
<tr>
<td>Curr WIN ===&gt; 1</td>
<td>ALT WIN ===&gt;</td>
<td></td>
</tr>
<tr>
<td>W1 =RTPSD==============TCPIP====*========20JAN2010==11:16:46====MVIP=====D====1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection Info........</td>
<td>Outbound Info........</td>
<td></td>
</tr>
<tr>
<td>PU Name................</td>
<td>CNR000002 NLPs Sent................</td>
<td>0</td>
</tr>
<tr>
<td>CP Netid................</td>
<td>USBMCN01 Total Bytes Sent................</td>
<td>0</td>
</tr>
<tr>
<td>CP Name................</td>
<td>EECCPCCOM Data Bytes Sent................</td>
<td>0</td>
</tr>
<tr>
<td>COS Name................</td>
<td>CPSVCMG Largest NLP Sent................</td>
<td>277</td>
</tr>
<tr>
<td>Activation TOD...........</td>
<td>01/19/10 17:50 NLPs Retransmitted.........</td>
<td>0</td>
</tr>
<tr>
<td>LU-LU Sessions..........</td>
<td>2 NLPs Wait-to-SendQ........</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>NLPs Wait-for-AckQ................</td>
<td>0</td>
</tr>
<tr>
<td>Status Info...............</td>
<td>Max NLPs Wait-for-AckQ................</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Max Wait-for-AckQ TOD.....................</td>
<td>01/19/10 17:50</td>
</tr>
<tr>
<td>Status........................</td>
<td>CONNECTED Max NLPs Outbound WorkQ.........</td>
<td>2</td>
</tr>
<tr>
<td>Path Switch...............</td>
<td>NO Max NLPs Outbound WorkQ TOD................</td>
<td>01/19/10 17:50</td>
</tr>
<tr>
<td>Pipe Congested...........</td>
<td>NO Max Network Pkt Size...................</td>
<td>768</td>
</tr>
<tr>
<td>Pipe Stalled...............</td>
<td>NO Inbound Info................</td>
<td></td>
</tr>
<tr>
<td>ARB Information...........</td>
<td>NLPs Received................</td>
<td>0</td>
</tr>
<tr>
<td>ARB Mode.................</td>
<td>GREEN Total Bytes Received........</td>
<td>0</td>
</tr>
<tr>
<td>RTP Pacing Algorithm...</td>
<td>RESPONSIVE Data Bytes Received..........</td>
<td>0</td>
</tr>
<tr>
<td>Initial Rate............</td>
<td>7864 Largest NLP Received........</td>
<td>255</td>
</tr>
<tr>
<td>Allowed Rate.............</td>
<td>7864 NLPs on Out-of-SeqQ........</td>
<td>0</td>
</tr>
<tr>
<td>Actual Rate.............</td>
<td>1 Max NLPs Out-of-SeqQ................</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Actual Rate......</td>
<td>3 NLPs on Inbound Seqd........</td>
<td>0</td>
</tr>
<tr>
<td>Curr Rcvr Threshold.....</td>
<td>37000 Max NLPs on Inb WorkQ........</td>
<td>1</td>
</tr>
<tr>
<td>Max Rcvr Threshold......</td>
<td>37000 Path Switch Info....................</td>
<td></td>
</tr>
<tr>
<td>Min Rcvr Threshold......</td>
<td>17000 Path Switch Info....................</td>
<td></td>
</tr>
<tr>
<td>Timer Information........</td>
<td>Last Path Switch TOD......................</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Path Switch Reason................</td>
<td>N/A</td>
</tr>
<tr>
<td>Liveness Timer(secs)....</td>
<td>180 Initiated from Remote RTP...............</td>
<td>0</td>
</tr>
<tr>
<td>Smoothed RT Time(ms).....</td>
<td>497 Initiated from Local RTP...............</td>
<td>0</td>
</tr>
<tr>
<td>Short Req Timer(ms)......</td>
<td>311 Due to Local Failure..................</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Due to Local PSRetry......................</td>
<td>0</td>
</tr>
</tbody>
</table>

**Enterprise Extender Connectivity test**

The TEST and TESTD action from the Enterprise Extender (EE) view test the availability, address resolution, and ultimately partner reachability. This is similar to the DISPLAY EEDIAG,TEST=YES command. The TEST command displays the formatted EE connectivity test output and the TESTD command displays the VTAM output from the DISPLAY EEDIAG,TEST=YES command.
To use the EEDIAG view

1. From the EZIP menu, select EE Connections from the Communications Server section, and then press Enter.

2. From the EE Connections menu, enter the TEST or TESTD action on the EE line to be tested.

   The EEDIAG will display the formatted EE connectivity test output.

**SNMP data collection in MainView for IP**

MainView for IP provides the information that you need to monitor the network control path. The SNMP Data views display TCP, UDP, IP, system, interface, OSPF, and Cisco router information.

SNMP views display data that was collected in the last interval. You can drill down in order to access real-time data. 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.

Table 17 on page 56 describes the views that provide information about network routes and router performance.

**Table 17: SNMP data collection views**

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPDEF</td>
<td>Lets you specify IP nodes that you want to monitor</td>
</tr>
<tr>
<td>SNMPIF</td>
<td>Displays interface information for SNMP node</td>
</tr>
<tr>
<td>SNMPIP</td>
<td>Displays IP information for SNMP node</td>
</tr>
<tr>
<td>SNMPSYS</td>
<td>Displays system information for SNMP node</td>
</tr>
<tr>
<td>SNMPTCP</td>
<td>Displays TCP information for SNMP node</td>
</tr>
<tr>
<td>SNMPUDP</td>
<td>Displays UDP information for SNMP node</td>
</tr>
</tbody>
</table>

**Defining SNMP parameters in MainView IP**

Use the following procedure to update SNMP parameters dynamically for each IP node that you want monitored through MainView for IP.
To define SNMP parameters

1. From the EZIP menu, select **SNMP Data** from the TCP/IP Activity section, and press **Enter**.

2. From the EZSNMP menu, select **Define** from the Detail Views section, and press **Enter**.

The Define view (SNMPDEF) is displayed *(Figure 19 on page 57)*.

**Figure 19: SNMP Define view**

<table>
<thead>
<tr>
<th>08JUL2002 12:34:30</th>
<th>INFORMATION DISPLAY</th>
<th>SCROLL ===&gt; PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Curr Win ===&gt; 1</td>
<td>Alt Win ===&gt;</td>
<td></td>
</tr>
<tr>
<td>&gt;W1 =SNMPDEF=-------MCBSYS1=*=-------08JUL2002==12:34:30==MVIP====D====4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cmd</th>
<th>Host</th>
<th>IP Address</th>
<th>Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>$DEFAULT</td>
<td>000.000.000.000</td>
<td>public</td>
<td></td>
</tr>
<tr>
<td>ipor12p.houlab.bmc.com</td>
<td>192.168.1.253</td>
<td>public</td>
<td></td>
</tr>
<tr>
<td>ipor321.houlab.bmc.com</td>
<td>192.168.3.253</td>
<td>IPO</td>
<td></td>
</tr>
<tr>
<td>UNKNOWN</td>
<td>192.168.2.253</td>
<td>public</td>
<td></td>
</tr>
</tbody>
</table>

3. To add an IP address to the list of nodes that are monitored, type **ADD** in the **COMMAND** field.

**Tip**

You can delete an IP address from the list, by typing **DEL** in the **COMMAND** field.

4. In the **IP Address** field, 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.

5. Press **Enter**.

**Interfaces in MainView for IP**

This topic provides information about interfaces on your network.

With MainView for IP, you can see the following 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 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. You can see suspicious performance information and identify performance problems.

The Network Devices use the NMI to gather SMC-R (Shared Memory Communications over RDMA) and RoCE interface data. You can call the network connection information and view it in the different displays available.

The Network Routes view displays information about network routes that are defined on a TCP/IP stack.

The OSA Cards menu provides access to views that display information about Open Systems Adapter (OSA) devices. You can use these views to see OSA configuration information, utilization statistics, network device details, network link details, and Ethernet-like statistics.

The OSA statistics are collected through SNMP. If a community name is used, other than the default community name public, you must add a node to the SNMPDEF view. You can either add a host name of LOOPBACK or an IP address of 127.0.0.1 to the community name. When MainView for IP collects the OSA statistics, it will search the SNMPDEF view first. It looks for a match on the IP address 127.0.0.1, which determines the community name to use for the OSA SNMP collection.

**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*. You can display OSA information even if OSA/SF and the other address spaces are not active.

The HiperSockets menu provides quick access to views for devices that use HiperSockets. HiperSockets provide high-speed TCP/IP connectivity between servers running in different logical partitions (LPARs). These devices include devices, links, routes, sessions, and channel data (CMF).

**Note**
Before using the HiperSockets views, ensure that your operating system meets the minimum requirements. You must have HiperSockets defined on your TCP/IP system or MainView for IP HiperSockets cannot show that view. Customization tasks and minimum requirements are described in the *MainView for IP Customization Guide*.
Table 18 on page 59 describes the views that provide detailed information about your network interfaces.

### Table 18: Interface views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHANNEL</td>
<td>Displays network Channel Data (CMF) information that uses HiperSockets</td>
</tr>
<tr>
<td></td>
<td>The CMF Monitor product is required to display the CHANNEL view</td>
</tr>
<tr>
<td>DEVS</td>
<td>Displays information about network devices that are defined to the IP stack</td>
</tr>
<tr>
<td>HSDEVS</td>
<td>Displays network device information that uses HiperSockets</td>
</tr>
<tr>
<td>HSLINKS</td>
<td>Displays network link information that uses HiperSockets</td>
</tr>
<tr>
<td>HSROUTES</td>
<td>Displays network route information that uses HiperSockets</td>
</tr>
<tr>
<td>HSCONS</td>
<td>Displays network session information that uses HiperSockets</td>
</tr>
<tr>
<td>LINKS</td>
<td>Displays information about network links</td>
</tr>
<tr>
<td>OSAETH</td>
<td>Displays Ethernet-like statistics</td>
</tr>
<tr>
<td>OSACONF</td>
<td>Displays OSA configuration information</td>
</tr>
<tr>
<td>OSADEVS</td>
<td>Displays OSA device information</td>
</tr>
<tr>
<td>OSALINKS</td>
<td>Displays OSA link information</td>
</tr>
<tr>
<td>OSAUTIL</td>
<td>Displays OSA utilization information</td>
</tr>
<tr>
<td>OSALPAR</td>
<td>Displays OSA by LPAR information</td>
</tr>
</tbody>
</table>

**Routes in MainView for IP**

MainView for IP provides the information you need to monitor the routing used by the TCP/IP stack through your network.

Use the following views to obtain routing information:

- Use the ROUTES (Network Routes) view to see the routing information defined on the default TCPIP stack. The information displayed on this view includes the gateway IP address, interface name, status and active users. The routes in the TCPIP stack’s main routing table and the routes in the TCPIP stack’s policy-based routing tables can be displayed. These routes can be static routes, routes learned from routing daemons, and routes learned by other ICMP information, such as redirects.

- Use the OSPF Neighbor Stats (OMPNBR) view to see the OSPF routing neighbors as well as all the parameters and statistics related to an OSPF neighbor.
You can use the OSPF Interface stats (OSPFINTF) to see the OSPF Interfaces that are configured and current run-time statistics and parameters.

The OSPF Network stats (OSPFNETW) view can be used to see all OSPF neighbors with DR Priority and shows the link and device name associated with each OSPF neighbor.

Table 19 on page 60 describes the Routes views.

### Table 19: Routes views

<table>
<thead>
<tr>
<th>View</th>
<th>Display</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROUTES</td>
<td>Network routes for the TCPIP stack</td>
</tr>
<tr>
<td>OMPNBR</td>
<td>OSPF neighbor information and statistics</td>
</tr>
<tr>
<td>OSPFINTF</td>
<td>Currently configured OSPF interfaces and run-time statistics and parameters</td>
</tr>
<tr>
<td>OSPFNETW</td>
<td>Link and Device name associated with all OSPF neighbors with DR Priority</td>
</tr>
<tr>
<td>OMPRIP</td>
<td>Routing Information Protocol configuration information</td>
</tr>
<tr>
<td>OMPRTT</td>
<td>Routes in the OMPRoute main routing table</td>
</tr>
</tbody>
</table>

### Storage information in MainView for IP

This topic provides real-time statistics related to buffer pools and storage usage.

For this information you can 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. In these views, you can monitor and manage the storage allocations that are required to run your system at optimum levels.

Table 20 on page 60 describes the views that provide detailed information about your buffer pools and storage usage.

### Table 20: Storage views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSMJOB</td>
<td>Displays storage allocation and CSM buffer pool information</td>
</tr>
<tr>
<td>CSMSUMM</td>
<td>Displays CSM summary information</td>
</tr>
<tr>
<td>VTMBUFF</td>
<td>Displays VTAM buffer pool statistics</td>
</tr>
<tr>
<td>VTAMCSA</td>
<td>Displays CSA usage and limit information</td>
</tr>
<tr>
<td>TCPSTOR</td>
<td>Displays TCP/IP private and common storage usage information by the stack</td>
</tr>
</tbody>
</table>
Shared Memory Communications over RDMA

MainView for IP enables you to use the NMI to gather new Shared Memory Communications over RDMA (SMC-R) and RoCE interface data. The data collected includes:

- SMC Link data
- RoCE Interface data
- RoCE tuning stats data

To gather SMC-R and RoCE data using the NMI

1. Select **EZSMCR** from the **EZIP** menu.
2. Select one of the following links to retrieve the data.
   - **SMCLINKS**— SMC Links
   - **SMCCONS**— SMC Connections
   - **STACKSMC**— SMC Stack stats
   - **ROCEINTF**— RoCE Interfaces

   The relevant information is displayed in the view.

FTP statistics in MainView for IP

MainView for IP uses the IBM network management interface (NMI) to collect FTP data. File Transfer Protocol (FTP) is a method for exchanging files between computers on the Internet.

If you enable the IBM NMI, MainView for IP can provide real-time statistics for active FTP control ports and for the data traffic ports. The FTP connections views display response times, transfer rates, progress, and diagnostic information. For information about customizing the IBM NMI, see the *MainView for IP Customization Guide*.
Before using the FTP Servers views, ensure that you have completed the required customization tasks and that your operating system meets the minimum requirements. Customization tasks and operating-system requirements are described in the *MainView for IP Customization Guide*.  

Table 21 on page 62 describes the views that provide detailed or summary information about FTP servers and connections.

**Table 21: FTP statistics views**

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTPSA</td>
<td>Displays active FTP control connections</td>
</tr>
<tr>
<td>FTPSC</td>
<td>Displays closed FTP sessions information</td>
</tr>
<tr>
<td>FTPLF</td>
<td>Displays unsuccessful FTP logons</td>
</tr>
<tr>
<td>FTPLFC</td>
<td>Displays unsuccessful FTP client logons</td>
</tr>
<tr>
<td>FTPLFS</td>
<td>Displays unsuccessful FTP server logons</td>
</tr>
<tr>
<td>FTPFU</td>
<td>Displays FTP file transfer information by user ID</td>
</tr>
<tr>
<td>FTPFUZ</td>
<td>Displays FTP file transfer information summerized by user ID</td>
</tr>
<tr>
<td>FTPFI</td>
<td>Displays FTP file transfer information by IP address</td>
</tr>
<tr>
<td>FTPFIZ</td>
<td>Displays FTP file transfer information summerized by IP address</td>
</tr>
<tr>
<td>FTPFF</td>
<td>Displays FTP file transfer information by file name</td>
</tr>
<tr>
<td>FTPFFZ</td>
<td>Displays FTP file transfer information summerized by file name</td>
</tr>
</tbody>
</table>

The view shown Figure 20 on page 63 displays FTP information for active and complete file transfers that occurred during the interval. An FTP process consists of two connections: the control port and the data port. The data transfer of an FTP
occurs on the data port connection. The FTPFI view shows the data port connections. The FTPSA view shows the control connections.

Figure 20: FTPFI View

| Remote IPAddr | Remote Port | Local Port | FTP Rate | Bytes/sec | Local User | User Name | Name
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>170.225.15.26</td>
<td>20</td>
<td>18866</td>
<td>2.0M</td>
<td>0...100000</td>
<td>+ IOAMAINT</td>
<td>anonymou CSGI.P</td>
<td></td>
</tr>
<tr>
<td>170.225.15.26</td>
<td>20</td>
<td>18867</td>
<td>272.0K</td>
<td></td>
<td>IOAMAINT</td>
<td>anonymou CSGI.P</td>
<td></td>
</tr>
<tr>
<td>170.225.15.26</td>
<td>20</td>
<td>18868</td>
<td>305.8K</td>
<td></td>
<td>IOAMAINT</td>
<td>anonymou CSGI.P</td>
<td></td>
</tr>
<tr>
<td>170.225.15.26</td>
<td>20</td>
<td>18869</td>
<td>200.1K</td>
<td></td>
<td>IOAMAINT</td>
<td>anonymou CSGI.P</td>
<td></td>
</tr>
<tr>
<td>170.225.15.26</td>
<td>20</td>
<td>18870</td>
<td>3675.9</td>
<td></td>
<td>IOAMAINT</td>
<td>anonymou CSGI.P</td>
<td></td>
</tr>
<tr>
<td>170.225.15.26</td>
<td>20</td>
<td>18871</td>
<td>925.7K</td>
<td></td>
<td>IOAMAINT</td>
<td>anonymou CSGI.P</td>
<td></td>
</tr>
<tr>
<td>170.225.15.26</td>
<td>20</td>
<td>16486</td>
<td>345.9K</td>
<td></td>
<td>MSAXR1</td>
<td>anonymou IMSVS.</td>
<td></td>
</tr>
<tr>
<td>170.225.15.26</td>
<td>20</td>
<td>16487</td>
<td>9225.0</td>
<td></td>
<td>MSAXR1</td>
<td>anonymou MSAXR</td>
<td></td>
</tr>
<tr>
<td>170.225.15.62</td>
<td>20</td>
<td>16488</td>
<td>377.0K</td>
<td></td>
<td>MSAXR1</td>
<td>anonymou IMSVS.</td>
<td></td>
</tr>
<tr>
<td>170.225.15.62</td>
<td>20</td>
<td>21123</td>
<td>2.6M</td>
<td></td>
<td>+ CSTRXF2</td>
<td>anonymou CSTRXF</td>
<td></td>
</tr>
<tr>
<td>172.17.1.50</td>
<td>20</td>
<td>60141</td>
<td>19.5M</td>
<td></td>
<td>+ RDAMPR2</td>
<td>marodrig ESD.BM</td>
<td></td>
</tr>
<tr>
<td>172.17.1.50</td>
<td>20</td>
<td>60143</td>
<td>15.9M</td>
<td></td>
<td>+ RDAMPR2</td>
<td>marodrig ESD.BM</td>
<td></td>
</tr>
<tr>
<td>172.164.204</td>
<td>20</td>
<td>16583</td>
<td>124.0K</td>
<td></td>
<td>IOAMAINT</td>
<td>5ESAMAP PDB.MX</td>
<td></td>
</tr>
<tr>
<td>172.164.204</td>
<td>20</td>
<td>16584</td>
<td>2.6M</td>
<td></td>
<td>+ IOAMAINT</td>
<td>5ESAMAP PDB.MX</td>
<td></td>
</tr>
<tr>
<td>172.164.204</td>
<td>20</td>
<td>16585</td>
<td>1.6M</td>
<td></td>
<td>+ IOAMAINT</td>
<td>5ESAMAP PDB.MX</td>
<td></td>
</tr>
<tr>
<td>172.164.204</td>
<td>20</td>
<td>16586</td>
<td>1.2M</td>
<td></td>
<td>+ IOAMAINT</td>
<td>5ESAMAP PDB.MX</td>
<td></td>
</tr>
<tr>
<td>172.164.204</td>
<td>20</td>
<td>16587</td>
<td>80.0</td>
<td></td>
<td>IOAMAINT</td>
<td>5ESAMAP PDB.MX</td>
<td></td>
</tr>
<tr>
<td>172.164.204</td>
<td>20</td>
<td>16588</td>
<td>263.6K</td>
<td></td>
<td>IOAMAINT</td>
<td>5ESAMAP PDB.MX</td>
<td></td>
</tr>
<tr>
<td>172.164.204</td>
<td>20</td>
<td>16589</td>
<td>3.4M</td>
<td></td>
<td>+ IOAMAINT</td>
<td>5ESAMAP PDB.MX</td>
<td></td>
</tr>
</tbody>
</table>

IP Security Views in MainView for IP

The IPSEC view displays security and defensive filtering configuration information for the TCPIP stack. It also displays summary IKE, IPSec, and IP Filtering data for the TCPIP Stack.

The following Table 22 on page 63 shows the available IPSec views

<table>
<thead>
<tr>
<th>View</th>
<th>Description of view display</th>
<th>View name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec Status</td>
<td>Security and defensive filtering configuration information for the TCPIP stack. It also displays summary IKE, IPSec, and IP Filtering data for the TCPIP Stack</td>
<td>IPSECD</td>
</tr>
<tr>
<td>Dynamic Tunnel Stats</td>
<td>Dynamic Tunnel statistics</td>
<td>DYNTUUNN</td>
</tr>
<tr>
<td>Active IP Filters</td>
<td>Current active IP filters for the TCPIP stack. These filters can be either the default IP security filters or policy IP security filters. Any defensive filters that are installed are also included</td>
<td>IPCFILTR</td>
</tr>
<tr>
<td>Default IP Filters</td>
<td>Default IP filters for the TCPIP stack. These filters originate from the TCP/IP profile</td>
<td>IPDFILTR</td>
</tr>
</tbody>
</table>
Intrusion detection views in MainView for IP

Security is provided by Intrusion Detection Services (IDS). MainView for IP provides views that display information about defined IDS policies.

IDS provides the following support:

- Scan detection and reporting
- Attack detection, reporting, prevention
- Traffic regulation for TCP connections and UDP receive queues

IDS policies are used to specify what events are to be detected, under what circumstances and what action to take. Scans are recognized as the result of multiple gathering events from a single source IP within a defined period of time. An attack can be a single packet designed to crash or hang a system, and can also consist of multiple packets designed to consume a limited resource causing devices to be unavailable to their intended users (that is, denial of service). IDS attack policy allows you to turn on attack detection for categories of attacks independently of each other.

The IDS categories of attacks are:

- Malformed packet events
- Inbound fragment restrictions
- IP protocol restrictions
- IP option restrictions
- UDP perpetual echo
- ICMP redirect restrictions
- Outbound raw restrictions
Flood events

Table 23 on page 65 describes the views that provide detailed information about your intrusion detection service.

Table 23: IDS views

<table>
<thead>
<tr>
<th>View</th>
<th>Description of display</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDSS</td>
<td>A summary of the Intrusion Detection Services policies</td>
</tr>
<tr>
<td>IDSFLOOD</td>
<td>All active interface floods</td>
</tr>
<tr>
<td>IDSTCPPL</td>
<td>Information about active Intrusion Detection Services policies for the TCP protocol</td>
</tr>
<tr>
<td>IDSUDPPL</td>
<td>Information about active Intrusion Detection Services policies for the UDP protocol</td>
</tr>
</tbody>
</table>

Name Resolver using NMI

MainView for IP monitors resolver configuration information and GLOBALTCPIPDATA file contents by accessing data from the NMI callable services EZBREIFR. The RESOLVER view displays the name resolver configuration information.

Figure 21: Name Resolver view
Diagnostics in MainView for IP

In MainView for IP, you can perform actions that provide diagnostic information.

- When performing a ping in the Ping view, you can control the ping by also specifying the size of the ping (up to 65 kilobytes) and the number of repetitions (up to 32 echo messages).
  
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)

- In the Traceroute Information view, you can perform a traceroute and view information about the traceroute. 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.

- In the Packet Tracing views, you can quickly start, stop, write, or display a trace on a packet. The Packet Tracing views provide all of the TCP/IP header and packet data to help you diagnose a problem on your network.
  
  The Packet Tracing view displays all of the packet data or the amount of data that has been specified in the Pkt Len field.

  **Note**
  
  The Packet Tracing view displays all of the packet data or the amount of data that has been specified in the Pkt Len field.

- In the Packet Tracing view, multiple active traces are available for TCP/IP stacks. If a packet matches the filter for multiple traces on a given TCP/IP stack, it can be traced for each started packet trace that it matches.

- In the Packet Tracing view, you can write a RAW packet trace to a data set in the raw IBM component trace format. This file is used as input into interactive problem control system (IPCS) to format the packet trace output, or to any other IBM utilities (for example, Stayton formatter). This file is also sent to IBM as diagnostics for debugging purposes.

- In the Packet Tracing view, you can write a packet trace to a data set in SNIFFER format. This file is used as input into Wireshark.
- In the Packet Headers view, you can display header information for packets that were traced. The packet headers will be written to MainView history files. The Log Packet Hdrs field must be set to YES when the packet trace is started.

- In the Socket Tracing views, you can start, stop, write, 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.

**WARNING**

If you are tracing a packet or a socket, and you cancel the PAS, you might receive an abend. BMC recommends that you shut down the PAS normally or stop the trace.

Table 24 on page 67 describes the views that provide detailed information about pings, packet traces, socket traces, and traceroutes.

**Table 24: Diagnostics views**

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PINGT</td>
<td>Lets you perform a ping</td>
</tr>
<tr>
<td>PING</td>
<td>Displays information about a ping that you have performed</td>
</tr>
<tr>
<td>PKTTRACD</td>
<td>Displays details about a packet that has been traced</td>
</tr>
<tr>
<td>PKTTRACF</td>
<td>Lets you specify the filtering parameters for displaying or writing packet traces</td>
</tr>
<tr>
<td>PKTTRACE</td>
<td>Lets you start, stop, write, or display a trace on a packet</td>
</tr>
<tr>
<td>PKTTRACH</td>
<td>Displays details about packet headers for packets that have been traced</td>
</tr>
<tr>
<td>SKTTRACD</td>
<td>Displays details about a socket that has been traced</td>
</tr>
<tr>
<td>SKTTRACF</td>
<td>Lets you specify the filtering parameters for displaying or writing socket traces</td>
</tr>
<tr>
<td>SKTTRACE</td>
<td>Lets you start, stop, write, or display a trace on a socket</td>
</tr>
<tr>
<td>TRACERTE</td>
<td>Lets you perform a traceroute, and then displays information about the traceroute</td>
</tr>
<tr>
<td>TRACE</td>
<td>Displays information about the number of hops that were required to trace the IP address, and the time (reported in hundredths of a second) that was required to perform each hop</td>
</tr>
<tr>
<td>TRACED</td>
<td>Displays detailed information for each hop of a trace</td>
</tr>
</tbody>
</table>

**Pinging a device in MainView IP**

Use the following procedure to ping a device.

You can ping a device by using one of the following methods:
To use the Ping line command

1. From the EZIP menu select **Ping Information** from the **Diagnostics** section, and press **Enter**.

2. Type **P** in the **COMMAND** field.

3. In the **Ping IPAddr** field, type an IP address or a domain name that you want to ping, and press **Enter**.

   Note
   You can also specify the following parameters:
   - The size of the ping by typing the ping size in bytes (up to 65 kilobytes) in the **Ping Size** field
   - The number of ping echo repetitions (up to 32 echo messages) in the **Ping Count** field
   - The TCP IP stack name in the **TCPIP Stack** field

To select an IP address in the Ping IPAddr field

1. From the EZIP menu select **Ping Information** from the **Diagnostics** section, and press **Enter**.

   The Ping view (PING) is displayed (Figure 22 on page 68)

   **Figure 22: Ping view**

<table>
<thead>
<tr>
<th>17JAN2012 07:35:38</th>
<th>MAINVIEW WINDOW INTERFACE (V6.0.00)</th>
<th>COMMAND ====&gt;</th>
<th>SCROLL ====&gt;</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CURR WIN ====&gt; 1</td>
<td>ALT WIN ====&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt;W1 =PING=============(ALL======*=======)17JAN2012==07:35:38====MVIP=====D====2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CMD Ping IPAddr</td>
<td>Ping Ping TCPIP Domain</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--- or DNS Name</td>
<td>Count Size Stack Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>1 256</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>1 256</td>
<td>default.host.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. From the **Ping IPAddr** field, select the IP address of the device that you want to ping, and press **Enter**.
If the IP address you want to ping is not shown in the list, enter the address in the Ping IPAddr field.

**To type a Ping command on a command line**

1. When using MainView for IP, type one of the following commands on any COMMAND line and press Enter:

   - `PING ipAddress`
   - `PING domainName`

   Replace the variables as follows:

   - `ipAddress` 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.

**Performing a traceroute on a device in MainView for IP**

Use the following procedure to perform a traceroute on a device.

*Note*

The data that is displayed on the Tracerte Information view might not be complete data or real-time data. The traceroute task is asynchronous; because a traceroute might take several minutes to complete, MainView for IP can display data while the traceroute is running. The status of the traceroute request registers in the Tracerte Status field.

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

- “To issue the traceroute line command” on page 70
- “To select an IP address in the Tracerte IPAddr field” on page 70
- “To type a traceroute command on a COMMAND line” on page 70

*Note*

You can also Issue the TR line command from a Connections view.
To issue the traceroute line command

1. From the EZIP menu, select **Tracerte Information** from the **Diagnostics** section, and press Enter.

2. In the CMD field next to the IP address you want to trace, type **TR**, and press Enter.

To select an IP address in the Tracerte IPAddr field

1. From the EZIP menu, select **Tracerte Information** from the Diagnostics section, and press Enter.

The Tracerte view (TRACERTE) is displayed(Figure 23 on page 70).

Figure 23: Traceroute Information detail view

2. From the **Tracerte IPAddr** field, select the IP address of the device that you want to trace, and press Enter.

You can configure the following additional filtering parameters:

- **Trace Port** is the port to be used for the TraceRoute
- **Max Hops** is the maximum number of Hops on the TraceRoute (valid values are 1-64, the default is 30)
- **Max Wait** - is the he maximum wait on each hop of the TraceRoute (valid values are 1-255, the default is 5 seconds)
- **TCPIP Stack name** is the TCPIP Stack to use when issuing the PING command

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

To type a tracercue command on a COMMAND line

1. Type one of the following commands on a COMMAND line, and press Enter:

   - **TRACE iPAddress**
   - **TRACE domainName**
Replace the variables as follows:

- **iPAddress** 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.

## Accessing more traceroute information in MainView IP

Use this procedure to drill down in the TRACE view to access more information about a specific hop on a traceroute.

### To access more traceroute information

1. From the TRACE view select the hop in the **Current Hop** field for which you want to see more information, and press **Enter**.

The More traceroute information (TRACED) panel is displayed (Figure 24 on page 71).

### Figure 24: Traceroute details

```
07OCT2009  12:19:52 ++++ MAINVIEW WINDOW INTERFACE (V6.0.00) +++++++++
COMMAND     ==>         SCROLL    ==>  PAGE
CURR WIN     ==>  1        ALT WIN    ==>
W1=TRACED========TCP/IP==07OCT2009==12:19:52==MVIP=====D====1

Tracerte Information....
Tracerte IP addr............ 172.17.4.175
Domain Name.................. mgw.bmc.com
Total Hops...................
Hop Delay...................

Tracerte Hop Analysis...
Hop Sequence Number....... 4
Hop IP addr................. 172.18.255.10
Hop Domain Name............. mgw.bmc.com

Tracerte Response Times.
Min Response................. 0
Max Response................. 2
Avg Response................. 1
```

**Tip**

To see ping information for the hop, in the PING view, select the **Hop IPaddr** field and press **Enter**.

## Starting a packet trace in MainView IP

Use the following procedure to start a packet trace.
The packet trace can be started for a specific IP address, source port, destination port, protocol type, and packet length.

A packet trace may also be started by a MainView alarm on any connection views for a specific connection. When the alarm triggers a packet trace is started. It ends when the trace is stopped. This automated packet trace requires the MainView for Networks solution as well as an AUTOOPERATOR (AO) rule.

**WARNING**

If you are tracing a packet (or a socket), and you cancel the PAS, you might encounter an abend. BMC recommends that you shut down the PAS normally before starting the trace or stop the trace before you stop the PAS.

You can perform a packet trace by using one of the following methods:

- Issue the STA line command from the Packet Trace view.
- Issue the PKT line command from a Connections view.

**To start a packet trace**

1. From the EZIP menu, select **Packet Tracing** from the Diagnostics section, and press **Enter**.

   The Packet trace view (PKTTRACE) is displayed (Figure 25 on page 72):

   ![Packet trace view](image)

   **Figure 25: Packet trace view**

   1. To trace packets, type **STA** or **START** or **STARTALL** (to start all the packet traces), in the **Command** field, and press **Enter**.

   2. **(optional)** You can apply the following filters by changing their field entry:

      - **Time type** for local or GMT
      - **Trace Identifier** for an identifier to be associated with the trace
      - **Packet Length** for length of the packet to be traced
      - **Duration** for the duration before active trace is stopped (hh:mm:ss)
- **Protocol Type** for the protocol type to be traced
- **Port Number** for which you can specify up to 4 port numbers to be matched on either destination or source port in all packets.
- **IP Address** to specify up to 4 IP Addresses (separate by commas)

4. (Optional) To trace encrypted packets, type **YES** in the **IPSec Data** field.

**Note**
The **EZB.TRCSEC.sysname.tcpname.IPSEC** resource profile must be authorized.

5. Press **F3** to complete the task

---

**Writing a RAW packet trace to a data set in MainView IP**

Use the following procedure to write a packet trace in a RAW IBM component trace format to a data set. The file can then be used as input to IPCS or other IBM utilities to display the packet trace.

**Before you begin**

You must preallocate a data set before you begin writing a raw packet trace to a data set. This process is not performed within the program. The RAW Packet data set attributes must be as follows:

- Organization: **PS**
- Record format: **VB**
- Record Length: **32756**
- Block Size: **32760**

For more information, see the **MainView for IP Customization Guide**.

**WARNING**
The USERID for the MainView for IP started-task-address-space is used when the packet trace is written to a data set. The operation will fail if the USERID does not have SAT authority to write to the data set. You can enable the packet trace write function by granting the proper access and write authority to the PAS.
Tip
To specify whether the packet trace wraps to the end of the trace table, use the MVIP Parm Configuration (MVIPCONF) view to set the Pkttrace Wrap parameter. For more information, see the MainView for IP Customization Guide.

To write a RAW packet trace to a data set

1. From the EZIP menu select Packet Tracing from the Diagnostics section, and press Enter.

2. In the Command field of the packet tracing view (PKTTRACE), type R or RAW, and press Enter.

3. Type the name of the data set in the File Name field, and any other types of filters that you want, and press Enter.

Tip
Before pressing F3, you can limit the parameters of the raw packet trace by typing an entry in one or more of the following fields:

- Start Date
- Start Time
- Stop Date
- Stop Time
- Protocol
- IP Address
- Port Number

4. Press F3 or type END to complete the task.

Message TACI9231I is confirms that the raw packet trace is being written to the specified data set.

Writing a packet trace in Sniffer format to a data set

Use the following procedure to write a packet trace in Network Associates Sniffer format to a data set. The file can then be used as input to Wireshark.
Before you begin

You must preallocate a data set before you begin writing a packet trace to a data set in Sniffer format. This process is not performed within the program. The packet data set attributes must be as follows:

- Organization: PS
- Record format: VB
- Record Length: 1600
- Block Size: 27998

For more information, see the MainView for IP Customization Guide.

---

**WARNING**

The USERID for the MainView for IP started-task-address-space is used when the packet trace is written to a data set. The operation will fail if the USERID does not have SAT authority to write to the data set. You can enable the packet trace write function by granting the proper access and write authority to the PAS.

---

**Tip**

To specify whether the packet trace wraps to the end of the trace table, use the MVIP Parm Configuration (MVIPCONF) view to set the Pkttrace Wrap parameter. For more information, see the MainView for IP Customization Guide.

---

To write a packet trace in Sniffer format to a data set

1. From the EZIP menu select **Packet Tracing** from the Diagnostics section, and press Enter.

2. In the Command field of the packet tracing view (PKTTRACE), type **SNIFF**, and press Enter.

3. Type the name of the data set in the File Name field, and any other types of filters that you want, and press Enter.
Tip
Before pressing F3, you can limit the parameters of the packet trace by typing an entry in one or more of the following fields:

- Start Date
- Start Time
- Stop Date
- Stop Time
- Protocol
- IP Address
- Port Number
- Data Length

4 Press F3 or type END to complete the task.

A message is displayed that confirms the packet trace is being written to the specified data set.

Writing a packet trace to a data set

Use this procedure to write a packet trace to a sequential data set.

The WRITE command allows you to write the Packet Trace formatted to a data set.

Before you begin

You must allocate a sequential data set FB(80) before you begin writing a packet trace to a data set. This process is not done within the program. For more information about preallocating a sequential data set, see Writing a RAW packet trace to a data set.

To specify whether the packet trace wraps to the end of the trace table, use the MVIP Parm Configuration (MVIPCONF) view to set the Pkttrace Wrap parameter. For more information, see the MainView for IP Customization Guide.
To write a packet trace to a data set

1. From the EZIP menu select Packet Tracing from the Diagnostics section, and then press Enter.

2. In the Command field of the Packet Tracing view (PKTTRACE), type W or WRITE, and press Enter.

3. Type the name of the data set in the File Name field, and any other types of filters that you want, and press Enter.

   **Tip**

   Before completing the procedure, you can limit the parameters of the write packet trace by typing an entry in one or more of the following fields:

   - Start Date
   - Start Time
   - Stop Date
   - Stop Time
   - Protocol
   - IP Address
   - Port Number

4. Press F3 to complete the task.

   Message TACI9225I is displayed to indicate that the trace is being written to the specified data set.

**Stopping a packet trace**

Use the following procedure to stop a packet trace

**To stop a packet trace**

1. On the PKTTRACE view verify that ACTIVE is displayed in the Trace Status field.

2. In the Command line field, type STO, or STOP, or STOPALL (to stop all active packet traces) and press Enter.
Message TACI92111 confirms that the trace has been terminated.

3 Press **Enter** to return to the PKTTRACE view.

**STOPPED**, or **NOT ACTIVE** is displayed in the **Trace Status** field.

**Note**
If there is an abnormal stop, one of the following status appear in the appropriate field:

- **STOP/NWRAP** notifies that the packet trace has been stopped because the trace table has wrapped and you specified no wrap for Packet Trace
- **STOP/ABEND** notifies that the packet trace has been stopped because the abend limit has been exceeded in the Packet Trace routine

---

**Displaying a packet trace**

Use the following procedure to display a packet trace.

The display packet trace command shows the information about the first 37,500 traced packets from the PKTTRACE view.

**To display a packet trace**

1 Enter D in the **Command** field and press **Enter**.

The Packet Tracing Details (PKTTRACD) view is displayed.
Viewing packet details

Use the following procedure to drill down in the PKTTRCD2 view to access more information about a specific packet that has been traced.

To view packet details

1. In the PKTTRCD2 view, position the cursor over one of the following headings.
   - IP Header
   - Protocol Hdr
   - Packet Data

2. Press Enter.

More packet details are displayed (Figure 26 on page 79).

Figure 26: More packet details view

15APR2003 12:47:20 ------- MAINVIEW WINDOW INTERFACE(V4.1.05)------------------
COMMAND ===> SCROLL ===> PAGE
CURR WIN ===> 1 ALT WIN ===> >W1 =PKTTRCD2==MCSBMSA==*==15APR2003==12:47:20==MVIP==D==5
 Offset ---------------Data----------------  ---- EBCDIC ----  ---- ASCII -----
00000 DC072910 00010000 00000001 20454345  ................  ü.)......... ECE
000010 50454346 48454945 4A464545 46434143  &...............  PECFHEIEJFEEFCAC
000020 41434143 41434143 41434141 44000020  ................  ACACACACACAAD..
000030 0001C00C 00200001 00054400 00066000  ..{...........-.  ..{.. ....F...-.
000040 AC130390                             ....              Ð..°

3. To see more pages of the PKTTRCD2 view, scroll down by pressing F8.

Filtering a packet trace in MainView IP

Use this procedure to filter the records displayed. You can select to display records for a date, range of dates, a port, IP address and protocol.

The packet trace view displays the first 37,500 packet trace records that match the filter criteria entered.

To filter a packet trace

1. From the PKTTRACD panel position the cursor next to the column title Search Criteria, and press Enter.

The Search Criteria expands displaying the Packet Trace filter fields (Table 25 on page 80).
### Table 25: Packet Trace Filter fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Date</td>
<td>A specific date or the starting point of a range of dates to limit the records displayed based on the date of the packet.</td>
</tr>
<tr>
<td>Start Time</td>
<td>A specific time or the starting point of a range of times to limit the records displayed based on the time of the packet.</td>
</tr>
<tr>
<td>Stop Date</td>
<td>An ending date for a range of dates. Use this field with the Start Date field.</td>
</tr>
<tr>
<td>Stop Time</td>
<td>An ending time for a range of times. Use this field with the Start Time field.</td>
</tr>
<tr>
<td>Port</td>
<td>A port number to filter the packet trace based on source and destination port. The packet trace view displays any records that match either source or destination port.</td>
</tr>
<tr>
<td>IP Address</td>
<td>An IP address to filter the packet trace based on source and destination IP address. The packet trace view displays any records that match either source or destination IP address.</td>
</tr>
<tr>
<td>Protocol</td>
<td>A type of protocol such as TCP, UDP or ICMP.</td>
</tr>
<tr>
<td>Max Records</td>
<td>A number from 1-37,500 to define the maximum number of packet trace records to display. The default value is 37,500.</td>
</tr>
</tbody>
</table>

2. Enter the filter criteria and press **Enter**

   The packet trace view searches through all the trace records and displays the records that match the criteria entered up to the maximum number of records (Max Records) defined.

### Accessing detailed packet trace information

Use the following procedure to access more information about a specific packet that has been traced.

**To access more packet trace information**

1. From the **PKTTRACD** view position the cursor over the date of the packet for which you want to see more information and press **Enter**.

   **Note**

   To see more pages of the PKTTRCD view, scroll down by pressing **F8**.
Accessing packet trace header information

Use the following procedure to access information about packet headers that have been traced.

To access packet trace header information

1. From the EZIP menu, select Packet Headers from the Diagnostics section and press Enter.

   The Packet Headers (PKTTRACH) view is displayed.

   09JUN2013  09:01:20 ------ MAINVIEW WINDOW INTERFACE (V6.1.00) ---------
   COMMAND ===> SCROLL ===> PAGE
   CURR WIN ===> 1  ALT WIN ===>
   >W1 =PKTTRACH=TPCIP=09JUN2013==09:01:20==MVIP===D==366
   + Search Criteria      Packet Trace Filters             + Show Fixed section
   Pkt        Source           Src   Dest             Dest
   Date     Time         Len   Flow IPAddr           Port  IPAddr           Port
   06/09/13 09:00:52.763    40 ---> 172.24.48.130       23 192.168.215.66   49326
   06/09/13 09:00:52.888   576 ---> 172.24.48.130       23 192.168.215.66   49326
   06/09/13 09:00:52.888   576 ---> 172.24.48.130       23 192.168.215.66   49326
   06/09/13 09:00:52.888   152 ---> 172.24.48.130       23 192.168.215.66   49326
   06/09/13 09:00:53.078    40 <--- 192.168.215.66   49326 172.24.48.130       23
   06/09/13 09:00:53.087    48 <--- 192.168.215.66   49326 172.24.48.130       23
   06/09/13 09:00:53.087    40 ---> 172.24.48.130       23 192.168.215.66   49326
   06/09/13 09:01:20.534   444 ---> 172.24.48.130     1027 172.24.51.0       2001
   06/09/13 09:01:20.535    52 <--- 172.24.51.0       2001 172.24.48.130     1027
   06/09/13 09:01:20.535    48 <--- 172.24.48.130     1027 172.24.51.0       2001
   06/09/13 09:01:20.535    52 <--- 172.24.51.0       2001 172.24.48.130     1027

2. From the PKTTRACH view, position the cursor over the date of the packet for which you want to see more information and press Enter.
The Packet Headers detail view is displayed.

```
09JUN2013  09:14:58 ------ MAINVIEW WINDOW INTERFACE (V6.1.00) ---------------
COMMAND ====>          SCROLL ====> PAGE
CURR WIN ====> 1        ALT WIN ===>>
>W1 =PKTTRACH=PKTTRCHD=TCPIP=======*========09JUN2013==09:14:01====MVIP=====D====1
```

** Link Name.........   GIGF7  
** Link Type.........   Ipaqenet  
** Date..............   06/09/13  
** Time..............   09:00:53.801779  

** IP Header   **
** Source IPAddr.....   172.24.48.130  
** Dest IPAddr.......   172.24.51.0  
** IP Version........       4  
** Packet Len........     448  
** TOS...............      00  
** Ident Nbr.........    BCEA  
** Frag Offset.......   0  
** Time to Live......      64  
** Checksum..........  
** Header Len........      20  
** Offset....    ----------- IP Header -------------
00000000....   450001C0 BCEA0000 40860000 AC183082
00000010....   00000000 00000000 00000000 00000000

** Protocol Hdr **
** Protocol..........   TCP  
** Source Port.......    1027  
** Dest Port.........    2001  
** Header Len.......      32  
** Offset....    -------- Protocol Header ----------
00000000....   040307D1 BE3C809E 4EECF80F 80180FFF
00000010....   00000000 0101080A F258183A 0F308853
00000020....   00000000 00000000 00000000 00000000

Deleting a packet trace

Use the following procedure to delete a packet trace.

** Before you begin **

The packet trace must be non-active before you can delete it. You must stop it to make it nonactive. See Stopping a packet trace.

** To delete a packet trace **

1 On the PKTTRACE view verify that STOPPED is displayed in the Trace Status field.

2 In the Command field, type DEL or DELETE, or DELALL (to delete all of the stopped packet traces), and press Enter.

Message TACI9215I confirms that the trace has been deleted.

3 Press Enter to return to the PKTTRACE view.
Navigating records

Use this procedure to move between records.

To move between records

1. From the PKTTRACD view position the cursor over the date of the packet for which you want to see more information and press Enter.

   The More Packet Tracing Details (PKTTRCD2) view is displayed. To see more pages of the PKTTRCD view, scroll down by pressing F8.

2. To go from one record to the next, type NEXTE on the COMMAND line.

3. To go back one record, type PREVE on the COMMAND line.

   **Tip**

   For easy access, you can assign these commands to F keys. For more information about how to assign commands to F keys, see the MainView User Guide.

   **Note**

   Each time you use the NEXTE command, the record moves forward one record. For example, if you use the NEXTE command five times, you will move forward five records. To exit from several records, you must use the PREVE command an equal number of times.

   To quickly exit out of the records, type QUIT or Q. This command returns you to the Network Management Solutions menu. Type 1 to go to the MainView for IP menu.

Starting a socket trace in MainView IP

Use the following procedure to start a socket trace.

The socket trace can be started for a specific MVS job name, source port, destination port, and destination IP address.

The START socket trace command initiates a socket trace with the specified filters (for example, job name, and so on.). The socket trace can be viewed through the display command. Only one socket trace can be active per stack at a time.
**WARNING**
If you are tracing a packet (or a socket), and you cancel the PAS, you might encounter an abend. BMC recommends that you shut down the PAS normally or stop the trace.

---

**To start a socket trace**

1. From the EZIP menu select **Socket Tracing** from the Diagnostics section, and press **Enter**.

   The Socket Tracing view (SKTTRACE) is displayed ([Figure 27 on page 84](#)).

   **Figure 27: Socket Tracing view**

   | 26OCT2009 09:12:43 -------- MAINVIEW WINDOW INTERFACE (V6.0.00) --------------- | Command Trace Userid Nbr Job Dest Source Dest Local/
   | -------- Status Started Recs Name IPAddr Port Port GMT | NOT ACTIVE 0 LOCAL |

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

   **Tip**
   You can also type IP address, source port and destination port filters in this window to limit the parameter of the trace.

   **Note**
   A socket trace can only be started for a non-active trace.

3. Press **F3** to complete the task.

   Message TACI9309I confirms that the trace has been activated.

4. Press **Enter** to return to the SKTTRACE view.

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

   Other status types include:

   - **ACTIVE** to indicate that the socket trace is currently active and tracing.
   - **STOPPED** to indicate that the socket trace has been stopped.
   - **NOT ACTIVE** to indicate that the socket trace is not currently active.
Note
If the status type is Not Active press Enter to refresh the panel.

Writing a socket trace to a data set in MainView IP

Use the following procedure to write a socket trace to a sequential data set.

The WRITE command allows you to write the socket trace formatted to a data set.

WARNING
The USERID for the MainView for IP started-task-address-space is used when the socket trace is written to a data set. The operation will fail if the USERID does not have SAT authority to write to the data set. You can enable the socket trace write function by granting the proper access and write authority to the PAS.

Note
- You can specify whether the socket trace wraps to the end of the trace table by using the MVIP Parm Configuration (MVIPCONF) view to set the Skttrace Wrap parameter. For more information, see the MainView for IP Customization Guide.
- You must pre-allocate a sequential data set FB(80) before you begin writing a packet trace to a data set. This process is not performed within the program. For more information about pre-allocating a sequential data set, see Writing a RAW packet trace to a data set.

To write a socket trace to a data set

1. From the EZIP menu select Socket Tracing from the Diagnostics section, and press Enter.
2. In the Command field, type W or WRITE, and press Enter.
3. Type the name of the data set in the File Name field.
   Tip
   You can also type File Name, Time Type, Start and Stop Date, and Start and Stop Time filters in this window to limit the parameter of the write socket trace.
4. Press F3 or type END to complete the task.
   Message TACI9317I confirms that the trace is being written to the specified data set.
Stopping a socket trace

Use the following procedure to terminate an active socket trace. The socket trace can then be viewed through the display command.

**To stop a socket trace**

1. On the SKTTRACE view, verify that ACTIVE is displayed in the **Trace Status** field.

2. In the **Command** field, type **STO** or **STOP**, and press **Enter**.
   
   Message TACI9310I confirms that the trace has been terminated.

3. Press **Enter** to return to the SKTTRACE view.

   One of the following is displayed in the **Trace Status** field:
   - STOPPED
   - NOT ACTIVE
   - STOP/NWRAP
   - STOP/ABEND

Displaying a socket trace in MainView IP

Use the following procedure to DISPLAY socket trace command to show the socket trace records. The SKTTRACE view displays information about the first 90,000 traced packets.

**To display a socket trace**

1. Enter **D** in the **Command** field and press **Enter**.
The Socket Packet Tracing Details (SKTTRACD) view is displayed (Figure 28 on page 87).

**Figure 28: Socket packet tracing details view**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Job</th>
<th>Socket</th>
<th>Socket Before/ Return</th>
<th>Return</th>
<th>Value</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/27/09</td>
<td>04:32:10.0320</td>
<td>MV$CAS</td>
<td>BPX1AIO</td>
<td>4 Before</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/27/09</td>
<td>04:32:10.0320</td>
<td>MV$CAS</td>
<td>BPX1AIO</td>
<td>4 After</td>
<td>00000094 00000000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/27/09</td>
<td>04:32:10.0325</td>
<td>MV$CAS</td>
<td>BPX1AIO</td>
<td>4 Before</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/27/09</td>
<td>04:32:10.0326</td>
<td>MV$CAS</td>
<td>BPX1AIO</td>
<td>4 After</td>
<td>00000000 0000044F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/27/09</td>
<td>04:32:10.3323</td>
<td>MV$CAS</td>
<td>BPX1AIO</td>
<td>4 Before</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/27/09</td>
<td>04:32:10.3324</td>
<td>MV$CAS</td>
<td>BPX1AIO</td>
<td>4 After</td>
<td>00000000 00000000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/27/09</td>
<td>04:32:10.3324</td>
<td>MV$CAS</td>
<td>BPX1AIO</td>
<td>4 Before</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Filtering a socket trace in MainView IP

Use the following procedure to filter the packet trace entries.

**To filter a socket trace**

1. From the EZIP menu select **Socket Tracing** from the Diagnostics section, and press **Enter**.
2. In the **Command** field type **Filter** or **F**, and press **Enter**.
3. Type the filters that you want to limit for the filter socket trace. **Tip** You can also type **Stack Name, Time Type, Start and Stop Date, and Start and Stop Time** filters in this window. Typing filters limits the parameter of the filter socket trace.
4. Press **F3** or type **END** to complete the task.

The filtered Socket Packet Tracing details (SKTTRACD) view is displayed (Figure 29 on page 87).

**Figure 29: Filtered Socket packet tracing details view**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Job</th>
<th>Socket</th>
<th>Socket Before/ Return</th>
<th>Return</th>
<th>Value</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/27/09</td>
<td>04:32:10.3324</td>
<td>MV$CAS</td>
<td>BPX1AIO</td>
<td>4 Before</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Deleting a socket trace

Use the following procedure to delete a socket trace.

**Note**
The socket trace must be nonactive before you can delete it. You must stop it to make it nonactive. See **Stopping a socket trace**.

---

### To delete a socket trace

1. On the SKTTRACE view verify that STOPPED is displayed in the **Trace Status** field.

2. In the **Command** field, type **DEL** or **DELETE**, or **DELALL** (to delete all of the stopped socket traces) and press **Enter**.

   Message **TACI9314I** confirms that the trace has been terminated.

3. Press **Enter** to return to the SKTTRACE view.

---

Drilling down for socket trace information

Use the following procedure to access more information about a specific socket that has been traced.

### To access additional, detailed socket trace information

1. From the **SKTTRACD** view, select the date of the socket for which you want to see more information and press **Enter**.
Figure 30 on page 89 shows the More Socket Tracing Details (SKTTRCD2) view.

**Figure 30: More Socket Tracing Details view**

29JUN2005  14:32:47 ------ MAINVIEW WINDOW INTERFACE (V4.2.04) -----------
COMMAND  ===>                                                 SCROLL ===> PAGE
CURR WIN ===> 1        ALT WIN ===> W1 =SKTTRACD=SKTTRCd2=RW8ESAM===99JUN2005==14:32:41==MVIP==D1

Date......... 06/29/05
Time......... 14:18:00.8492
Jobname...... NQART574
ASID......... 8E
TCB.......... 009C22B0

Socket Type.. GetHostByName
Before/After. Before
Local Port... 2560
Remote Port.. 0.0.1.48
Remote IPAddr
Return Value.
Return Code..
Reason Code..

<table>
<thead>
<tr>
<th>Parm</th>
<th>Name</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7EBC3BCC</td>
<td>00000000</td>
</tr>
<tr>
<td>2</td>
<td>7EBC3BEC</td>
<td>00000020</td>
</tr>
<tr>
<td>3</td>
<td>7EBC4000</td>
<td>00000000</td>
</tr>
<tr>
<td>4</td>
<td>7EBC3C04</td>
<td>00000000</td>
</tr>
<tr>
<td>5</td>
<td>7EBC3C08</td>
<td>00000000</td>
</tr>
<tr>
<td>6</td>
<td>FEBBC3C0C</td>
<td>00000000</td>
</tr>
</tbody>
</table>

**Note**

You can see more pages of the SKTTRCD view by pressing F8 to scroll down

---

**Dynamic Virtual IP Address in MainView for IP**

A virtual IP address (VIPA) refers to an Internet address on a 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 host 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 you can use to monitor the DVIPAs on your 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
z/OS TCP/IP stacks.

The SYSPLEX views show all the dynamic VIPA’s for all the TCP/IP stacks in the
syplex. You can drill down on each dynamic VIPA and get more detailed
information.

Table 26 on page 90 describes the views that provide information about your
DVIPAs:

Table 26: Dynamic VIPA views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EZVIPA</td>
<td>Provides access to the Dynamic VIPA menu</td>
</tr>
<tr>
<td>SYSPLEX</td>
<td>Displays dynamic virtual IP addresses (VIPAs) for all the TCP/IP stacks in the same sysplex as the current stack.</td>
</tr>
<tr>
<td>SYSPLEXCF</td>
<td>Displays all TCP/IP stacks in the sysplex, and the dynamic cross-system coupling facility (XCF) address that each stack is using.</td>
</tr>
<tr>
<td>VIPACFG1</td>
<td>Displays VIPA backup configuration information</td>
</tr>
<tr>
<td>VIPACFG2</td>
<td>Displays VIPA definition configuration information</td>
</tr>
<tr>
<td>VIPACFG3</td>
<td>Displays VIPA range configuration information</td>
</tr>
<tr>
<td>VIPADST</td>
<td>Displays VIPA distribution configuration information</td>
</tr>
<tr>
<td>VIPACFG5</td>
<td>Displays VIPA service level agreement policy information</td>
</tr>
<tr>
<td>VIPACFG6</td>
<td>Displays VIPA route configuration information</td>
</tr>
<tr>
<td>VIPACONN</td>
<td>Displays the connections that are being routed through the sysplex distributor to the dynamic VIPA</td>
</tr>
<tr>
<td>VIPADYN</td>
<td>Displays general information about DVIPA</td>
</tr>
<tr>
<td>VIPAPORT</td>
<td>Displays the VIPA destination port table information, which exists only on distributing stacks</td>
</tr>
<tr>
<td>VIPAROUT</td>
<td>Displays route information</td>
</tr>
</tbody>
</table>

The VIPCONN view displays all the connections that are being routed through the
syplex distributor to the dynamic VIPA(Figure 31 on page 90)

Figure 31: VIPACONN view

```
19FEB2012  02:45:05 ------- MAINVIEW WINDOW INTERFACE (V6.0.00) ---------------
COMMAND  ===>                                                 SCROLL ===> PAGE
CURR WIN ===> 1        ALT WIN ===>
M1 =VIPACONN========TCP1P2=======19FEB2012==02:45:05==MVIP==D==0
Dest           Dest   Source           Source Destination      Stack
IPAddr          Port   IPAddr           Port   XCFAddr          Name
172.19.170.20   21 172.18.198.67       3150 172.19.170.130   TCPIP2
172.19.170.20   21 172.18.198.67       3157 172.19.170.130   TCPIP2
172.19.170.20   21 172.18.198.67       3161 172.19.170.130   TCPIP2
172.19.170.20   21 172.18.198.67       3159 172.19.170.130   TCPIP2
```
The VIPAPORT view displays the VIPA destination port table information (Figure 32 on page 91). The destination port table exists only on distributing stacks.

**Figure 32: VIPAPORT view**

<table>
<thead>
<tr>
<th>Dest IPAddr</th>
<th>Dest Port</th>
<th>Dest XCF Address</th>
<th>RDY Conns</th>
<th>Active Conns</th>
<th>WLM Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.24.49.130</td>
<td>3049</td>
<td>172.24.49.141</td>
<td>0</td>
<td>0</td>
<td>Roundrobin</td>
</tr>
<tr>
<td>172.24.49.130</td>
<td>3049</td>
<td>172.24.49.142</td>
<td>0</td>
<td>0</td>
<td>Roundrobin</td>
</tr>
<tr>
<td>172.24.49.131</td>
<td>20</td>
<td>172.24.49.142</td>
<td>0</td>
<td>0</td>
<td>ServerWLM</td>
</tr>
<tr>
<td>172.24.49.131</td>
<td>21</td>
<td>172.24.49.142</td>
<td>1</td>
<td>0</td>
<td>ServerWLM</td>
</tr>
</tbody>
</table>

**Using IP pacing to delay outbound data**

You can delay (or "pace") outbound data from any TCP/IP application. This function allows more processing time for business-critical applications, and you can display information about applications that have been paced.

Table 27 on page 91 describes the views that provide detailed information about IP pacing.

**Table 27: IP pacing views**

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPPACCFG</td>
<td>Displays the IP pacing configuration entries</td>
</tr>
<tr>
<td>IPPACSTA</td>
<td>Displays IP pacing statistics</td>
</tr>
</tbody>
</table>

**Adding a job name to the IP pacing configuration**

Use this procedure to add a job name to the IP pacing configuration. By adding the job name you can provide more processing time to business-critical applications.

**To add a job name to the IP pacing configuration**

1. From the EZIP menu select **Configuration** from the **IP Pacing** section, and press Enter.
The IP Pacing Configuration view (IPPACCFG) is displayed (Figure 33 on page 92).

Figure 33: IP Pacing Configuration view

<table>
<thead>
<tr>
<th>Cmd</th>
<th>Job</th>
<th>Pacing</th>
<th>Local Start Time</th>
<th>Stop Time</th>
<th>M-F</th>
<th>SAT</th>
<th>SUN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$DEFAULT</td>
<td>LOCAL 09:00</td>
<td>17:00</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FTP*</td>
<td>1200 LOCAL 09:00</td>
<td>17:00</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FTPJOBS</td>
<td>5000 LOCAL 09:00</td>
<td>17:00</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>JOBA*</td>
<td>2000 GMT 12:00</td>
<td>23:00</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PR*</td>
<td>1000 LOCAL 09:00</td>
<td>17:00</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RCHRWBX2</td>
<td>200 LOCAL 09:00</td>
<td>21:00</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RCHRWBX3</td>
<td>400 LOCAL 09:00</td>
<td>21:00</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RCHRWBX4</td>
<td>800 LOCAL 09:00</td>
<td>21:00</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RCHRWBX5</td>
<td>1000 LOCAL 09:00</td>
<td>21:00</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RCHRWBX6</td>
<td>10000 LOCAL 09:00</td>
<td>21:00</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2 In the **Cmd** field, type A.

3 Edit the fields in the **Add IP Pacing entry** pop-up window according to this list:

- **Job name** for the name of the job that you want to delay.
- **Pacing Time** for the type the amount of time (in hundredths of a second) that you want the job delayed.
- **Time Type** for Local time or GMT.
- **Start** for the time when you want the delay to start.
- **Stop** for the time when you want the delay to stop.
- **M-F, SAT, or SUN** to specify the days of the week that you want the job delayed.

**Tip**

First delete any characters that are not part of the job name you are adding.

4 Press **Enter**.

Deleting a job name from the IP pacing configuration

Use this procedure to delete a jobname from the IP pacing configuration.
To delete a jobname from the IP pacing configuration

1. From the EZIP menu, select **Configuration** from the IP Pacing section, and press **Enter**.

   The IP Pacing Configuration view (IPPACCFG) is displayed.

2. In the **command** field of the IP Pacing Configuration view (IPPACCFG), type **DEL** next to the job name that you want to remove from the list and press **Enter**.

Displaying IP pacing statistics in MainView IP

Use this procedure to display IP pacing statistics about a job name that has been configured to delay outbound data from a TCP/IP application.

To display IP pacing statistics

1. From the EZIP menu select **Statistics** from the IP Pacing section, and press **Enter**

   The IP Pacing Statistics view (IPPACSTA) is displayed, as shown in Figure 34 on page 93:

   ![Figure 34: IP pacing statistics view](image)

   10APR2003  15:55:43 ------ MAINVIEW WINDOW INTERFACE(V4.1.05)-------------------
COMMAND ===>                                                 SCROLL ===> PAGE
CURR WIN ===> 1        ALT WIN ===>
W1 =IPPACSTA========MCBESAM==*========10APR2003==15:55:43====MVIP=====D====5
Job      Sends  Total Wait  Sends
Name     Paced  Time (sec)  Skipped
RCHRWBX2    17           3        0
RCHRWBX3    17           6        0
RCHRWBX4    17          13        0
RCHRWBX5    17          17        0
RCHRWBX6    17         170        0

Using IP resource Hyperlinks

MainView for IP provides access to MainView for z/OS, MainView for UNIX System Services, MainView for VTAM, and MainView for WebSphere Application Server through hyperlinks. Hyperlinks are 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 alternative window.

For more information about hyperlinks, see the MainView User Guide.

Table 28 on page 94 shows where to find the hyperlink and describes the information that can be accessed when the hyperlink is activated:

**Table 28: IP resource links**

<table>
<thead>
<tr>
<th><strong>MainView for IP view</strong></th>
<th><strong>Field name</strong></th>
<th><strong>Resource link</strong></th>
<th><strong>Resource link description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CACHE</td>
<td>Web Server</td>
<td>MainView for WebSphere Application Server</td>
<td>Summary of WebSphere Application Server performance statistics</td>
</tr>
<tr>
<td></td>
<td>Stack CPU Resources</td>
<td>MainView for z/OS</td>
<td>Summary of CPU utilization statistics</td>
</tr>
<tr>
<td>STACKCPU</td>
<td>Stack Pag Resources</td>
<td>MainView for z/OS</td>
<td>Summary of paging statistics, including the number of pages per second</td>
</tr>
</tbody>
</table>

**Service levels view**

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 contains the following information:

- Services (and service levels) that users should expect
- Describes user responsibilities in addressing problems
- Defines problem-resolution paths

*Note*

To use the Service Level Agreement Policy view, you must be running the Policy Server (PAGENT).

Table 29 on page 95 describes the views that provide detailed information about your service levels.
Table 29: Service levels views

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
</table>
| CACHE | 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. This view helps you 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 (SLAP). The following are available in this view:  
  ■ Displays Fast Response Cache Accelerator statistics  
  ■ Provides information for web cache analysis  
  ■ Provides a hyperlink to MainView for WebSphere Application Server |
| SLAP | Displays SLA policy statistics |
| EZRESP | Provides menu access to response-time information, including subnet response time summary information |

Tools and menus in MainView for IP

The Tools and Menus section on the MainView for IP menus provides you with the following options:

- **Select View** displays a list of view names and descriptions of the views that are available in MainView for IP
- **Return** displays the previous view

Batch reports

You display the MainView Batch Reports panel to access the Batch Reports option. MainView can obtain historical performance reports through the submission of batch jobs.

An ISPF dialog panel will assist you in generating the JCL to produce MainView batch reports of your historical data.

For more information about setting up and using MainView Batch Reports, see the *MainView User Guide*. 

Chapter 3 Using the views of MainView for IP 95
**Historical data sets**

With Historical Data Sets, you can re-create the operating environment as it existed during a previous time period. This feature stores information about your operating environment at the end of each interval so that you can compare its current performance with a previous performance.

**Exiting MainView for IP**

Use the following procedure to exit MainView for IP.

**To return to the MainView Selection menu**

1. Issue one of the following commands on the COMMAND line field:
   - Quit
   - Return
Historical data display in MainView for IP

Mainview for IP enables you to view historical data. You can use historical data to look at system data as it existed an hour ago, yesterday, last week, last month, or last year.

Overview of the historical data display

You can use historical data to re-create the operating environment from a specific point in time, and compare the performance of the recreated environment to the performance of the current environment. This will enable you to determine whether there is a problem in your system.

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

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

Note

- For information about the historical database and how it operates in the MainView environment, see the MainView Administration Guide.
- For information about how to generate historical performance reports, see the MainView User Guide.
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

1. Type **DSLIST** on the COMMAND line.

2. Press **Enter**.

   The DLIST is displayed (Figure 35 on page 98).

**Figure 35: DLIST view**

<table>
<thead>
<tr>
<th>DDNAME</th>
<th>From Date</th>
<th>Time</th>
<th>To Date</th>
<th>Time</th>
<th>Rec Status</th>
<th>Pending</th>
<th>Data set name</th>
</tr>
</thead>
<tbody>
<tr>
<td>HISTDS00</td>
<td>14NOV2003</td>
<td>15:43</td>
<td>28NOV2003</td>
<td>15:16</td>
<td>Yes</td>
<td>Active</td>
<td>TAC22.SYSN.HIS</td>
</tr>
<tr>
<td>HISTDS02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>Closed</td>
<td>TAC22.SYSN.HIS</td>
</tr>
<tr>
<td>HISTDS01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TAC22.SYSN.HIS</td>
</tr>
</tbody>
</table>

**Note**

BMC recommends that you check DLIST 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** might 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

**Tip**

If you do not see the date or time that you want on the DLIST view, the information may have been archived on tape or in an offline data set, or may have been purged. If you need to determine whether the data was archived or purged, contact your product administrator (if you are the administrator, see the MainView Administration Guide).
TIME command in MainView for IP

You 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. If you need data that spans a greater time frame, 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 the *MainView User Guide*.

Viewing JOBNAME response times in MainView for IP

Use the following procedure to use the TIME command to view historical data for the TCPCONS Response Times view.

For instructions about specifying the time frame or on displaying the DSLIST, see the *MainView User Guide*.

**Before you begin**

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

- Specify the time frame 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.

**To view historical data**

1. Display the TCPCONS view.
2. Position the cursor where you want to split the screen.
3. On the command line, type `HS`, and press **Enter**.
The screen splits horizontally (Figure 36 on page 100). In the window information line, the current time is displayed as 15:23:33.

**Figure 36: TCPCONS with an open window**

4 Display TCPCONS in Window 2 by typing TCPCONS on the COMMAND line and pressing Enter.

5 On the COMMAND line, type TIME to set the time frame for Window 2.

The SET TIME FRAME dialog box is displayed (Figure 37 on page 100).

**Figure 37: SET TIME FRAME dialog**

6 Type 2D in the Requested Time Frame: Duration field to display the historical data for a two-day time frame.

7 To save your changes and return to the view, press F3.

The interval information is displayed in Window 2. You can customize the order in which the data is displayed by using the CUST command.
Example

In this example, the data is displayed by remote IP addresses in descending order (Figure 38 on page 101).

Figure 38: TCPCONS in two time frames

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 time frames displayed in the same screen, you can compare them to determine whether a 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.

8 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 until:

- You issue another TIME command
- The window is closed
- You press F3
Displaying Intvl Time field

Use the following procedure to determine the Interval time to be displayed.

**Before you begin**

Select one of the following methods to access the MainView Parameter Editors menu:

- 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.

**To display the Intvl Time field**

1. From the *MainView Parameter Editors Menu*, select option 2, *Display*.

2. Move the cursor to the *Show Time* field, and type Y.

3. To save your updates, press End.

4. To hide the field from views when you do not want it displayed, on the COMMAND line, type EXclude TIMe.

5. To redisplay the field, type INclude TIMe.

**Tip**

To see the date for which the data was gathered, use the INclude DATE command to reveal the *Intvl Date* field. This is useful if your time frame is more than 24-hours.

---

Moving between time frames in MainView for IP

Use the following procedure to move between time frames.

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. The NEXT and PREV parameters enable you to...
do this by using the duration that was last specified to move the time frame forward (NEXT) or backward (PREV) by the same amount.

To move between time frames

1. Split the screen horizontally by placing the cursor approximately halfway down the screen, type HS on the COMMAND line, and press Enter.

2. In Window 2, type JOBRSPZ on the COMMAND line and pressing Enter.

3. On the COMMAND line, type TIME = = PREV. Press Enter.

--- Note ---

Insert a space between each parameter.

--- Example ---

Figure 39 on page 103 is an example of the screen that is displayed. In this example, the current time was compared to a previous time.

Figure 39: Time frame menu

--- Note ---

You can compare two historical times and you can continue to type NEXT and PREV to move through different time frames, compare two historical times, and continue to type NEXT and PREV to move through different time frames.
You can define an F 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

Discrepancies may occur in the Time and Duration fields on the window information line 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.

Discrepancies occur because data is not always available for the intervals that you request. This might happen because the product address space (PAS) 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.

**Example**

At 9:00 A.M. you want to look at JOBRSPZ to determine the highest response times that occurred between 5:00 A.M. and 8:00 A.M. You display the JOBRSPZ view and type the following command:

**Figure 40: Time command**

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

**Figure 41: Time command example code**

```
>W1
-JOBRSPZ--------SJSC=====*======03FEB2010==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 example:

**Figure 42: Time command example code result**

```
>W1
-JOBRSPZ--------SJSC=====*======03FEB2010==7:15==115M====MVIP========59======
```

In our example, 7:15 A.M. was the last interval within the time frame 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 time frame that you requested).
MainView for IP alarm settings manager

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

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

MainView Alarm Manager

MainView for IP is a tool that, with other MainView products, notifies you when exception conditions occur. You can display a single view that shows exceptions for all MainView performance monitors within your MVS enterprise.

MainView Alarm Manager can monitor multiple systems simultaneously. 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 that produced the exception
- Trigger an automated alert or action from MainView AutoOPERATOR for quick problem resolution

MainView Alarm Manager will generate alarms when thresholds from specific MainView product views are exceeded. Alarms can be based on summarized data from multiple systems and subsystems that use the MainView 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 severity level, from informational to critical.
Threshold conditions are defined as one of the following priority levels:

- Information
- Warning
- Minor
- Major
- 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 the MainView User Guide. For more information about MainView Alarm Manager, see the MainView Alarm Management Guide.

**Setting alarms**

Use the following procedure to set alarms. The alarm that you set up by using the following tasks is triggered when the threshold value for the average response time on the JOBRSPZ view exceeds 50 or 75 milliseconds.

**To set alarms**

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.

2. In the MainView for IP monitor, issue the `tso isrddn` command and examine the BBVDEF concatenation.

   This information is required for Step 9.

3. Set an alarm threshold.

   The alarm threshold is set in the JOBRSPZ view.

4. In the MainView for IP monitor issue the **cust** command.

5. Enter `t` (for **threshold**) on the View Customization **COMMAND** line, and select the column where the threshold value should be set.
6 Set condition and attribute values.

**Example**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Attr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st =&gt; = 50 =&gt; 9 reverse red</td>
<td></td>
</tr>
<tr>
<td>2nd =&gt; &gt; 75 =&gt; 2 yellow</td>
<td></td>
</tr>
</tbody>
</table>

7 Check field entries.

Field entries that match threshold values are highlighted in the attribute color.

8 Press **F3** to display the Exit Views Customization panel.

9 Save changes to the Exit Views Customization panel.

To display the Exit Views Customization panel, press **F3**.

10 Copy the USER BBVDEF data set. When the new view is saved in USER BBVDEF, copy it into the GROUP BBVDEF data set.

11 Add the GROUP BBVDEF data set in front of BBVDEF concatenation.

You must add the data set to the MainView Alarm Manager PAS and the MainView for IP PAS.

12 Use the sample JCL in *HLQ.UBBSAMP(MVALPAS)* to start the MainView Alarm Manager PAS.

13 Perform a MainView for IP PAS recycle

**Note**

For more detailed information see the *MainView User Guide*

14 Issue the command **Setalarm 00** from the **COMMAND** line.

15 In the MainView Alarm Manager Easy Menu (MVALARM), select Current Alarms, and install and save the alarm.

16 Verify the installation of Alarm 00 by selecting **List Alarm Groups**.

**Note**

For more detailed information about all of these steps, see *MainView Alarm Management Guide*
Sample alarms shipped with MainView for IP

MainView for IP ships sample alarm definitions in {HLQBBACTDEF}.

The ALRMDIST view lists the sample alarm definitions, that can be installed by using an ADD line command. Table 30 on page 110 describes the sample alarms provided with MainView for IP. You can customize these sample alarms to meet your specific monitoring needs.

### Table 30: Sample alarms in MainView for IP

<table>
<thead>
<tr>
<th>Alarm name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMON</td>
<td>Availability monitoring for device</td>
</tr>
<tr>
<td>AMONAPPL</td>
<td>Availability monitoring for IP address and port number</td>
</tr>
<tr>
<td>AMONDEVS</td>
<td>Availability monitoring for DEVS</td>
</tr>
<tr>
<td>AORTT</td>
<td>Automated packet trace on high response times (RTT)</td>
</tr>
<tr>
<td>AODUPACK</td>
<td>Automated packet trace on duplicate ACKS (DUPACK)</td>
</tr>
<tr>
<td>AORXMIT</td>
<td>Automated packet trace on high retransmitted packets (REXMIT)</td>
</tr>
<tr>
<td>APING</td>
<td>Availability ping information</td>
</tr>
<tr>
<td>EEINACT</td>
<td>Enterprise Extender</td>
</tr>
<tr>
<td>JOBACKZ</td>
<td>Acknowledgements (ACKs) by jobname</td>
</tr>
<tr>
<td>JOBRETZ</td>
<td>Retransmits by jobname</td>
</tr>
<tr>
<td>OSAUTIL</td>
<td>OSA card utilization</td>
</tr>
<tr>
<td>TNCCONS</td>
<td>Connections</td>
</tr>
<tr>
<td>TNCONSAH</td>
<td>TN3270 RT is greater than 300 ms</td>
</tr>
</tbody>
</table>

Alarm definitions in MainView for IP

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
Operator commands in MainView for IP

This appendix describes the operator commands that you use to control the operation of MainView for IP.

Commands in MainView for IP

This topic provides descriptions of the following operator commands.

- **DUMP** - Dump for MainView for IP address and data space on page 113
- **OPTIONS** - Display MainView for IP options status on page 113

**DUMP - Dump for MainView for IP address and data space**

Use this command to create a dump of the MainView for IP address space and data space.

You can print the output, and send it to your BMC Software customer support representative. Additionally can provide a dump of the MainView for IP address space and data space, by issuing the command `/subsysid Dump` from the MVS console.

**OPTIONS - Display MainView for IP options status**

You can determine the status of the MainView for IP options by issuing the command `/subsysid OPTIONS` from the MVS console. `subsysid` is the four-character name established for the subsystem.
Figure 43 on page 114 is an example of the resulting display for subsystem MVIP. The term OPTIONS refers to startup parameters or operator commands. For a description of the startup parameters, see the MainView for IP Customization Guide.

Figure 43: MVIP options display
Troubleshooting MainView for IP

This appendix describes MainView for IP messages and actions you can take to troubleshoot the error described in the message.

This appendix covers the following information:

- Message format on page 115
- Contacting BMC Software customer support on page 116
- Gathering problem report documentation on page 117
- Selecting debug data collection points on page 119

Message format

This topic describes the format of the messages you will see in MainView for IP.

The following is an example of a BMC message:

--- Example
BMCnnnnnnX LOAD failed for module modulename
---

- All BMC Software messages begin with **BMC**.
- *nnnnn* is the BMC message number. This is a two to five digit number. You can look up additional information about the message on the BMC Documentation Center by searching for **BMCnnnnn**.
- X is the message severity code. **Table 31 on page 116** is a list of severity codes, their description, and required user action.
- The information following the message number and severity code describes the reason for the message.
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Action</td>
<td>Immediate action is required.</td>
</tr>
<tr>
<td>E</td>
<td>Error</td>
<td>The function that you requested was not completed. Action is required.</td>
</tr>
<tr>
<td>I</td>
<td>Information</td>
<td>This message is for information only. No action is required.</td>
</tr>
<tr>
<td>R</td>
<td>Reply</td>
<td>You must reply to the message before the system can continue.</td>
</tr>
<tr>
<td>S</td>
<td>Severe</td>
<td>A severe error occurred. Action is required.</td>
</tr>
<tr>
<td>W</td>
<td>Warning</td>
<td>The system is still operating and no immediate action is required, further investigation is needed.</td>
</tr>
</tbody>
</table>

**Note**

All messages with severity code E and some with severity code A or I are sent to the system console.

---

**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 have answers to some or, preferably, all of 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.

You can gather information about a problem by doing one of the following procedures:

- “To gather problem report documentation” on page 117
- “To use a TSO command line interface” on page 118
- “To run a sample batch job” on page 119

To gather problem report documentation

1. Enable the appropriate debug collection points by using the MVIPCONF view. For more information, see Selecting debug data collection points.

2. Re-create the problem.

3. Send the JES2 job log that contains the debugging information to your MainView for IP customer support representative.

4. Type the command MVIPDIAG at any MainView for IP screen, print the output, and send it to your MainView for IP customer support representative.

5. Type the command /mvip options on the console, print the output, and send it to your MainView for IP customer support representative.

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.

7. Check for log message IEA911 to confirm that the dump is a complete dump, not a partial dump.

8. Send the dump to your MainView for IP customer support representative by using one of the following methods:
   - Use the TRSMAIN command to compress the dump.
   - 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

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

**To use a TSO command line interface**

1. Use TSO to access FTP.BMC.COM.
2. At the prompt, enter ANONYMOUS as your ID.
3. Enter Your_Email@company.com as the password.
4. Enter CD incoming and then enter BINARY.
5. Enter PUT ‘MVS.DATASET.NAME.TRS’ cnnnnnn_dump1.trs.
6. Enter QUIT.

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

7. Notify your MainView for IP customer support representative that the dump has been uploaded.
To run a sample batch job

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
/*
```

2 Notify your MainView for IP customer support representative that the dump has been uploaded.

Selecting debug data collection points

Use the MVIP Parms Configuration view to enable debug data collection points.

MainView for IP dynamically allocates a data set to collect the debug data for each collection point you enable.

To select debug data collection points

1 From the EZIP menu, select **MVIP Parms** in the Utilities section, and then press **Enter**.

2 From the EZPARMS menu, select **MVIP Parms Configuration** in the Detail Views section, and then press **Enter**.

3 In the MVIPCONF panel select the system to configure, and press **Enter**.
The MVIP Parms Configuration (MVIPCNFD) panel is displayed.

**Figure 44: MVIP Parms Configuration (MVIPCNFD) panel**

4. In the Debug Settings section, type **ON** in the fields related to the areas that you want to debug.

**Table 32 on page 120** lists the fields in the Debug Settings section.

**Table 32: Debug Settings on the MVIPCONF view**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APing</td>
<td>Availability ping</td>
</tr>
<tr>
<td>Cach</td>
<td>WebSphere cache</td>
</tr>
<tr>
<td>Config</td>
<td>TCP/IP configuration</td>
</tr>
<tr>
<td>Connections</td>
<td>TCP/IP connections</td>
</tr>
<tr>
<td>Connection NMI</td>
<td>End of Connections</td>
</tr>
<tr>
<td>CSM Buffer</td>
<td>CSM Buffer</td>
</tr>
<tr>
<td>Devlinks</td>
<td>Network and OSA devices</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>EE</td>
<td>Enterprise Extender</td>
</tr>
<tr>
<td>FTP NMI</td>
<td>FTP Sessions/File Transfers</td>
</tr>
<tr>
<td>IDSS</td>
<td>Intrusion detection</td>
</tr>
<tr>
<td>IPSEC NMI</td>
<td>IPSec configuration and Statistics</td>
</tr>
<tr>
<td>Kill</td>
<td>Drop connection</td>
</tr>
<tr>
<td>EMCS</td>
<td>EMCS internal tracing</td>
</tr>
<tr>
<td>OSA</td>
<td>OSA</td>
</tr>
<tr>
<td>Ping</td>
<td>Ping IP address</td>
</tr>
<tr>
<td>Ports</td>
<td>Port definitions</td>
</tr>
<tr>
<td>Resolver</td>
<td>Name Resolver data</td>
</tr>
<tr>
<td>Routes</td>
<td>Network routes</td>
</tr>
<tr>
<td>RTP</td>
<td>RTP</td>
</tr>
<tr>
<td>SLAP</td>
<td>Service Level Policy</td>
</tr>
<tr>
<td>SMC-R</td>
<td>SMC-R data</td>
</tr>
<tr>
<td>SNMP API</td>
<td>SNMP API tracing</td>
</tr>
<tr>
<td>Stack Stats</td>
<td>TCP/IP Stack Statistics</td>
</tr>
<tr>
<td>SAW Data</td>
<td>VTAM Sessions SAW data</td>
</tr>
<tr>
<td>Sysplex XCF</td>
<td>Sysplex XCF data</td>
</tr>
<tr>
<td>TnMonitoring</td>
<td>TN3270 performance monitoring</td>
</tr>
<tr>
<td>TraceRoute</td>
<td>TraceRoute IP address</td>
</tr>
<tr>
<td>TTLS Connections</td>
<td>AT-TLS connections</td>
</tr>
<tr>
<td>VIPA</td>
<td>DVIPA Configuration and Connections</td>
</tr>
<tr>
<td>VTAM PPO</td>
<td>VTAM PPO messages</td>
</tr>
<tr>
<td>EMCS console</td>
<td>EMCS console messages</td>
</tr>
</tbody>
</table>
Index

{Common Storage Area.}  See: CSA
{coordinating address space.}  See: CAS
{prepackaged alarms.}  See: sample alarms
{product:address space.}  See: PAS
{resource links.}  See: hyperlinks
{VIPA (Virtual IP Address).}  See: DVIPA
{write-to-operator.}  See: WTO

32 bits 26

A
abend 66, 71
accessing information
  socket trace 88
ACTCONS view 38, 39
add command
  availability ping 34
  domain name 36
Alarm Manager, MainView 107
Alias Target 23
ALLCONS view 38
applications
  connections 38
APPN 52
availability monitoring
  configuration 30
  description 29
  view 31
availability ping
  add command 34
  add domain name 36
  starting 34
availability, historical data 98

B
batch jobs, sample 117
batch reports 95
BBSAMP members
  MVALPAS 108
  TACSNMP 56
BBVDEF data sets 108

C
CAS (coordinating address space) 17
changing SNMP parameters 56
CLSxRESP views 37
commands
  adding IP address availability ping 34
  deleting packet trace 82
  deleting socket trace 88
  devices, ping 42
  displaying socket trace 86
  filtering socket trace 87
  MVIP DIAG 117
  NEXTE 83
  PREVE 83
  setalarm 108
  socket trace 86
  starting availability ping 34
  starting socket trace 83
  TIME 96
  TRSMAIN 117
tso isrddn 108
writing packet trace 76
writing RAW packet trace 73
writing Sniffer packet trace 74
writing socket trace 85
community name, SNMPDEF 57
compressed
IPv6 26
conventions, documentation 10

D
data set members
   MVALPAS 108
data sets
   BBVDEF 108
   FB(80) 76, 85
data sets, writing packet trace 76
debugging 66
delete command
   packet trace 82
   socket trace 88
devices
   performing Traceroutes 44
   stopping packet traces 77
display command
   socket trace 86
displaying IPv6 addresses 27
documentation information 9
DSLST, list historical data 98
dumps
   compress 117
   sending 117

E
EE RTP Info 53
EE RTP information 52
EE UDP Traffic 53
EE view 52
EEDIAG view 55
electronic documentation 9
electronic documentation, online Help 17
Enterprise Extender 55
EZ menus
   EZIP Menu 17

F
FB(80), data sets 76, 85
filter command, socket trace 87
FTP (File Transfer Protocol)
   sending dumps 117

H
Help
   online 9
Help key 17
HiperSockets 57
historical data
   displaying Intvl Time field 102
   how to generate performance reports 97
   reasons for unavailability 98
   reports 97
   sets 96
   window status indicator 99
hyperlinks
   activating 94

I
interfaces 57
IP (Internet Protocol) 27
   displaying pacing statistics 93
IP address
   compressed form 27
IPACKZ view 47
IPRETZ view 47
IPv6
   compressed form 26
   displaying addresses 27
   hexadecimal number 26

J
JOBACKZ view 47
JOBRETZ view 47

L
line command
   ping 67
      TR (traceroute) 69
list, historical data 98
loopback 57
LSTCONS, connection views 38
M
managing views 20
measured response times 37
menus
    and tools 95
    EZIP Menu 17
    overview 19
Monitor and Auto Activate VTAM Resources 50
mv 25, 97
MVALPAS data set member 108
mvip 115
M VIP DIAG command 117

N
Name Resolver using NMI 65
navigation 20
NEXTE command 83

O
online Help 9, 17
option, select view 25
OSA (Open Systems Adapter) 57, 91

P
pacing statistics, displaying 93
Packet Trace
    writing to data set 74
packet traces, deleting 82
packet tracing
    drill-down function 79
    limiting trace parameters 71, 73, 74, 83
    PKTTRACd view 79, 80, 83, 88
    PKTTRACF view 78
    PKTTRACH view 81
    PKTTRACS view 71, 73, 74, 76, 83, 85, 87
    writing data set 76
parameters
    default 33, 36
    historical data 99
    Session Control Parameters panel 17
PAS (product address space) 66
PCONS view 53, 67
ping
    information view 53, 67
    view, PING 31, 42
PKTTRACd view 79, 80, 83, 88
PKTTRACF view 78, 86
PKTTRACH view 81
PKTTRACS view 71, 73, 74, 76, 83, 85, 87
PORTACKZ view 47
PORTRETZ view 47
PREVE, command 83
primary menu 17
protocols
    FTP 117
    UDP 51
publications, related 9
PUNAME 53

R
RAW Packet Trace
    USERID 73
data sets 73
    writing to data set 73
related publications 9
reports
    historical performance 97
    how to generate historical 97
response times
    measured 37
    statistics 37
 Restarting VTAM Resources 33
RTPS view 52
RTPSd view 52

S
sample batch job 117
scenario, time frames 102
Selection Menu, MainView 17
sequential data set FB(80) 76, 85
Session Control Parameters panel 17
setalarm command 108
Shared Memory 61
SKTTTRACF view 66
Sniffer Packet Trace
    USERID 74
data sets 74
SNMP (Simple Network Management Protocol) 56
SNMPDEF community name 57
SNMPDEF view 56
socket traces
  USERID 85
  accessing information 88
  deleting 88
  displaying 86
  filtering 87
  starting 83
  stopping 86
  writing to data set 85
SSID (subsystem ID), session parameters 17
start command
  availability ping 34
  socket trace 83
stop command
  socket trace 86
storage
  view 60
summary response-time statistics 37
summary throughput 37
syntax statement conventions 10

T
TACFTPU view 61
TCONS view 34, 69
TCPCONS view 38, 39
terminating connections 40
TIME command
  NEXT and PREV parameters 102
  overview 97
time frames, moving between 102
TNCONS view 38, 39
TRACE view 44
TRACEDET view 71
traceroute
  Information view 34, 69
Traffic Response Times Views 37
TRSMAIN command 117
TSO command line 117
tso isrddn command 108

U
UDPCONS view 38
USERID
  RAW Packet Trace 73
  Sniffer Packet Trace 74
  socket traces 85

V
views
  drilling down 71, 80, 81
  LSTCONS 38
  option 25
  PCONS 30, 31, 53, 67
  PING 31, 42
  PKTTRACd 79, 80, 83, 88
  PKTTRACH 81
  PKTTRACS 71, 73, 74, 76, 83, 85, 87
  SKTTRACF 66
  SNMPDEF 56
  storage 60
  TACFTPU 61
  TCONS 34, 69
  TRACE 44
  TRACEDET 71
  traffic response times 37
VTAM resources 33
VTAM Resources views 49

W
write command
  packet trace 76
  RAW packet trace 73
  Sniffer packet trace 74
  socket trace 85
WTO (write-to-operator) 40