MainView for IP Customization Guide

Supporting

Version 3.5.00 of MainView for IP

May 2016
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  Fax 1 713 918 8000
or
1 800 841 2031

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.

IBM, IBM z, MVS, RACF, S/390, System z, VTAM, WebSphere, and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

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 UNPUBLISHED—RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES.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. 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.

About this book .......................... 7
Related publications ......................................................... 7
Conventions ......................................................... 8
Syntax statements ......................................................... 8

Chapter 1    Installation overview .......................... 11
MainView for IP installation requirements ...................... 11
  System requirements for MainView for IP ........................................ 11
  OSA requirements for MainView for IP ........................................ 12
  Network management interface requirements ........................ 12
  Packet Trace Requirements of MainView for IP ................................ 12
  RACF requirements of MainView for IP ........................................ 14
  SNMP Manager API .................................................................. 15
Product authorization ........................................................... 15

Chapter 2    Customizing z/OS services ...................... 17
Customizing z/OS services for OSA data collection in MainView for IP .......................... 17
Customizing z/OS services for IBM data collection in MainView for IP .......................... 18
  Managing the IBM SNA NMI ............................................... 18
  Managing the IBM TCP IP NMI ............................................ 20
  Managing the IPSec network management interface ..................... 23
  Managing the VTAM SAW (session awareness) interface ................ 25
  Managing the VTAM PPO interface ....................................... 27
  Managing TN3270 response time data collection ....................... 28
  Suppressing output from the EMCS console ............................ 30

Chapter 3    Configuring MainView for IP .................. 33
Selecting history data to collect in MainView for IP ...................... 33
  History interval values ......................................................... 34
Controlling SNMP and OSA data collection in MainView for IP .......................... 36
Configuring the availability ping in MainView for IP ...................... 37
Automating Packet Trace ....................................................... 38
Defining Packet Trace table options in MainView for IP ...................... 39
Saving packet trace data upon recycle of MainView for IP PAS ...................... 39
Defining Socket Trace table options in MainView for IP ...................... 40
Configuring TN3270 network and host response time collection in MainView for IP ................................................................. 41
Configuring domain name resolution in MainView for IP ........................................ 41
Configuring the IPv6 short form display format in MainView for IP ........................ 42
Configuring IP pacing in MainView for IP ................................................................. 43
Configuring MainView for IP for zIIP exploitation .................................................. 43
Configuring IBM data collection in MainView for IP .............................................. 44
  Controlling the MainView for IP NMI ................................................................. 44
  Filtering the end-of-connection data in MainView for IP .................................... 45
  Configuring IPSec Filter logging ........................................................................ 47
Controlling VTAM SAW data collection in MainView for IP ................................ 49
  Filtering the VTAM SAW data collection in MainView for IP .............................. 50
  Controlling VTAM PIU trace data collection in MainView for IP .......................... 52
Using SAWFILTR view for PIU trace filtering ...................................................... 53
  Controlling VTAM message collection in MainView for IP ................................ 54
  Filtering VTAM message collection in MainView for IP ..................................... 56

Appendix A  Configuration settings ........................................... 59
Debug settings in MainView for IP ........................................................................... 59
History settings in MainView for IP ......................................................................... 59
Data collection settings in MainView for IP .............................................................. 66
Trace settings in MainView for IP ............................................................................ 67
  Pkttrace Wrap - Enable disable wrapping in MainView for IP ............................ 67
  Pkttrace DS Size definition in MainView for IP .................................................. 67
  Sktttrace wrap - Enable disable in MainView for IP .......................................... 68
  Sktttrace DS Size - Specify size of socket trace table in MainView for IP ............ 68
IPSec filtering logging settings ................................................................................. 68
Additional settings .................................................................................................. 69
  EMCS Timeout in MainView for IP ................................................................. 70
  IPv6 address short format in MainView for IP .................................................. 70

Appendix B  NMI settings ........................................................... 73
NMI settings in MainView for IP .............................................................................. 73
  End-of-Connection NMI table in MainView for IP ............................................. 74
VTAM SAW settings in MainView for IP ................................................................. 75
VTAM PIU trace settings in MainView for IP .......................................................... 77
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 or value. If a variable is represented by two or more words, initial capitals distinguish the second and subsequent words.</td>
<td>alias probes databaseDirectory serverHostName</td>
</tr>
<tr>
<td>Brackets indicate optional items. Do not type the brackets when you enter the option. A comma means that you can choose one or more of the listed options. You must use a comma to separate the options if you choose more than one option.</td>
<td><code>[tableName, columnName, field] [-full, -incremental, -level]</code></td>
</tr>
<tr>
<td>Braces indicate that at least one of the enclosed items is required. Do not type the braces when you enter the item.</td>
<td>`{DBDName</td>
</tr>
<tr>
<td>UNLOAD device={disk</td>
<td>tape, fileName</td>
</tr>
<tr>
<td>A vertical bar means that you can choose only one of the listed items. 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 many times as necessary.</td>
<td><code>columnName...</code></td>
</tr>
</tbody>
</table>
Installation overview

This chapter explains how to prepare for installing the MainView for IP product.

You use the Installation System from BMC to install and customize MainView for IP. The Installation System provides a consistent distribution, installation, customization, and maintenance process for integrated BMC products that execute on the IBM z/OS platform.

**Note**
MainView for IP can monitor several Internet Protocol (IP) stacks simultaneously. If your data center runs MainView for IP on an MVS system with multiple IP stacks, no installation or configuration steps are required other than those provided by the BMC Installation system.

MainView for IP installation requirements

This topic describes the system, network, and security product prerequisites.

System requirements for MainView for IP

The following system prerequisites are required for MainView for IP:

- MainView Infrastructure PAS
- z/OS 1.13 or later
- IBM TCP/IP stack

**Note**
Other TCP/IP stacks are not supported.
For more information about prerequisites, including FMIDs and target libraries that you need for the installation, see the *Installation System Reference Manual* and the MainView for IP release notes.

**OSA requirements for MainView for IP**

Before you can use the Open Systems Adapter (OSA) views, ensure that you have completed the required customization tasks.

*Related Information*

- "Customizing z/OS services" on page 17

**Network management interface requirements**

MainView for IP uses the IBM Network Management Interface (NMI) to collect data. After completing the required customization tasks, you can use network management interfaces to view any data that MainView for IP collects.

*Related Information*

- "Customizing z/OS services" on page 17

**Packet Trace Requirements of MainView for IP**

Packet Trace uses the IBM NMI which requires SAF resources to be authorized. The following topics describe the necessary requirements to perform packet traces.

**RACF resources for Packet Trace**

MainView for IP uses the NMI real time Packet Trace callable service (EZBRCIFR) for z/OS 2.1 and later. The NMI interface requires SAF resources be authorized to control application access using the NMI to gather real-time packets.

READ access must be given to the User ID associated with the MainView for IP PAS for the resources defined in the SERVAUTH class

The following SAF resource profiles require authorization:
- EZB.TRCCTL.sysname.tcpame.OPEN
- EZB.TRCCTL.sysame.tcpname.PKTTRACE
- EZB.TRCSEC.sysame.tcpname.IPSEC (only for IPSEC encrypted connections)

The resources are defined in the SERVAUTH class. You are required to have READ access associated with the MainView for IP PAS.

**Note**

If profiles protecting these resources are not defined, MainView for IP will not be authorized to start a packet trace.

## Dataset Allocation

You must pre-allocate the data sets used to save packet trace data.

Table 1 on page 13 lists the data set attributes needed to pre-allocate the data set for the following types of traces:

- RAW packet trace
- WRITE packet trace for a formatted file
- SNIFTER packet trace

### Table 1: Packet trace data set attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>RAW</th>
<th>WRITE</th>
<th>SNIFTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>PS</td>
<td>PS</td>
<td>PS</td>
</tr>
<tr>
<td>Record Format</td>
<td>VB</td>
<td>FB</td>
<td>VB</td>
</tr>
<tr>
<td>Record Length</td>
<td>32756</td>
<td>80</td>
<td>1600</td>
</tr>
<tr>
<td>Block Size</td>
<td>32760</td>
<td>6160</td>
<td>27998</td>
</tr>
</tbody>
</table>

To save packet traces upon recycle of the MainView for IPPAS, pre-allocate a data set with the following attributes:

- Organization: PS
- Record Format: VB
- Record Length: 27998
- Block Size: 32760
For more information, see the topics on saving packet trace data in the MainView for IP Customization Guide.

**RACF requirements of MainView for IP**

The z/OS eNetwork Communications Server IP environment requires a security product such as the IBM Resource Access Control Facility (RACF).

The MainView for IP PAS can issue VTAM and TCPIP commands as well as is authorized to issue these commands. The user associated with the MainView for IP PAS must be authorized for the following RACF profiles under the OPERCMDS class:

- MVS.VARY.TCPIP
- MVS.VARY.NET

Any actions issued on the VTAM Resources views will require authority to the MVS.VARY.NET RACF profile. Any dynamic changes to fields on the TCPIP configuration views will use the V TCPIP,TCPIP,OBEFYILE command and will require authorization to the MVS.VARY.TCPIP profile.

Each unit of work in the system that requires UNIX System Services (USS) must be associated with a UNIX System Services identity. A valid identity refers to the presence of:

- A valid UNIX user ID (UID),
- A valid UNIX group ID (GID)
- A valid HOME directory for the user

The UID and the GID are defined through the OMVS segment, in the RACF profile, and in the RACF group profile.

For more information about RACF, see the IBM IP Planning and Migration Guide.

**WARNING**

If the Started Task is not defined to a user ID that has a defined OMVS segment, error messages might be issued. If the HOME directory is not specified for the user ID, the socket call might fail.
SNMP Manager API

The SNMP Manager API is used to collect both SNMP MIBs and OSA MIBs. The SNMP Manager API requires an SNMP Manager API configuration file only if using SNMPv3.

The configuration file must be a z/OS UNIX file. It is defined on the MVIPCNFD view.

Note
For users not using SNMPv3, SNMP and OSA, the data collection will be done without any configuration files. Also, the configuration file is documented in Chapter 5 of the IP Programmer's Guide and Reference.

The MainView for IP PAS will require the hlq.TOSZLINK dataset in STEPLIB along with the hlq.BBLINK dataset. The SYS1.SIEALNKE file must reside in the LNKLIST as well.

Product authorization

Before using MainView for IP, you must perform product authorization.

You can use the BMC Product Authorization utility to authorize your copy of MainView for IP. For more information see the Installation System Reference Manual.

Note
If you are upgrading the product from a earlier version, you can copy the password in load module BFXTBL3P to your new load library.
Customizing z/OS services

This chapter provides information about customizing the IBM z/OS services for the MainView for IP product.

Customizing z/OS services for OSA data collection in MainView for IP

You can enable data collection for the Open Systems Adapter (OSA) views by configuring the OSA support and setting up the SNMP TCP/IP subagent.

**Note**

You must configure your `SNMPD.CONF` or `PW.SRC` file so that the SNMP agent can accept requests from IP address 127.0.0.1 (Loopback). MainView for IP sends requests from IP address 127.0.0.1 to collect OSA statistics through SNMP. For more information about configuring the SNMP agent, see the *IBM z/OS Communications Server: IP Configuration Guide*.

When you use OSA-Express Direct Support, the IOBSNMP address space is required to run with OSNMPD.

You complete the following tasks to configure the OSA data collection service:

1. Configure the OSA support as instructed in the *IBM z/OS Communications Server: IP Configuration Guide*.

2. Set up the SNMP TCP/IP subagent as instructed in the *IBM S/390: OSA-Express Customer’s Guide and Reference*. 
Customizing z/OS services for IBM data collection in MainView for IP

MainView for IP collects data on your system by accessing the IBM network management interface (NMI).

MainView for IP collects data from the following IBM NMIs:

- IBM SNA NMI to provide Enterprise Extender and HPR RTP data
- IBM TCP/IP NMI to provide FTP and connections data
- IBM IPSEC NMI to provide IP filters for each TCP/IP stack and summary statistics for IKE, IPsec, and IP Filtering

MainView for IP collects session awareness data on your system by accessing the IBM VTAM ISTPDCLU interface (IBM VTAM SAW).

MainView for IP collects VTAM messages on your system by accessing the IBM Primary Program Operator (PPO) Interface (IBM VTAM PPO).

---

**Related Information**

- “Managing the IBM SNA NMI” on page 18
- “Managing the IBM TCP/IP NMI” on page 20
- “Managing the IPSec network management interface” on page 23
- “Managing the VTAM SAW (session awareness) interface” on page 25
- “Managing the VTAM PPO interface” on page 27
- “Managing TN3270 response time data collection” on page 28

---

**Managing the IBM SNA NMI**

The IBM SNA NMI gathers the following data:

- EE connections and performance data
- High Performance Routing (HPR) Rapid Transfer Protocol (RTP) connections
Enabling the IBM SNA NMI

Use the following procedure to enable the IBM SNA network interface.

To enable the IBM SNA NMI

1. Access the VTAM start options list and set the SNAMGMT option to **YES** and the HPR option to **YES** or **RTP**.

2. Set security access to the SNA NMI levels for the MainView for IP PAS by using one of the following methods:
   - Assign superuser status to the user who is associated with the MainView for IP PAS.
   - Add a RACF resource in the SERVAUTH class as follows:
     ```
     IST.NETMGMT.sysName.SNAMGMT
     ```
     The variable `sysName` is the name of the MVS system on which the PAS is running.

3. Define an OMVS segment for VTAM.

4. Give the VTAM OMVS user ID write access to the /var directory.

Disabling the IBM SNA network management interface

Use the following procedure to disable the IBM SNA network management interface.

To disable the IBM SNA NMI

1. Access the VTAM start options list and set the SNAMGMT option to **NO**.

---

*Note*

For more information, see the *IBM zOS Communication Server: IP Programmer's Guide and Reference*.
Displaying the current setting of the SNAMGMT option

Use the following procedure to display the current setting of the SNAMGMT option.

To display the current setting of the SNAMGMT option

1. Use the following command to display the current setting of the SNAMGMT option.
   
   ```shell
   DISPLAY vtamProcName,VTAMOPTS,OPTION=SNAMGMT
   ```

   The variable `vtamProcName` represents the job name that is associated with the VTAM started task procedure.

   **Note**
   For more information, see the *IBM z/OS Communication Server: IP Programmer's Guide and Reference.*

Managing the IBM TCP IP NMI

MainView for IP uses the SYSTCPSM and SYSTCPCN NMI to gather the following data:

- FTP Data (SYSTCPSM Interface)
- End of Connections Data (SYSTCPCN Interface)

You can manage the TCP/IP NMI by enabling it, adjusting the connection lifetime, or disabling the interface.

**Related Information**

- “Customizing z/OS services for IBM data collection in MainView for IP” on page 18
- “Enabling the IBM TCP IP NMI” on page 21
- “Adjusting the TCP IP minimum connection lifetime” on page 22
- “Disabling the IBM TCP IP NMI” on page 23
Enabling the IBM TCP IP NMI

Use the following procedure to edit the NETMONITOR statement in the TCP/IP profile data set to enable data collection from the IBM TCP/IP NMI.

To enable the IBM TCP/IP NMI

1 Include the ON parameter on the NETMONITOR statement in the TCP/IP profile data set.

Note

After enabling the IBM TCP/IP interface this way, all interfaces (such as the SYSTCPSPM and SYSTCPCN interfaces) are enabled and all options specific to an interface are set to their defaults.

For more information about the NETMONITOR statement, see the IBM z/OS Communications Server: IP Configuration Reference.

To collect FTP data from the SYSTCPSPM interface

1 Include one of the following parameters on the NETMONITOR statement in the TCP/IP profile data set:

   - SMFSERVICE to enable the SYSTCPSPM interface
   - ON to enable all interfaces

If either the NOSMFSERVICE or the OFF parameter is specified on the NETMONITOR statement, the connection from the MainView for IP PAS to the SYSTCPSPM NMI fails, and no FTP data is collected.

To collect connections data from the SYSTCPCN interface

1 Include one of the following parameters on the NETMONITOR statement in the TCP/IP profile data set:

   - TCPCONNSERVICE to enable the SYSTCPCN interface
   - ON to enable all interfaces

If either the NOTCPCONNSERVICE or the OFF parameter is specified on the NETMONITOR statement, the connection from the MainView for IP PAS to the SYSTCPCN NMI fails, and the associated connections data is not collected.

To enable security

1 Perform one of the following tasks:
Make the user ID that is associated with the MainView for IP PAS a superuser

Add a RACF resource in the SERVAUTH class as follows:

```
EZB.NETMGMT.sysname.tcpprocname.SYSTCPCN
EZB.NETMGMT.sysname.tcpprocname.SYSTCPSM
```

where:

- **sysname**
  
  Name of the MVS system on which the PAS is running

- **tcpprocname**
  
  Job name associated with the TCP/IP started task procedure

**Related Information**

- “Managing the IBM TCP IP NMI” on page 20

---

**Adjusting the TCP IP minimum connection lifetime**

Use the following procedure to adjust the number of seconds a connection must remain active before it is reported by the SYSTCPCN network management interface.

**To adjust the TCP/IP minimum connection lifetime**

This procedure uses the MINLIFETIME option of the TCPCONNSERVICE parameter

1. On the NETMONITOR statement in the TCP/IP profile data set, change the value of the MINLIFETIME option of the TCPCONNSERVICE parameter.

   The default value, 3 seconds, applies if you do not specify a value for MINLIFETIME.

**Example**

Specify MINLIFETIME=10 if you want the interface to report only connections that last longer than 10 seconds.

**WARNING**

MINLIFETIME=0 reports all connections, which could significantly increase overhead and storage used by the MainView for IP PAS.
Disabling the IBM TCP/IP NMI

Use the following procedure to disable data collection from the IBM TCP/IP NMI.

To disable the IBM TCP/IP NMI

1. On the NETMONITOR statement in the TCP/IP profile data set, specify one or more of the parameters shown in Table 2 on page 23.

Table 2: NETMONITOR parameters for disabling the IBM TCP/IP NMI

<table>
<thead>
<tr>
<th>To disable</th>
<th>Use the parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection of FTP data and connections data</td>
<td>OFF</td>
</tr>
<tr>
<td>(which disables all interfaces such as SYSTCPSM and SYSTCPCN)</td>
<td></td>
</tr>
<tr>
<td>Collection of FTP data</td>
<td>NOSMPFSERVICE</td>
</tr>
<tr>
<td>Collection of connections data</td>
<td>NOTCPCONNSERVICE</td>
</tr>
</tbody>
</table>

Managing the IPSec network management interface

MainView for IP uses the IPSEC network management interface to gather the following data:

- IPSec filtering rules for each TCP/IP stack
Summary statistics for IKE, IPSec, and IP Filtering

**WARNING**

Turn on the PCONFIG IPSECURITY configuration in the TCP/IP profile data set only if you are implementing IP Security (IPSEC) on your TCP/IP stack.

An active IP security policy is required to enable a z/OS system to classify any IP packet that comes across a network interface. In addition, the z/OS system will then allow specific action according to the defined filtering rules. The filter rule can be used to filter out unwanted packets.

**Note**

For more information about configuring IP security, see the *IBM z/OS Communications Server: IP Configuration Guide*.

**Related Information**

- “Customizing z/OS services for IBM data collection in MainView for IP” on page 18
- “Enabling the IPSec NMI” on page 24

## Enabling the IPSec NMI

Use the following procedure to enable the IPSec network management interface.

**Note**

If the IKE Daemon (IKED) address space is not active, the NMI will not connect and will fail with `RC =468 RSN=120D0253`.

**To enable the IPSec NMI**

1. You can enable security by using one of the following methods:
   - Assign superuser status to the user who is associated with the Mainview for IP PAS.
   - Add a RACF resource in the SERVAUTH class as follows:
     ```plaintext
     EZB.NETMGMT.sysName.tcpProcName.IPSEC.DISPLAY
     ```
     The variable *sysName* is the name of the MVS system on which the PAS is running.
Managing the VTAM SAW (session awareness) interface

MainView for IP uses the IBM VTAM SAW interface (CNMI application) to collect session awareness data by connecting to the ISTPDCLU VTAM application.

The VTAM session data is stored in a MainView for IP data space and then written to history files at each defined interval. MainView for IP displays both real-time and historical data for any VTAM session for the LPAR where the MainView for IP PAS runs.

You can collect session awareness data by defining a VTAM application, so that MainView for IP can open an access control block (ACB) and acquire a session with the ISTPDCLU application. The default name of the ACB is MVIPCNMA. You can specify the name of the ACB on the MainView for IP Saw Configuration view (MVIPSAWD).

**Note**
The ISTPDCLU VTAM application has a session limit of 1 for the SAW data session. Only one product’s VTAM application at a time can acquire a session with the ISTPDCLU application on each LPAR.

The MVIPSAWD view displays the current status of the ACB. If MainView for IP is connected to the ISTPDCLU application and is collecting data, the status Open/Active is displayed on the view. Also, MainView for IP writes the following message to the MainView for IP PAS job log:

```
BMC257017I MAINVIEW/IP SAW interface connected to ISTPDCLU, VTAM session data will be collected.
```

Related information:

- [Customizing z/OS services for OSA data collection in MainView for IP on page 17](#)
- [Enabling VTAM SAW data collection and VTAM PIU tracing on page 26](#)
- [Filtering VTAM SAW data that is passed to MainView for IP on page 26](#)
- [Customizing z/OS services for IBM data collection in MainView for IP on page 18](#)
- [Customizing z/OS services on page 17](#)
Enabling VTAM SAW data collection and VTAM PIU tracing

Use the following procedure to enable VTAM session awareness data collection and VTAM PIU Tracing.

**To enable VTAM SAW data collection and VTAM PIU tracing**

1. Add VTAM definition to the VTAMLST as follows:
   ```
   VBUILD TYPE=APPL
   MVIPCNMA APPL AUTH=(CNM,VPACE,SPO,ACQ),EAS=2,PARSESS=YES
   ```

2. Activate the VTAM application by issuing the following command:
   ```
   V NET,ACT,ID=MVIPCNMA,ALL
   ```

3. *(optional)* Specify the ACB name by using the MVIPSAWD view.

   **Note**
   
   For more information about configuring VTAM session data collection and PIU tracing, see the topics about configuration settings in MainView for IP.

**Related information:**

- Managing the VTAM SAW (session awareness) interface on page 25

Filtering VTAM SAW data that is passed to MainView for IP

The default VTAM SAW data filter allows all data for all sessions to pass through the VTAM SAW interface.
To filter VTAM SAW data that is passed to MainView for IP

The default filter is defined in the ISTMGC10 member in the VTAMLIB data set.

1 Use the KEEPMEM, KCLASS and MAPSESS macros to define a VTAM SAW data filter.

--- Note ---
For more information, see the IBM Communications Server SNA Network Implementation Guide.

--- Related Information ---
- “Managing the VTAM SAW (session awareness) interface” on page 25

Managing the VTAM PPO interface

MainView for IP uses the IBM VTAM PPO interface to collect all VTAM messages.

The VTAM messages can be stored in a MainView for IP data space and then written to history files at each defined interval. The messages can also be written to the system console.

MainView for IP can display the real-time VTAM messages and also historical data for VTAM messages for the LPAR where the MainView for IP PAS runs.

You can activate the VTAM application by issuing the following command:

```
V NET,ACT,ID=MVIPPPOA,all
```

You can collect VTAM messages by defining a VTAM application, so that MainView for IP can open an access control block (ACB) and establish a session with VTAM as a VTAM PPO Application. The default name of the ACB is MVIPPPOA. You can specify the name of the ACB on the MainView for IP VTAM PPO Configuration view (MVIPPPOD).

--- Note ---
Only one application at a time can be a primary operator using the VTAM PPO interface.

The MVIPPPOD view displays the current status of the ACB. If MainView for IP is Active as the VTAM PPO application and receiving VTAM messages, the status
Open/ Active is displayed on the view. Also, MainView for IP writes the following message to the MainView for IP PAS job log:

```
BMC257214I MAINVIEW/IP PPO interface active, all VTAM messages will be sent to MVIP PPO ACB
```

**Related Information**

- “Customizing z/OS services for IBM data collection in MainView for IP” on page 18
- “Enabling the VTAM PPO interface” on page 28

---

## Enabling the VTAM PPO interface

Use the following procedure to enable the PPO interface.

**To enable the VTAM PPO interface**

1. Add VTAM definition to the VTAMLST as follows:

   ```
   VBUILD TYPE=APPL
   MVIPPOA APPL AUTH=PPO
   ```

2. (optional) Specify the ACB name by using the MVIPPOD view.

   **Note**
   
   For more information about configuring VTAM PPO interface data collection, see the topics about configuration settings in MainView for IP.

   **Related Information**

   - “Managing the VTAM PPO interface” on page 27

---

## Managing TN3270 response time data collection

MainView for IP can optionally use the IBM network management interface to collect TN3270 response time data.

**Note**

Mainview for IP is already configured to collect TN3270 response time data if you have enabled **TN3270 Resp Times** on the MVIPCNFD view.
The TN3270 response time data that is collected by the Telnet Server includes response time statistics, IP and SNA response times for a TN3270 connection, and response time counts by time bucket. The response time statistics include life-of-connection response time averages and sliding-window response time averages.

MainView for IP displays the monitor groups that are defined in the Telnet Server Profile data set on the TNMONGR view. The response time statistics are displayed on the TNPREF view. IP and SNA response times are also displayed on the TNCONS view.

Related Information

- “Customizing z/OS services for IBM data collection in MainView for IP” on page 18
- “Enabling TN3270 response time data collection” on page 29
- “Viewing TN3270 monitor groups” on page 30

Enabling TN3270 response time data collection

Use the following procedure to enable TN3270 response time data collection.

Note

For more information, see the IBM z/OS Communications Server: IP Configuration Reference.

To enable TN3270 response time data collection

1. In the BEGINVTAM section of the Telnet Server Profile data sets, add MONITORGROUP statements to define the data collection options.

   Options for the MONITORGROUP statement include the inclusion and exclusion of averages, counts by time bucket, and whether the IP network should be included in measurements.

2. In the same section, add MONITORMAP statements, to map the connection identifiers to the data collection options that the MONITORGROUP statements defined.

   When a MONITORGROUP is mapped to Client Identifiers with the MONITORMAP statement, the requested data is collected for those connections.
Related Information

- “Managing TN3270 response time data collection” on page 28

Viewing TN3270 monitor groups

Use the following command to verify that you have set up the TN3270 monitor groups correctly:

```
D TCPIP,tnproc,TELNET,CONN
```

Use the following command to display information for a single connection:

```
D TCPIP,tnproc,TELNET,CONN,CONN=connid
```

If data is being collected, the MONGROUP will be displayed along with the response time statistics and bucket counts.

**Note**

For more information, see the *IBM z/OS Communications Server: IP Configuration Guide*.

Related Information

- “Managing TN3270 response time data collection” on page 28

Suppressing output from the EMCS console

To collect VTAM information for monitor displays, MainView for IP issues commands via the EMCS (internal) console. Console output is written to the VTAM JES/JCL job log, which can become very large over time. Use the following procedure to prevent writing EMCS console messages to the log.

**Note**

TAC9MPF0 is a module in *HLQ.BBLINK*.

To suppress output from the EMCS console

1. Copy the module *HLQ.BBLINK(TAC9MPF0)* into your LNKLIST library and refresh the LLA.
The copied module contains the MPF exit program TAC9MPF0. When installed in SYS1.PARMLIB(MPFLSTxx), this program suppresses EMCS console output.

2 Add IST*,SUP(NO),USEREXIT(TAC9MPF0) into MPFLSTxx.

3 Add IVT*,SUP(NO),USEREXIT(TAC9MPF0) into MPFLSTxx.

4 Add EZZ*,SUP(NO),USEREXIT(TAC9MPF0) into MPFLSTxx.

5 Refresh the MPF by issuing the TMPF=xx command through the console.

6 Issue the D MPF command to verify that IST*, IVT*, and EZZ* have been defined for the USEREXIT.

The TAC9MPF0 exit program will now detect CART (Command and Response Token), IST*, IVT*, and EZZ* messages and prevent them from going to the job log.
Configuring MainView for IP

This chapter describes how to configure MainView for IP by using the panels available in the product.

Selecting history data to collect in MainView for IP

By default MainView for IP collects history data from all areas of the application. Use the following procedure if you want to collect history data for some areas but not for others.

To select history data to collect

1. From the EZIP menu, select MVIP Parms (EZPARMS) in the Utilities section, and press Enter.

2. From the EZPARMS menu, select MVIP Parms Configuration (MVIPCONF) in the Detail Views section, and press Enter.

3. In the MVIPCONF panel, select the required LPAR and press Enter.

   The current settings are displayed. For each parameter displayed in the History Settings section, Table 3 on page 33 shows which application area the parameter controls.

4. In the History Settings section, enter ON to start or OFF to stop collection of history data.

Table 3: History settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Collects history data for</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMON</td>
<td>Availability monitoring</td>
</tr>
<tr>
<td>APing</td>
<td>Availability ping</td>
</tr>
<tr>
<td>Parameter</td>
<td>Collects history data for</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>Cache</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>CSM Buffers</td>
<td>Communications Storage Manager</td>
</tr>
<tr>
<td>Devlinks</td>
<td>Network and OSA device</td>
</tr>
<tr>
<td>EE</td>
<td>Enterprise Extender</td>
</tr>
<tr>
<td>FTP</td>
<td>FTP connections</td>
</tr>
<tr>
<td>IDSS</td>
<td>Intrusion detection</td>
</tr>
<tr>
<td>Links</td>
<td>Network links</td>
</tr>
<tr>
<td>OSA</td>
<td>OSA historical data</td>
</tr>
<tr>
<td>Ports</td>
<td>Port definitions</td>
</tr>
<tr>
<td>Routes</td>
<td>Network routes</td>
</tr>
<tr>
<td>RTPS</td>
<td>RTP</td>
</tr>
<tr>
<td>SLAP</td>
<td>Service Level Policy</td>
</tr>
<tr>
<td>SNMP</td>
<td>SNMP</td>
</tr>
<tr>
<td>Stack Stats</td>
<td>TCPIP stack statistics</td>
</tr>
<tr>
<td>VIPA Config</td>
<td>DVIPA configuration</td>
</tr>
<tr>
<td>VIPA Connections</td>
<td>DVIPA connections</td>
</tr>
<tr>
<td>VTAM Buffers</td>
<td>VTAM buffer</td>
</tr>
<tr>
<td>IPSec</td>
<td>IPSec</td>
</tr>
<tr>
<td>OSPF interfaces</td>
<td>OSPF</td>
</tr>
<tr>
<td>OSPF Neighbors</td>
<td>OSPF neighbors</td>
</tr>
</tbody>
</table>

**History interval values**

If you have allocated historical data sets, historical reporting begins as soon as the PAS is initialized. Data is recorded at the interval that is specified in the `HLQ.BBPARM` data set member `TACTIR00`. The following parameters are in `TACTIR00`:

- **INTVAL** is the length of the interval for which data is collected (in minutes).
SYNCVAL indicates how long to wait (in minutes after the start of the hour) before starting the first interval.

The INTVAL and SYNCVAL settings trigger end-of-interval processing.

**Note**

You can change the parameters by copying the TACTIR00 member to `HLQ.UBBPARM(TACTIR00)` and make changes. You can also specify SMF to synchronize the collection time with the SMF interval.

Table 4 on page 35 lists values that can be specified for INTVAL and SYNCVAL.

**Table 4: History interval values**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Acceptable values</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTVAL</td>
<td>SMF</td>
<td>SMF or nn</td>
</tr>
<tr>
<td></td>
<td>Note: If INTVAL=&quot;SMF&quot; is specified, the SYNCVAL parameter is ignored. The interval time is set to 15 minutes</td>
<td>nn must be an integer of 60:1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60</td>
</tr>
<tr>
<td>SYNCVAL</td>
<td>00</td>
<td>00 or INTVAL-1</td>
</tr>
<tr>
<td></td>
<td>The interval starts at the beginning of the hour</td>
<td></td>
</tr>
</tbody>
</table>

By default, intervals are synchronized on the hour (SYNCVAL="00"). For example, if INTVAL is specified as 15 minutes and extraction begins at 7:49 A.M., the first interval lasts until 8:00 A.M. (only 11 minutes). Successive intervals are 8:00 to 8:15, 8:15 to 8:30, and so on.

Figure 1 on page 35 shows a sample of the TACTIR00 member.

**Figure 1: Sample TACTIR00 member in BBPARM**

`<INTERVAL INTVAL="15" SYNCVAL="0"/>`

Where to go from here:

- If you are upgrading MainView for IP you can migrate your settings by submitting the JCL `HLQ.BBSAMP(TACMIGR)`.
- Customize the operating environment for MainView for IP as described in the topics on customizing z/OS services.
Controlling SNMP and OSA data collection in MainView for IP

MainView for IP provides SNMP and Open Systems Adapter (OSA) information that you need to monitor your network. Use the following procedure to control collection of SNMP and OSA data.

MainView for IP monitors the following information:

- SNMP data collection views show detailed and summary router performance information.
- OSA views show information about OSA devices. You can use the OSA views to see:
  - OSA configuration information
  - utilization statistics
  - network device details
  - network link details
  - Ethernet-like statistics.

MainView for IP parameters control:

- Whether SNMP data is collected
- Whether OSA data is collected
- How frequently the data is collected

To control SNMP and OSA data collection

1. From the EZIP menu, select MVIP Parms (EZPARMS) in the Utilities section, and press Enter.

2. From the EZPARMS menu, select MVIP Parms Configuration (MVIPCONF) in the Detail Views section, and press Enter.

3. To enable SNMP and OSA data collection, enter values in the appropriate fields based on the information in Table 5 on page 37.
Table 5: Parameters that control SNMP and OSA data collection

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>Specifies whether SNMP data is collected. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>ON</strong> enables data collection</td>
</tr>
<tr>
<td></td>
<td>- <strong>OFF</strong> disables data collection</td>
</tr>
<tr>
<td>OSA</td>
<td>Specifies whether OSA data is collected. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>ON</strong> enables data collection</td>
</tr>
<tr>
<td></td>
<td>- <strong>OFF</strong> disables data collection</td>
</tr>
<tr>
<td>SNMP Interval (minutes)</td>
<td>Specifies the interval in minutes between execution of the subtask that collects SNMP data</td>
</tr>
</tbody>
</table>

Configuring the availability ping in MainView for IP

With the availability ping, you can automatically ping an IP network device to determine its availability and provide device response times.

**To configure the availability ping**

1. From the EZIP menu, select **MVIPParms (EZPARMS)** in the Utilities section, and press **Enter**.

2. From the EZPARMS menu, select **MVIPParms Configuration (MVIPCONF)** in the Detail Views section, and press **Enter**.

3. In the MVIPCONF panel, select the system that you want to configure and click **Enter**.

4. In the Data Collection section, select the **Availability Ping** field and type **ON** or **OFF** to enable or disable this utility.
Automating Packet Trace

Alarms are defined on connections views to automate a packet trace when an error condition occurs. You create the MainView alarm on any connection view. The Start Message ID must be BMCPKTSTART and the Start message text must contain the following values for the positional parameters:

- &STACKNM
- &FIPADDSC
- &FPORT
- &LIPADDSC
- &LPORT
- &CLIENTID

The End Message ID must be BMCPKTSTOP and the End Message Text must contain the following values for the positional parameters:

- &STACKNM
- &CLIENTID

The alarm could trigger on network errors such as duplicate ACKs, retransmits, or high response times (RTT).

Note

The user can change the Start and End Message ID in the MainView alarm, but it must match the Alarm ID in the AO rule set.

The automated packet trace also requires an AUTOOPERATOR (AO) rule to be triggered by the MainView alarm. The AO rule will start the packet trace for the specified TCP connection. Sample alarms AORTT, AODUPACK, and AORXMTS are shipped as distributed alarms with MainView for IP. In addition, sample AUTOOPERATOR rule RULPKTTR is shipped with MainView for IP.

Note

The automated packet trace requires the MainView for Networks solution.
Defining Packet Trace table options in MainView for IP

Use the following procedure to define Packet Trace table options. The Packet Tracing views provide TCP/IP header and packet data to help you diagnose problems on your network. These options define how much trace data is saved and whether any data might be overwritten during a trace.

To define Packet Trace table options

1. From the EZIP menu, select MVIPParms (EZPARMS) in the Utilities section, and press Enter.

2. From the EZPARMS menu, select MVIPParms Configuration (MVIPCONF) in the Detail Views section, and press Enter.

3. Select the partition (LPAR) that you want to configure and click Enter.

4. In the Pkttrc DS Size field, type the number of megabytes you want to allocate to the Packet Trace table.

5. In the Pkttrace Wrap field, type ON to enable or OFF to prevent wrapping of the packet trace data when the end of table is reached.

Saving packet trace data upon recycle of MainView for IP PAS

Use the following procedure to save packet trace data to a data set upon recycle of the MainView for IP PAS.

Before you begin

You must allocate a data set before you can save packet trace upon recycle of the MainView for IP PAS. This process is not performed within the program. The data set attributes must be as follows:

- Organization: PS
- Record format: VB
- Record Length: 27998
To save packet trace data upon recycle of the MainView for IP PAS

1 From the EZIP menu, select MVIP Parms (EZPARMS) in the Utilities section, and press Enter.

2 From the EZPARMS menu, select MVIP Parms Configuration (MVIPCONF) in the Detail Views section, and press Enter.

3 Select the partition (LPAR) that you want to configure and click Enter.

4 In the Save Pkt at Shutdown field, type YES to enable or NO to disable saving of packet trace data.

5 In the Packet Trace File field, type the name of the data set where MainView for IP should write the trace data when the PAS is shut down.

Defining Socket Trace table options in MainView for IP

You can use the Socket Trace table options to define how much trace data is saved and whether it is overwritten during a trace. The Socket Tracing views provide detailed information about a socket call, including all socket parameters and return codes.

To define Socket Trace table options

1 From the EZIP menu, select MVIP Parms (EZPARMS) in the Utilities section, and press Enter.

2 From the EZPARMS menu, select MVIP Parms Configuration (MVIPCONF) in the Detail Views section, and press Enter.

3 Select the partition (LPAR) that you want to configure and click Enter.

4 In the Skttrec DS Size field, type the number of megabytes that you want to allocate to the socket trace table.

5 In the Sktttrace Wrap field, type ON to enable or OFF to prevent wrapping of the socket trace data when the end of table is reached.
Configuring TN3270 network and host response time collection in MainView for IP

MainView for IP collects TN3270 performance data from the IBM NMI and real-time response time data on all active TN3270 TCP connections. Use the following procedure to configure TN3270-related data collection.

Note
The TNCONS view provides the real-time response time data.

To configure TN3270 network and host response time collection

1. From the EZIP menu, select MVIPParms (EZPARMS) in the Utilities section, and press Enter.

2. From the EZPARMS menu, select MVIPParms Configuration (MVIPCONF) in the Detail Views section, and press Enter.

3. Select the system that you want to configure and click Enter.

4. In the MVIPCONF panel, select the partition (LPAR) that you want to configure and click Enter.

5. In the TN3270 Resp Times field, in the MVIPCNFD panel, from the Data Collection section, type ON to enable or OFF to disable this utility.

Configuring domain name resolution in MainView for IP

Domain name resolution resolves an IP address to a domain name, and provides the IP address of a domain name.

To configure name resolution

1. From the EZIP menu, select MVIPParms (EZPARMS) in the Utilities section, and press Enter.

2. From the EZPARMS menu, select MVIPParms Configuration (MVIPCONF) in the Detail Views section, and press Enter.
The MVIPCONF panel is displayed.

3 In the MVIPCONF panel, select the partition (LPAR) that you want to configure and click Enter.

4 In the Name Resolution field of the IPFilter Settings section, type ON to enable or OFF to disable this utility.

### Configuring the IPv6 short form display format in MainView for IP

On MainView for IP tabular views, only 16 bytes are displayed for IP addresses. For IPv6 addresses that are more than 16 bytes, MainView for IP displays the short form of the IPv6 address.

**Note**

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

#### To configure the IPv6 short display format

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

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

3 Select the system that you want to configure and click Enter.

4 In the IPv6 Short Format field, type the format in the form \((x, y)\), where:
   - \(x\) represents the number of characters to display at the beginning of the IPv6 address
   - \(y\) represents the number of characters to display at the end of the IPv6 address

Both \(x\) and \(y\) must be between 0 and 14 and the two numbers must add up to 14. For more information, refer to IPv6 address short format in MainView for IP on page 70.
Configuring IP pacing in MainView for IP

With MainView for IP, you can delay (or "pace") outbound data from any TCP/IP application to provide more processing time to business-critical applications. You can also display information about applications that have been paced.

To configure IP pacing

1. From the EZIP menu, select MVIP Parms (EZPARMS) in the Utilities section, and press Enter.

2. Select MVIP Parms Configuration (MVIPCONF) in the Detail Views section, and press Enter.

3. Select the system that you want to configure and click Enter.

4. In the IP Pacing field of the IP Pacing Settings section, type ON to enable or OFF to disable this utility.

Configuring MainView for IP for zIIP exploitation

MainView for IP accommodates zIIP processing, which lets you offload some processing from the mainframe to IBM System z Integrated Information Processors (zIIPs), if available.

To enable zIIP processing

1. From the EZIP menu, select MVIP Parms (EZPARMS) in the Utilities section, and press Enter.

2. From the EZPARMS menu, select MVIP Parms Configuration (MVIPCONF) in the Detail Views section, and press Enter.

3. Change the zIIP enabled parameter from No to Yes, and press Enter.

4. Insert the percentage (1-100) of zIIP processing to be used, and press Enter.
Configuring IBM data collection in MainView for IP

MainView for IP uses the following IBM interfaces to collect performance data:

- The IBM SNA NMI collects:
  - Enterprise Extender (EE) connections and performance data
  - High-performance-routing rapid transfer protocol (RTP) connections
- The IBM TCP/IP NMI collects:
  - TN3270E performance data
  - FTP performance data
  - End-of-connections data
- The IBM IPSec NMI collects:
  - IPSec performance data
  - IP filtering rules
  - Logging data
- The IBM VTAM SAW interface collects:
  - VTAM session data
  - Virtual and explicit route data
  - VTAM PIU tracing

Controlling the MainView for IP NMI

Use the following procedure to control which interfaces MainView for IP should utilize to collect information.

You can activate data collection for the following areas:

- EE and RTP connections
- TN3270E performance data
- FTP performance data
- End-of-connections data
- IP filtering rules

**Note**
Deactivating data collection in the MVIPNMI view does not affect the configuration of the IBM NMI.

IBM NMI services must be configured before MainView for IP can collect data. For more information, see IBM documentation for z/OS services customization and the IBM zOS Communications Server.

**To control the MainView for IP NMI**

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

2. From the EZPARMS menu, select **MVIP NMI settings** (MVIPNMI) in the Detail Views section, and press **Enter**.

3. From the MVIPNMI panel select the required system and click **Enter**.

4. In the Mainview/IP NMI Settings section of the MVIPNMID panel, enter **ON** or **OFF** in each field shown in Table 6 on page 45 to enable or disable data collection for that field.

**Table 6: MainView for IP NMI data collection settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTAM EE/RTP NMI Interface</td>
<td>Controls whether data is collected from the IBM SNA NMI</td>
</tr>
<tr>
<td>TN3270E Performance Monitoring</td>
<td>Controls whether data is collected from the IBM TN3270E NMI</td>
</tr>
<tr>
<td>IP FTP NMI Interface</td>
<td>Controls whether FTP data is collected from the IBM TCP/IP NMI</td>
</tr>
<tr>
<td>End of Connection NMI Interface</td>
<td>Controls whether end-of-connection data is collected from the IBM TCP/IP NMI</td>
</tr>
<tr>
<td>IPSec NMI interface</td>
<td>Controls whether data is collected from the IBM IPSec NMI</td>
</tr>
</tbody>
</table>

**Filtering the end-of-connection data in MainView for IP**

You can use End of Connection filtering to limit the volume of end-of-connection data that is collected.
MainView for IP can filter the end-of-connection data by:

- Job name
- Port number

**Related Information**

- “Filtering end-of-connection data by job name in MainView for IP” on page 46
- “Filtering by port number in MainView for IP” on page 47

---

**Filtering end-of-connection data by job name in MainView for IP**

Use the following procedure to set up job-name filtering of the end-of-connection data.

*Note*

You can filter by job name or by port number but not by both.

**To filter by job name**

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

2. From the EZPARMS menu, select **MVIP NMI Settings (MVIPNMI)** in the Detail Views section, and then press **Enter**.

3. From the MVPNMI panel select the required system and click **Enter**.

4. In the MVPNomid panel, in the **Include or Exclude Table** field of the End of Connection Filter section, type one of the following:

   - **Include** to collect data only the jobs specified in the **Jobname1** through **Jobname8** fields
   - **Exclude** to collect data from all the the jobs specified in the **Jobname** fields

5. In the **Jobname Table** field, type **ON** to filter by job name.

*Note*

To filter by Job name, the **Port Table** field must be set to **OFF**.
6 In the **Jobname** fields (Jobname1 through Jobname8), type the names of the jobs to use for filtering.

## Filtering by port number in MainView for IP

Use the following procedure to set up filtering by port number of the end-of-connection data.

**Note**

You can filter by either job name or port number but not by both.

### To filter by port number

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

2. From the EZPARMS menu, select **MVIP NMI Settings** (MVIPNMI) in the Detail Views section, and press Enter.

3. From the MVPNMI panel select the required system and click Enter.

4. In the MVIPNMID panel, in the **Include or Exclude Table** field of the End of Connection Filter section Port table enter:
   - **Include** to collect data from only those ports that match the entries in the Port1 through Port8 fields
   - **Exclude** to collect data from all ports except from those ports that match the entries in the Port1 through Port8 fields

5. In the **Port Table** field, enter ON to filter by port.

**Note**

To filter by port number, the **Jobname Table** field must be set to OFF.

6. In the **Port** fields (Port1 through Port8), type the port numbers to use for filtering.

## Configuring IPSec Filter logging

Use the following procedure to specify which IPSec Filtering messages MainView for IP will log.
Before you begin

The Traffic Regulation Management daemon (TRMD) must be active and IPSec Filter logging must be enabled in the IPSEC rules before you can enable IPSec filter logging in MainView for IP.

To configure IPSec filter logging

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

2. In the EZPARMS panel, in the detail views section, select MVIP Parms Configuration and press **Enter**.

3. Select the system name required and press **Enter**.

4. In the **Logging** field, type **ON** or **OFF** to enable or disable logging.

5. In the **Logging Type** field, type one of the options shown in Table 7 on page 48.

**Table 7: IPSEC filter options**

<table>
<thead>
<tr>
<th>Logging type option</th>
<th>Filter activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>Logs all IP Filtering Messages (default)</td>
</tr>
<tr>
<td>PERMIT</td>
<td>Logs EZD0814I and EZD0836I messages</td>
</tr>
<tr>
<td>DENY</td>
<td>Logs EZD0815I, EZD0821I, EZD0822I, and EZD0832I messages</td>
</tr>
<tr>
<td>DENYPERMIT</td>
<td>Logs DENY and PERMIT messages</td>
</tr>
<tr>
<td>TRMD</td>
<td>Logs all messages from the TRMD address space</td>
</tr>
</tbody>
</table>

6. In the **Max Entries** field, enter a value from 10000 to 99999 to indicate the number of entries in the IP Filtering table.

   The default value is 10000.

   **Note**

   If you adjust the value in the **Max Entries** field, you must recycle the MainView for IP PAS to register the change.
Controlling VTAM SAW data collection in MainView for IP

Use the following procedure to control the collection of VTAM session awareness (SAW) data from the IBM VTAM ISTPDCLU Interface.

To control VTAM SAW data collection

1. In the EZIP menu, select MVIP Parms (EZPARMS) and press Enter.
2. From the EZPARMS menu, select MVIP SAW Settings (MVIPSAW) and press Enter.
3. From the MVIPSAW panel, select the required system name and press Enter.
4. In the SAW Collection field, type ON to enable or OFF to disable SAW data collection.

Note
If Fail is shown in the SAW Collection field, the SAW ACB Status field indicates the reason for failure. For information about the reasons for failure, access online Help by clicking F1.

5. (optional) If you enabled SAW data collection, enter values in the appropriate fields based on the information in Table 8 on page 49.

Table 8: VTAM SAW data collection settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind failures</td>
<td>Specifies whether BIND failures will be collected</td>
</tr>
<tr>
<td>Init failures</td>
<td>Specifies whether INIT failures will be collected</td>
</tr>
<tr>
<td>Abnormal UNBIND</td>
<td>Specifies whether Abnormal UNBINDs will be collected</td>
</tr>
<tr>
<td>Normal session end</td>
<td>Specifies whether normal Session Ends will be collected as part of the VTAM session data. If set to OFF, only active sessions will be displayed and collected for history.</td>
</tr>
<tr>
<td>SAW Data Buffers</td>
<td>Defines the number of SAW data buffers used when interfacing with the ISTPDCLU trace session. Valid values are in the range 2 to 255 and the default value is 2.</td>
</tr>
<tr>
<td>SAW Data Buffer Size</td>
<td>Defines the SAW data buffer size when interfacing with the ISTPDCLU trace session. Valid values are in the range 2048 to 32767 and the default value is 4096.</td>
</tr>
</tbody>
</table>
Filtering the VTAM SAW data collection in MainView for IP

Use filtering to limit the volume of VTAM session awareness (SAW) data that is collected and determine which VTAM sessions will be globally traced.

MainView for IP checks the SAW filters in the order they are listed on the SAW Filter (SAWFILTR) panel.

**To filter the VTAM SAW data collection**

1. From the EZPARMS menu, select MVIP Parms (EZPARMS) from the Utilities section, and press **Enter**.

2. From the EZPARMS menu, select MVIP SAW settings (MVIPSAW) in the Detail Views section, and press **Enter**.

3. From the MVIPSAW panel, select the required system, and press **Enter**.

4. From the MVIPSAWD panel, select **SAW Filters** and press **Enter**.

   The SAWFILTR view is displayed. The first time you enter the SAWFILTR view, no filters are defined and only a DummyPLU entry is shown (Figure 2 on page 50).

**Figure 2: SAWFILTR view**

<table>
<thead>
<tr>
<th>04JUN2013 11:06:08 ------- MAINVIEW WINDOW INTERFACE (V6.1.00) -----------</th>
<th>SCROLL ===&gt; PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CURR WIN ===&gt; 1 ALT WIN ===&gt;</td>
<td>W1 =SAWFILTR====TCPIP====*04JUN2013==11:02:16====MVIP=====D====1</td>
</tr>
<tr>
<td>CMD</td>
<td>Keep Log</td>
</tr>
<tr>
<td>DummyPLU</td>
<td>DummySLU</td>
</tr>
</tbody>
</table>

5. In the **Command** field, type **ADD** next to the DummyPLU entry, and then press **Enter**.

   **Note**

   When entries are already present, you can use the following commands to update or delete an entry:

   - **U** to update the entry
   - **DEL** to delete the entry
The SAW filter data entry screen is displayed, as shown in Figure 3 on page 51

**Figure 3: SAW filter data entry screen**

```
05JUN2013  04:10:45 ------ MAINVIEW WINDOW INTERFACE (V6.1.00) -----------
Essssssssssssssssssssssssssssss Add SAW Filter sssssssssssssssssssssssssssss
  COMMAND ===> SCROLL ===> PAGE
  e COMMAND ===>
  e Primary LU: DummyPLU
  e Secondary LU: DummySLU
  e SAW: Yes (Yes/No)
  e Keep PIU: 7 (0-999)
  e Log PIU: No (Yes/No)
  e Order: 1
  e END to Add SAW Filter
  e CANCEL to NOT Add SAW Filter
  e HELP to view related help
```

6 Add a filter in the data entry screen by typing the required information as described in Table 9 on page 51

**Table 9: Required entries in the SAW filter data entry screen**

<table>
<thead>
<tr>
<th>Field</th>
<th>User entry</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary LU</strong></td>
<td>Defines the primary logical unit (PLU) criteria to match against the VTAM SAW data. You can use masking when defining the Primary LU. The following characters are valid for masking:</td>
</tr>
<tr>
<td></td>
<td>■ An asterisk (*) - matches the rest of the PLU name</td>
</tr>
<tr>
<td></td>
<td>■ A question mark (?) - matches any single character</td>
</tr>
<tr>
<td><strong>Secondary LU</strong></td>
<td>Defines the secondary logical unit (SLU) criteria to match against the VTAM SAW data. You can use masking when defining the Secondary LU. The following characters are valid for masking:</td>
</tr>
<tr>
<td></td>
<td>■ An asterisk (*) - matches the rest of the SLU name</td>
</tr>
<tr>
<td></td>
<td>■ A question mark (?) - matches any single character</td>
</tr>
</tbody>
</table>
Controlling VTAM PIU trace data collection in MainView for IP

Use the following procedure to control the collection of trace data for VTAM path information units (PIUs).

**To control VTAM PIU trace data collection**

1. In the EZIP menu, select MVIP Parms (EZPARMS) and press **Enter**.
2. From the EZPARMS menu, select MVIP SAW Settings (MVIPSAW) and press **Enter**.
3. From the MVIPSAW panel, select the required system name and press **Enter**.
4. In either of the following fields, type **ON** to enable or **OFF** to disable PIU trace data collection.
   - Global LU Trace
   - Global SSCP Trace
5. *(optional)* If you enabled PIU trace data collection, enter values in the appropriate fields based on the information in Table 8 on page 49.
Table 10: VTAM PIU trace data collection settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Log Trace PIUs         | Specifies whether traced PIUs are logged to MainView history when the VTAM session ends. This setting is used only if the VTAM session is not found in the SAW filter table. Valid values are:  
  ■ YES  
  ■ NO (default)                                            |
| PIU Trace Time Type    | Defines the time to display when viewing PIU Traces. Valid values are:  
  ■ GMT  
  ■ LOCAL (default)                                        |
| PIU Trace Data Buffers | Defines the number of PIU trace data buffers used when interfacing with the ISTPDCLU trace session. Valid values are in the range 2 to 255 and the default value is 2. |
| PIU Trace Buffer Size  | Defines the PIU trace data buffer size when interfacing with the ISTPDCLU trace session. Valid values are in the range 2048 to 32767 and the default value is 4096. |
| Keep PIU Records       | Specifies how many trace PIUs are kept for each VTAM session. This setting is used only if the VTAM session is not found in the SAW filter table. Valid values are in the range 0 through 999 and the default value is 7.  
  Note: The Keep PIU records value affects the amount of virtual and DASD storage used. |

Using SAWFILTR view for PIU trace filtering

The VTAM session views can display the VTAM PIUs. You can use the SAWFILTR view to filter and match VTAM sessions.
To use the SAWFILTR view for PIU trace filtering

MainView for IP matches the filters as follows:

- When a VTAM session starts, MainView for IP finds the first match and uses the settings in that filter entry.
- If the VTAM sessions is already active when Mainview for IP is started, the filters are matched during initialization of MainView for IP.
- If no SAW filters are specified, or if a match is not found, then MainView for IP uses the default values from the MVIPSAWD view.

1. Open the SAWFILTR view and create a filter. For more details of the SAWFILTR view, see “Filtering the VTAM SAW data collection in MainView for IP” on page 50.

   **Note**
   If global PIU tracing is enabled, the SAWFILTR view enables you to specify how many PIUs are kept for the VTAM session, and to specify if the PIUs are logged to the MainView history file when the VTAM session ends.
   Masking is allowed on the PLU and SLU name fields. The '*' matches the rest of the LU name, and '?' matches an individual character.
   For global PIU Tracing, only the first 40 bytes of the PIU are traced.

   **Tip**
   You can update the options for each VTAM session from the VTAM session views. From the VTAM session views you can start a PIU trace on a specific VTAM LU that traces the whole VTAM PIU.

Controlling VTAM message collection in MainView for IP

Use the following procedure to control the collection of VTAM messages using MainView for IP as a VTAM PPO application.

**To control VTAM message collection in MainView for IP**

1. In the EZIP menu, select MVIP Parms (EZPARMS) and press Enter.

2. From the EZPARMS menu, select MVIP PPO Settings (MVIPPO) in the Detail Views section, and press Enter.

3. From the MVIPPO panel, select the required system name and press Enter.
4 In the VTAM PPO Collection field, type ON to enable or OFF to disable VTAM message collection.

Note
If Fail is shown in the VTAM PPO Collection field, the VTAM PPO ACB Status field indicates the reason for failure. For information about the reasons for failure, access online Help by clicking F1.

5 (optional) If you enabled VTAM message collection, enter values in the appropriate fields based on the information in Table 11 on page 55.

Table 11: VTAM message collection settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Logging Action</td>
<td>Determines whether to write the VTAM messages to the Mainview log if there is no match on the PPO filter table. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ NO indicates messages are not to be written to the MainView log.</td>
</tr>
<tr>
<td></td>
<td>■ ALL indicates all messages are to be written to the MainView log.</td>
</tr>
<tr>
<td></td>
<td>■ n represents a number in the range 1 through 200. Every nth message is written to the MainView log.</td>
</tr>
<tr>
<td>Default WTO Action</td>
<td>Determines whether to write the VTAM messages to the system console if there is no match on the PPO filter table. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ NO indicates messages are not to be written to the system console</td>
</tr>
<tr>
<td></td>
<td>■ ALL indicates all messages are to be written to the system console</td>
</tr>
<tr>
<td></td>
<td>■ n represents a number in the range 1 through 200. Every nth message is written to the system console</td>
</tr>
<tr>
<td>VTAM PPOLOG Start Option</td>
<td>Specifies whether VTAM commands entered at the system console and messages VTAM issues in response are recorded in the VTAM PPO log. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ YES indicates VTAM commands and response messages are recorded in the VTAM PPO log</td>
</tr>
<tr>
<td></td>
<td>■ NO indicates VTAM commands and response messages are not recorded in the VTAM PPO log</td>
</tr>
</tbody>
</table>
Filtering VTAM message collection in MainView for IP

Use filtering to limit the volume of VTAM messages that are collected.

MainView for IP checks the VTAM message filters in the order they are listed on the PPOFILTR panel.

**To filter VTAM message collection in MainView for IP**

1. From the EZPARMS menu, select MVIP Parms (EZPARMS) from the Utilities section, and press **Enter**.

2. From the EZPARMS menu, select MVIP PPO Settings (MVIPPPO) in the Detail Views section, and press **Enter**.

3. From the MVIPPPO panel, select the required system name and press **Enter**.

4. From the MVIPPPOD panel, select **VTAM PPO Filters** and press **Enter**.

   The PPOFILTR view is displayed. The first time you enter the PPOFILTR view, no filters are defined and only a ISTXXXXX entry is shown (Figure 4 on page 56).

5. In the **Command** field, type **ADD** next to the ISTXXXXX entry, and then press **Enter**.

   **Note**

   When entries are already present, you can use the following commands to update or delete an entry:

   - **U** to update the entry
   - **DEL** to delete the entry
The PPO filter data entry screen is displayed, as shown in Figure 5 on page 57.

**Figure 5: PPO filter data entry screen**

```
06JUN2013  14:03:56 ---- MAINVIEW WINDOW INTERFACE (V6.1.00) --------------
Eessssssssssssssssssssssssssssss Add PPO Filter sssssssssssssssssssssssssssss
e COMMAND ===>                                              SCROLL ===> PAGE e
e                                                                             e
e  Message Number: ISTXXXXX                                                   e
e  Log Message:    All       (All/No/1-200)                                   e
e  WTO Message:    All       (All/No/1-200)                                   e
e  Order:          1                                                          e
e                                                                             e
e                                                                             e
e END to Add PPO Filter                                                       e
e CANCEL to NOT Add PPO Filter                                                e
e HELP to view related help                                                   e
```

6 Add a filter in the data entry screen by typing the required information as described in Table 9 on page 51

**Table 12: Required entries in the PPO filter data entry screen**

<table>
<thead>
<tr>
<th>Field</th>
<th>User entry</th>
</tr>
</thead>
</table>
| **Message Number** | Defines the VTAM message number criteria to match against the VTAM SAW data. You can use masking when defining the message number. The following characters are valid for masking:  
  ■ An asterisk (*) - matches the rest of the message number  
  ■ A question mark (?) - matches any single character |
| **Log Message** | Determines whether to write the VTAM messages to the Mainview log. Valid values are:  
  ■ NO indicates messages are not to be written to the MainView log  
  ■ ALL indicates all messages are to be written to the MainView log  
  ■ \( n \) represents a number in the range 1 through 200. Every \( n \)th message is written to the MainView log. |
<table>
<thead>
<tr>
<th>Field</th>
<th>User entry</th>
</tr>
</thead>
</table>
| WTO Message| Determines whether to write the VTAM messages to the system console if there is no match on the PPO filter table. Valid values are:  
  - NO indicates messages are not to be written to the system console  
  - ALL indicates all messages are to be written to the system console  
  - $n$ represents a number in the range 1 through 200. Every $n$th message is written to the system console |
| Order      | Defines the order in which the PPO filter entries are checked. |
Configuration settings

This appendix describes the parameters that can be configured in MainView for IP.

Debug settings in MainView for IP

Debug settings control debug data collection for different areas of the application. The Debug Settings section of the MVIPCONF view lists the debug settings (such as APing, TraceRoute, and VIPA).

If you encounter a problem with MainView for IP, contact BMC Customer Support for guidance of the settings to activate.

Note
You should activate debug settings only after consulting BMC Customer Support.

History settings in MainView for IP

This topic describes the history settings that are available in MainView for IP.

Table 13 on page 59 lists the history settings, the application area affected, and the related views.

Table 13: Settings for collection

<table>
<thead>
<tr>
<th>Setting</th>
<th>Controls collection of</th>
<th>For views</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMON</td>
<td>Availability monitoring</td>
<td>AMON</td>
</tr>
<tr>
<td>APing</td>
<td>Availability ping</td>
<td>■ APING</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ APNGD</td>
</tr>
<tr>
<td>Setting</td>
<td>Controls collection of</td>
<td>For views</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Cache</td>
<td>WebSphere cache</td>
<td>CACHE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CACHED</td>
</tr>
<tr>
<td>Config</td>
<td>TCP/IP configuration</td>
<td>TCPCONF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDPCONF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPCONF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP6CONF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SMFCONF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GLOBCONF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DATCONF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AUTCONF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All associated detailed views, D at end</td>
</tr>
<tr>
<td>Connections</td>
<td>TCP/IP connections</td>
<td>ACTCONS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TNCONS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPCONS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDPCONS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PORTSP*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JOBRESP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All associated detailed views</td>
</tr>
<tr>
<td>Setting</td>
<td>Controls collection of</td>
<td>For views</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>CSM Buffers</td>
<td>Communications storage manager</td>
<td>■ CSMJOB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ CSMJOBD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ CSMSUMM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ CSMSUMMD</td>
</tr>
<tr>
<td>Devlinks</td>
<td>Network and OSA device</td>
<td>■ DEVS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ OSADEVS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ DEVSD</td>
</tr>
<tr>
<td>EE</td>
<td>Enterprise Extender</td>
<td>■ EE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ EED</td>
</tr>
<tr>
<td>Setting</td>
<td>Controls collection of</td>
<td>For views</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>FTP</td>
<td>FTP connections</td>
<td>■ FTPF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ FTPFD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ FTPFF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ FTPFI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ FTPFU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ FTPLF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ FTPLFC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ FTPLFD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ FTPLFS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ FTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ FTPSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ FTPSC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ FTPSD</td>
</tr>
<tr>
<td>IDSS</td>
<td>Intrusion detection</td>
<td>■ IDSS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ IDSFLOOD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ IDSTCPPL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ IDSUDPPL</td>
</tr>
<tr>
<td>IPSec</td>
<td>IPSec</td>
<td>■ IPSEC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ IPSECD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ IPSECLG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ IPSECLGD</td>
</tr>
<tr>
<td>Setting</td>
<td>Controls collection of</td>
<td>For views</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Links</td>
<td>Network links</td>
<td>▪ LINKS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ OSALINKS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ LINKSD</td>
</tr>
<tr>
<td>OSA</td>
<td>open systems adapter (OSA)</td>
<td>▪ OSACONF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ OSACONFD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ OSAETH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ OSAETHD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ OSALPAR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ OSALPARD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ OSAUTIL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ OSAUTILD</td>
</tr>
<tr>
<td>OSPF</td>
<td>open short path first (OSPF)</td>
<td>▪ OSPFINTD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ OSPFINTF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ OSPFNETW</td>
</tr>
<tr>
<td>OSPF Neighbors</td>
<td>OSPF Neighbors</td>
<td>▪ OMPNBR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ OMPNBRD</td>
</tr>
<tr>
<td>Ports</td>
<td>Port definitions</td>
<td>▪ PORTS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ PORTSD</td>
</tr>
<tr>
<td>Routes</td>
<td>Network routes</td>
<td>▪ ROUTES</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ ROUTESD</td>
</tr>
<tr>
<td>Setting</td>
<td>Controls collection of</td>
<td>For views</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>RTPS</td>
<td>rapic transfer protocol (RTP)</td>
<td>■ RTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ RTPSD</td>
</tr>
<tr>
<td>SLAP</td>
<td>Service level policy</td>
<td>■ SLAP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SLAPD</td>
</tr>
<tr>
<td>SNMP</td>
<td>SNMP</td>
<td>■ SNMPCSCO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPCSCD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPIF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPIFD1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPIFD2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPIPD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPOSPPF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPOSPD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPSYS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPSYSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPTCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPTCPD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPUDP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SNMPUDPDP</td>
</tr>
<tr>
<td>Setting</td>
<td>Controls collection of</td>
<td>For views</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Stack Stats</td>
<td>TCP/IP stack statistics</td>
<td>■ STACKTCP&lt;br&gt; ■ STACKTCD&lt;br&gt; ■ STACKUDP&lt;br&gt; ■ STACKUDD&lt;br&gt; ■ STACKIP&lt;br&gt; ■ STACKIPD</td>
</tr>
<tr>
<td>VIPA Config</td>
<td>dynamic virtual IP address (DVIPA) &lt;br&gt;configuration</td>
<td>■ VIPACFG&lt;br&gt; ■ VIPACFG1&lt;br&gt; ■ VIPACFG2&lt;br&gt; ■ VIPACFG3&lt;br&gt; ■ VIPACFG4&lt;br&gt; ■ VIPACFG5&lt;br&gt; ■ VIPACFG6&lt;br&gt; ■ VIPADYN&lt;br&gt; ■ VIPAPORT&lt;br&gt; ■ VIPAPRTD&lt;br&gt; ■ VIPAROUT</td>
</tr>
<tr>
<td>VIPA Connections</td>
<td>DVIPA connections</td>
<td>■ VIPACCONN&lt;br&gt; ■ VIPACNND</td>
</tr>
</tbody>
</table>
Data collection settings in MainView for IP

This topic describes the data collection settings that are available in MainView for IP.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Controls collection of</th>
<th>For views</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTAM Buffers</td>
<td>VTAM buffer</td>
<td>■ VTMBUFF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ VTMBUFFD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ VTMBUFQ</td>
</tr>
</tbody>
</table>

### Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability ping</td>
<td>Determines whether the availability ping (APNG) runs at startup. You can use APNG to ping an IP network device automatically to determine its availability and provide device response times. <strong>Note:</strong> To use IP pacing when pacing is enabled, you must add IP pacing entries (job names) on the IPPACCFG view.</td>
</tr>
<tr>
<td>IP pacing</td>
<td>Determines whether to use IP pacing to delay (or &quot;pace&quot;) outbound data from any TCP/IP application. You can use IP pacing to provide more processing time to business critical applications. <strong>Note:</strong> To use IP pacing when pacing is enabled, you must add IP pacing entries (job names) on the IPPACCFG view.</td>
</tr>
<tr>
<td>Domain name resolution</td>
<td>Determines whether the domain name resolution (DNR) function is available. The DNR function resolves an IP address to a domain name, and provides the IP address of a domain name. Domain name resolution is enabled by default.</td>
</tr>
<tr>
<td>OSA data collection</td>
<td>Determines whether OSA data is collected. OSA is enabled by default.</td>
</tr>
<tr>
<td>SNMP data collection</td>
<td>Determines whether SNMP data is collected (SNMP is enabled by default).</td>
</tr>
<tr>
<td>SNMP interval definition</td>
<td>Defines the interval, in minutes, during which the subtask that collects SNMP data will run.</td>
</tr>
<tr>
<td>TN3270 response time collection</td>
<td>Determines whether TN3270 network and host response times are collected.</td>
</tr>
</tbody>
</table>
Trace settings in MainView for IP

This topic describes the trace settings that are available in MainView for IP.

**Related Information**

- “Pkttrace Wrap - Enable disable wrapping in MainView for IP” on page 67
- “Pkttrc DS Size definition in MainView for IP” on page 67
- “Skttrace wrap - Enable disable in MainView for IP” on page 68
- “Skttrc DS Size - Specify size of socket trace table in MainView for IP” on page 68

**Pkttrace Wrap - Enable disable wrapping in MainView for IP**

This setting indicates whether a packet trace will wrap to the beginning of the trace table when the end of the trace table is reached. Wrapping overwrites packet trace data at the beginning of the table.

**Related Information**

- “Trace settings in MainView for IP” on page 67

**Pkttrc DS Size definition in MainView for IP**

This setting defines the size of the packet trace table.

The value specified is in megabytes. Any changes to this setting will take effect after the MainView for IP PAS is recycled. The default size is 25 megabytes and the maximum size is 200 megabytes.
Sktttrace wrap - Enable disable in MainView for IP

This setting indicates whether a socket trace will wrap to the beginning of the trace table when the end of the trace table is reached. Wrapping overwrites socket trace data at the beginning of the table.

Sktttrc DS Size - Specify size of socket trace table in MainView for IP

This setting defines the size of the socket trace table.

The value specified is in megabytes. Any changes to this setting will take effect after the MainView for IP PAS is recycled. The default size is 25 megabytes and the maximum size is 200 megabytes.

IPSec filtering logging settings

This section covers IPSec filtering logging settings in MainView for IP.

You can configure the IPSec filtering logging settings as described in Table 14 on page 69.
### Table 14: Settings for IPSec filtering logging configuration

<table>
<thead>
<tr>
<th>IP filter</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>Specifies whether to log IPSec filtering messages (EZD08* messages that TRMD sends to SYSLOGD). You have the option of collecting these messages for display on the IPSECLG view. The TRMD address space must be active, and you must specify IPSec filtering logging in the IPSec rules for the PAGENT address space</td>
<td>OFF</td>
</tr>
</tbody>
</table>
| Logging Type | Specifies which type of IPSec Filtering messages MainView for IP will log. The possible values are:  
  - ALL - logs all messages  
  - PERMIT - logs the EZD0814I and EZD0836I messages  
  - DENY - logs the EZD0815I, EZD0821I, EZD0822I, EZD0832I, and EZD0833I messages  
  - DENYPERMIT - logs DENY and PERMIT messages  
  - TRMD - logs all messages from the TRMD address space | ALL |
| Max Entries | Specifies the number of entries in the IPSec Filtering table in the data space. The value must be between 10000 and 99999. The records are written at interval time, and the dataspace is cleared. If more records are written to the IP Filtering table than the maximum value allowed during an interval, no more records will be logged.  
  **Note:** Any changes to the Max Entries value will require a recycle of the MainView for IP PAS to allow the change to register. | 10000 |

---

## Additional settings

This section describes additional settings that are available in MainView for IP.

### Related Information

- “EMCS Timeout in MainView for IP” on page 70
- “IPv6 address short format in MainView for IP” on page 70
EMCS Timeout in MainView for IP

The EMCS Timeout field specifies, in seconds, the time-out value when collecting data from the MVS console commands.

**Note**

BMC recommends that this field be changed only at the request of BMC Customer Support.

**Related Information**

- “Additional settings” on page 69

EMCS Route Code

The EMCS Route Code field specifies the route code to be used when the EMCS console is opened. Any changes to the fields will require a recycle of the MainView for IP PAS. A value of zero indicates that no route codes are being used.

SAF Check

The SAF Check field indicated whether MainView for IP should complete System Authorization Facility (SAF) checking on the TSO user ID when performing actions against any IBM VTAM resource. Setting this field to **YES** checks the MVS.VARY.NET resource CLASS(OPERCMDS).

IPv6 address short format in MainView for IP

IPv6 addresses that exceed 16 bytes are displayed in MainView for IP a the short form. The IPv6 Short Format setting controls the form of those addresses.

The IPv6 Short Format setting uses the format \((x,y)\):

- The value of \(x\) represents the number of characters to display from the beginning of the IPv6 address.

- The value of \(y\) represents the number of characters to display from the end of the IPv6 address. For this setting, \(x\) and \(y\) must be numbers between 0 and 14, and the numbers must add up to 14.

The beginning and end characters will be separated by a double period (‘..’), making a character string of 16-bytes.
The default short format setting is (7.7). You might want to change the setting, depending on how your IPv6 addresses are defined in your environment. For example, if the uniqueness of your IPv6 addresses is in the first few octets, you could use a setting of (14.0). If the uniqueness is at the end of the IPv6 address, you could use 0.14. You can display a shortened address as a full address by using a hyperlink: either to a pop-up with the full IPv6 address or to a detailed view with the full IPv6 address.

**Related Information**

- “Additional settings” on page 69
NMI settings

This appendix describes the settings that control MainView for IP data collection from the IBM network management interface (NMI).

NMI settings in MainView for IP

In the MVIPNMID view, the NMI settings section contains the fields that control how MainView for IP collects data from configured IBM NMIs.

Table 15 on page 73 lists the fields in this section of the MVIPNMID view. Turning one of these settings on or off does not affect the configuration of the IBM NMI services.

Note
For more information about configuration of the IBM NMI services, see the topics on customizing z/OS services and the IBM documentation on the zOS Communications Server.

Table 15: MainView for IP NMI fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTAM EE/RTP NMI Interface</td>
<td>Specifies whether the collection of Enterprise Extender (EE) and Rapid Transfer Protocol (RTP) data from the IBM SNA NMI is enabled</td>
</tr>
<tr>
<td>TN3270E Performance Monitoring</td>
<td>Specifies whether the collection of TN3270E performance data from the IBM TCP/IP NMI is enabled</td>
</tr>
<tr>
<td>IP FTP NMI Interface</td>
<td>Specifies whether the collection of FTP data from the IBM TCP/IP NMI (SYSTCPSM) is enabled</td>
</tr>
<tr>
<td>End of Connection NMI Interface</td>
<td>Specifies whether the collection of end-of-connection data from the IBM TCP/IP NMI (SYSTCPCN) is enabled</td>
</tr>
</tbody>
</table>
## End-of-Connection NMI table in MainView for IP

In the MVIPNMID view, the End-of-Connection NMI table section contains fields that define limits for collected end-of-connection data.

**Note**

All TN3270 connections data are collected, regardless of the criteria defined in these fields.

Table 16 on page 74 lists the fields in this section of the MVIPNMID view.

### Table 16: End-of-Connection NMI table fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include or Exclude Table</td>
<td>Defines whether collect or exclude the data specified for the Job name Table or the Port Table. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ Include (default)</td>
</tr>
<tr>
<td></td>
<td>■ Exclude</td>
</tr>
<tr>
<td>Jobname Table</td>
<td>Determines whether the end-of-connection data is filtered by job name. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ ON</td>
</tr>
<tr>
<td></td>
<td>■ OFF (default)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can filter end-of-connection data either by jobname or port number.</td>
</tr>
<tr>
<td>Jobname1</td>
<td>Defines the jobname criteria to match against the end-of-connection data. You can define up to eight jobname criteria. If any one of these criteria match the connection, the connection is processed or ignored at the end of connection, depending on the setting of the <strong>Include or Exclude Table</strong> field. Masking is allowed when defining the job name criteria.</td>
</tr>
<tr>
<td>Jobname2</td>
<td><strong>Note:</strong> These fields are valid only if the <strong>Jobname Table</strong> field is set to ON.</td>
</tr>
<tr>
<td>Jobname3</td>
<td></td>
</tr>
<tr>
<td>Jobname4</td>
<td></td>
</tr>
<tr>
<td>Jobname5</td>
<td></td>
</tr>
<tr>
<td>Jobname6</td>
<td></td>
</tr>
<tr>
<td>Jobname7</td>
<td></td>
</tr>
<tr>
<td>Jobname8</td>
<td></td>
</tr>
</tbody>
</table>
### VTAM SAW settings in MainView for IP

The MVIPSAWD view, which is reached from the EZPARMS view, allows you to configure the settings for collecting VTAM session awareness (SAW) data.

*Table 17 on page 75* lists the fields in the MainView/IP SAW settings section of the MVIPSAWD view.

**Table 17: MainView for IP SAW settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Displays the MVS system name related to the settings displayed. This field is read only.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SAW Collection</td>
<td>Specifies whether to collect VTAM SAW data from the IBM VTAM communications NMI. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ ON (default)</td>
</tr>
<tr>
<td></td>
<td>■ OFF</td>
</tr>
<tr>
<td></td>
<td>■ FAIL (a display-only value indicating that data collection from the IBM VTAM communications NMI was unsuccessful for the reason specified in the SAW ACB Status field.)</td>
</tr>
<tr>
<td>SAW Application Name</td>
<td>Specifies the ACB Name to be used for the MainView for IP CNMI application that will initiate a session with ISTPDCLU</td>
</tr>
<tr>
<td>SAW ACB Status</td>
<td>Displays the Access Control Block (ACB) status. This field is read only. For an explanation of the displayed status press F1 for online help</td>
</tr>
</tbody>
</table>

Table 18 on page 76 lists the fields in the VTAM Session Data Filters section of the MVIPSAWD view.

Table 18: VTAM Session Data Filters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind failures</td>
<td>Specifies whether to collect BIND failures as part of the VTAM session data. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ ON (default)</td>
</tr>
<tr>
<td></td>
<td>■ OFF</td>
</tr>
<tr>
<td>Init failures</td>
<td>Specifies whether to collect INIT failures as part of the VTAM session data. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ ON (default)</td>
</tr>
<tr>
<td></td>
<td>■ OFF</td>
</tr>
<tr>
<td>Abnormal UNBIND</td>
<td>Specifies whether to collect abnormal UNBINDs as part of the VTAM session data. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ ON (default)</td>
</tr>
<tr>
<td></td>
<td>■ OFF</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Normal session end</td>
<td>Specifies whether to collect normal session ends as part of the VTAM session data. If you set the field to OFF, then only active sessions will be displayed and collected for history. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ ON (default)</td>
</tr>
<tr>
<td></td>
<td>■ OFF</td>
</tr>
<tr>
<td>SAW Data Buffers</td>
<td>Defines the number of SAW data buffers used when interfacing with the ISTPDCLU trace session. Valid values are in the range 2 to 255 and the default value is 2.</td>
</tr>
<tr>
<td>SAW Data Buffer Size</td>
<td>Defines the SAW data buffer size when interfacing with the ISTPDCLU trace session. Valid values are in the range 2048 to 32767 and the default value is 4096.</td>
</tr>
</tbody>
</table>

**VTAM PIU trace settings in MainView for IP**

The MVIPSAWD view, which is reached from the EZPARMS view, allows you to configure the settings for collecting VTAM PIU trace data.

Table 19 on page 77 lists the fields in the VTAM PIU Trace Settings section of the MVIPSAWD view.

### Table 19: MainView for IP VTAM PIU Trace Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global LU Trace</td>
<td>Specifies whether the application should start the Global LU Trace. The Global LU trace performs traces for all LU-LU sessions. The first 40 bytes of each VTAM PIU is traced. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ ON</td>
</tr>
<tr>
<td></td>
<td>■ OFF (default)</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If logging is turned on, global tracing can require large amounts of virtual and DASD storage.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Global SSCP Trace</strong></td>
<td>Specifies whether the application should start the Global SSCP Trace. The Global SSCP trace performs traces for the following sessions:</td>
</tr>
<tr>
<td></td>
<td>■ SSCP-LU</td>
</tr>
<tr>
<td></td>
<td>■ SSCP-PU</td>
</tr>
<tr>
<td></td>
<td>■ SSCP-SSCP</td>
</tr>
<tr>
<td></td>
<td>■ CP-CP</td>
</tr>
<tr>
<td></td>
<td>The first 40 bytes of each VTAM PIU is traced. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ ON</td>
</tr>
<tr>
<td></td>
<td>■ OFF (default)</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If logging is turned on, global tracing can require large amounts of virtual and DASD storage.</td>
</tr>
<tr>
<td><strong>Log Trace PIUs</strong></td>
<td>Specifies whether traced PIUs are logged to MainView history when the VTAM session ends. This setting is used only if the VTAM session is not found in the SAW filter table. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ YES</td>
</tr>
<tr>
<td></td>
<td>■ NO (default)</td>
</tr>
<tr>
<td><strong>PIU Trace Time Type</strong></td>
<td>Defines the time to display when viewing PIU Traces. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>■ GMT</td>
</tr>
<tr>
<td></td>
<td>■ LOCAL (default)</td>
</tr>
<tr>
<td><strong>PIU Trace Data Buffers</strong></td>
<td>Defines the number of PIU trace data buffers used when interfacing with the ISTPDCLU trace session. Valid values are in the range 2 to 255 and the default value is 2.</td>
</tr>
<tr>
<td><strong>PIU Trace Buffer Size</strong></td>
<td>Defines the PIU trace data buffer size when interfacing with the ISTPDCLU trace session. Valid values are in the range 2048 to 32767 and the default value is 4096.</td>
</tr>
<tr>
<td><strong>Keep PIU Records</strong></td>
<td>Specifies how many trace PIUs are kept for each VTAM session. This setting is used only if the VTAM session is not found in the SAW filter table.</td>
</tr>
<tr>
<td></td>
<td>Valid values are in the range 0 through 999 and the default value is 7.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The Keep PIU records value affects the amount of virtual and DASD storage used.</td>
</tr>
</tbody>
</table>
Index

{Internet Protocol. }. See: See:IP

A
Automating Packet Trace 38

B
BBPARM data set, member TACTIR00 34

C
conventions, documentation 8

D
data set members
   TACTIR00 34
data sets
   BBPARM 34
documentation information 7

E
electronic documentation 7

F
FMIDs and target libraries 11

H
Help
   online 7

I
installation
   prerequisites 11
interval recorder data set member, TACTIR00 34
IP (Internet Protocol) 14

O
online Help 7
OSA (Open Systems Adapter)
   data collection 17
   requirements 17

P
Packet Trace 12
   data sets 39
   writing to data set 39
parameter files, syntax rules 33
parameters
   TACTIR00 sample 34
prerequisites, installation 11
product authorization codes, temporary 15
publications, related 7

R
related publications 7
requirements
   OSA 12, 17

S
sample parameter, TACTIR00 34
SAWFILTR view 53
syntax rules, parameter file 33
syntax statement conventions 8

target libraries and FMIDs 11
temporary product authorization codes 15
TN3270 28
TNCONS 28
TNMONGR 28
TNPERF 28

TACTIR00 member 34