IBM Z OMEGAMON Network Monitor
Version 5.6

Planning and Configuration Guide

Note

Before using this information and the product it supports, read the information in “Notices” on page 601.

Edition notice

July 2020 Edition

This edition applies to V5.6 of IBM Z OMEGAMON Network Monitor and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

Chapter 1. Planning

The planning section provides information specific to configuration of IBM Z OMEGAMON Monitor for z/OS.

The *IBM Z Monitoring Suite Products: Preinstallation Requirements and Instructions* technote and the *Planning* section of the *IBM Z Monitoring and Tivoli® Management Services on z/OS®: Shared documentation* contain planning information that is common to the deployment and configuration of all IBM Z Monitoring agents and Tivoli Management Services components on z/OS.

Software and hardware prerequisites

Tivoli Management Services must already be installed. Versions of all the required products for IBM Z OMEGAMON Network Monitor are provided in the product package.

However, if you already installed V5.1.0 of another IBM Z OMEGAMON monitoring agent on z/OS in your enterprise, you can use the currently installed Tivoli Management Service components. A complete list of the product components is found in the *IBM Z Monitoring Agents on z/OS: Quick Start Guide*, and the z/OS prerequisites are found in the *IBM Z OMEGAMON Network Monitor: Program Directory*. Information about z/OS and distributed prerequisites are found in the sections that follow.

Required software

The required levels of software for Tivoli Management Services components, PARMGEN configuration, SAF product, z/OS, IBM® Tivoli NetView® for z/OS, and other software are explained in the section that follows.

Software product and levels

The following software products and levels are required for running the Tivoli Management Services components and the IBM Z OMEGAMON Network Monitor monitoring agent.

PARMGEN configuration requirements

IBM Z OMEGAMON Network Monitor is configured by using the PARMGEN method.

If the hub monitoring server and the remote monitoring server reside on z/OS, they must also be modified to use LIMIT(24,X). Follow the process outlined in the *Configuring the Tivoli Enterprise Monitoring Server on z/OS* book and ensure that the **Maximum storage request size (Extended)** value is set to greater than or equal to 24.

Also, you cannot migrate or configure an OMEGAMON® monitoring agent on z/OS earlier than v4.2.0 by using the PARMGEN method. See the *IBM Z Monitoring and Tivoli Management Services on z/OS: PARMGEN Reference*.

Software requirements for Tivoli Enterprise Portal, Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, and Tivoli Data Warehouse on distributed operating systems

Before you install the IBM Z OMEGAMON Network Monitor monitoring agent into an existing Tivoli Management Services environment, ensure that you have upgraded this environment to version 6.3.0 Fix Pack 2 or later.

Best practice: Version 6.3.0 Fix Pack 4 or later.

Detailed software requirements for all distributed components of the Tivoli Management Services are found in *IBM Tivoli Monitoring: Installation and Setup Guide*.

Software requirements for the enhanced 3270 user interface

To use the functionality provided by the enhanced 3270 user interface, you should install PTF UA66193 or later.

Best practice: PTF UA69205.

Software requirements for the Tivoli Enterprise Portal on z/OS

Detailed software requirements for a Tivoli Enterprise Portal running on z/OS are found in *IBM Z Monitoring and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*. Other environment planning decisions about the Tivoli Enterprise Portal on z/OS are also found in this book.

Software requirements for historical data collection and the Tivoli Data Warehouse

Software requirements for storing and retrieving historical data in the Tivoli Data Warehouse are found in *IBM Tivoli Monitoring: Installation and Setup Guide*.

Supported system authorization facility (SAF) products for a Tivoli Enterprise Portal on z/OS

Security on Tivoli Enterprise Portal on z/OS is based on password validation that uses the local operating system. You can use the Resource Access Control Facility (RACF®), which is part of the z/OS operating system, or another SAF product to provide user authentication.

In V5.1.0 and later of this monitoring agent, you can use the SAF security class that is defined for the runtime environment to control access to the IBM Z OMEGAMON Network Monitor commands, or you can use a separate security class. Unlike previous releases, these commands fail RACF authorization unless SAF security is configured. See "Authorizing users to issue Take Action commands" on page 56 for information about configuring SAF security for Take Action commands.

Supported versions of z/OS for the IBM Z OMEGAMON Network Monitor monitoring agent

z/OS systems on which zSeries monitoring agents such as IBM Z OMEGAMON Network Monitor are installed must be running z/OS V1.13 or later. For information about APARs required, see the *IBM IBM Z OMEGAMON Monitoring Suite: Program Directory*. For late-breaking information, see the Preventive Service Planning (PSP) bucket for this monitoring agent.

If you recently migrated to z/OS v2.1, you might find OMVS errors in the system log when you launch the IBM Z OMEGAMON Network Monitor monitoring agent. Be aware that as of z/OS V2R1, the ability to use default OMVS segments has been removed. All z/OS UNIX users or groups must now have OMVS segments defined for user and group profiles with unique user IDs (UIDs) and group IDs (GIDs).

Supported versions of Tivoli NetView for z/OS

If you want to use the Tivoli NetView dynamic workspace links (DWL) feature or launch the NetView packet trace feature from the IBM Z OMEGAMON Network Monitor monitoring agent, ensure that you are running IBM Tivoli NetView for z/OS. Versions 5.4, 6.1, 6.2, and 6.2.1 are supported.

Optional software

Tivoli NetView Performance Monitor V2R7 is provided as an optionally orderable, no-cost feature to support customers using SNA or moving from SNA to IP. Tivoli NetView Performance Monitor runs as a z/OS Communications Server application program. You can use Tivoli NetView Performance Monitor to collect and monitor performance data, collect accounting data, and determine problems in the network for SNA networks. NetView Performance Monitor is provided as part of the IBM Z OMEGAMON Network Monitor product package.

Supported hardware

Most of the hardware that is required to run IBM Z OMEGAMON Network Monitor is determined by operating system considerations.

For example, the requirements for the UNIX systems where parts of the IBM Tivoli Monitoring platform are running are determined by the operating system. For most hardware prerequisites, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

The following remaining prerequisites apply to IBM Z OMEGAMON Network Monitor product.

Requirements for z/OS systems where monitoring agents are deployed

IBM Z OMEGAMON Network Monitor monitoring agents can be deployed on any z/OS system that can run z/OS V1.13 or higher.

You must also ensure that you have adequate direct access storage device (DASD) space to accommodate the products you are installing. Before you install your OMEGAMON products, you must review the space requirements and considerations for an SMP/E installed environment to make sure that sufficient DASD storage is available.

Note: Program directories cover DASD requirements for SMP/E target and distribution data sets. You can also use the Job Generator (JOBGEN) Reallocation Facility to analyze your DASD requirements and compute your persistent data store requirements. Remember that you also have DASD requirements for runtime libraries and short-term history. Ensure that you define enough DASD for short-term historical data storage. See "Disk space requirements for historical data tables" on page 509 for more information about sizing your persistent data store. See http://www-01.ibm.com/support/docview.wss?uid=swg21417935 for information about the JOBGEN tool.

The *IBM Z OMEGAMON Monitoring Suite: Program Directory* contains the approximate DASD space requirements for IBM Z OMEGAMON Network Monitor. Be aware that this estimate presupposes that these products are installed as standalone applications. When multiple OMEGAMON products are installed into a shared CSI environment, DASD requirements can be less.

The *IBM Z OMEGAMON Monitoring Suite: Program Directory* provides the basic space requirements for the Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Portal, the Tivoli Enterprise Portal Server, and for the monitoring agents. These basic space requirements do not include additional space that is required for maintaining historical data files.

Because of the variations in design characteristics such as client distributed systems, system size, and number of managed systems, providing specific disk space requirements for historical data collection is difficult. You might want to experiment to determine how much space you need. Start out by using the default disk space requirements to configure the data store. Then observe how quickly space is used. Eventually you might want to allocate enough space so that maintenance procedures only need to run once a day. Use the information in "Disk space requirements for historical data tables" on page 509 to help determine how much space to allocate.

Requirements for OSA-Express adapters

You can use IBM Z OMEGAMON Network Monitor to monitor the performance of the OSA adapters in your environment. OSA-Express and OSA-Express2 (except OSA-Express2 10 Gigabit) adapters are supported by both OSA/SF and OSA-Express Direct SNMP.

For more information, see the following resources:

- The section on configuring the Open System Adapter in *Open System Adapter-Express Customer's Guide and Reference* (SA22-7476)
- *zEnterprise® 196, System z10®, System z9, and eServer zSeries Open Systems Adapter-Express Customer's Guide and Reference* (SA22-7935)
- "Starting the OSA adapter SNMP subagent" on page 23 and "Verifying the z/OS environment setup" on page 24 in this book

To support the latest version of the OSA-Express MIB, the Licensed Internal Code (LIC) levels of the OSA-Express adapters must meet the following criteria:

- If you are running the OSA module on an IBM eServer™ zSeries 900 or 800 system, you must have a licensed internal code (LIC) V3.33 or higher installed.
- If you are running the OSA module on an IBM eServer zSeries 990 processor or higher, all LIC levels are supported.
- Monitoring OSA-Express3 adapters requires the use of the OSA-Express Direct SNMP subagent (IOBSNMP).

The OSA-Express LIC level requirements are outlined at the following Web site: https://www.ibm.com/servers/resourcelink/lib03010.nsf/pages/osaLibrary?OpenDocument&pathID=&Start=1.

Planning for configuration

Several variables that affect planning decisions contribute to the amount of CPU, memory, and disk space used by IBM Z OMEGAMON Network Monitor and the Tivoli Management Services components.

Collecting, processing, and storing data consumes system and network resources. Several variables contribute to the amount of CPU, memory, and disk space used by IBM Z OMEGAMON Network Monitor and the OMEGAMON XE platform components. The amount of CPU, memory, and disk space used on each monitored system is dependent on the number of resources being monitored, how often performance data is collected and whether you choose to store historical data.

This section identifies options to consider while planning the configuration and deployment of this product to meet the needs of your enterprise. This chapter also provides information to consider when creating and modifying situations and workspaces.

Additional deployment and environment design recommendations are found in the *IBM Tivoli Monitoring: Installation Guide*, on the IBM Knowledge Center.

CPU usage for monitoring networks on z/OS systems

Total CPU usage attributed to running the IBM Z OMEGAMON Network Monitor monitoring agent includes the percentage of CPU used by the agent and the additional CPU usage resulting from collecting data.

Additional CPU usage is associated with the following activities:

- Using the z/OS Communications Server network management interfaces (NMI). As a result, you will notice a slight increase in the amount of CPU used by the TCP/IP address space.
- Querying SNMP MIBs. This activity is represented by processing incurred by OSNMPD. You must start an instance of the OSNMPD address space for each TCP/IP address spaces where OSA channels, LPARs and ports data is to be collected.
- Querying the IOASNMP or IOBSNMP subagent. The IOASNMP subagent OR the IOBSNMP subagent is required on systems where OSA channels, LPARs and ports data is to be collected. OSA-Express3 and OSA-Express4s adaptors are supported only with the OSA Direct Express® SNMP subagent (IOBSNMP).
- The z/OS Communication Server external I/O control (IOCTL) function calls are used to retrieve route information when the monitoring is running in an address space on z/OS 1.10 or later. SNMP was previously used to obtain this data. The change in data retrieval methods was made to reduce CPU utilization when a large number of routes are defined.

Note: Remember that the IBM Z OMEGAMON Network Monitor monitoring agent might not be the only application or user querying SNMP.

Understanding how real-time data is collected

Real-time data collection allows you to monitor performance of your network and system resources in an effort to resolve potential problems before they affect the user.

The IBM Z OMEGAMON Network Monitor monitoring agent is designed to collect z/OS TCP/IP and VTAM® performance data. You must run the monitoring agent on each LPAR being monitored. The agent monitors all of the TCP/IP address spaces running on the LPAR.

The monitoring agent can be used to collect several types of performance data, allowing you to monitor TCP/IP address spaces, TN3270 server sessions, High Performance Routing connections, Enterprise Extender connections, FTP sessions and transfers, OSA adapters, TCP/IP connections, interfaces, gateways, Communication Storage Manager, VTAM buffer pools, and VTAM environment. Performance data is collected using the z/OS Communications Server network management interface (NMI), by querying SNMP MIBs and using the VTAM Performance Monitor Interface. The IBM Z OMEGAMON Network Monitor monitoring agent is designed with performance in mind, providing an efficient mechanism for collecting large amounts of network performance data.

Total storage associated with real-time data collection, as shown in Table 1 on page 5, includes the storage used in the monitoring agent address space as well as the following dataspaces used during data collection:

Table 1. Names and sizes for data spaces used during data collection

Dataspace name	Size	Description
KN3ACTCS	928 MB	This data space is used to store data that has been collected using SNMP, Performance Monitor Interface data, data collected using the z/OS Communications Server network management interface (NMI), the z/OS Communication Server external I/O control (IOCTL) function data, and Take Action command data. The storage area is reused each time the monitoring agent performs a collection. The actual amount of storage used is determined by the number of resources being monitored.
N3TCPIP	2 GB	This data space is used to store data collected using the z/OS Communications Server network management interface (NMI). A maximum of 225 MB is used for VTAM data. A maximum of 225 MB for each TCP/IP address space is used for TCP/IP data. The storage area is reused each time the monitoring agent performs a collection. The actual amount of storage used is determined by the number of resources that are being monitored.
N3FTP	2 GB	This data space is used to store data collected for FTP sessions and transfers. A maximum of 256 MB is used for each TCP/IP address space. Over time, all 256 MB is used because each new row of data is added to the existing data. When all 256 MB has been used, the data space wraps and new data is written to the beginning of the storage area.
N3TN3270	2 GB	This data space is used to store data collected for TN3270 server sessions. A maximum of 256 MB is used for each TCP/IP address space. The actual amount of storage used is determined by the number of resources being monitored. One record for each active session and one record for each session that closed in the last 24 hours is stored in the data space.

The data spaces are created when the monitoring agent initializes and are deleted when the monitoring agent is stopped. The sizes are not configurable. However, the amount of storage used is determined by the number of TCP/IP address spaces and the types of data you configure the monitoring agent to collect.

Determining which systems and TCP/IP address spaces to monitor

All production LPARS and TCP/IP address spaces should be monitored because they represent the core of your business enterprise.

You might choose to collect data less frequently on some systems, especially non-production LPARs, to minimize the cost of monitoring your networks.

Since V4.2.0 and later, you can decide whether to monitor a TCP/IP address space on a per-address-space basis. To learn about this new feature and how to select not to monitor some TCP/IP address spaces, see Adding, changing or updating a monitored system definition.

Determining which types of real-time data to collect

The IBM Z OMEGAMON Network Monitor monitoring agent allows you to customize which network resources are monitored.

The monitoring agent includes two data collector components:

- The **TCPC** component that includes these data types:
  - TCP/IP Connection and Application Performance statistics collection
  - Routing Table statistics collection
  - TN3270 server statistics collection
  - IPSec security collection (if configured)
  - FTP data collection
  - Enterprise Extender and High Performance Routing statistics collection
  - Communications Storage Manager (CSM) buffer pools
  - OSA statistics
  - Interface statistics
  - Data Link Control (DLC) statistics
  - TCP/IP Stack layer statistics
- The **SNAC** component (if configured), including Buffer Pool and VTAM Environment data collection

By default, both of these components start automatically at startup and run for the life of the monitoring agent. Data collection for these components or any of the individual data types they include can be stopped and started between recycles using the KN3FCCMD commands. See "KN3FCCMD command reference" on page 220 for more information about stopping and starting collections of various types of data.

By default, the IBM Z OMEGAMON Network Monitor monitoring agent is configured to monitor all resources. The monitoring agent always collects a required minimum amount of real-time data. You may choose to disable one or more of these data types. The following tables show the storage costs for monitoring the required and optional types of resources. These tables are provided to inform you of the relative size of attribute tables and the frequency in which data is collected. You might use this information to determine what to monitor: which types of resources, which systems and at what collection interval.

The monitoring agent monitors itself. Configuration and status information for the agent is displayed in the Agent Status workspace. This workspace is part of a special group of workspaces known as the *Agent and TCP/IP Subnode workspaces*. These workspaces include high-level views accessed from the Agent node in the Navigation tree that display configuration, status, and command execution information about the instance of the IBM Z OMEGAMON Network Monitor monitoring agent represented by the specified node. Data for these workspaces is stored in internal control blocks maintained by the agent. The data is gathered from the control blocks whenever a user navigates to one of these workspaces or refreshes the view for that workspace. There is no collection interval for this data. There is also no memory in a data space for this data. Status data for these workspaces is always available and cannot be disabled through configuration of any kind. Table 2 on page 7 shows the data gathered every time you display or refresh Agent and TCP/IP Subnode workspaces.

Table 2. Data collected every time the Agent or TCP/IP subnode workspaces are displayed or refreshed			
LPAR name			
Type of data	**Real-time data attributes group**	**Row size in bytes**	**Frequency per display/refresh**
Agent Subnode	KN3 Agent Status	224	1 row
	KN3 SNA Collector Status	104	1 row
	KN3 TCP Collector Status	756	1 row per monitored TCP/IP stack
	KN3 Take Action Command	596	A maximum of 33130 rows of data
	KN3 Take Action Command Response	312 Multiple rows of command responses can be associated with a given Take Action command. .	A maximum of 390427 rows of data.

The data shown in Table 3 on page 8 is collected once every collection interval and stored in memory (in a data space). The memory is reused each collection interval. When a user navigates to a workspace, a query will result in the monitoring agent retrieving the appropriate data from a data space. Use this table to calculate the memory usage by multiplying the row size by the number of resources. Add the numbers in the memory usage column to obtain the total memory used to hold data collected in an interval for a TCP/IP address space. Perform these calculations for each TCP/IP address space you are monitoring.

Table 3. Data collected once every collection interval				
LPAR name				
TCP/IP address space name				
Type of data	**Real-time data attributes table**	**Row size in bytes**	**Frequency per interval**	**Memory usage**
TCP/IP Stack Layer statistics	TCPIP Address Space	624	1 row per TCPIP address space	
	KN3 ICMP Global Counters	100	Up to 2 rows per TCPIP address space	
	KN3 ICMP Type Counters	80	Up to 2 rows per TCPIP address space	
	KN3 IP Counter Statistics	232	Up to 2 rows per TCP/IP address space	
	KN3 IP General Statistics	84	1 row per TCP/IP address space	
	KN3 TCP Counter Statistics	280	1 row per TCP/IP address space	
	KN3 UDP Counter Statistics	128	1 row per TCPIP Address Space	
	TCPIP Stack Layer	608	1 row per TCP/IP address space	
Interface statistics collection	TCPIP Devices	432	1 row per device	
	Interfaces	472	1 row per TCP/IP interface	
	KN3 Interface Address	132	1 row per TCP/IP interface address	
	KN3 Interface Statistics	304	1 row per active strategic TCP/IP interface (max 256)	
	KN3 Interface Status	344	1 row per TCP/IP interface	
Data Link Control statistics collection	KN3 Interface Read Queue	312	1 row per read queue per active OSA Queued Direction I/O (QDIO) or HiperSockets interface	
	KN3 Interface Write Queue	200	1 row per configured queue priority per OSA-Express Queued Direct I/O (QDIO) or HiperSockets interface	

Table 3. Data collected once every collection interval (continued)				
LPAR name				
TCP/IP address space name				
Type of data	**Real-time data attributes table**	**Row size in bytes**	**Frequency per interval**	**Memory usage**
OSA statistics collection	OSA Channels	416	1 row per OSA Channel	
	OSA-Express LPARS	106	16 rows per OSA Channel per LPAR per local channel subsystem	
	OSA-Express Ports	768	1 row per OSA channel of channel subtype: gigabitEthernet,fastEthernet or oneThousandBaseTEthernet per port	
	OSA 10 Gigabit Ports Control	390	1 row per OSA channel of channel subtype: tenGigabitEthernet per port	
	OSA 10 Gigabit Ports Errors	424	1 row per OSA channel of channel subtype: tenGigabitEthernet per port	
	OSA 10 Gigabit Ports Summary	480	1 row per OSA channel of channel subtype: tenGigabitEthernet per port	
	OSA 10 Gigabit Ports Throughput	420	1 row per OSA channel of channel subtype: tenGigabitEthernet per port	
	OSA-Express3 Ports Control	390	1 row per OSA channel of channel subtype: osaexp3gigabitEthernet, osaexp3oneThousandBaseTEthernet or osaexp3tenGigabitEthernet per port	
	OSA-Express3 Ports Errors	480	1 row per OSA channel of channel subtype: osaexp3gigabitEthernet, osaexp3oneThousandBaseTEthernet or osaexp3tenGigabitEthernet per port	
	OSA-Express3 Ports Summary	696	1 row per OSA channel of channel subtype: osaexp3gigabitEthernet, osaexp3oneThousandBaseTEthernet or osaexp3tenGigabitEthernet per port	
	OSA-Express3 Ports Throughput	484	1 row per OSA channel of channel subtype: osaexp3gigabitEthernet, osaexp3oneThousandBaseTEthernet or osaexp3tenGigabitEthernet per port	
	KN3 OSA-Express5S Ports Control	132	1 row per OSA channel of channel subtype: osaexp5StenGigabitEthernet per port	
	KN3 OSA-Express5S Ports Errors	252	1 row per OSA channel of channel subtype: osaexp5StenGigabitEthernet per port	
	KN3 OSA-Express5S Ports Summary	332	1 row per OSA channel of channel subtype: osaexp5StenGigabitEthernet per port	
	KN3 OSA-Express5S Ports Throughput	330	1 row per OSA channel of channel subtype: osaexp5StenGigabitEthernet per port	

Table 3. Data collected once every collection interval (continued)				
LPAR name				
TCP/IP address space name				
Type of data	**Real-time data attributes table**	**Row size in bytes**	**Frequency per interval**	**Memory usage**
TCP/IP and VTAM (required collection)”	TCPIP Memory Statistics	472	1 row per TCP/IP address space	
TCP/IP Connection and Application Performance statistics collection	TCPIP Applications	656	1 row per TCP/IP application	
	TCPIP Connections	632	1 row per TCPIP connection	
	TCPIP Details	616	1 row per TCP connection	
	TCP Listener	268	1 row per TCP listener	
	UDP Connections	360	1 row per UDP endpoint	
Routing Table statistics collection	TCPIP Gateways	600	1 row per TCP/IP gateway collected on Routing Table Collection Frequency	
IPSec Security Collection	IPSec Status	360	1 row per TCP/IP address space	
	Current® IP Filters	812	1 row per IP filter	
	Dynamic IP Tunnels	1024	1 row per dynamic IP tunnel	
	IKE Tunnels	664	1 row per IKE tunnel	
	Manual IP Tunnels	364	1 row per manual IP tunnel	

The data shown in Table 4 on page 10 is collected once every collection interval and stored in memory. This data is collected for each LPAR you monitor. The memory is reused each collection interval. Use this table to calculate the memory usage by multiplying the row size by the number of resources. Total the memory usage column to obtain the total memory used to hold data collected in an interval for these resources.

Table 4. Data collected for each monitored LPAR				
LPAR name				
Type of data	**Real-time data attribute group**	**Row size in bytes**	**Frequency per interval**	**Memory usage**
TCP/IP and VTAM (required collection)	VTAM Summary Statistics	72	1 row	
Enterprise Extender (EE) and High Performance Routing (HPR) statistics collection	EE Connections	248	1 row per EE connection	
	EE Connections Details	240	5 rows per EE connection	
	HPR RTP Connections	568	1 row per HPR RTP connection	
Communications Storage Manager (CSM) buffer reporting	CSM Storage	176	1 row	
	KN3CSM Storage by Owner	168	1 row per address space that owns CSM storage	

Table 4. Data collected for each monitored LPAR (continued)				
LPAR name				
Type of data	**Real-time data attribute group**	**Row size in bytes**	**Frequency per interval**	**Memory usage**
Buffer Pool and VTAM Environment data collection	VTAM Address Space	244	1 row	
	VTAM I/O	72	1 row for each of 6 resources	
	VTAM Buffer Pools	154	1 row for each of 14 resources	
	VTAM Buffer Pool Extents	96	1 row per buffer pool extent	
	VTAM Buffer Usage by Address Space	72	1 row per address space using IO00 or CRPL buffers	
	VTAM Buffer Usage by Application	80	1 row per application per address space using IO00 buffers	
	VTAM Buffer Usage by Category	68	1 row for each of 12 resources	

The FTP data shown in Table 5 on page 11 is collected when a new session or transfer is opened or when an existing session or transfer is closed. This data is collected when z/OS Communications Server notifies the monitoring agent that data is available and therefore does not adhere to a collection interval. As explained previously, new records are appended to the previously collected data until the table in the data space is full, at which time the table wraps. Therefore, over time 256 MB per TCP/IP address space will be used to hold FTP data.

This data is collected for each TCP/IP stack where FTP is running.

Table 5. FTP data collected				
LPAR name				
TCP/IP address space name				
Type of data	**Real-time data attribute group**	**Row size in bytes**	**Frequency**	**Maximum rows stored**
FTP Data Collection	FTP Sessions	384	2 rows per FTP session	25,000
	TCPIP FTP	2464	2 rows per FTP transfer	100,000

The TN3270 session workspaces display information about open, closed and active TN3270 sessions for a TCP/IP address space. Data for open and closed sessions is provided when z/OS Communications Server notifies the monitoring agent that data is available and therefore is not driven by a collection interval. Data for active sessions is collected once per collection interval.

Memory used to store data for one session is reused for the same session each collection interval and for the data collected when the session is closed. Approximately 24 hours after a session is closed, the memory used to hold that session's data will be made available for a new session.

Use Table 6 on page 12 to calculate the memory usage by multiplying the row size by the number of resources. Total the memory usage column to obtain the total memory used to hold TN3270 data collected for a TCP/IP address space. Perform these calculations for each TCP/IP address space you are monitoring.

Note: The TN3270 Response Time Buckets table is not collected or stored as a separate table. Instead, it is a different view into the TN3270 Server Sess Avail table. When a query is issued to retrieve TN3270 Response Time Buckets data, the appropriate TN3270 Response Time Buckets rows (one row for each of

the five response time buckets) are created from the corresponding row in the TN3270 Server Sess Avail table.

Table 6. TN3270 data collected

LPAR name				
TCP/IP address space name				
Type of data	**Real-time data attribute table**	**Row size in bytes**	**Frequency**	**Maximum rows stored**
TN3270 Server Statistics Collection	TN3270 Server Sess Avail	432	1 row per TN3270 server session that is active or was closed in the last 24 hours	
	TN3270 Response Time Buckets	204	0 rows	0

Use the PARMGEN configuration method or the z/OS `MODIFY` command to enable or disable data collection for specific types of data. See "KN3FCCMD command reference" on page 220 for more information about these commands.

Defining data collection intervals

The collection intervals control how often real-time data is collected. Each time you collect data, the monitoring agent incurs a certain amount of CPU usage. How much processing is incurred depends on the number and type of resources you monitor.

Collection intervals are specified in minutes and have a valid range of 1 to 60. The default value for a collection interval is 5 minutes. This default value satisfies the monitoring needs of many customers who require near "real time" access to data.

The collection intervals are specified with the PARMGEN method, or you can modify a collection interval by executing a `MODIFY` *`procname`*`,KN3FCCMD` command (see "KN3FCCMD command reference" on page 220 for more information about the MODIFY commands). Specify values for the following collection intervals:

- **KN3_TCP_SAMPLE_INTERVAL**: the collection interval used to control most of the data collection, with the exceptions that follow.
- **KN3_SNA_VTAM_SNAC_SNACINTV**: controls the Buffer Pool and VTAM Environment data collection. This interval is only used if you enter **Y** for **KN3_SNA_VTAM_COLLECT_DATA**.

The z/OS Communications Server network management interface (NMI) and Performance Monitoring Interfaces maintain performance information between collection intervals. For example, spikes are identified in such attributes as "Maximum Authorized Private Storage Allocated." Over- and under-utilization values are identified in such attributes as "Total Bytes Sent."

The network performance data displayed in the Tivoli Enterprise Portal is the latest collection interval; a user request to view data does not initiate a new data collection. Therefore, increasing the frequency of data collection (that is, decreasing the collection interval) by the monitoring agent generally results in your network operators viewing more recent data but results in higher CPU consumption by the monitoring agent. By decreasing the frequency of data collection (for example, from 5 to 15 minutes), you reduce the number of times per hour that the monitoring agent collects data (from 12 to 4 times per hour), thus reducing the total CPU consumption (by a factor of approximately 3).

You can further reduce the CPU consumption by changing the KN3_TCP_ROUTE_TBL_FREQ parameter using the PARMGEN method or on a `KN3FCCMD START ROUTE` command. See "KN3FCCMD command reference" on page 220 for information about this command. The KN3_TCP_ROUTE_TBL_FREQ parameter controls how often the Routing Table Statistics (Gateway table) are collected. By default, this data is collected once every 10 collection intervals (once every 50 minutes when the default collection

interval is used). The frequency does not affect the amount of storage used; it affects only CPU consumption.

Set the collection intervals and routing table frequency to meet your monitoring needs, ensuring that you are promptly alerted to problems so they can be resolved quickly. But, also be aware that each data collection comes with a cost in CPU usage.

Run IBM Z OMEGAMON Network Monitor and use Tivoli OMEGAMON XE on z/OS or the Resource Measurement Facility (RMF) to measure CPU usage. Adjust the collection intervals until you have achieved the desired balance between currency of data and CPU usage.

Defining display intervals

A display interval determines how long a session or transfer will be available for display at the Tivoli Enterprise Portal or OMEGAMON Enhanced 3270 user interface.

During configuration of the monitoring agent, specify values for FTP and TN3270 display intervals. The value is specified as a number of hours (1 to 24 are valid values). FTP and TN3270 workspaces display session and transfer information that was collected during the specified display interval. Note that some workspaces also have default query filters that will determine which data or how much data to display.

When a `MONITORGROUP` statement is included in a Telnet profile for z/OS Communications Server, the TN3270 server provides additional performance information about the TN3270 sessions that map to this group. Refer to "Enabling the z/OS Communications Server network management interface" on page 21. The IBM Z OMEGAMON Network Monitor agent collects this additional performance information each collection interval. Therefore, the active TN3270 sessions mapping to a monitor group would always be displayed, since the row for the TN3270 session is always within the display interval.

Setting a display interval to a lesser value might reduce the amount of CPU used by the monitoring agent when retrieving data for display at the Tivoli Enterprise Portal or OMEGAMON Enhanced 3270 User Interface. Similarly, setting a display interval to a higher value might increase the amount of CPU usage. Balance your need to view data for sessions or transfers that occurred up to 24 hours ago with the CPU usage.

An alternative to increasing the display interval is to enable historical collection for the data table and viewing historical data instead of real-time data in the Tivoli Enterprise Portal or OMEGAMON Enhanced 3270 User Interface. See the *IBM Z OMEGAMON Network Monitor: Tivoli Enterprise Portal User's Guide* for more information about the display intervals used for FTP and TN3270 workspaces.

Defining and running situations

Situations are used to identify monitored resources that meet certain performance criteria, raising an alert when the criteria is met.

A situation definition includes a sampling frequency, a set of conditions, and a list of monitored systems. Each of these situations has implications on CPU and storage consumption. Also, the cumulative effect of all the active situations has implications on performance.

IBM Z OMEGAMON Network Monitor provides 100 predefined situations (none of which are autostarted) to detect some of the most common mainframe network problems. Autostarted situations run automatically when the IBM Z OMEGAMON Network Monitor monitoring agent is started. See the *IBM IBM Z OMEGAMON Network Monitor: Tivoli Enterprise Portal User's Guide* for a list and description of the product-provided situations. If you are upgrading from a previous version of this monitoring agent, then whatever customization and autostart settings you have on current situations are retained after upgrading.

A situation can include a Take Action command that runs when the situation is triggered. By using a Take Action command, you can automate a response to a specific system condition. In addition, each situation can include text describing the probable cause and expert advice that helps you to address and resolve problems quickly.

Any triggered situation raised by IBM Tivoli Monitoring or any of the OMEGAMON XE monitoring agents can be forwarded to the Netcool® OMNIbus Event List. IBM Tivoli Monitoring and the OMEGAMON agents monitor systems and can proactively alert you to warnings or detect critical situations when they occur.

Those alerts or situation events can be forwarded by means of the Event Integration Facility, (EIF). The Netcool OMNIbus Event List shows details like the severity of the event, (Warning, Critical, informational) and the status, (open, closed, acknowledged). The capability to drill down into the event to determine what thresholds were exceeded or which parts of the network are affected is available with Event Integration. If the Netcool OMNIbus user determines that the problem is being addressed, the user can acknowledge it, attach a journal entry, or close the event. The user can also escalate events or suppress escalation.

When planning for configuration and deployment of IBM Z OMEGAMON Network Monitor, evaluate all situations provided by the product. Determine which situations to autostart. If necessary, modify existing situations and create new situations to meet the needs of your enterprise.

For each situation that you choose to run, determine the importance and therefore the desired sampling frequency. All situations that query a specific attribute table should be defined with the same sampling frequency to enable the OMEGAMON XE platform to group situations and thereby optimize performance.

For situations to be grouped, they must be active when the hub Tivoli Enterprise Monitoring Server starts (autostarted), have the same sampling frequency, and test conditions on attributes in the same attribute table.

Verify that the conditions evaluated by each situation are appropriate for your environment. Check both the set of conditions and individual conditions. The predefined situations attempt to use the most efficient means to identify problems. There might be alternative conditions that identify the same problems but are less expensive to evaluate in your environment. Ensure that the values being checked are correct for your environment.

After you modify situations that are auto-started, stop and start the hub Tivoli Enterprise Portal. The process of combining situations occurs only during initialization of the hub Tivoli Enterprise Portal.

Understanding how historical data is collected

Before you can configure historical data collection, understand the difference between short-term and long-term historical data and how both are collected.

Historical data collection is an optional feature that is enabled using the Tivoli Enterprise Portal or OMEGAMON Enhanced 3270 User Interface. The OMEGAMON platform provides the following types of historical data collection:

- Short-term historical data is stored in the persistent data store on z/OS systems or in files on distributed systems. To optimize performance, configure the persistent data store at the monitoring agent, meaning that you will have a persistent data store on each z/OS system you are monitoring.

  Short-term historical data typically refers to data that is stored for 24 hours or less. However, the amount and age of the short-term data that is retained depends on the number of resources being monitored and the amount of disk space configured for use by the persistent data store.
- Long-term historical data is stored in the Tivoli Data Warehouse. The long-term history database can retain data collected by IBM Z OMEGAMON Network Monitor monitoring agents for as long as you like (days, weeks, months or years).

Short-term historical data is best used for analysis during problem determination. Additional prerequisite software is not required for short-term historical data collection, however the data sets used by the persistent data store must be configured using the PARMGEN configuration method.

Long-term historical data is better used for trend analysis and to determine workload balance. See the chapter about configuring the warehouse proxy for Tivoli Data Warehouse in the *IBM Tivoli Monitoring: Installation and Setup Guide* for the list of supported databases, releases and operating system platforms. Long-term history also requires installation of the warehouse proxy software (provided) and configuration of an Open Database Connectivity (ODBC) connection. Use the warehouse proxy installation default support for defining database tablespaces and creating the ODB connection. Short-term historical data collection must be enabled and configured if you want to perform long-term historical data collection.

After historical data collection is enabled, an icon is displayed in qualifying views in Tivoli Enterprise Portal workspaces. Allow time for historical data to be stored, to produce meaningful reports. You can click this icon to extend any existing Tivoli Enterprise Portal view (also called a report) to include historical data. Tivoli Enterprise Portal reports automatically pull data from short-term and long-term history, based upon the time period you specify for the report.

The collection interval for historical data can be configured to be different from the collection interval for real-time data. To avoid excessive processing activities and decrease storage consumption, historical data collection is typically performed less frequently than real-time data collection. You can configure a short-term historical data collection interval of 1, 5, 15, 30 or 60 minutes or 1 day.

Writing the data to long-term history can be configured for 15 or 30 minutes or 1, 12, or 24 hours. If you configure long-term history, use a warehousing interval of 1 hour to avoid transferring 24 hours worth of historical data at one time. This shorter interval reduces the duration of CPU usage associated with writing data to the warehouse by spreading the writing across 24 periods.

The following example illustrates the rate of accumulation of historical records, assuming the following intervals have been specified:

- **Real-time data collection interval:** 5 minutes
- **Short-term historical data collection interval:** 15 minutes
- **Long-term warehousing interval**: 1 hour

1. At 1:57, data collection is initiated for 1 TCP/IP Address Space.
2. One row of data (512 bytes) is collected at 1:57, another row at 2:02, another at 2:07, 2:12, 2:17, and so on. Only the current row of data is stored because the old row is discarded when a new row arrives. Because the real-time data collection interval is 5 minutes, 12 collections are made per hour.
3. At 1:58, collection of historical data is initiated for 1 TCP/IP Address Space.
4. One row of data (540 bytes) is stored in short-term history at 2:00, the second row is collected at 2:15, the third at 2:30, 2:45, 3:00, and so on. Short-term history uses the most recent collection and therefore does not initiate another data collection. The row stored at 2:00 would use the 1:57 collection. The row stored at 2:15 would use the 2:12 collection.
5. Because the short-term historical data collection interval is 15 minutes, 4 collections are made per hour. All measurements are stored for future use.
6. After one hour, all (4) rows of short-term historical data are transferred by the warehouse proxy to the long-term history SQL database.
7. After 24 hours, 96 (24 x 4) rows of data will be stored in the Tivoli Data Warehouse.

Determining which types of historical data to collect

When deciding which types of data to store in short-term and long-term history and how long to store it, you must recognize that data collection consumes CPU cycles and disk space.

Note: Long-term history is not displayed for the Enterprise_Networks workspaces and the following additional workspaces:

- Active TN3270 Server Sessions for Selected Port
- EE Connection Summary
- FTP Transfers for Session

The queries for these workspaces contain clauses that are not supported by Tivoli Data Warehouse. You can view long-term history for the same attribute groups from workspaces accessed from the physical navigator.

Writing data to short-term history is cost effective and typically much less costly than writing to long-term history. Retrieving short-term history data to display historical reports increases CPU usage at the hub Tivoli Enterprise Monitoring Server (monitoring server) and at the monitoring agent, when short-term history data is stored at the monitoring agent.

Short-term historical data is written to disk, typically performed at the monitoring agent, consuming CPU cycles on the z/OS monitoring agent system. Additional CPU cycles are used when the Warehouse Proxy extracts data from short-term history and transfers it to the Data Warehouse. If you have collected a large amount of data in short-term history, the extraction process will significantly increase the monitoring agent's CPU usage. Similarly, when a table contains thousands of rows, the retrieval process for a Tivoli Enterprise Portal display of historical data will significantly increase the monitoring agent's CPU usage.

Depending on your needs, you may configure historical data collection for only a subset of attribute tables. Using only a subset of attribute tables is an effective means for limiting storage and CPU consumption, particularly if you choose not to perform historical data collection for high volume attribute tables such as TCP connections or attribute tables with many bytes per row (many attributes), such as FTP transfers. Collect only data that you will use in historical reports. Collect those tables only as frequently as your enterprise needs. Selecting a less frequent historical collection interval (30 minutes instead of 15 minutes) will reduce both storage and CPU consumption.

The tables in the "Determining which types of real-time data to collect" on page 6 section allow you to calculate storage consumption based on real-time data collection. The information you gather for these tables also provide the basis for calculating the storage requirements for historical collection.

The additional storage cost for short-term historical data collection equals the number of bytes of real-time data storage, per row of data, plus 28 bytes. The additional storage cost for long-term historical data collection, in the Tivoli Data Warehouse, is the same number of bytes. To calculate storage associated with historical data, add 28 bytes to each row of real-time data. See "Disk space requirements for historical data tables" on page 509 for detailed calculations.

You can use this information as a basis for choosing which attribute tables to enable for historical collection. You can select individual attribute tables for historical collection, including specifying different historical collection intervals and warehouse intervals. Here is a list of attribute tables that are likely to have a large number of resources and therefore require higher amounts of storage and CPU consumption when enabled for historical collection

- TCPIP Connections
- TCPIP Details
- TN3270 Server Sess Avail
- TCPIP Devices
- Interfaces
- EE Connections
- EE Connections Details
- HPR Connections
- VTAM Buffer Pool Extents

If you choose to not collect all attribute tables, TCPIP Connections is a logical choice to omit. All of the data in TCPIP Connections is also available in TCPIP Details, TCP Listener and UDP Connections. This choice affects which workspaces can draw historical reports, but the data is there if needed for reporting.

By default historical reports retrieve up to 24 hours of data from short-term history. If your persistent data store is not allocated with sufficient space, you will not have 24 hours of short-term data to retrieve. Allocate your persistent data store to hold a full 24 hours of data or change the default of 24 hours. You may also want to change the default in order to retrieve less data from short-term history and more data from long-term history in order to reduce the CPU consumed by the monitoring agent to process queries for historical data. See "Tuning OMEGAMON XE components" on page 19 for information about how to change the default of 24 hours.

Because historical data accumulates, you must also determine how long you want to keep the data. Short-term history data in the persistent data store automatically wraps, and thus does not need to be maintained. You can also run a KPDXTRA job to write short-term history to flat files, for backup, or for analysis in a statistical or graphing package. See the *IBM Tivoli Monitoring: Administrator's Guide* for details on KPDXTRA.

Long-term history, in the Tivoli Data Warehouse, does not automatically prune old records. You must determine how much data to retain, and either use the database manager tools to manually delete old records or configure the IBM Tivoli Monitoring Summarization and Pruning agent to run automatically to delete old records.

For detailed instruction about setting up historical data collection, see the section on configuring your system for Tivoli Enterprise Portal in the *IBM Tivoli Monitoring: Installation and Setup Guide* book. Additional agent configuration information about the warehouse proxy is found in the *IBM Tivoli Monitoring: Administrator's Guide*. For information about reporting, see *IBM Tivoli Monitoring: User's Guide*.

Designing workspaces

When a user navigates to a workspace, one or more queries are processed by the OMEGAMON XE components in order to display the requested workspace. Those same queries are processed again when the user requests a refresh or periodically in the cases where the workspace is configured to refresh automatically.

When a user navigates to a workspace, one or more queries are processed by the IBM Z Monitoring components in order to display the requested workspace. Those same queries are processed again when the user requests a refresh or periodically in the cases where the workspace is configured to refresh automatically.

The workspaces and queries provided in the IBM Z OMEGAMON Network Monitor product have been designed with performance in mind. However, your environment and the resources you monitor might require customization of the product-provided workspaces and queries.

The following are tips to improve the performance for users viewing workspaces. See *IBM Z OMEGAMON Network Monitor: Tivoli Enterprise Portal User's Guide* to see the default filters provided for each workspace.

The query assigned to a chart or table view requests data from a particular attribute table. It runs when you open or refresh the workspace. The Tivoli Enterprise Portal Server sends the query to the hub Tivoli Enterprise Portal.

The hub Tivoli Enterprise Portal distributes the query to the appropriate monitoring agent or agents and aggregates the resulting rows. The Tivoli Enterprise Portal Server retrieves the results and holds the entire result set in memory. The Tivoli Enterprise Portal retrieves one page of the results to display and holds both the current and previous page in memory.

You can dramatically reduce the amount of data retrieved by doing the following:

- Reducing the number of rows or attributes retrieved
- Applying the same query to multiple views in a workspace
- Adjusting the auto-refresh rate
- **Reducing the number of rows retrieved**

  One of the best ways to improve the performance of queries is to reduce the number of rows retrieved. The Query Editor allows you to add filters that reduce the number of rows that are returned. You might want to change the existing filter values of a query or add filters to the query. For example, the Applications workspace contains a table view that displays all applications that have TCP/IP connections. You might be interested in only those applications that have active connections. You could customize the query by adding a filter in the Query Editor for "Active Connections" greater than 0. See *IBM Z OMEGAMON Network Monitor: Tivoli Enterprise Portal User's Guide* to see the default filters provided for each workspace.

  Do not confuse custom queries with view filters, which can also be invoked from the TEP properties dialog. View filters have no effect on reducing the CPU and storage consumption by the monitoring agent and actually increase the Tivoli Enterprise Portal client CPU consumption.

  View filters are applied by the client and affect only the current page. If more than one page is returned by the query, only a subset of the data is viewed on each page. Increasing the page size is an option

available in Tivoli Enterprise Portal. Increasing the page size typically provides more filtered data on each page, but increases the client's memory requirements because now the two pages per query stored at the client are larger. It is more efficient to filter in the queries.

- **Reducing the number of attributes retrieved**

  Most product-provided queries return all attributes. There might be 50 attributes in an attribute table, yet you might want to view only 25 of them. Creating a custom query to retrieve only those 25 attributes reduces Tivoli Enterprise Portal Server and client processing and memory requirements.

  For example, the IBM Z OMEGAMON Network Monitor applications attribute table contains 54 attributes. If you are creating a workspace that displays information about TCP applications, you are not required to select the 14 UDP attributes of the attribute table.

  Historical workspaces retrieve much more data than real-time workspaces. Accordingly, all of the queries used for predefined historical workspaces request only the most valuable subset of attributes on the source table. The queries used by predefined historical workspaces are good starting places for building better performing workspace views. See the *IBM Z OMEGAMON Network Monitor: Tivoli Enterprise Portal User's Guide* for more information about modifying or creating queries.

- **Applying the same query to multiple views in a workspace**

  Having multiple views in a workspace that retrieve data from different attribute tables is fine. But if you have a graph containing "Total Retransmissions" and a table containing "Transmit Segment Rate" (both available from the same attribute table), create one custom query for both views. By creating a single custom query, Tivoli Enterprise Portal will retrieve the data once for both views.

  The objective is to use only one query for each attribute table used in a workspace. When a workspace is displayed, the entire results set for each query is stored on the Tivoli Enterprise Portal Server. The 100 rows (default page size) from each query currently being viewed and the previous page of any pane viewed are stored on the Tivoli Enterprise Portal client.

- **Adjusting the auto-refresh rate**

  The operator can choose an automatic refresh rate from every 30 seconds to once per hour. Each time the workspace is refreshed, the data is retrieved from the data spaces that reside on the system where the monitoring agent is running. The happens only for the currently displayed workspace. Retrieving data from the agent consumes CPU so it is important to specify a refresh rate that meets your monitoring needs while avoiding unnecessary performance activities by the monitoring agent.

  When an operator clicks the **Time Span** button to display historical data, the auto-refresh rate defined for the workspace will continue to be used. The current auto-refresh rate can result in significant CPU consumption by the monitoring agent because the workspace is automatically refreshed (as frequently as once every 30 seconds). Consider changing the default auto-refresh rate to "On Demand" for workspaces that your users frequently use to display historical data.

For the enhanced 3270 user interface, you can edit the product-provided workspaces by copying an existing workspace and updating the attributes and the queries associated with it. See the "Customizing workspaces" topic in the *IBM Z Monitoring Suite and Tivoli Management Services on z/OS: OMEGAMON Enhanced 3270 User Interface Guide* to understand how to create workspaces for the enhanced 3270 user interface. You will also need to know **COLUMN** value for the attribute you want to code. This is found by locating the Object Definition Interchange (ODI) file for this monitoring agent. The KANDATV DD card points to the location of the KN3DOC file in your installation or you can look in the `Candle_Home\TEPS` directory for the dockn3 file. You need to search first on the name of the attribute group. See the mapping appendix of the *IBM Z OMEGAMON Network Monitor: Tivoli Enterprise Portal User's Guide* for the names of attribute groups. The same design principles discussed in this section apply to the design of 3270 workspaces.

Tuning OMEGAMON XE components

Once configuration is complete, you can tune some components to make them operate more efficiently. You can change data collection options, change the default value for short-term history, and tune Tivoli Data Warehouse.

This section includes some tuning information about the components of the IBM Z OMEGAMON Network Monitor monitoring agent that you might want to implement once the monitoring agent is installed.

- **Changing data collection options**

  While an IBM Z OMEGAMON Network Monitor monitoring agent is running, you can change the data that is being collected by using z/OS MODIFY commands to temporarily change how often data collection is performed.

  Using z/OS MODIFY commands, you can reduce the z/OS system resources used to monitor your networks while a larger than normal workload is being performed. You can also monitor more of your network resources while you are investigating a problem.

  Changes made using the z/OS MODIFY command are temporary. The next time that the monitoring agent is started, the agent reverts to the definitions made using the PARMGEN configuration method. In other words, the changes made using the z/OS MODIFY command are not retained when the monitoring agent is stopped.

  Changes associated with the tolerate TCP/IP recycle option reimplement the configured monitoring options whenever the state of a network monitoring interface (NMI) AF-UNIX socket changes, which may further reduce the effects of changing the monitoring options using the command line interface. Monitoring options that require permanency should be made using the PARMGEN configuration method.

  The following z/OS operator command causes the monitoring agent to stop collecting applications and connections data from the TCP/IP address space named TCPIPB.

  ```
  MODIFY proc_name,KN3FCCMD STOP CONN TCPNAME(TCPIPB)
  ```

  The output from this command is:

  ```
  KLVOP191   'KN3FCCMD STOP CONN TCPNAME(TCPIP)' KN3C115I STOP FOR
    COMPONENT CONN ACCEPTED.
  TCPNAME: TCPIP KN3FC000 KN3FCCMD PROCESSING COMPLETE
  ```

  Note: After you have issued this command, you might experience a delay (the default is up to 30 minutes) before this output is written to RKLVLOG. To see the output immediately, enter the following z/OS operator command:

  ```
  MODIFY proc_name,FLUSH
  ```

  To reset to the data collection you specified during configuration of the monitoring agent, you can either stop and start the started task procedure or issue the following z/OS operator commands to stop all data collection and start the data collection as configured using the PARMGEN configuration method:

  ```
  MODIFY proc_name,KN3FCCMD STOP TCPC
  MODIFY proc_name KN3FCCMD START TCPC
  ```

  See “KN3FCCMD command reference” on page 220 for detailed information on the z/OS MODIFY command support.

- **Tuning the TMS:Engine LIMIT value**

  IBM Tivoli Management Services: Engine (TMS:Engine) is a common component for both the Tivoli Enterprise Monitoring Server and for IBM Z OMEGAMON Network Monitor Monitoring. It has startup parameters that are defined with appropriate defaults for many customer environments, and these parameters are defined in the data set pointed to by the RKLVIN DD statement in the started task procedure.

  If you see this message:

```
KN3I008E CALL TO ADDDATA FUNCTION FAILED, RETURN CODE=retcode, FOR TABLE=table
```

An error has occurred when the monitoring agent tried to return data for the table specified by the table variable and failed. The most common cause of this error is a query that returns a large number of rows of data, causing an out-of-memory condition.

Options are to either modify the query so that it returns fewer rows of data or change the LIMIT and MINIMUM values in *&rhilev..&midlev.*RKANPARU.

The current recommendation for the IBM Z OMEGAMON Network Monitor Agent is MINIMUM(768000,X) and LIMIT(24,X) as specified in member (KN3SYSIN). The current recommendation for the Tivoli Enterprise Monitoring Server in (KDSSYSIN) is MINIMUM(768000,X) and a LIMIT value of 24 or greater.

The LIMIT parameter can be used to specify the largest block of primary storage or extended storage that can be allocated. The syntax for setting the largest block of extended storage is shown in the example (note that setting the limit for primary storage is not recommended): LIMIT(n,X)

This value is specified in bytes, as a power of 2. For example, if n is 22, the largest block that can be allocated is 4 MB. If the LIMIT value is too small and a process in ITMS:Engine attempts to allocate a block of storage larger allowed by LIMIT, a program interruption U0100 or U0200 results When managing a large number of connections or TN3270 sessions, use a value of LIMIT (25,X) or greater.

- **Changing the default value for short-term history from 24 hours**

  By default, historical data from the last 24 hours is retrieved from the persistent data store for display at the Tivoli Enterprise Portal. Historical data from earlier time periods is retrieved from the Tivoli Data Warehouse.

  You can alter this default by modifying the KFW_REPORT_TERM_BREAK_POINT environment variable in the kfwenv file on the Tivoli Enterprise Portal Server. Information about the environment variable is found in *IBM Tivoli Monitoring: Administrator's Guide*. This variable is specified in seconds. The default is **86400** (= 60 seconds * 60 minutes * 24 hours). Increasing this value will result in historical data being retrieved from the persistent data store for time periods farther in the past. Decreasing this value will result in historical data being retrieved from the Tivoli Data Warehouse for more recent time periods.

  You might want to increase the value of this environment variable if you have not implemented Tivoli Data Warehouse. By increasing the value, you can view more historical data, assuming the persistent data stores are allocated large enough to contain more than 24 hours of data.

  You might want to decrease the value of this environment variable if you configured the warehouse interval to be one hour. By decreasing the value, you can view all historical data with smaller persistent data stores.

- **Tuning considerations for the Tivoli Data Warehouse**

  The default database manager settings provided by DB2® may not be sufficient to support warehousing of large amounts of monitor data from IBM Z OMEGAMON Network Monitor. Review the appendix "Relational database design and performance tuning for DB2 database servers" appendix in the *IBM Tivoli Monitoring: Administrator's Guide* to learn about DB2 tuning considerations.

Planning security

As you plan the configuration of this monitoring agent, understand how security is provided.

Security for monitoring agents, such as IBM Z OMEGAMON Network Monitor, is provided by Tivoli Management Services through the local system registry or an external, LDAP-enabled registry.

Access to the Tivoli Enterprise Portal is controlled by user accounts (user IDs) defined to the portal server. In addition to defining the user IDs that are authorized to log on to the Tivoli Enterprise Portal, these accounts define the permissions that determine the Tivoli Enterprise Portal Server features a user is authorized to see and use, the monitored applications the user is authorized to see, and the Navigator views (and the highest level within a view) the user can access. An initial **sysadmin** user ID with full administrator authority is provided at installation so you can log in to the Tivoli Enterprise Portal and add

more user accounts. No password is required to log on to the Tivoli Enterprise Portal unless user authentication is enabled.

Authentication of user IDs can be enabled through the hub Tivoli Enterprise Monitoring Server or through the Tivoli Enterprise Portal Server. User IDs authenticated through the hub monitoring server can be authenticated by either the local system registry or an external LDAP-enabled central registry. User IDs authenticated through the Tivoli Enterprise Portal Server can be authenticated only by an external LDAP-enabled registry. User IDs that are required to make SOAP Server requests (including user IDs that issue CLI commands that invoke SOAP server methods) must be authenticated through the hub monitoring server. User IDs that require single sign-on (SSO) capability for launching into other IBM products must be authenticated through the portal server. LDAP authentication must be enabled through the portal server before SSO can be configured.

See the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide* for an overview of the security options. See *IBM Tivoli Management Services on z/OS: Configuring the Tivoli Enterprise Monitoring Server on z/OS* and the *IBM Tivoli Monitoring: Administrator's Guide* for instructions on setting various types of security.

In V5.1.0 or later, the new 3270 and existing Tivoli Enterprise Portal Take Action commands fail unless explicit security definitions are configured that enable these commands to be issued. Security for this monitoring agent's Take Action commands is implemented through direct SAF (System Authorization Facility) calls and is based on resource profiles. Both user ID and command are validated.

At the end of the configuration process for the IBM Z OMEGAMON Network Monitor monitoring agent, two additional agent-specific security tasks must be performed:

- "Define monitoring agent access to the network management interfaces and commands" on page 44
- "Give users authorization and resource access to run the VARY TCPIP DROP command" on page 46

Preparing your z/OS environment

These z/OS environment setup tasks must be completed on the z/OS system or LPAR where this monitoring agent is running.

To make the IBM Z OMEGAMON Network Monitor environment fully operational, you must perform some z/OS environment setup. The following setup operations must be performed on each z/OS system on which the IBM Z OMEGAMON Network Monitor monitoring agent will run.

Enabling the z/OS Communications Server network management interface

One of the configuration steps you must perform on every z/OS system where the monitoring agent will be running is to enable the z/OS Communication Server network management interface for FTP, TN3270, SNA, and IPSec.

z/OS Communication Server provides a set of network management interface (NMI) APIs that allow network management applications to programmatically obtain data in real time. To enable these interfaces to collect specific data types, you must update your TCP/IP profile and your VTAM start list.

Enabling FTP and TN3270 monitoring

Update your TCP/IP profile to include the following statement to activate the profile configuration options for FTP and TN3270 monitoring:

```
NETMONitor SMFService
```

See the *IBM z/OS Communications Server: IP Configuration Reference* (SC31-8776) for more information about this statement.

If you modify the TCP/IP profile, you must stop and start TCP/IP for the changes to take effect.

Note: You can also use the `VARY TCPIP,,OBEYFILE` command to dynamically enable the real-time SMF information service. See the *IBM z/OS Communications Server: IP System Administrator's Commands* (SC31-8781) for information on how to use this command.

If you wish to collect TN3270 response time data, ensure that the BEGINVTAM block of your Telnet profile includes a MONITORGROUP statement that applies the monitoring characteristics required by the IBM Z OMEGAMON Network Monitor monitoring agent to the set of resources in your organization that requires Telnet support. The MONITORGROUP statement defines the parameters for monitoring the performance of connections mapped to this group. At a minimum, this statement must include these parameters: AVERAGE (indicates whether sliding averages should be calculated) and BUCKETS (indicates whether time buckets are being used), as in this example:

```
MONITORGROUP MONGRP1
   AVERAGE
   BUCKETS
ENDMONITORGROUP
MONITORMAP  MONGRP1 Client_Identifier
```

where *Client_Identifier* is one of the client identifier types supported by z/OS Communications Server. For more information about supported client identifiers, see the "Client identifier types and definitions" topic in the *IBM z/OS Communications Server: IP Configuration Reference* (SC31-8776).

Note: Ensure that you specify *Client_Identifier* in a way that enables you to collect TN3270 response time data for the desired sessions. See also the "No data in FTP and TN3270 workspaces" topic in the *IBM Tivoli IBM Z OMEGAMON Network Monitor: Troubleshooting Guide*.

To retrieve data for all TN3270 sessions, you can use the IPGROUP parameter, as shown in this example:

```
IPGROUP IPALL 0.0.0.0:0.0.0.0 ENDIPGROUP
MONITORGROUP MONGRP1
AVERAGE
BUCKETS
ENDMONITORGROUP
MONITORMAP  MONGRP1 IPALL
```

Enabling SNA monitoring

Update your VTAM start list (ATCSTRxx, if LIST=xx entered) to activate Communications Storage Manager (CSM), Enterprise Extender (EE), and High Performance Routing (HPR) monitoring. Include the following statement to activate the SNA NMI:

```
SNAMGMT=YES
```

If you modify the VTAM start list, you must stop and start VTAM for the changes to take effect.

Note: You can also activate the SNA NMI dynamically using the following MODIFY command:

```
F <vtam_procname>,VTAMOPTS,SNAMGMT=YES
```

where *<vtam_procname>* is the name of your VTAM procedure where the SNA NMI is to be activated. The response should look similar to the following example, indicating that the MODIFY statement was accepted:

```
IST097I MODIFY ACCEPTED
IST223I MODIFY COMMAND COMPLETED
IST1925I SOCKET OPENED BY SNAMGMT SERVER SUBTASK
```

The MODIFY statement is in effect until you either restart VTAM or issue another MODIFY command to change this setting.

Enabling IPSec monitoring

IPSec is enabled in the TCP profile data set. If your organization is using IP Security, then this update to the TCP/IP profile data set should already have been made.

On each z/OS system where you will monitor IP filters and IPSec tunnels, the IKE daemon and Policy Agent daemon must be started. The NMI for IP filters and IPSec tunnels is available for monitoring agents without updating the TCP/IP profile.

Enabling SNMP manager functions

The SNMP manager agent and subagent must be active on every system where the monitoring agent is running.

The IBM Z OMEGAMON Network Monitor monitoring agent uses the Simple Network Management Protocol (SNMP) Management Information Base (MIB) to obtain TCPIP performance data. The IBM Z OMEGAMON Network Monitor monitoring agent requires that the SNMP manager agent and subagent be active. The chapter about SNMP in the *IBM z/OS Communications Server: Configuration Guide* (SC31-8775) explains the configuration procedure for running the TCP/IP SNMP agent and subagent. The chapter also explains how to automatically start the SNMP agent when TCP/IP starts.

The SNMP subagent, a task in the TCP/IP address space, is a z/OS UNIX system services application that communicates with the SNMP agent using an AF_UNIX socket. Consequently, the AF_UNIX domain must be configured in your BPXPRMxx member of SYS1.PARMLIB. Consult the BPXPRMxx chapter in the *IBM MVS Initialization and Tuning Reference* for details about activating the AF_UNIX domain.

If your SNMP agent and subagent are not already configured and running, use the information in the *IBM z/OS Communications Server: Configuration Guide* to configure them. Steps 3 and 4 under "Verifying the z/OS environment setup" on page 24 tell you how to verify that this setup was performed correctly.

This setup is only part of the SNMP configuration task. The second part is performed after the monitoring agent is installed. The PARMGEN configuration method creates sample SNMP system definition files and stores them in *&hilev.&midlev.&rtename.*RKANSAMU. These sample files are named KN3SNMP. Edit the SNMP system definition file or files to add a configuration statement for each SNMP agent from which data will be collected (one per TCP/IP stack). You must create this configuration file and save it to the correct location before you can monitor and collect TCP/IP data using the SNMP agent and subagent.

- See "Format of the SNMP configuration file" on page 543 for more information about the format of the KN3SNMP configuration file.
- See "Configuring the IBM Z OMEGAMON Network Monitor SNMP manager functions" on page 51 for more information about SNMP validation in the "Complete the configuration" process for the IBM Z OMEGAMON Network Monitor monitoring agent.

Starting the OSA adapter SNMP subagent

Follow these steps to start the OSA adatper SNMP subagent.

About this task

You can use IBM Z OMEGAMON Network Monitor to monitor the performance of the OSA adapters in your environment. The OSA data is obtained from z/OS Communications Server SNMP subagents. Before you can collect OSA data, either the OSA-Express Direct SNMP subagent, or the TCP/IP SNMP subagent and the OSA/SF application, must be configured and running. You should use the OSA-Express Direct SNMP subagent because it provides additional attributes not available from the TCP/IP SNMP subagent, and does not require the OSA/SF applications.

To enable the OSA data support, perform the following steps:

Procedure

1. Verify that the Licensed Internal Code of the OSA adapters meet the requirements listed in the *IBM Z OMEGAMON Network Monitor Program Directory*.
2. Configure and start the SNMP subagent.
   - **OSA-Express Direct SNMP subagent**

     The SNMP subagent for OSA-Express Direct SNMP subagent is started by using the cataloged procedure, IOBSNMP. A sample IOBSNMP procedure can be found in z/OS Communications Server target data set `hlq.SEZAINST`.
   - **TCP/IP SNMP subagent**

     To obtain the OSA data from the TCP/IP SNMP subagent, perform the following steps:

a. Configure the subagent TCP/IP profile statement, SACONFIG.
b. Configure and start the OSA/SF application (IOAOSASF) and the TCP/IP SNMP subagent (IOASNMP). Sample cataloged procedures for these applications can be found in the OSA/SF target data set `IOA.SIOASAMP`.

3. Configure your TCP/IP profile to match your OSA configuration.
   - If you are using the TCP/IP SNMP subagent for OSA adapter data, specify OSAENABLED and OSASF on the SACONFIG statement in your TCP/IP profile. Reserve a port on the PORT statement. For example:

     ```
     SACONFIG OSAENABLED OSASF 721 COMMUNITY public
     ```

   - Define the OSA adapter to TCP/IP using DEVICE and LINK or INTERFACE statements.
4. If you are using the OSA-Express Direct SNMP subagent for OSA adapter data, install the OSA MIB in the MIBS.DATA data set.

Results

For more information about configuring and starting the OSA subagent, see the following:

- The section on configuring the Open System Adapter in *z/OS Communications Server: IP Configuration Guide Open Systems Adapter-Express Customer's Guide and Reference* (SA22-7476).
- *Open Systems Adapter-Express Customer's Guide and Reference* (SA22-7935).
- OSA-Express MIB support is described at **http://www.ibm.com/servers/resourcelink**. After logging in, select **Library**. Under **Library shortcuts**, select **Open System Adapter (OSA) Library**.
- The OSA Redbook *OSA-Express Implementation Guide* (SG24-5948) is available at **http://publib-b.boulder.ibm.com/abstracts/sg245948.html?Open**.

Verifying the z/OS environment setup

Several short commands can verify that you have your environment set up correctly.

About this task

Issue the following commands to confirm the environment setup:

Procedure

1. Verify that TCP/IP is configured correctly by issuing this command:

   ```
   D TCPIP,<tcpip_procname>,NETSTAT,CONFIG
   ```

   where *<tcpip_procname>* is the name of the TCP/IP stack that you want to monitor.

   These two lines should be included in the response that you receive:

   ```
   NETWORK MONITOR CONFIGURATION INFORMATION:
   PKTTRCSRV: YES   TCPCNNSRV: NO   SMFSRV: YES
   ```

   The correct value for SMFSRV is critical for IBM Z OMEGAMON Network Monitor. If you receive the response shown in the preceding example, then TCP/IP was configured successfully for the network management interfaces (NMIs) used by IBM Z OMEGAMON Network Monitor. If you plan to use NetView for z/OS packet trace feature, then the values for the PKTTRCSRV TCP/IP parameters should be **YES**.

2. Confirm that the SNA NMI is enabled by issuing this command:

   ```
   D NET,VTAMOPTS,OPTION=SNAMGMT
   ```

   SNA management is enabled if the following message is displayed:

```
IST1189I SNAMGMT = YES
```

3. Confirm that the z/OS Communications Server SNMP Agent, OSNMPD, is configured correctly.

   Note: If you have specified that OSA data should be collected using the PARMGEN method, then perform this step. If you have specified that OSA data should **not** be collected, then skip to Step "6" on page 26.

   Issue the z/OS UNIX snmp command from the UNIX System Services command line with the following syntax:

   ```
   snmp  –c <community_name> –h <host_name_name> -v  get sysUpTime.0
   ```

   where *<community_name>* and *<host_name_name>* are the SNMP community name and host name for the z/OS system where you will be running the IBM Z OMEGAMON Network Monitor monitoring agent. If OSNMPD is configured correctly, the sysUpTime value is displayed. This value is the time in seconds that OSNMPD has been active. If the command times out, OSNMPD is not configured correctly.

   For the TCP/IP SNMP subagent, issue the z/OS UNIX snmp command from the UNIX System Services command line with the following syntax:

   ```
   snmp –c <community_name> –h <host_name_name> -v get ibmMvsTcpipProcname.0
   ```

   where *<community_name>* and *<host_name_name>* are the SNMP community name and host name for the z/OS system where you will be running the IBM Z OMEGAMON Network Monitor monitoring agent. If the TCP/IP subagent is configured correctly, the name of the TCP/IP stack under which the subagent is running is displayed. If the command times out, or you receive a value of `noSuchName` or `noSuchObject`, then either OSNMPD is not configured correctly or the TCP/IP subagent is not active. Verify that the TCP/IP profile statement SACONFIG has been specified correctly.

   Note: Only one SNMP Agent should be started per monitored TCP/IP stack.

4. Verify that the SNMP subagent for OSA is started for each TCP/IP stack:

   - **OSA-Express Direct SNMP subagent**

     Issue the z/OS `D A,L` console command and verify that IOBSNMP is started. If the subagent is not started, start it. You can also look for this message on the console or in the JES log:

     ```
     IOB021I timestamp OSA SNMP subagent initialization complete.
     ```

     To determine which TCP/IP stack the message applies to, look for this message in the JES log:

     ```
     IOB028I timestamp Using stack name TCP_procname
     ```

     where *timestamp* is the time that the command was issued and TCP_procname is the name of the TCP/IP procedure used to start the stack.

   - **TCP/IP SNMP subagent and OSA/SF application**

     Issue the z/OS `D A,L` console command and verify that IOAOSASF and IOASNMP are started. If they are not started, start them.

5. Confirm that the SNMP subagent for OSA is correctly configured.

   - **OSA-Express Direct SNMP subagent**

     Issue the z/OS UNIX snmp command from the UNIX System Services command line with the following syntax:

     ```
     snmp  –c <community_name> –h <host_name_name> -v walk 1.3.6.1.4.1.2.6.188.1.1.1.1
     ```

     If you receive a "No valid PDUs returned" message, then the OSA-Express Direct SNMP subagent is not configured correctly.

   - **TCP/IP SNMP subagent**

Issue the z/OS UNIX snmp command from the UNIX System Services command line with the following syntax:

```
snmp  –c <community_name> –h <host_name_name> -v walk  ibmMvsOsaExpChannelNumber
```

If you receive a "No valid PDUs returned" message, then the TCP/IP SNMP subagent is not configured correctly.

6. On each z/OS system where you plan to monitor IP filters and IPSec tunnels, confirm that the IKE daemon and Policy Agent daemon have started. For each stack that you plan to monitor IP filters and IPSec tunnels, also confirm that IP security is enabled.

   a) Verify that the IKE daemon and PAGENT daemon have started by issuing this command:

   ```
   D A,L
   ```

   This command displays what is running on your system. Look at the output of this command and validate that the procedure names for the IKE daemon (IKED) and the Policy Agent (PAGENT) are listed. The output of this command will be similar to this:

   ```
   IEE114I 16.42.25 2009.119 ACTIVITY 312
     JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
    00005    00019    00001      00029    00010    00001/00300       00021
     LLA      LLA      LLA      NSW  S  VLF      VLF      VLF      NSW  S
     JES2     JES2     IEFPROC  NSW  S  VTAM     VTAM     VTAM     NSW  SO
     RACF     RACF     RACF     NSW  S  TSO      TSO      STEP     OWT  S
     TCPIP    TCPIP    TCPIP    NSW  SO TN3270   TN3270   TN3270   NSW  SO
     INETD4   STEP1    OMVSKERN OWT  AO SYSLOGD8 STEP1    OMVSKERN NSW  AO
     RXSERVE  RXSERVE  RXSERVE  OWT  SO OSNMPD   OSNMPD   OSNMPD   OWT  SO
     FTPD1    STEP1    OMVSKERN OWT  AO TCPCS2   TCPCS2   TCPCS2   NSW  SO
     OSNMPD2  OSNMPD2  OSNMPD   OWT  SO TCPCS4   TCPCS4   TCPCS4   NSW  SO
     TRMD1    STEP1    TRMD     IN   AO OSNMPD4  OSNMPD4  OSNMPD   OWT  SO
     TRMD1    STEP1    TRMD     OWT  AO IKED     IKED     IKED     NSW  SO
     PAGENT   PAGENT   PAGENT   OWT  SO IOBSNMP  IOBSNMP  IOBSNMP  OWT  SO
     CANSN3   CANSN3   AGENT    NSW  SO CANSDSST CANSDSST TEMS     NSW  SO
   ```

   Note the highlighted lines. You can also search the log for the following messages

   ```
   HASP373 PAGENT   STARTED
   IEF403I PAGENT - STARTED - TIME=15.09.32
   EZZ8431I PAGENT STARTING
   EZZ8432I PAGENT INITIALIZATION COMPLETE
   EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR image : type
   EZD1059I IKE CONNECTED TO PAGENT
   EZD1058I IKE STATUS FOR STACK stack_name   IS UP
   EZD1068I IKE POLICY UPDATED FOR STACK stack_name
   EZD1133I IKE STATUS FOR STACK stack_name    IS ACTIVE WITHOUT IPSECURITY
   SUPPORT
   EZD1128I IKE STATUS FOR STACK stack_name   IS ACTIVE WITHOUT POLICY
   EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR stack_name : IPSEC
   EZD1046I IKE INITIALIZATION COMPLETE
   EZD1058I IKE STATUS FOR STACK stack_name   IS UP
   EZD1068I IKE POLICY UPDATED FOR STACK stack_name
   ```

   If the daemons have not started, start them. See the *IBM z/OS Communications Server: IP Configuration Guide* (SC31-8775) for more information about the IKE daemon and Policy Agent daemon. If the stack is up but does not have security enabled, you would see the following message:

   ```
   EZD1133I IKE STATUS FOR STACK stack_name IS ACTIVE WITHOUT IPSECURITY
   ```

   b) Verify that IP security is enabled for a stack by issuing this command

   ```
   D TCPIP,<tcpip_procname>,NETSTAT,CONFIG
   ```

   The response from this command includes information about the IP configuration table and the IPv6 configuration table. Search for IPSECURITY in these sections. A value of **YES** indicates that IP

security is enabled for IPv4, IPv6, or both. Here, for example, is an excerpt from a response that indicates IP security is enabled for IPv4 and not for IPv6:

```
IP CONFIGURATION TABLE:
FORWARDING: YES    TIMETOLIVE: 00064  RSMTIMEOUT:  00060
IPSECURITY: YES

...

IPV6 CONFIGURATION TABLE:
FORWARDING:    YES  HOPLIMIT:   00255  IGREDIRECT:  NO
SOURCEVIPA:    NO   MULTIPATH:  NO     ICMPERRLIM:  00003
IGRTRHOPLIMIT: NO
IPSECURITY: NO
```

Defining monitoring agent access to the NMI and commands

Edit and run the KN3UAUTH job to give the monitoring agent access to the commands used to collect data and the commands issued on behalf of Tivoli Enterprise Portal and Enhanced 3270 UI users.

Some security configuration is required to grant the IBM Z OMEGAMON Network Monitor monitoring agent access to the z/OS Communications Server network manager interface (NMI) application programming interfaces and to commands. The monitoring agent must have access to one or more of these management interfaces depending on the data you want collected:

- SNA network monitoring
- Local IPSec
- Real-time SMF data

The monitoring agent must also be given access to commands used to collect data and commands issued on behalf of Tivoli Enterprise Portal users. Give access to the monitoring agent by editing and running the KN3UAUTH job created in “Define monitoring agent access to the network management interfaces and commands” on page 44.

Chapter 2. Upgrade overview

The IBM Z OMEGAMON Network Monitor monitoring agent requires Tivoli Management Services V6.3 Fix Pack 2 or later applied. If you are not currently running at the required level, you must, at a minimum, upgrade the Tivoli Enterprise Portal desktop client, the Tivoli Enterprise Portal Server, and the hub Tivoli Enterprise Monitoring Server to V6.3 Fix Pack 2 before you install your first monitoring agent. Upgrade your monitoring agents and any Tivoli Enterprise Monitoring Server the agents report to. In addition, upgrade the Tivoli Data Warehouse components at the same time you upgrade the Tivoli Enterprise Portal Server. All OMEGAMON XE monitoring agents support a staged migration.

See the *OMEGAMON XE and Tivoli Management Services on z/OS: Upgrade Guide* for upgrade scenarios.

Upgrading to the new release

In addition to the common upgrade requirements documented in the *IBM Z Monitoring and Tivoli Management Services on z/OS: Upgrade Guide*, these technology updates might affect your upgrade plans.

Configuring a high availability hub and converting a static hub to a remote

If you intend to enable the self-describing agent (SDA) feature, and you have an agent configured to run in the hub monitoring server address space, configure a high availability (HA) hub on the LPAR and convert the static hub to a static remote monitoring server that connects to the new HA hub. In addition, you must reconfigure all the remote monitoring servers that connected to the previous hub to connect to the new HA hub.

For instructions on configuring an HA hub, see the *IBM Tivoli Monitoring: Configuring Tivoli Enterprise Monitoring Server on z/OS*.

To convert a static hub to a remote, you must make the following changes:

- Change TCP communication values for the monitoring server:
  - The name or IP address of the hub
  - The port of the HA hub
- Change the type of the local monitoring server type from hub to remote.
- Change the hub type that the remote connects to HA Hub.
- If the static hub was excluded from proxy eligibility, change it to proxy eligible.
- Set the virtual IP address type for connecting to the hub.
- Add TEMS network interface list support.

Complete the steps for scenario 4 in the *OMEGAMON XE and Tivoli Management Services on z/OS: PARMGEN Reference*.

Performing a staged upgrade

To make product upgrades easier, IBM Z OMEGAMON Network Monitor supports upgrading agents gradually, by allowing a mixture of monitoring agents of the current version and the previous version in the same environment.

You can deploy new monitoring agents to your z/OS systems along with older monitoring agents of the same product, during an upgrade transition period.

Important: To operate in a mixed environment, monitoring agents must have the correct maintenance applied. Check the IBM Z OMEGAMON Network Monitor Preventative Services Planning (PSP) bucket for the required PTFs.

Upgrade considerations for the IBM Z OMEGAMON Network Monitor monitoring agent

As you upgrade your IBM Z OMEGAMON Network Monitor monitoring agents from an earlier version to V5.6.0, use the following guidelines:

Upgrading a persistent data store

When you upgrade your Tivoli Enterprise Monitoring Server, the data set allocation values that were defined in a previous release will likely need to be changed.

Determine your persistent data store allocation values by using the information in "Disk space requirements for historical data tables" on page 509. If persistent data store allocation values need to be modified, delete any existing IBM Z OMEGAMON Network Monitor persistent data store data sets so that these data sets can be reallocated with the correct size during configuration of the product.

History situations that use the persistent data store operate correctly without change. The persistent data store automatically adds columns to short-term historical record when CATs, ATRs, and PDICTs are updated. No reformatting of the persistent data store data sets is required.

Migrating historical data in the Tivoli Data Warehouse for Tivoli Enterprise Portal

When you enable long-term historical collection for a table, the warehouse proxy creates tables in the Tivoli Data Warehouse.

The tables are created when long-term historical collection is first enabled for a table. When you upgrade to a new release of IBM Z OMEGAMON Network Monitor, the tables that were created in Tivoli Data Warehouse must be updated to contain columns for all the current attributes or the tables must be dropped from the Tivoli Data Warehouse.

Data in the Tivoli Data Warehouse is migrated automatically. No action on your part is required.

Upgrade issues related to SNMP configuration

To configure SNMP collection, you need to set up a configuration file for IBM Z OMEGAMON Network Monitor

The Simple Network Management Protocol (SNMP) engine used to collect data was modified in IBM Z Monitoring . An updated sample started task procedure for both of these products will be generated during configuration.

A sample SNMP configuration file is generated during the initial configuration of the monitoring agent. This file must be customized for your environment. The KN3SNMP DD card of your IBM Z OMEGAMON Network Monitor started task procedure must point to the SNMP configuration file. Failure to copy these updated started task procedures to your PROCLIB data set will result in the monitoring agent not collecting any SNMP data.

For more information about the format of the SNMP configuration file, see "Format of the SNMP configuration file" on page 543.

Upgrade issues related to running different product versions

Be prepared for some unanticipated behaviors in a mixed environment (not all components at the same level) that might be found during an upgrade.

Tivoli Management Services supports running a mixture of V4.2, V5.1, V5.3, and V5.6 monitoring agents in your environment during an upgrade period. The expectation is that a single Tivoli Enterprise Portal client can be used to monitor all systems, independent of the version of the monitoring agent.

At startup, the monitoring agents identify their versions with the Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal. The version determines the attributes that the monitoring agent can provide. This version identification enables the Tivoli Enterprise Portal to conditionally select version-specific objects for Managed System Lists, Situations, Queries, Policies, and Workspaces.

When users of the enhanced 3270 user interface run multiple versions of OMEGAMON agents during a staged upgrade period, they might experience operational limitations. The common upgrade guide summarizes related operational considerations by product. See the "Running the products in a mixed environment" topic in the *IBM Z Monitoring Suite and Tivoli Management Services on z/OS: Upgrade Guide* for more information.

Chapter 3. Configuring IBM Z OMEGAMON Network Monitor

You configure IBM Z OMEGAMON Network Monitor by accepting or customizing the values of parameters that begin with KN3.

You configure the IBM Z OMEGAMON Network Monitor component of the monitoring product to define enterprise-level entities, install product-specific data on the Tivoli Enterprise Monitoring Server, and register the IBM Z OMEGAMON Network Monitor monitoring agent to the Tivoli Enterprise Monitoring Server address space. You also configure the persistent data store for the product historical data and allocate the data sets to store enterprise data. These parameters are specified in the KN3 section of the PARMGEN configuration profile.

Default values are provided for all required parameters and some optional ones. If you do not want to customize these parameters, and you do not want to enable optional features, you can complete the configuration by accepting these defaults. Alternatively, you can specify custom values. You can also specify custom values for optional parameters that have no defaults. You must specify values for these parameters in order to activate those features.

For guidance on setting parameter values, see the following sources of information:

- Comments in the configuration profiles
- Online help for the configuration profile

  If the supplied KCIRPLBS macro has been copied to your SYSPROC concatenation, you can enter TSO KCIRPLBS at the ISPF command line to run the help macro. Place the cursor anywhere on the line that contains the parameter for which you want help text displayed, and press PF14.
- *IBM Tivoli OMEGAMON XE and IBM Tivoli Management Services on z/OS: PARMGEN Reference*
- *IBM Tivoli OMEGAMON XE and IBM Tivoli Management Services on z/OS: Common Parameter Reference*
- *IBM Z OMEGAMON Network Monitor: Parameter Reference.*

After you configure the IBM Z OMEGAMON Network Monitor agent using the PARMGEN method, complete the tasks listed in “Completing the configuration” on page 42.

Table 7. Tasks to complete before configuring IBM Z OMEGAMON Network Monitor

Configuration task	**Location of instructions**
Set up PARMGEN work libraries for the runtime environment.	*IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*
Set up the PARMGEN configuration profile for the runtime environment.	*IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*
Configure a Tivoli Enterprise Monitoring Server on z/OS.	*IBM Tivoli Management Services on z/OS: Configuring the Tivoli Enterprise Monitoring Server on z/OS* and *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Parameter Reference*

Table 7. Tasks to complete before configuring IBM Z OMEGAMON Network Monitor (continued)	
Configuration task	**Location of instructions**
(Optional) Configure the OMEGAMON enhanced 3270 user interface address space.	*IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide* **Note:** You only need to configure one OMEGAMON enhanced 3270 user interface address space. If you have already configured this address space for another version 5.1.0 OMEGAMON monitoring agent on z/OS, you do not need to repeat this configuration step.

Tip: If you are enabling self describing agents, configure a stand-alone high-availability hub monitoring server. Installing a high-availability hub lets you apply maintenance or upgrades without recycling the hub. If you have an existing static hub to which agents report, convert the hub to a remote and configure all the remotes to report to the new high-availability hub.

After you have configured IBM Z OMEGAMON Network Monitor (and any other agents you want to configure) using the runtime environment profile, you must complete several configuration tasks outside of the profile. See "Completing the configuration" on page 42.

Configuring the enhanced 3270 user interface using the PARMGEN method

You configure the Enhanced 3270 User Interface using the *rtename* configuration profile for the runtime environment.

To configure the interface, you can accept the defaults or specify site-specific values for the started task name, the VTAM node definition, and the VTAM applid in the following section:

```
* ****************************************************************
KOB$    BEGIN *----  Tivoli OMEGAMON Enhanced 3270 User Interface ----*
** ============================   ================================
** PARMLIB CONFIG Parameter       PARMLIB CONFIG Value
** ============================   ================================

** Tivoli OMEGAMON Manager (TOM) started task options:
KOB_TOM_STC                      CANSTOM    * STC name
KOB_TOM_VTAM_NODE                CTDOBN     * VTAM node
KOB_TOM_VTAM_APPL_LOGON          CTDOBAP    * VTAM logon applid

KOB$    END   *---- Tivoli OMEGAMON Enhanced 3270 User Interface ----*
```

where:

KOB_TOM_STC
Is the name of the interface started task.

KOB_TOM_VTAM_NODE
Is the name of the VTAM major node used by the Enhanced 3270 User Interface.

KOB_TOM_VTAM_APPL_LOGON
Is the VTAM logon applid used by the interface.

After configuring all the components and agents in the runtime environment, you complete the configuration by submitting the PARMGEN jobs and completing the required "Complete the configuration" steps. If you are configuring other products in this runtime environment, you can perform these steps after you completed all configuration. These steps include:

- Copy the OMEGAMON Enhanced 3270 User Interface started task from WKANSAMU to PROCLIB.
- Copy the VTAM major node from WKANSAMU to VTAMLST.
- Vary the VTAM major node active.
- APF-authorize the following load libraries (if this is a full runtime environment):

- &*hilev*.&*rte*.RKANMODU
- &*hilev*.&*rte*.RKANMOD
- &*hilev*.&*rte*.RKANMODP

See "Completing the configuration" on page 42 for more information about these tasks.

Note that if you run the WKANSAMU(KCIJcSYS) job (where *c* = P if SYSV is not enabled; V if SYSV is enabled), all the STCs and VTAM major nodes are copied to the system libraries that are specified for the GBL_DSN_SYS1_* parameter in the configuration profile. If you are using the global VTAM node (RTE_VTAM_GBL_MAJOR_NODE parameter), you can use the WKANSAMU(*cccc*APF) imbed member to VARY the node and APF authorize the load libraries. To use *cccc*APF, uncomment the placeholder INAPF INCLUDE statement in each started task:

```
//*****************************************************************
//* Uncomment out the INAPF statement if are using this composite
//* member to APF-authorize the libraries concatenated in the
//* STEPLIB and RKANMODL DDNAMEs.
//*INAPF INCLUDE MEMBER=CANSAPF
```

If you are using a local node, you must VARY the node active and authorize the libraries yourself.

IBM Z OMEGAMON Network Monitor configuration parameters

The parameters used by this monitoring agent for the PARMGEN configuration method are grouped logically in the configuration profile.

With the PARMGEN configuration method, you edit a comprehensive list of parameters for configuring all installed products and components. You then submit a series of jobs to create a complete runtime environment with the parameter values that you specified.

If you are an existing Configuration Tool user and already have a runtime environment, you can convert it to PARMGEN. See the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: PARMGEN Reference* for information about migrating to PARMGEN.

These parameters are found in the configuration profile, which can be generated from an existing RTE. If your installation is new or if you do not want to base the configuration profile on an existing RTE, a default configuration profile is provided and can be edited. Refer to the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: PARMGEN Reference* to understand the other scenarios for using PARMGEN.

In the configuration profile, the OMEGAMON XE parameters are organized into the groups found in Table 8 on page 36. The most important two groups of parameters for configuring this monitoring agent are the **Agent Parameters** that set the global values for all configurable parameters that are unique to this monitoring agent and the **Define TCP monitoring systems member** parameters that set the stack-specific values that override the global parameters. For comprehensive information about these parameters, see the *IBM Z OMEGAMON Network Monitor: Parameter Reference*

Table 8. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile

PARMGEN classification	**Parameters in this group**	**Explanation**
Additional IBM Z OMEGAMON Network Monitor Agent settings	• KN3_X_AGT_CONFIRM_SHUTDOWN • KN3_X_AGT_KDC_DEBUG • KN3_X_AGT_DEBUG_TRACE • KN3_X_AGT_LGSA_VERIFY • KN3_X_AGT_LSRPOOL_BUFFER_NUM • KN3_X_AGT_LSRPOOL_BUFSIZE • KN3_X_AGT_SDUMP_SVC_SYS1_DUMP • KN3_X_AGT_STORAGE_LIMIT_EXTEND • KN3_X_AGT_STORAGE_LIMIT_PRIMARY • KN3_X_AGT_STORAGE_RESERVE_EXT • KN3_X_AGT_STORAGE_RESERVE_PRI • KN3_X_AGT_STORAGE_STGDEBUG • KN3_X_AGT_TASKS_ATTACHED_NUM • KN3_X_SECURITY_USER_EXIT • KN3_X_SECURITY_RESOURCE_CLASS	Specifies settings for initializing Tivoli Monitoring: Services (TMS: Engine). These values are usually found in the KN3SYSIN member in the *rhilev*.*midlev*.*rtename*.RKANPARU library and are usually updated only with the assistance of IBM Software Support.
Advanced Agent configuration values	• KN3_AGT_FLUSH_LSR_BUFR_INT_HR • KN3_AGT_FLUSH_LSR_BUFR_INT_MIN • KN3_AGT_ICU_LANGUAGE_LOCALE • KN3_AGT_KGL_WTO • KN3_AGT_KLX_TCP_TOLERATERECYCLE • KN3_AGT_STORAGE_DETAIL_INT_HR • KN3_AGT_STORAGE_DETAIL_INT_MIN • KN3_AGT_STORAGE_MINIMUM_EXTEND • KN3_AGT_VIRTUAL_IP_ADDRESS • KN3_AGT_VTAM_APPL_NCS • KN3_AGT_WTO_MSG	Specifies a wide range of essential agent configuration parameters, including parameters that define where console messages are displayed, whether TCP/IP can be recycled, language of the interface, virtual addresses, and storage-related values.
Agent nonstandard parameters	• KN3_AGT_NSNEWn_VALUE • KN3_AGT_NONSTDn_DSN • KN3_AGT_NONSTDn_MBR • KN3_AGT_NONSTDn_PARM • KN3_AGT_NSOLDn_VALUE	Nonstandard parameters are customer-defined or hidden options that do not correspond to fields in the Configuration Tool interactive panels. This set of parameters defines the values required to establish a nonstandard parameter. Create these parameters under the guidance of IBM Software Support.

Table 8. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile (continued)

PARMGEN classification	Parameters in this group	Explanation
Agent parameters: TCP/IP information	• KN3_SNA_VTAM_COLLECT_DATA • KN3_SNA_VTAM_SNAC_SNACINTV • KN3_SNMP_CONFIG_FILE • KN3_TCP_ALLHPR • KN3_TCP_COLLECT_STACK • KN3_TCP_CONN • KN3_TCP_CSM • KN3_TCP_EEHPR • KN3_TCP_FTP • KN3_TCP_FTP_DSPINTV • KN3_TCP_GLBS • KN3_TCP_INTE • KN3_TCP_INT • KN3_TCP_IPSEC • KN3_TCP_OSA • KN3_TCP_ROUTE_TBL • KN3_TCP_ROUTE_TBL_FREQ • KN3_TCP_SAMPLE_INTERVAL • KN3_TCP_TN3270 • KN3_TCP_TN3270_DSPINTV • KN3_TCP_VIO_UNIT	Sets the global values for all configurable parameters that are unique to the IBM Z OMEGAMON Network Monitor monitoring agent.
Agent's Applids	• KN3_AGT_VTAM_APPL_AA • KN3_AGT_VTAM_APPL_KN3INVPO • KN3_AGT_VTAM_APPL_NCS • KN3_AGT_VTAM_APPL_OPERATOR • KN3_AGT_VTAM_APPL_CNM_SPO	Specifies the VTAM application IDs (applids) that the agent uses to define communication with the Tivoli Enterprise Monitoring Server. Applids are used for communication with the monitoring server, except for KN3_AGT_VTAM_ APPL_CNM_SPO, which is used to collect CNM data. These parameters are not used unless you are using SNA (instead of TCP/IP) to communicate with the monitoring server.
Agent's local TCP/IP information	• KN3_AGT_TCP_HOST • KN3_AGT_TCP_STC • KN3_AGT_TCP_KDEB_INTERFACELIST (If the Agent requires network interface list support) • KN3_AGT_PARTITION_NAME (If the Agent requires address translation support–optional)	Provides the TCP/IP information that the Tivoli Enterprise Monitoring Server uses to communicate with the monitoring agent.

Table 8. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile (continued)

PARMGEN classification	Parameters in this group	Explanation
Agent's local VTAM and logon information	• KN3_AGT_VTAM_APPL_PREFIX • KN3_AGT_VTAM_NODE	Specifies the values that are used by the agent for creating VTAM definitions specific to the monitoring agent.
Agent's primary TEMS TCP/IP information	• KN3_TEMS_TCP_HOST **Note:** KN3_TEMS_TCP_HOST and KN3_AGT_TCP_HOST must be the same value if KN3_TEMS_LOCAL _CONNECT_FLAG=Y (Agent connects to local TEMS).	Specifies the host name of the Tivoli Enterprise Monitoring Server that is specific to this monitoring agent. This field is required if this server is to communicate with agents using TCP/IP.
Agent's Primary TEMS VTAM information:	• KN3_TEMS_VTAM_LU62_DLOGMOD • KN3_TEMS_VTAM_LU62_MODETAB • KN3_TEMS_VTAM_NETID • KN3_TEMS_VTAM_APPL_LLB_BROKER	Specifies the VTAM information that is used by the Tivoli Enterprise Monitoring Server to communicate with the monitoring agent.
Audit parameters	• KN3_AGT_AUDIT_ITM_DOMAIN • KN3_AGT_AUDIT_MAX_HIST • KN3_AGT_AUDIT_TRACE	Specifies the amount of detail, maximum number of entries, and identifier for z/OS SAF tracing.
Define TCP monitoring systems member **Note:** Specify KN3_TCPXxx_* row for each TCP/IP monitored stack. Global default is $$$$ (monitor all TCP/IP stacks).	• KN3_TCPX • KN3_TCPXnn_OVRD_GLBS • KN3_TCPXnn_OVRD_INTE • KN3_TCPXnn_OVRD_INTS • KN3_TCPXnn_OVRD_OSA • KN3_TCPXnn_ROW • KN3_TCPXnn_SYS_NAME • KN3_TCPXnn_TCP_STC • KN3_TCPXnn_TCPIP_PROFILES_DSN • KN3_TCPXnn_OVRD_GLOBAL_FLAG • KN3_TCPXnn_OVRD_COLLECT_STACK • KN3_TCPXnn_OVRD_CONN • KN3_TCPXnn_OVRD_IPSEC • KN3_TCPXnn_OVRD_ROUTE_TBL • KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ • KN3_TCP_ROUTE_TBL • KN3_TCP_ROUTE_TBL_FREQ • KN3_TCPXnn_OVRD_FTP • KN3_TCPXnn_OVRD_FTP_DSPINTV • KN3_TCPXnn_OVRD_TN3270 • KN3_TCPXnn_OVRD_TN3270_DSPINTV • KN3_TCPXnn_TCPIP_PROFILES_MBR	Sets the stack-specific values that override the global parameters for all configurable parameters that are unique to the IBM Z OMEGAMON Network Monitor monitoring agent.

Table 8. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile (continued)

PARMGEN classification	Parameters in this group	Explanation
Define TN3270 Telnet session link user values	• KN3_TN3270_DXL_APPLID • KN3_TN3270_DXL_USERDATA	Specifies the IBM Tivoli NetView for z/OS user ID and password that IBM Z OMEGAMON Network Monitor logs onto dynamically. The applid is for the Tivoli NetView on z/OS application. The user data is the user ID and password that must be passed to NetView for z/OS to complete the login.
Enable self-describing agent processing	• KN3_AGT_TEMA_SDA	Specifies whether this monitoring agent plans to use the self-describing agent feature.
If the Agent requires address translation support	• KN3_AGT_PARTITION_NAME	Specifies the partition name that identifies the location of this TEMS (namespace) relative to the firewall(s) used for address translation.
If the Agent requires network interface list support	• KN3_AGT_TCP_KDEB_INTERFACELIST	Specifies a list of network interfaces that the monitoring agent uses. This parameter is required for sites that are running multiple TCP/IP interfaces or network adapters on the same z/OS image.
Persistent datastore table space allocation overrides	• KN3_PD • KN3_PD_CYL • KN3_PD_GRP • KN3_PD_ROW • KN3_X_PD_HISTCOLL_DATA_AGT_STC • KN3_X_PD_HISTCOLL_DATA_TEMS_STC	Specifies the information that is required for this monitoring agent to override the global RTE defaults for space allocation for the persistent data store libraries and for overhead information such as the product dictionary, table records, index records, and buffers to hold overflow data.
Protocol port numbers for Agent connection to TEMS	• KN3_TEMS_TCP_PIPE_PORT_NUM • KN3_TEMS_TCP_PIPES_PORT_NUM • KN3_TEMS_TCP_PIPE6_PORT_NUM • KN3_TEMS_TCP_PIPE6S_PORT_NUM • KN3_TEMS_TCP_UDP_PORT_NUM • KN3_TEMS_TCP_UDP6_PORT_NUM	Specifies the port numbers that are used by the protocols specified under "Specify communication protocols preference for TEMS connection" for communication between the monitoring agent and Tivoli Enterprise Monitoring Server.
Secondary TEMS configuration	• KN3_TEMS_BKUP1_NAME_NODEID	Specifies the name of the secondary monitoring server if you defined a backup Tivoli Enterprise Monitoring Server. The BKUP1 values are found in the KN3ENV member in the *rhilev*.*midlev*.*rtename*.RKANPARU library to communicate with the backup Tivoli Enterprise Monitoring Server.

Table 8. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile (continued)

PARMGEN classification	Parameters in this group	Explanation
Secondary TEMS TCP/IP information	• KN3_TEMS_BKUP1_TCP_HOST	Specifies TCP/IP information for a backup Tivoli Enterprise Monitoring Server if you defined a backup monitoring server. The BKUP1 values are found in the KN3ENV member in the *rhilev*.*midlev*.*rtename*.RKANPARU library to communicate with the backup Tivoli Enterprise Monitoring Server.
Secondary TEMS VTAM information:	• KN3_TEMS_BKUP1_VTAM_APPL_LLB_BKR • KN3_TEMS_BKUP1_VTAM_LU62_DLOGMOD • KN3_TEMS_BKUP1_VTAM_NETID	Specifies VTAM or SNA information for the backup Tivoli Enterprise Monitoring Server if you defined a backup monitoring server. The BKUP1 values are found in the KN3ENV member in the*rhilev*.*midlev*.*rtename*.RKANPARU library to communicate with the backup Tivoli Enterprise Monitoring Server.
Specify communication protocols preference for TEMS connection	• KN3_AGT_COMM_PROTOCOLn	Details the protocol possibilities for communication between the monitoring agent and Tivoli Enterprise Monitoring Server in the order in which the protocols will be used.
Take Action commands security settings	• KN3_AGT_PPI_RECEIVER • KN3_AGT_PPI_SENDER • KN3_SECURITY_ACTION_CLASS	Defines the connection between IBM Z OMEGAMON Network Monitor and Tivoli NetView for z/OS if you use Tivoli NetView for z/OS and specifies whether to override the SAF security value specified for the runtime environment at the agent.
Values that describe the address space	• KN3_AGT_CONFIGURATION_MODE • KN3_AGT_STC	Specifies the name of the address space in which you are running and the name of your agent PROC.
Values that describe the Primary TEMS the Agent will connect to	• KN3_TEMS_LOCAL_CONNECT_FLAG • KN3_TEMS_NAME_NODEID	Defines the information required to connect to the local Tivoli Enterprise Monitoring Server.
VTAM Secondary Program Operator (SPO) for Communication Network Management (CNM) interface (optional)	• KN3_AGT_VTAM_NODE_OMXE • KN3_AGT_VTAM_APPL_CNM_SPO	Defines how the IBM Z OMEGAMON Network Monitor monitoring agent communicates with the VTAM CNM interface to collect monitoring information.

Configuring security for Take Action commands

You must supply custom values for the security class and SAF validation for Take Action commands.

The security for Take Action commands provided with the IBM Z OMEGAMON Network Monitor is implemented through direct System Authorization Facility (SAF) calls and is based on profiles and resource names. These commands cannot be run unless security is configured.

IBM Z OMEGAMON Network Monitor agent Take Action commands cannot be issued unless a security class is defined to the SAF security manager and the security class name is configured in each runtime environment in which an IBM Z OMEGAMON Network Monitor monitoring agent is configured.

To secure Take Action commands, you must configure the global security parameter (RTE_SECURITY_CLASS). Optionally, you can use the SAF class name override parameter (KN3_SECURITY_ACTION_CLASS) to specify a separate class for securing IBM Z OMEGAMON Network Monitor Take Action commands. After you define each security class, you must create profiles to control access to individual commands and give user IDs UPDATE access to those profiles. See "Prefixed Take Action commands" on page 56.

Finding previous PARMGEN configuration sessions

If you configured an RTE by using the PARMGEN method and exit the PARMGEN tool, you might have difficulty locating your work from the previous session when you restart the PARMGEN tool.

When you open the PARMGEN Workflow Welcome panel for the second time, the fields at the top are blank, as shown in Figure 1 on page 41 and it seems that the work from your previous session is lost.

```
--------------- PARAMETER GENERATOR (PARMGEN) WORKFLOW - WELCOME -------------
OPTION ===>                                                  SCROLL ===>

Enter PARMGEN parameter values appropriate for your environment:
GBL_USER_JCL:   ____________________________________________
                PARMGEN global user JCL library (CONFIG DD in STCs)
RTE_PLIB_HILEV: ____________________________________________
                High-Level Qualifier (HLQ) of work libraries (IK*,WCONFIG,WK*)
RTE_NAME:       _________  (Type ? for a list of configured RTEs)
                Runtime environment (RTE) name for this LPAR

Enter n  (1-11) to perform tasks.                    Status     Date
Enter ns (1s-11s) to display detailed status.       --------- ---------

1.  KCIJPCFG Set up PARMGEN work environment for an RTE.
2.  $JOBINDX Review PARMGEN job index.
3.  KCIJPCCF Clone customized WCONFIG members.  (Optional)
4.  KCIJPUP1 Update interim libraries and create profiles.
5.  KCIJPMC1 Merge profile from backup MIG420   (Optional)
6.  KCIJPMC2 Merge profile from model RTE.      (Optional)
7.  KCIJPCNV Convert an ICAT RTE Batch member.  (Optional)
8.  MIG420   Customize PARMGEN configuration profiles.
9.  KCIJPVAL Validate PARMGEN profile parameter values.
10. $PARSE   Create the RTE members and jobs.
11. SUBMIT   Submit batch jobs to complete PARMGEN setup.
U   Utility  Access PARMGEN utilities.          (Optional)
R   New RTE  Reset RTE, Status and Date fields. (Optional)

Enter=Next  F1=Help  F3=End/Cancel
```

Figure 1. PARMGEN Workflow Welcome panel on entry

To locate your work from a previous session, you must provide values for the **GBL_USER_JCL** field, which displays PARMGEN global user JCL library (CONFIG DD in the started tasks). If you provide this value and press **Enter**, then configuration information from the previous session is displayed. Also, the **Status** and **Date** for each PARMGEN option that you completed is displayed, providing an accurate record of your progress.

Ensuring that your runtime environment supports the NetView for z/OS packet trace using PARMGEN

You must set values for these three parameters before you use NetView for z/OS packet trace.

If you plan to use the Dynamic XE to 3270 functionality that enables you to access the NetView for z/OS packet trace function, the settings for your runtime environment must include the information that is required for 3270 applications to link to Tivoli NetView for z/OS.

If you are creating your runtime environment for the first time, make sure that the information for these three RTE_TN3270 parameters is correct:

- RTE_TN3270_DXL_HOSTADDRESS for specifying the Hostname
- RTE_TN3270_DXL_TN3270PORT for specifying the Port Number
- RTE_TN3270_DXL_LUGROUP for specifying the LUGROUP

The requirements for these fields are described briefly in Table 9 on page 42 and more completely in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*.

Table 9. ***Update Runtime Environment parameters***

Parameter	Explanation
Hostname	If the system on which you are defining a runtime environment does not have an active Telnet listener, you can specify the network address of a system that does have an active Telnet listener. You can specify a network address as one of the following values: • Fully qualified hostname (for example, sys.ibm.com) • First qualifier of the fully qualified hostname (for example, sys for sys.ibm.com) • 32-bit IPv4 address in dotted decimal notation (for example, 9.67.1.100) To get this value, issue the TSO HOMETEST command on the system of the Telnet listener.
Port number	The default port number of the Telnet listener is 23. To override this value, specify the port number of the Telnet listener.
LUGROUP	The Dynamic XE to 3270 (NetView for z/OS) linking feature requires the VTAM Unformatted System Services (USS) screen to accept a LOGON APPLID() DATA() command. If the default Telnet USS screen does not accept this command, supply the name of a Logical Unit (LU) group that does accept it. The TN3270 session is joined to that LU group.

Note:

1. Complete this panel only if you are configuring products that support the Dynamic XE to 3270 (NetView for z/OS) linking feature and you need to override the default values.
2. The default values or the override values you specify on this panel are displayed during TN3270 logon and can be modified for an individual TN3270 session.

Completing the configuration

Use this information to understand the flow of tasks completed outside the PARMGEN for the IBM Z OMEGAMON Network Monitor monitoring agent.

There are a number of steps you must take outside of PARMGEN to complete the configuration of IBM Z OMEGAMON Monitor for z/OS. The remaining steps you have depend on what steps you have already taken, what options you have chosen, and what you intend to monitor.

Attention: Some steps required to complete the configuration of the IBM Z Monitoring monitoring agent are not found in the online help for PARMGEN. To ensure that you perform all the steps required and perform them in the correct order, use this chapter for product configuration, not the PARMGEN online help.

Before you start the common tasks, perform agent-specific security configuration:

- "Define monitoring agent access to the network management interfaces and commands" on page 44
- "Give users authorization and resource access to run the VARY TCPIP DROP command" on page 46

These common tasks must be completed for every product and can be completed all at one time for all the products.

- "Add support for the SYSTCPD DDNAME in the started tasks " on page 47
- "Copy the started task procedures to your procedure library" on page 47
- "Vary the VTAM major node active and copy it to your VTAMLST library" on page 48
- "APF authorize your libraries" on page 48
- "Enable historical data store maintenance" on page 48

The following tasks are completed for the IBM Z OMEGAMON Network Monitor product only:

- "Making the performance monitor interface (PMI) exit available to VTAM" on page 50
- "Enabling CSA tracking to display TCP/IP CSA usage" on page 50
- "Configuring the IBM Z OMEGAMON Network Monitor SNMP manager functions" on page 51
- "Authorize the IBM Z OMEGAMON Network Monitor started tasks for TCP/IP privileges" on page 51

If you intend to collect historical data:

- "Configuring historical data collection" on page 52

If you intend to warehouse the historical data in the Tivoli Data Warehouse, but the hub monitoring server is not located on the same computer as the Tivoli Enterprise Portal Server:

- "Enable Warehouse agents on a z/OS hub monitoring server" on page 53

Perform the following tasks to complete the configuration:

- "Install application and language support" on page 54
- "Verify the configuration" on page 55
- "Enable security" on page 55, which includes the following tasks:
  - "Enabling security at Tivoli Enterprise Portal" on page 55
  - "Enabling SNMP V3 passwords for autonomous agents" on page 55
  - "Authorizing users to access IBM Z OMEGAMON Network Monitor managed systems on the enhanced 3270 user interface" on page 56
  - "Authorizing users to issue Take Action commands" on page 56

Finally, if you use the batch facility to clone agent configuration from one LPAR to another and the release level of z/OS is other than the release level of the system where the SMP/E installation of the IBM Z OMEGAMON Network Monitor monitoring agent was installed, perform this task:

- "Deploy the configuration" on page 61
- "Relink the runtime environments" on page 62

Perform agent-specific security configuration

As part of the configuration done outside of PARMGEN, you must perform agent-specific security configuration for the IBM Z OMEGAMON Network Monitor monitoring agent.

If your hub Tivoli Enterprise Portal is running on z/OS, then you configured RACF or your system authorization facility (SAF) product to authenticate your Tivoli Enterprise Portal users when you set up

your Tivoli Enterprise Monitoring Server on z/OS. Additional RACF authorization described in the following section is required when you configure the IBM Z OMEGAMON Network Monitor monitoring agent. User IDs were also defined on the UNIX and Windows systems that are part of your distributed components.

For more information about security issues in the Tivoli Management Services environment, see *IBM Tivoli Monitoring: Installation and Setup Guide*. For more information about supported SAF products, see "Required software" on page 1.

Additionally, you must perform these two security configuration tasks for the IBM Z OMEGAMON Network Monitor monitoring agent:

Define monitoring agent access to the network management interfaces and commands
As part of the configuration done outside of PARMGEN, you must define monitoring agent access to the network management interfaces and commands for the IBM Z OMEGAMON Network Monitor monitoring agent.

About this task

If your site has the security profiles defined for the z/OS Communications Server network management interfaces (NMIs), then the IBM Z OMEGAMON Network Monitor monitoring agent must be authorized to access these interfaces. One or more of the following security profiles may be defined in the SERVAUTH class:

- EZB.NETMGMT.systemname.tcpipprocname.*
- EZB.NETMGMT.systemname.tcpipprocname.SYSTCPCN
- EZB.NETMGMT.systemname.tcpipprocname.SYSTCPSM
- EZB.NETMGMT.systemname.tcpipprocname.IPSEC.DISPLAY
- IST.NETMGMT.systemname.SNAMGMT

If the security profiles are not defined in order to control access to the NMIs, the user ID under which the monitoring agent procedure runs must be a superuser. A superuser is an ID which has a numeric value of 0 and which has been permitted to the BPX.SUPERUSER profile in the FACILITY class.

If your site has security profiles defined for the OPERCMDS class, then the IBM Z OMEGAMON Network Monitor monitoring agent must be authorized to access the following commands:

```
VARY TCPIP,,DROP
DISPLAY NET
DISPLAY TCPIP
DISPLAY A
```

Access to these commands is controlled by the following profiles in the OPERCMDS class:

```
MVS.VARY.TCPIP.DROP
MVS.DISPLAY.NET
MVS.DISPLAY.TCPIP
MVS.DISPLAY.JOB
```

The PARMGEN configuration method copies the sample JCL, KN3UAUTH, to your PROCLIB if you ran the JCL to copy to your PROCLIB. Otherwise, this JCL is found in *&rhilev.&midlev.&rtename*.RKANSAMU.

- IST.NETMGMT.systemname.SNAMGMT in the SERVAUTH class
- EZB.NETMGMT.systemname.tcpipprocname.* in the SERVAUTH class
- MVS™.VARY.TCPIP.DROP in the OPERCMDS class

Additionally, the JCL contains commented out sample statements that grant the agent access to the security profiles that control access to the `DISPLAY NET`, `DISPLAY TCPIP`, and `DISPLAY A` commands:

- MVS.DISPLAY.NET in the OPERCMDS class
- MVS.DISPLAY.TCPIP in the OPERCMDS class
- MVS.DISPLAY.JOB in the OPERCMDS class

This job is run outside of the PARMGEN. Make the following changes to this job before you run it:

- If your site controls access to z/OS commands by defining resources in the OPERCMDS class, you will need to give the agent user ID access to the `MVS.DISPLAY.NET` , `MVS.DISPLAY.TCPIP` and `MVS.DISPLAY.JOB` resources profiles in the OPERCMDS class. To do this you can remove the comment delimiters in front of the statements that define (RDEFINE) these resources and permit (PERMIT) the agent user ID to access them. You do not need to remove the comment delimiters on the statements that define the resources if they are already defined at your site.
- Change **omvsgrp** to a valid OMVS group in RACF and **password** to a valid password for your enterprise.
- Change **systemname** to the system name where the monitoring agent will run.
- Change **agentproc** to the started procedure name for the IBM Z OMEGAMON Network Monitor monitoring agent. The default is **IBMN3**.
- Change **tcpipprocname** to your TCP/IP startup procedure name for the TCP/IP stack that you want to monitor. Repeat this pair of lines (RDEFINE and PERMIT) for every TCP/IP address space you want to monitor.

  Note:

  1. The RDEFINE and PERMIT statements for IST.NETMGMT* do not need to be repeated.
  2. If you start your TCP/IP address space using the `S procedure` syntax, use procedure for *tcpipprocname*. If you start your TCP/IP address space using the `S procedure.identifier` syntax, use identifier for *tcpipprocname*.

For information about values in this job that you need to edit, see comments in the JCL job.

Your security administrator must run this job from a user ID that has RACF SPECIAL and UID(0) authority or code USERID and PASSWORD on the jobcard for an ID that has RACF SPECIAL and UID(0) authority. KN3USER is the default user ID. If you choose to use a different ID, change all occurrences of KN3USER in the job. Make these changes and review this job before you provide it to your security department. It should run with a zero return code.

Note that a user ID defined with UID(0) authority (SUPERUSER) has automatic access to the NMI resources required by the IBM Z OMEGAMON Network Monitor agent. Although sometimes appropriate, the least desirable method of defining superusers is to assign a UID of 0 in the UID parameter in the OMVS segment of the ADDUSER or ALTUSER commands. In this environment, you risk entering commands that can damage the file system. If you installation does not permit the creation of a UID(0) user ID, consider defining a userid which is a non-zero UID and granting it access to the BPX.SUPERUSER resource in the FACILITY class. Using the BPX.SUPERUSER resource in the FACILITY class is another way for users to get the authority to do most of the tasks that require superuser authority. However, if your installation does not permit the creation of a UID(0) user ID, the KN3UAUTH sample job must still be run in order to establish the proper rules required by the agent task. The KN3UAUTH sample job contains sample RACF statements that demonstrate how a user ID (KN3USER) can be created with a non-zero UID. In the JCL example, the value UID(12345) is used for demonstration purposes, but any valid, non-zero number acceptable by the UID parameter can be used to define the user ID. Once the userid is defined with a non-zero UID, the next step is to associate that userid with the BPX.SUPERUSER resource in the FACILITY class. For example:

```
PERMIT BPX.SUPERUSER CLASS(FACILITY) ID(KN3USER) ACCESS(READ)
```

For details on how to grant superuser authority to a userid, without explicitly associating that userid with UID(0), see Changing a superuser from UID(0) to a unique nonzero UID in the *z/OS UNIX System Services Planning* manual.

If the KN3UAUTH job has defined UID(0) for the Agent User Name, then the Agent User Name attribute in the Agent Status workspace will show a value of ROOT. If the UID is not UID(0), the Agent User ID is displayed as the KN3USER user ID (the default in the sample file) or the user ID that the system administrator coded on the RACF ADDUSER statement.

For the PARMGEN configuration method, all started tasks and the KN3UAUTH job are created during $PARSE processing. When you run the KCIJPSYS JCL job, the KN3UAUTH job is copied to the PROCLIB that you specified. The default location is SYS1.PROCLIB.

Give users authorization and resource access to run the VARY TCPIP DROP command
As part of the configuration done outside of PARMGEN, you give users authorization and resource access to run the VARY TCPIP DROP command for the IBM Z OMEGAMON Network Monitor monitoring agent.

About this task

z/OS Communications Server protects data and other system resources accessed by applications included in the z/OS Communications Server component. This protection requires that the identity of the user requesting access be verified (identification and authentication) and that access be limited to only those resources permitted to this user (access control).

z/OS Communications Server applications use RACF for identification and authentication and for access control, though you may use other supported security access facility (SAF) programs. Users authenticated with a SAF program are granted access to only those z/OS resources for which they have permission. The RACROUTE macro instruction is the SAF interface for all products that provide resource control.

SAF programs must be configured correctly for the IBM Z OMEGAMON Network Monitor VARY TCPIP,*tcpip_jobname*,CMD=DROP,CONNECTION=*connection_number* command to function correctly. The permissions granted to a given Tivoli Enterprise Portal user determine the network resources against which the DROP command can be executed.

TCP/IP uses SAF profiles in the OPERCMD resource class to determine access to network resources. The MVS.VARY.TCPIP.DROP profile can be used by a SAF product to restrict access to the DROP command. If the MVS.VARY.TCPIP.DROP profile is defined, the monitoring agent restricts access to the DROP command to only those users who have CONTROL or higher access to the MVS.VARY.TCPIP.DROP profile.

The SAF program validates the DROP command before passing it to the appropriate service routine.

- If RACROUTE verification fails for any reason, the command and a message indicating that SAF validation has failed are written to the command log.
- If RACROUTE verification is successful, or a SAF rule prohibiting access does not exist (resulting in a NO DECISION), then the command request is queued to the service routine and executed. The command response returned depends on the command issued.

The security configuration should be as follows:

1. The KN3UAUTH member of RKANSAMU should be customized to enable the IBM Z OMEGAMON Network Monitor monitoring agent to issue a DROP command anywhere in the system that the user chooses to allow these actions.
2. When a DROP Connection command is issued from the dialog, the IBM Z OMEGAMON Network Monitor agent will check the Tivoli Enterprise Portal or Enhanced 3270UI User ID to validate that the user issuing the command has CONTROL access to the MVS.VARY.TCPIP.DROP profile using a RACROUTE call.
   a. If the user has access to the MVS.VARY.TCPIP.DROP profile, then IBM Z OMEGAMON Network Monitor issues the following command:

      ```
      VARY TCPIP,tcpip_jobname,CMD=DROP,CONNECTION=connection_number
      ```

   b. If the user does not have access to the MVS.VARY.TCPIP.DROP profile, then IBM Z OMEGAMON Network Monitor does **not** issue the following command:

      ```
      VARY TCPIP,tcpip_jobname,CMD=DROP,CONNECTION=connection_number
      ```

      An error explaining the reason that the command was not executed is returned to the user.

Add support for the SYSTCPD DDNAME in the started tasks

As part of the configuration done outside of PARMGEN, users of other monitoring agents must add support for the SYSTCPD DDNAME in the started tasks. This step is not necessary for IBM Z OMEGAMON Network Monitor users. This step is performed for you as part of a JCL job.

About this task

Note: This step is not necessary for IBM Z OMEGAMON Network Monitor users. This step is performed for you as part of a JCL job.

SYSTCPD explicitly identifies which data set to use to obtain the parameters defined by TCPIP.DATA when no GLOBALTCPIPDATA statement is configured. If a monitoring server is using any of the IP.UDP-related or IP.PIPE-related communication protocols for connection, but the IP domain name resolution is not fully configured on the z/OS system, SYSTCPD must be supported by the monitoring server and the monitoring agents that report to it.

If you are certain that SYSTCPD is not needed at your installation, you can skip this step. However, note that you might gain a small performance benefit by avoiding multiple dynamic data set allocations if you supply a SYSTCPD DD statement.

To support SYSTCPD, uncomment the following statement in the started task members in your PROCLIB and provide the name of the SYSTCPD data set:

```
//*SYSTCPD DD DISP=SHR,
//* DSN=TCPIP.SEZAINST(TCPDATA)
```

The name of the SYSTCPD data set is installation-specific. Get the correct specification from your network administrator.

If you reconfigure products, you will need to uncomment the statement again.

If the monitoring server is using any of the IP.UDP-related or IP.PIPE-related communication protocols for connection, but the IP domain name resolution is not fully configured on this z/OS system, you must specify the SYSTCPD DDNAME in the IBMDS started task.

PARMGEN generated the IBMDS started task with the following commented out lines. Customize the SYSTCPD DDNAME accordingly if this scenario fits your environment:

```
//*SYSTCPD explicitly identifies which dataset to use to obtain
//*the parameters defined by TCPIP.DATA when no GLOBALTCPIPDATA
//*statement is configured. Refer to the IP Configuration Guide
//*for information on the TCPIP.DATA search order. The dataset
//*can be any sequential dataset or a member of a partitioned
//*dataset. TCPIP.SEZAINST(TCPDATA) is the default sample file.
//*TCPIP.TCPPARMS(TCPDATA) is another sample and is created as
//*part of the Installation Verification Program for TCP/IP.
//*Note: Uncomment out this DDNAME and point to appropriate
//*      TCPDATA library name supported at your site if domain
//*      name resolution is not fully configured.
//*SYSTCPD DD DISP=SHR,
//*       DSN=TCPIP.SEZAINST(TCPDATA)
```

Copy the started task procedures to your procedure library

As part of the configuration done outside of PARMGEN, you must copy the started tasks procedures to the procedure library used by the IBM Z OMEGAMON Network Monitor monitoring agent.

About this task

The PARMGEN method created started task procedures in *&rhilev.&midlev.&rtename.*RKANSAMU. If you did not run JCL that copies these procedures to your procedure library PROCLIB, update your started task library as follows:

1. If you have configured an agent address space, copy the IBM Z OMEGAMON Network Monitor monitoring agent started task (the default name is **IBMN3**) from *&rhilev.&midlev.&rtename.*RKANSAMU to your PROCLIB.

2. If you have configured a persistent data store for the IBM Z OMEGAMON Network Monitor monitoring agent, copy the persistent data store maintenance procedures (KPDPROC1 from *&rhilev.&midlev.&rtename.*RKANSAMU and KPDPROC from *&rhilev.&midlev.&rtename.*RKANSAM) to your PROCLIB.

You also need to copy the VTAM major node members from the *&rhilev.&midlev.&rtename*.RKANSAMU library to the system libraries (if applicable).

Vary the VTAM major node active and copy it to your VTAMLST library

As part of the configuration done outside of the PARMGEN method, you may need to vary the VTAM major node active and copy it to the VTAMLIST library used by the IBM Z OMEGAMON Network Monitor monitoring agent.

About this task

The PARMGEN method created VTAM definitions and stored them in *&rhilev.&midlev.&rtename.*RKANSAMU. These statements were added to PROCs. You uncomment these statements to vary the VTAM node active. PARMGEN also copies these statements to the VTAMLST you specified during configuration if you run the KCIJPSYS JCL jobs to do this.

You vary the VTAM node (**CTDN3N** is the default name) active by issuing the following command:

```
V NET,ACT,ID=CTDN3N
```

Whether the default CTDN3N VTAM major node is created will depend upon two things:

- If the IBM Z OMEGAMON Network Monitor monitoring agent is running in its own address space (the best practice configuration)
- If SNA data collection is configured

If both of these conditions are true, then the CTDN3N VTAM major node needs to be copied to VTAMLST and activated before the IBM Z OMEGAMON Network Monitor monitoring agent is started.

APF authorize your libraries

As part of the configuration done outside of PARMGEN, you must APF authorize the libraries used by the IBM Z OMEGAMON Network Monitor monitoring agent.

About this task

If you use APF authorization, add the following runtime load libraries to your list of APF-authorized libraries.

```
&rhilev.&midlev.&rtename.RKANMODU
&rhilev.&midlev.RKANMOD
&rhilev.&midlev.RKANMODL
```

Note: Any runtime libraries concatenated in the `STEPLIB DDNAME` and in the `RKANMODL DDNAME` of the `IBMN3` started tasks must be APF-authorized. You must uncomment these statements in the started tasks.

Enable historical data store maintenance

As part of the configuration done outside of PARMGEN, you must enable historical data store maintenance for the IBM Z OMEGAMON Network Monitor monitoring agent.

About this task

If you intend to enable historical data collection and have allocated and configured maintenance of the historical data set, you must perform three additional tasks to enable the maintenance:

1. **Provide access to the persistent data store files**

Ensure that KPDPROC1 procedure has the necessary authority to read, write, and update the persistent data store files. PARMGEN performs this task automatically and copies this procedure to the PROCLIB that you specified, so you can skip this step if you ran KCIJPSYS.

The KPDPROC1 procedure is used to maintain the physical files that constitute the persistent data store. Data store files are archived, exported or recycled according to the maintenance strategy that you specified for persistent data store file groups for the product. The persistent data store subsystem automatically submits maintenance jobs whenever a data store file becomes full. The maintenance procedure must be available in a system procedure library for the procedure to operate. The procedure is generic so it may be used by all runtime environments using this version of the persistent data store.

2. **Authorize the KPDDSCO module**

   The KPDPROCC REXX procedure runs in a TSO environment and must be enabled to run as an authorized program under TSO. Authorize the KPDDSCO module by adding KPDDSCO to the system PARMLIB(IKJTSOnn) under the AUTHPGM section and refresh the IKJTSOnn member by issuing the set command (T IKJTSO=nn). You might also request that authorized system programmers perform this step so it can be scheduled with the LPAR change control processes.

3. **Verify persistent data store configuration**

   To verify that the configuration and authorization of the procedures have been successful, perform the following steps:

   a. Bring up the started task (for monitoring server or monitoring agent) that will collect historical data into the product's persistent data store libraries. In the RKPDLOG DDNAME started task, find any persistent data store libraries in a non-Offline status (for example, Partial or Full status).

   b. From a z/OS operator console, issue the following z/OS MODIFY command:

   ```
   /F &stcname,KPDCMD RECOVER FILE=DSN:&pds_dataset
   ```

   (where *&stcname* is the name of the started task performing the persistent data store collection, and *&pds_dataset* is the persistent data store data set).

   For example, issue the following MODIFY command for the monitoring server:

   ```
   /F CIDSST,KPDCMD RECOVER FILE=DSN:&rhilev.&midlev.&rtename.RGENHIS1
   ```

   c. Wait 5 minutes.

   d. In the RKPDLOG DDNAME started task, find the following Command: and KPDDSTR: references as shown in the following monitoring server RKPDLOG DDNAME example that follows:

   ```
   Command: RESUME FILE=DSN:&rhilev.&midlev.&rtename.RKN3HIS1
   KPDDSTR: CONNECT processing started for DataStore file
   DSN:&rhilev.&midlev.&rtename.RKN3HIS1
   KPDDSTR: CONNECT processing ended for DataStore file
   DSN:&rhilev.&midlev.&rtename.RKN3HIS1
   ```

   e. If these references are not found, view the KPDPROC1 started task in SDSF and look for any obvious errors.

If you are upgrading an existing monitoring server or monitoring agent, you must also refresh the KPDPROC1 maintenance procedure in your system procedure library. See *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Upgrade Guide*.

Run the ITMSUPER Tools (optional)

Use the ITMSUPER Tools to learn about the health of your managed systems, situations, and environment configuration.

The ITMSUPER Tools are included in the IBM Support Assistant (ISA), a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. To install the ISA software, go to http://www.ibm.com/software/support/isa.

Making the performance monitor interface (PMI) exit available to VTAM

As part of the configuration done outside of PARMGEN, you must make the performance monitor interface exit available to VTAM for the IBM Z OMEGAMON Network Monitormonitoring agent.

You must make the PMI exit accessible to VTAM. Choose one of these two ways to do this task: by modifying the VTAM startup JCL or by copying the PMI Exit to VTAM.

Modifying the VTAM startup JCL

Follow these steps to modify the VTAM startup JCL.

1. Add a DD statement for the library containing the PMI exit to the VTAMLIB concatenation in your VTAM startup procedure. If you did not configure this OMEGAMON RTE to share with the SMP/E target libraries (that is, SHARING SMP), then you could add the following statement to the VTAMLIB concatenation. See the note in the XE configuration section on this topic if you select this option. Add this library:

   ```
   &rhilev.&midlev.&rtename.RKANMOD
   ```

   If you do configure the OMEGAMON RTE to share with the SMP/E libraries, then follow the steps in “Copying the PMI Exit to VTAM” on page 50.
2. Quiesce your network.
3. Restart VTAM.

Note: You should not add SMP/E target libraries to the VTAMLIB concatenation because this would be a problem when you apply maintenance in the future.

Copying the PMI Exit to VTAM

An alternate approach is to copy the PMI exit module and its ALIASes to an existing library in the VTAMLIB concatenation. The PMI Exit consists of module KN3AMVPX and its five ALIASes KN3AMV00-04. The PMI Exit must be found somewhere in the VTAMLIB concatenation in order for the exit to function correctly when the IBM Z OMEGAMON Network Monitor program tries to activate the exit.

If you do this, then there is no longer a need to quiesce VTAM when maintenance is applied.

A potential drawback to this method is that future changes to the VTAM PMI exit might not be picked up when you apply maintenance if you forget to recopy the PMI Exit program and its ALIASes to the library in the VTAMLIB concatenation after the maintenance is applied.

Another potential problem occurs if you copy the PMI exit to different libraries in the VTAM concatenation and have multiple copies of the PMI exit in your VTAMLIB concatenation. If you choose this approach, you must put a process in place for ensuring that the IBM Z OMEGAMON Network Monitor PMI exit program is correctly maintained.

Enabling CSA tracking to display TCP/IP CSA usage

As part of the configuration done outside of PARMGEN, you must enable CSA tracking so that TCP/IP CSA usage can be displayed for the OMEGAMON XE for Mainframe Networks monitoring agent.

About this task

The IBM-supplied default PARMLIB member is DIAG00, which contains the following:

```
…
    VSM TRACK CSA(ON) SQA(ON)
…
```

If this is not specified, then CSA information will not be available within the product.

Configuring the IBM Z OMEGAMON Network Monitor SNMP manager functions

As part of the configuration done outside of PARMGEN, you configure SNMP manager functions for the IBM Z OMEGAMON Network Monitor monitoring agent.

About this task

Follow this process to configure the SNMP manager functions.

See "Format of the SNMP configuration file" on page 543 for more information about this file format.

Procedure

1. Confirm that the SNMP configuration file named on the KN3SNMP DD card in the sample start procedure (IBMN3) exists. If it does not, allocate it.
2. Edit this file. See sample SNMP configuration file KN3SNMP in RKANSAMU for information about supported data characteristics and the syntax for data set allocation statements.
3. Add a configuration statement for each SNMP agent from which data will be collected (one per TCP/IP stack).
4. Save this data set.

Results

When you start the Tivoli Management Services environment and the IBM Z OMEGAMON Network Monitor monitoring agent, workspaces that use data collection services dependent on SNMP should display data.

Related reference

"Format of the SNMP configuration file" on page 543
Since V4.2, SNMP data collection in the IBM Z OMEGAMON Network Monitor monitoring agent was enhanced to give you greater flexibility when communicating with the SNMP agents.

Authorize the IBM Z OMEGAMON Network Monitor started tasks for TCP/IP privileges

Use this information to define a TCP/IP OMVS segment for the user ID associated with units of work requesting these UNIX System Services.

About this task

The IBM Z OMEGAMON Network Monitor TCP/IP data collector uses TCP/IP service components in z/OS Communications Server that exploit z/OS UNIX System Services. Using these components requires a UNIX System Services security construct, called an OMVS segment, for the user ID associated with units of work requesting these services.

The OMVS segment must be defined with **SuperUser** authority. [Note that a userid defined with **SuperUser** authority is not the same as UID(0).] Authorize the IBM Z OMEGAMON Network Monitor started task for TCP/IP privileges by creating an OMVS segment for RACF or another SAF product. Identify the IBM Z OMEGAMON Network Monitor started task IBMN3 as a **superuser**, as in this example:

```
ALU IBMN3 OMVS(UID(0) HOME(/) PROGRAM(/bin/sh))
```

See the *z/OS Communications Server IP Planning and Migration Guide* for an explanation of how to provide an OMVS segment for the IBM Z OMEGAMON Network Monitor started task.

Note: This command makes setting of **SuperUser** authority more explicit. This action has actually already taken place when you ran the JCL job described in "Define monitoring agent access to the network management interfaces and commands" on page 44.

If you recently migrated to z/OS v2.1, you might find OMVS errors in the system log when you launch the IBM Z OMEGAMON Network Monitor monitoring agent. Be aware that as of z/OS V2R1, the ability to use default OMVS segments has been removed. All z/OS UNIX users or groups must now have OMVS segments defined for user and group profiles with unique user IDs (UIDs) and group IDs (GIDs). For more information about this error and workarounds, see "OMVS and SNAMGMT errors found in system log on z/OS v2.1 systems" in the *IBM Z OMEGAMON Network Monitor: Troubleshooting Guide*.

Installing and configuring the distributed components

Use this information to understand the remaining steps for installing and configuring the OMEGAMON XE monitoring agent.

If you intend to collect historical data, there are several steps necessary to properly configure the historical data collection. If you intend to warehouse the data in the Tivoli Data Warehouse and the hub monitoring server is not located on the same computer as the Tivoli Enterprise Portal Server, then you will need to enable warehouse agents on the z/OS hub monitoring server.

Note: Some steps required to complete the configuration of the OMEGAMON XE monitoring agent are not found in the online help for PARMGEN. To ensure that you perform all the steps required and perform them in the correct order, use this information for product configuration, not the PARMGEN online help

Configuring historical data collection

This section discusses historical data and includes information that you can use to determine the disk space that is required to support historical data files.

Before you can view historical data, an authorized user must configure historical data collection and collect enough data to support the query that is used. To configure historical data collection in the OMEGAMON Enhanced 3270 user interface, select **View** > **History Configuration**. To configure historical data collection in the Tivoli Enterprise Portal, open the **History Collection Configuration** window.

Historical data collection

Historical data collection involves the periodic sampling of selected attribute groups to support investigation of past problems and performance analysis. This is an optional feature that is enabled through the Tivoli Enterprise Portal or the OMEGAMON Enhanced 3270 user interface.

Historical data is collected on a configured time interval from the monitoring agent and is initially stored in one of the following locations:

- At the IBM Z OMEGAMON Network Monitor monitoring agent (the best practice location) or the Tivoli Enterprise Monitoring Server on a z/OS system in the persistent data store. The persistent data store must be configured and allocated prior to enabling historical data collection.
- At the Tivoli Enterprise Monitoring Server on a distributed platform

This historical data is referred to as "near-term history" in the OMEGAMON Enhanced 3270 user interface (enhanced 3270UI) or as "short-term history" in the Tivoli Enterprise Portal.

Long-term historical data is stored in the Tivoli Data Warehouse. On a separate time interval, historical data is retrieved from the monitoring agent or the Tivoli Enterprise Monitoring Server and stored in the Tivoli Data Warehouse. This long-term historical data is available from a much longer time period - weeks, months, or even years. You can summarize and prune the long-term historical data to manage space and to view trends. See the *IBM Tivoli Monitoring: Installation and Setup Guide* for installation instructions

The *persistent data store* (PDS) is a set of physically sequential files used for storing and retrieving near-term historical data. When the active PDS file becomes full, persistent data store processing switches to the next empty file and checks to see if any empty PDS files remain. If there are no more empty files, processing empties the file that contains the oldest data. You can configure the number of PDS files used and the amount of storage allocated to them if the default settings are not sufficient for your environment. Sample estimates are provided in “Disk space requirements for historical data tables” on page 509.

Near-term historical data is written to the PDS files by the monitoring agent using its CPU cycles. Additional CPU cycles are used when the Warehouse Proxy extracts data from the PDS files and copies it to the Tivoli Data Warehouse. If you have collected a large amount of data in the PDS files, the extraction process will significantly increase the monitoring agent's CPU usage. Deciding how often to migrate data to the Data Warehouse and when to schedule it is dependent on the amount of data collected and how much space has been allocated to the PDS for storing near-term history. Data that is not warehoused by the time the persistent data store becomes full will be discarded.

For more information about the persistent data store and about collecting historical data, see the following topics:

- Whether to collect historical data and how to manage it
- Maintaining the persistent data store

Enabling historical data collection in the enhanced 3270UI
The OMEGAMON enhanced 3270 user interface (enhanced 3270UI) is designed for investigation of current problems or for problems that occurred in the recent past. Therefore, only near-term historical data can be displayed in the enhanced 3270UI workspaces.

Most, but not all IBM Z OMEGAMON Network Monitor attribute groups are available to configure for historical data collection. The same attribute groups can be configured for historical data collection in the enhanced 3270UI as in the Tivoli Enterprise Portal.

Attribute groups that you enable historical collection for using the enhanced 3270UI are also available for viewing and configuration in the Tivoli Enterprise Portal.

For more information about collecting historical data, refer to Whether to collect historical data and how to manage it. For more information about viewing and configuring near-term history in the enhanced 3270UI, refer to Near-term history in the *: OMEGAMON XE shared documentation.*

Enabling historical data collection in the Tivoli Enterprise Portal
The Tivoli Enterprise Portal can display historical data that is stored in the persistent data store and the Tivoli Data Warehouse. Most, but not all IBM Z OMEGAMON Network Monitor attribute groups are available to configure for historical collection within the Tivoli Enterprise Portal.

An attribute group that you enable historical collection for using the Tivoli Enterprise Portal is available for viewing and configuration using the OMEGAMON enhanced 3270 user interface (enhanced 3270UI).

For information about collecting historical data, refer to Whether to collect historical data and how to manage it in the *OMEGAMON XE shared documentation*. For information about creating historical collections in the Tivoli Enterprise Portal, refer to *IBM Tivoli Monitoring: Tivoli Enterprise Portal User's Guide*.

Enable Warehouse agents on a z/OS hub monitoring server

As part of the configuration done outside of PARMGEN, you must enable Warehouse agents on a z/OS hub monitoring server for the IBM Z OMEGAMON Network Monitor monitoring agent.

About this task

If you want to store long-term history data and your hub monitoring server is on z/OS, you must transfer the catalog and attribute files for the Warehouse Proxy agent and the Summarization and Pruning agent to the hub using Manage Tivoli Monitoring Services.

The catalog and attribute data files are installed on the Tivoli Enterprise Portal Server when you install application support for IBM Z OMEGAMON Network Monitor, using the *IBM Tivoli OMEGAMON Data Files for z/OS* CD. You can then FTP the files to the hub monitoring server.

If the portal server is installed on a Windows system, you can FTP the files to a z/OS hub using Manage Tivoli Monitoring Services:

1. On the host of the Tivoli Enterprise Portal Server, open the Manage Tivoli Monitoring Services application. For example:

   ```
   Start > IBM Tivoli Monitoring > Manage Tivoli Monitoring Services.
   ```

2. Right-click the name of the portal server and select **Advanced > Utilities > FTP Catalog and Attribute files**.

   The "Select attribute and catalog data for transfer" dialog box is displayed.

3. Select the catalog and attribute data for the Warehouse Proxy and the Summarization and Pruning agents, then press **OK**.

   The FTP TEMS Data to z/OS dialog box is displayed.

4. Provide the following information:
   - The name of the hub Tivoli Enterprise Monitoring Server
   - A valid FTP user ID and password
   - The name of the domain name server of the monitoring server where the RKANDATV data set is located

   When you have completed these fields, click **OK**. Click **OK** again in the confirmation window.
5. After the FTP operation is complete, you receive a message that the operation completed successfully. Click **OK** to end this operation.

After you complete these steps, restart the hub monitoring server.

Install application and language support

As part of the configuration done outside of PARMGEN, you must install application and language supported for the IBM Z OMEGAMON Network Monitor monitoring agent.

About this task

Before data collected by IBM Z OMEGAMON Network Monitor monitoring agents can be displayed in the Tivoli Enterprise Portal, support for the agents must be installed and enabled. Application support files provide agent-specific information for workspaces, helps, situations, templates, and other data. Application support for a monitoring agent includes two types of files:

- SQL files are required for adding product-provided situations, templates, and policies to the Enterprise Information Base (EIB) tables maintained by the hub monitoring server. These SQL files are also called seed data, and installing them on a monitoring server is also called seeding the monitoring server.
- Catalog and attribute (CAT and ATR) files are required for presenting workspaces, online help, and expert advice for the agent in Tivoli Enterprise Portal.

Application support must be configured on all instances of the following infrastructure components: Tivoli Enterprise Monitoring Server (both hub and remote monitoring servers), Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client, if the desktop client was installed from the installation media.

Application support for the monitoring agent is installed on the remote monitoring server when agents are registered with the local monitoring server.

The files required for support are contained in *IBM Tivoli OMEGAMON Data Files for z/OS* DVD included in the product package. You install support on the Tivoli Enterprise Portal Server and any desktop clients on the computer on which they are installed. If your hub is on Windows or a UNIX operating system (Linux®, AIX®, Solaris), you install support on the monitoring server locally (that is, on the computer on which it is installed). If your hub is on z/OS, you install support from a Windows computer that hosts either a Tivoli Enterprise Portal Server or a Tivoli Enterprise Monitoring Server. The hub monitoring server must be running while you are installing support.

Use the procedures documented in the *IBM Tivoli Monitoring: Installation and Setup Guide* to add support to Tivoli Enterprise Portal or a hub monitoring server on Windows, AIX, or Linux. Use the instructions in *IBM Tivoli Monitoring: Configuring the Tivoli Enterprise Monitoring Server on z/OS* to add support to a z/OS hub.

If you want application data, online help, and expert advice to be displayed in a language other than English, you must also install language support.

You install language support from the *IBM Z OMEGAMON Network Monitor Language Pack* CD on the same system where you install application support. Install the language packs on any system where you have installed the Tivoli Enterprise Portal or where you have installed a desktop client. (If you download and run a desktop client using Web Start, you do not need to install the language packs on the local system. They are downloaded from the portal server.) *Before you can install a language pack, you must install the component in English*.

For additional information about installing application and language support, including the most up-to-date files, see Technote 1255545 at http://www-01.ibm.com/support/docview.wss?uid=swg21255545.

Verify the configuration

The verification task must be performed at this juncture during configuration.

About this task

Follow the instructions in "Verifying configuration if you configured both Tivoli Enterprise Portal and the Enhanced 3270 user interface" on page 63 to verify that you have correctly configured the products and components.

Enable security

After your new environment is configured correctly, you can safely enable the required level of security on each of the components within your environment.

See "Enabling security at Tivoli Enterprise Portal" on page 55

If you are using the Tivoli Enterprise Portal to view data, you can create user accounts that authorize users to view the monitored data and set up authentication of those accounts by enabling security through the hub monitoring server or through the portal server. For instructions on enabling authentication on a hub monitoring server on Windows, Linux and UNIX operating systems, see the *IBM Tivoli Monitoring: Administrator's Guide*. For instructions on enabling authentication on a hub monitoring server on z/OS systems, see the *IBM Tivoli Management Services on z/OS: Configuring the Tivoli Enterprise Monitoring Server on z/OS*.

If you intend to use autonomous agents on a z/OS system, you can enable SNMP V3 passwords if the Integrated Cryptographic Service Facility (ICSF) subsystem is available on the z/OS system. See "Enabling SNMP V3 passwords for autonomous agents" on page 55.

If you are using the IBM Tivoli OMEGAMON enhanced 3270 user interface to view data, you can enable security by following the steps described in "Authorizing users to access IBM Z OMEGAMON Network Monitor managed systems on the enhanced 3270 user interface" on page 56.

In V5.1.0, the new 3270 and existing Tivoli Enterprise Portal Take Action commands fail unless explicit security definitions are configured that enable these commands to be issued. Security for this monitoring agent's Take Action commands is implemented through direct SAF (System Authorization Facility) calls and is based on resource profiles. Both user ID and command are validated. See "Authorizing users to issue Take Action commands" on page 56 to perform this security setup.

Enabling security at Tivoli Enterprise Portal

As part of the configuration done outside of PARMGEN, you must enable security at Tivoli Enterprise Portal.

About this task

To enable security for the Tivoli Enterprise Portal through either the hub monitoring server or the Tivoli Enterprise Portal Server, review the planning information in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide* and see the appropriate guide for instructions. To enable security for IBM Z OMEGAMON Network Monitor, see "Perform agent-specific security configuration" on page 43.

Enabling SNMP V3 passwords for autonomous agents

If you intend to use autonomous agents on a z/OS system, you can enable SNMP V3 passwords if the ICSF subsystem is available on the z/OS system.

See the Enabling SNMP V3 passwords for autonomous agents topic in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide* for more information about performing this task.

Authorizing users to access IBM Z OMEGAMON Network Monitor managed systems on the enhanced 3270 user interface

Logons to the IBM Z OMEGAMON Network Monitor enhanced 3270 user interface are controlled through the system authorization facility (SAF) interface. In addition, the OMEGAMON enhanced 3270 user interface performs SAF checks on users' authorization to view data for specific managed systems or managed system types and their authorization to issue Take Action commands.

By default, if no security class is configured, everyone is allowed to log on to the OMEGAMON enhanced 3270 user interface and to view data for any managed system. All Take Action commands are denied.

If a security class name is configured, resource profiles must be defined to control logon, data access, and Take Actions, and users must be given access to those profiles.

For instructions on configuring security for the OMEGAMON enhanced 3270 user interface, see the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS Common Planning and Configuration Guide*.

Authorizing users to issue Take Action commands

Certain commands, known as Take Action commands, can be issued from the Tivoli Enterprise Portal and OMEGAMON enhanced 3270 user interface. IBM Z OMEGAMON Network Monitor supports two types of Take Action commands: z/OS system commands and agent-provided commands. Users must be authorized to issue these commands.

z/OS commands

By default, Take Action commands issued by IBM Z OMEGAMON Network Monitor are issued as z/OS system commands.

However, a monitoring server or monitoring agent address space can be configured to redirect Take Action commands to NetView through the program to program interface (PPI). Take Action commands that are issued in NetView make full System Authorization Facility (SAF) calls for authorization. NetView uses the Tivoli Enterprise Portal user ID to determine the NetView operator on which the command authorization is performed. If command authorization passes, the command is processed by the NetView operator. Messages are written to the NetView log to provide an audit trail of the commands and the users that issued them. If you enable NetView command authorization on the monitoring server, you must also enable NetView to execute the commands.

For more information, see "Configuring NetView authorization of z/OS commands" in *IBM Tivoli Monitoring: Configuring the Tivoli Enterprise Monitoring Server on z/OS*.

Prefixed Take Action commands

IBM Z OMEGAMON Network Monitor provides a set of predefined Take Action commands:

```
Drop
Nslookup
Ping
Tracerte
```

These commands, which are prefixed by N3:, are known as agent commands. A subset of these commands, commands that cannot also be run as console commands, can be issued using the Take Action feature on the Tivoli Enterprise Portal. In the OMEGAMON enhanced 3270 user interface, these commands are available in action menus.

Security for IBM Z OMEGAMON Network Monitor Take Action commands is based on SAF security classes and resource profile names. During product configuration you specify the name of the SAF security class that is used to validate product specific take action commands. The SAF class that is used to validate take action commands is specified in the RTE_SECURITY_CLASS parameter in your PARMGEN parm deck. You can code the KN3_SECURITY_ACTION_CLASS parameter optionally if you want to have a separate SAF security class just for IBM Z OMEGAMON Network Monitor commands.

After you define the SAF security class, you define resource profiles to control access to the product-specific take action commands. If no resource profiles are created to control Take Action commands, all

commands are denied. The OMEGAMON enhanced 3270 user interface validates the following resource profile to see if users are authorized to issue the Take Action commands directed at z/OS Communication Server resources:

```
KN3.msn.TAKEACTION.*
```

where *msn* is managed system name.

At a minimum, you must create a profile by using the pattern shown in the previous sample for the global security class (RTE_SECURITY_CLASS) and give update access to the profile to all users you want to authorize to issue any Take Action commands from the enhanced 3270 user interface. The enhanced 3270 user interface address space uses SAF validation to determine whether a user is authorized to issue any Take Action commands.

SAF validation for product specific commands is performed by the monitoring agent. Create other profiles for more granular access control. For example, to control all IBM Z OMEGAMON Network Monitor Take Action commands on all managed systems, use the following command:

```
KN3.**.TAKEACTION.*
```

To control the ability to issue Take Action commands to an IBM Z OMEGAMON Network Monitor monitoring agent that is running on a system with an SMFID of TSTA and stack TCPIP, you would define a profile named:

```
KN3.TCPIP:TSTA.TAKEACTION.*
```

To control access to individual commands, you must define at least one profile with the following format in either the global security class or the override security class (KN3_SECURITY_ACTION_CLASS):

```
KN3.TCPIP:TSTA.TAKEACTION.commandname
```

or

```
KN3.**.TAKEACTION.commandname
```

where *commandname* is one of the supported IBM Z OMEGAMON Network Monitor Take Action commands.

To control access to the DROP command, create a profile in either the global security class or the override security class similar to the following:

```
KN3.**.TAKEACTION.DROP
```

Note: DROP commands also check the TCPIP.MVS.DROP profile of the OPERCMDS class in addition to any SAF checking done for the IBM Z OMEGAMON Network Monitor DROP command resource profile.

If a user attempts to issue a Take Action command without authorization, a series of messages similar to these messages here is written to the RKLVLOG:

```
2012.178 04:27:37.68 KN3A907I: USER=USER3    CLASS=$KOBSEC
RESOURCE=KN3.TCPIPG:SYS.TAKEACTION.PING
2012.178 04:27:37.68 KN3A908I: RACROUTE VERIFY  REG15=00000004 SAFPRRET=00000004
SAFPRREA=00000000
  SAFPSFRC=00000000 SAFPSFRS=00000
2012.178 04:27:37.68 000
2012.178 04:27:37.68 KN3A909I: USER=USER3    RESULT: USER NOT DEFINED TO ESM
```

Additionally, this message is displayed in a pop-up window in the enhanced 3270 user interface:

```
 _____________________________________________________
|              Take Action Command Failure            |
|                                                     |
| KN3A006E RACF AUTHORIZATION ERROR                   |
|_____________________________________________________|
```

In Tivoli Enterprise Portal or the enhanced 3270 user interface, you might also see the following messages in the Drop Connection dialog's Command Output display.

```
KN3A904E TAKE ACTION RACROUTE AUTH RC(FAILURE). CLASS=OPERCMDS,
  COMMAND=VARY TCP, USER=SYSADMIN
```

This message indicates that the user was validated in the IBM Z OMEGAMON Network Monitor resource profile, but the user was not permitted to the TCPIP.MVS.DROP profile of the OPERCMDS class.

For more information, see the "Enable security on the IBM Tivoli OMEGAMON enhanced 3270 user interface" topic in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*. For information on issuing Take Action commands from the enhanced 3270 user interface, see the *IBM Z OMEGAMON Network Monitor: Enhanced 3270 User Interface User's Guide.*

Restricting access to the Mainframe Networks Command Log and Response workspace

The IBM Z OMEGAMON Network Monitor monitoring agent has a unique workspace associated with prefixed Take Action commands: the Command and Response Log workspace. This enhanced 3270 workspace is similar to the Tivoli Enterprise Portal Command Log workspace. Commands in both workspaces are displayed in a "last in, first out" order. The Tivoli Enterprise Portal workspace displays the commands that are issued by the user ID that logged into Tivoli Enterprise Portal, unless the user is given UPDATE access to the `KN3.**.TAKEACTION.ADMIN` resource profile, in which case all commands and all responses issued by all users are displayed. A similar mechanism is available in the enhanced 3270 user interface workspace, an enhanced 3270-based Command and Response Log workspace, shown in Figure 2 on page 59.

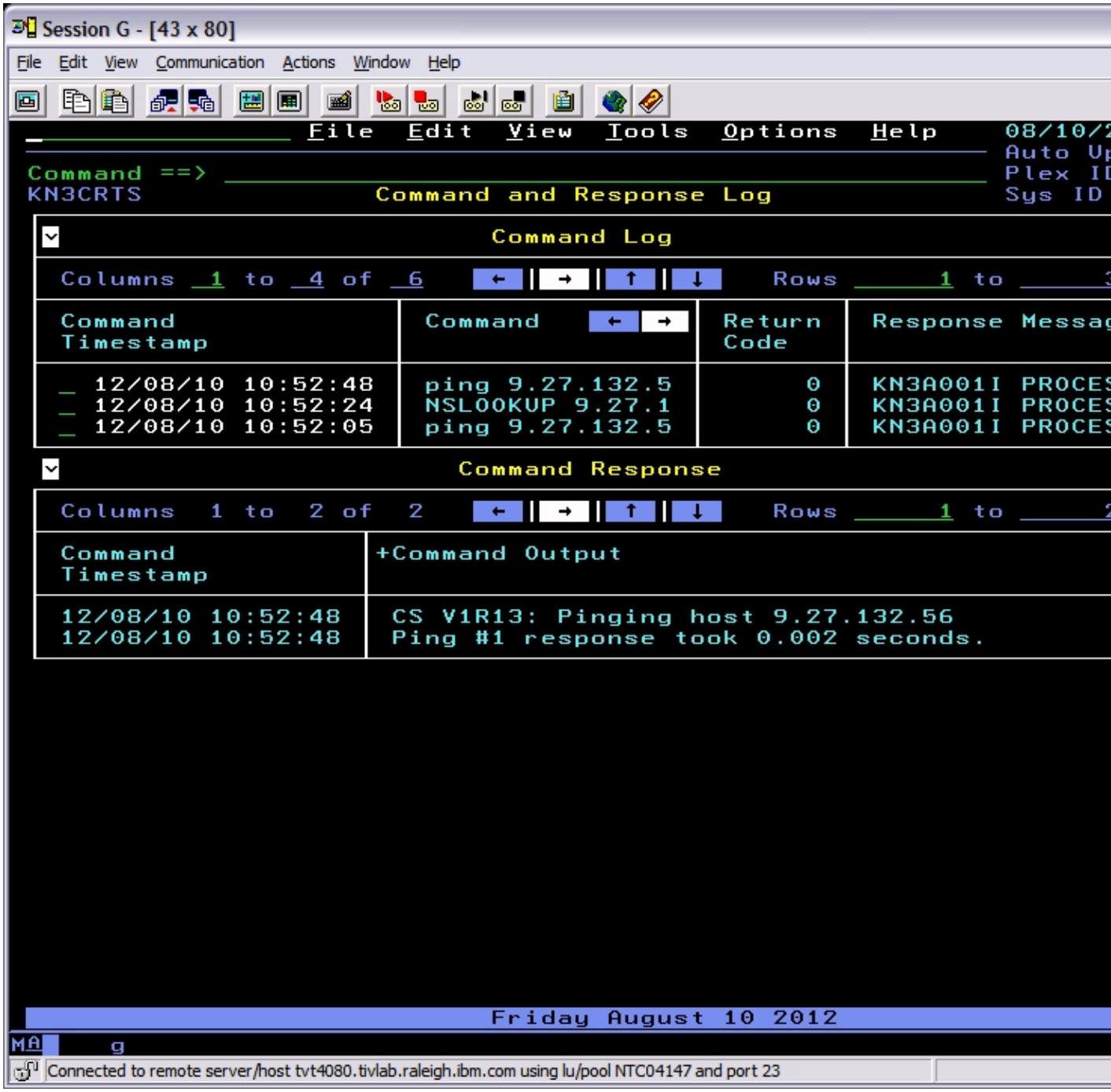


Figure 2. Command and Response Log workspace (KN3CRTS)

To control display of the commands and command output in the command log, create an ADMIN resource profile in either the global security class or the override security class, similar to the following:

```
KN3.**.TAKEACTION.ADMIN
```

where ADMIN means that a user or user group has permission to view all Take Action command and responses for that user and other users. If this resource is not defined and users or groups are not permitted or granted access to this resource, a user is only be allowed to see Take Action commands and responses issued by that user. Users with UPDATE access to `KN3.**.TAKEACTION.ADMIN` can see commands and command responses issued by all users. For information about setting up this command profile, see the SAF appendix of the *IBM Z OMEGAMON Network Monitor: User's Guide* .

Setting up a resource profile

The authority to transmit Take Action requests from the OMEGAMON enhanced 3270 user interface or TEP to an MfN agent instance is verified by checking for access to a SAF resource named in this pattern:

```
KN3.<msn>.TAKEACTION
```

Where *<msn>* is a managed system name. A managed system name typically identifies a unique Tivoli Enterprise Monitoring Server agent instance. In this statement, TAKEACTION is a literal. Unless a matching SAF profile exists to control access to a given Take Action command, any request to transmit an action to the managed system name is denied.

Typically you define a resource profile that restricts the access to all users (UACC(NONE)) and then PERMIT access to these resources for user IDs or groups. The following examples show resource definitions you may wish to define:

- To restrict access to issue IBM Z OMEGAMON Network Monitor Take Action commands from the enhanced 3270 user interface:

  ```
  RDEFINE security_class KN3.**.TAKEACTION UACC(NONE)
  ```

- To restrict access to issue IBM Z OMEGAMON Network Monitor Take Action commands from the enhanced 3270 user interface on a particular TCPIP stack and system:

  ```
  RDEFINE security_class KN3.<msn>.TAKEACTION UACC(NONE)
  ```

- To restrict access to IBM Z OMEGAMON Network Monitor Take Action Commands:

  ```
  RDEFINE security_class KN3.**.TAKEACTION.* UACC(NONE)
  RDEFINE security_class KN3.**.TAKEACTION.PING UACC(NONE)
  RDEFINE security_class KN3.**.TAKEACTION.TRACERTE UACC(NONE)
  RDEFINE security_class KN3.**.TAKEACTION.NSLOOKUP UACC(NONE)
  RDEFINE security_class KN3.**.TAKEACTION.DROP    UACC(NONE)
  ```

- To restrict access to view all Take Action commands:

  ```
  RDEFINE security_class KN3.**.TAKEACTION.ADMIN   UACC(NONE)
  ```

When these resource profiles are defined, refresh the security class by using the following command:

```
SETROPTS RACLIST(security_class) REFRESH
```

Note: This comment can replace all text up to the paragraph before the first PERMIT definition.

You can define a profile named KN3.*<msn>*.TAKEACTION by entering these commands:

```
RDEFINE $KN3SEC KN3.<msn>.TAKEACTION UACC(NONE)
SETROPTS RACLIST($KN3SEC) REFRESH
```

More generally, you could define a profile to control all Take Action commands:

```
RDEFINE $KN3SEC KN3.**.TAKEACTION.* UACC(NONE)
SETROPTS RACLIST($KN3SEC) REFRESH
```

Granting access to individual user IDs or groups

After the resources are defined, grant access to individual user IDs or groups by using definitions such as the ones that follow:

- To enable a user ID or group to issue all IBM Z OMEGAMON Network Monitor Take Action commands from the enhanced 3270 user interface on any system:

  ```
  PERMIT KN3.**.TAKEACTION ID(userid) ACCESS(UPDATE) CLASS(security_class)
  ```

- To enable a user ID or group to issue all IBM Z OMEGAMON Network Monitor Take Action commands on any system:

```
PERMIT KN3.**.TAKEACTION.* ID(userid) ACCESS(UPDATE) CLASS(security_class)
```

- To enable a user ID or group to issue all IBM Z OMEGAMON Network Monitor Take Action commands on a specific TCPIP stack and system:

```
PERMIT KN3.<msn>.TAKEACTION.* ID(userid) ACCESS(UPDATE) CLASS(security_class)
```

- To enable a user ID or group to issue a specific IBM Z OMEGAMON Network Monitor Take Action command on any system:

```
PERMIT KN3.**.TAKEACTION.DROP ID(userid) ACCESS(UPDATE) CLASS(security_class)
PERMIT KN3.**.TAKEACTION.PING ID(userid) ACCESS(UPDATE) CLASS(security_class)
PERMIT KN3.**.TAKEACTION.TRACERTE ID(userid) ACCESS(UPDATE) CLASS(security_class)
PERMIT KN3.**.TAKEACTION.NSLOOKUP ID(userid) ACCESS(UPDATE) CLASS(security_class)
```

- To enable a user ID or group to view all IBM Z OMEGAMON Network Monitor Take Action commands and responses issued by all users:

```
PERMIT KN3.**.TAKEACTION.ADMIN ID(userid) ACCESS(UPDATE) CLASS(security_class)
```

After you permit users to the various resource profiles, issue the following commands to ensure these permissions have taken effect.

```
SETROPTS GENERIC(security_class) REFRESH
SETROPTS RACLIST(security_class) REFRESH
SETROPTS GLOBAL(*) REFRESH
```

You can view the current SAF class definitions and permissions by issuing the following command:

```
RLIST security_class * AUTHUSER
```

If no matching SAF profile exists to protect a Take Action command, that Take Action is denied.

Deploy the configuration

Using PARMGEN and other methods for deploying configurations throughout your environment are not part of this product information.

The *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide* includes scenarios that illustrate various methods for using the PARMGEN method to replicate a configuration of Tivoli Management Services components and monitoring agents across an enterprise. These scenarios assume that you are using system variables (IBM symbolics) and consistent naming conventions for data set names, started tasks, and VTAM applids on all your LPARs.

Scenarios are available in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: PARMGEN Reference*. These implementation scenarios include:

- Scenario PGN01: Performing a pristine install of the monitoring server and two OMEGAMON agents
- Scenario PGN02: Performing a pristine install using shared libraries
- Scenario PGN03: Performing a pristine install of a high-availability hub monitoring server
- Scenario PGN04: Cloning an existing environment but converting its hub monitoring server to a remote
- Scenario PGN05: Upgrading an existing environment to the current release
- Scenario PGN06: Cloning an existing environment to run on a different LPAR
- Scenario PGN07: Upgrading an agent-only runtime environment to PARMGEN Phase 2
- Scenario PGN07A: Converting an environment from ICAT to PARMGEN
- Scenario PGN07B: Upgrading your environment to PARMGEN Phase 2

The *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Upgrade Guide* supports the following upgrade scenarios:

- Scenario A: Upgrading the z/OS monitoring server only
- Scenario B: Upgrading the z/OS monitoring server and monitoring agents
- Scenario C: Adding a monitoring agent and upgrading the z/OS monitoring server
- Scenario D: Upgrading monitoring agents in an existing runtime environment without a z/OS monitoring server
- Scenario E: Upgrading additional products in an upgraded environment

Relink the runtime environments

After all configuration is complete and you have loaded the runtime environment, you must relink the runtime environments by editing and running a linkedit job.

About this task

This linkedit operation is an option on the Parameter Generator Workflow - Welcome panel. From this menu, select option **11. Submit** to display the **SUBMIT BATCH JOBS TO COMPLETE PARMGEN SETUP** panel. From this panel, select option **9. KCIJPLNK ASM/Link RKANMODU modules**. See the *IBM Z Monitoring and IBM Tivoli Management Services on z/OS: Common Planning and Configuration Guide* for more information about performing this task in PARMGEN.

```
//* ****************************************************************
//* IMPORTANT: Before executing this JCL, update the jobcard with
//*            the following values appropriate for this system :
//*            thilev = SMP/E target high-level qualifier
//*            rhilev = Runtime high-level qualifier
//*            mhilev = mid level qualifier
//*            rtename= RTE name
//* ************************************************************
//* IBM Z OMEGAMON Network Monitor LOAD EXTENSIONS
//* ************************************************************
//LNKEDIT  EXEC PGM=IEWL,REGION=0M,
//         PARM='AMODE=31,MAP,XREF'
//SYSLIB   DD  DISP=SHR,
//         DSN=CEE.SCEELKED
//OBJMOD   DD  DISP=SHR,
//         DSN=thilev.TKANMODS
//SYSLMOD DD DISP=SHR,
//           DSN=rhilev.midlev.rtename.RKANMODU
//SYSPRINT DD  SYSOUT=*
//SYSLIN   DD  *
  INCLUDE OBJMOD(KN3ACTCM)
  ENTRY   CEESTART
  SETCODE AC(1)
  SETSSI D4E3C500
  NAME    KN3ACTCS(R)
/*
//* ************************************************************
//* IBM Z OMEGAMON Network Monitor LOAD EXTENSIONS #2
//* ************************************************************
//LNKEDT2  EXEC PGM=IEWL,REGION=0M,
//         PARM='AMODE=31,MAP,XREF'
//SYSLIB   DD  DISP=SHR,
//         DSN=CEE.SCEELKED
//         DD  DISP=SHR,
//         DSN=SYS1.CSSLIB
//OBJMOD   DD  DISP=SHR,
//         DSN=thilev.TKANMODS
//SYSLMOD DD DISP=SHR,
//           DSN=rhilev.midlev.rtename.RKANMODU
//SYSPRINT DD  SYSOUT=*
//SYSLIN   DD  *
  INCLUDE OBJMOD(KN3ANMLM)
  ENTRY   CEESTART
  SETCODE AC(1)
  SETSSI D4E3C500
  NAME    KN3ANMON(R)
/*
```

Verifying the configuration

After you configure your products and complete the post-configuration tasks, you are ready to confirm that the products and components can run and communicate with each other.

Two verification scenarios are supported:

Verifying configuration if you configured both Tivoli Enterprise Portal and the Enhanced 3270 user interface

Use this verification procedure if you configured both Tivoli Enterprise Portal and the Enhanced 3270 user interface (enhanced 3270UI).

About this task

Start the components and verify their operation, as described in this section. If you encounter problems, see the *IBM Tivoli Monitoring: Troubleshooting Guide* and the troubleshooting guides for each of your monitoring agents. If you see error messages, see *IBM Tivoli Monitoring: Messages*.

Procedure

1. Start your hub Tivoli Enterprise Portal using the following command (shown using the default started task procedure name). Issue the following command from the z/OS system console to start the Tivoli Enterprise Portal:

   ```
   S IBMDS
   ```

   Note: Use the stop command (P IBMDS) to stop the Tivoli Enterprise Monitoring Server.
2. Verify that the Tivoli Enterprise Monitoring Server has started successfully. You should see the following message displayed on the z/OS system console or in SYSLOG or in the RKLVLOG for the monitoring server (TEMS) started task procedure:

   ```
   KO4SRV032 Tivoli Enterprise Monitoring Server (TEMS) startup complete.
   ```
3. From the z/OS system console, issue the following command (shown using the default started task procedure name) to start the IBM Z OMEGAMON Network Monitor monitoring agent.

   ```
   S IBMN3
   ```

   Note: Use the stop command (P IBMN3) to stop the IBM Z OMEGAMON Network Monitor monitoring agent.
4. Verify that the IBM Z OMEGAMON Network Monitor Monitoring Agent has started successfully. You should see the following message displayed in the z/OS SYSLOG:

   ```
   IST1928I SNAMGMT CONNECTION TO KN3USER IS ACTIVE
   ```

   You should also see the following message displayed in the RKLVLOG for the IBM Z OMEGAMON Network Monitor monitoring agent:

   ```
   KN3PN001 IBM Z OMEGAMON Network Monitor INITIALIZATION COMPLETED
   ```
5. From the z/OS system console, issue the following command (shown using the default started task procedure name) to start the enhanced 3270UI.

   ```
   S IBMTOM
   ```

   Note: Use the stop command (P IBMTOM) to stop the enhanced 3270UI.
6. Verify that the enhanced 3270UI started successfully. You should see the following message displayed in the SYSPRINT log for the enhanced 3270UI:

   ```
   KOBGW0000I: Enhanced 3270 User Interface address space initialized successfully
   ```

7. Start the Tivoli Enterprise Portal Server and the **Tivoli Enterprise Portal Desktop** from the **Manage Tivoli Enterprise Monitoring Services** window. You can launch the **Manage Tivoli Enterprise Monitoring Services** window by selecting **Start > All Programs > IBM Tivoli Monitoring > Manage Tivoli Enterprise Monitoring Services**. Locate entries for Tivoli Enterprise Portal and **Tivoli Enterprise Portal Desktop** in the Managing Tivoli Enterprise Monitoring Server Services windows to verify that they are installed. Start these components. For example, on Windows systems, you would perform the following steps:
   a) Right-click **Tivoli Enterprise Portal Server** and choose **Start** to start Tivoli Enterprise Portal Server (if it is not already started). Verify that the status is **Started**.
   b) Right-click the **Tivoli Enterprise Portal Desktop** and choose **Start**. Log on to the Tivoli Enterprise Portal desktop client. The default user ID is **sysadmin**. There is no default password unless a password has been specified by your security administrator.
   c) Verify that the Tivoli Enterprise Portal starts and that the **Enterprise Status** window can be displayed.
8. Verify that the IBM Z OMEGAMON Network Monitor monitoring agent shows a status of **ONLINE** in the Managed Systems Status view of the Enterprise Status window.
9. Verify that the IBM Z OMEGAMON Network Monitor monitoring agent is configured correctly to collect the data you want:
   a) Open Tivoli Enterprise Portal and expand the z/OS Systems leaf on the Navigation tree.
   b) Find the z/OS system you have just configured the IBM Z OMEGAMON Network Monitor monitoring agent instance to monitor.
   c) Expand the navigation tree for that system until you can see the IBM Z OMEGAMON Network Monitor agent node, *mfnAgentProcName:systemSMFID*:KN3AGENT.
   d) Click on this node to display the Agent Status workspace. This workspace lets you easily review your Mainframe Networks configuration settings.
   e) Verify that you can see data in this workspace. If so, then the Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, Tivoli Enterprise Monitoring Server, and the IBM Z OMEGAMON Network Monitor monitoring agent are communicating successfully.
   f) Examine the information displayed in this workspace to ensure that it is consistent with how you configured this monitoring agent. Look for the following characteristics.
      - Verify that the Agent User Name and Group Name attributes are correct for your enterprise.
      - Verify that the collection options you specified are reflected correctly in the SNA Collector Status and the TCP Collector Status tables.
      - Does the TCP Collector SNMP Parameter Dataset Name attribute in the Agent Status table have a value of **UNKNOWN**? If so, SNMP data will not be collected. The agent procedure specified a file that could not be opened or did not specify a file at all. See “Format of the SNMP configuration file” on page 543.
      - Does the SNA Collection Started attribute in the Agent Status table have a value of **No**? If you configured this instance of the monitoring agent to collect VTAM environment and buffer pool data, the value should be **Yes**. If it is not, then there is a problem with the VTAM major node or the VTAM PMI exit. See “Vary the VTAM major node active and copy it to your VTAMLST library” on page 48.
      - Do the IP address, SNMP Agent Port, and SNMP Version columns in the TCP Collector Status table display correct information for the TCP/IP stacks you want to monitor? If not, you may have a problem with the information specified in the TCP Collector SNMP Parameter Dataset identified in the Agent Status table. See “Format of the SNMP configuration file” on page 543.
10. Continue to expand the Navigation tree until you see the leaves for a TCP/IP stack and for VTAM. Select **Applications** under one of the TCP/IP stacks and verify that data is being displayed.
11. Select the **OSA** subnode and verify that data is being displayed. If no data is being displayed and the value for the OSA Statistics Collection attribute in the Agent Status workspace is "Yes," ensure that the OSA-Express Direct SNMP subagent (IOBSNMP) started task is running. See “Starting the OSA

adapter SNMP subagent" on page 23 for information on how to configure IOBSNMP and "Verifying the z/OS environment setup" on page 24 for information on verifying this configuration.

12. Verify that the enhanced 3270UI is configured correctly to collect the data that you want. See Step 7 of "Verifying configuration if you configured only the Enhanced 3270 user interface" on page 65 for detailed information about performing this validation.

Results

For more information about the enhanced 3270UI, see the *Using* section of the *IBM Z OMEGAMON Network Monitor* documentation and the *Reference* section of the *IBM Z Monitoring and Tivoli Management Services on z/OS: Shared documentation*.

Verifying configuration if you configured only the Enhanced 3270 user interface

Use this verification procedure if did not configure Tivoli Enterprise Portal, but configured only the Enhanced 3270 user interface (enhanced 3270UI).

About this task

Start the components and verify their operation, as described in this section. If you encounter problems, see the *IBM Tivoli Monitoring: Troubleshooting Guide* and the troubleshooting guides for each of your monitoring agents. If you see error messages, see *IBM Tivoli Monitoring: Messages*.

Procedure

1. Start your hub Tivoli Enterprise Monitoring Server using the following command (shown using the default started task procedure name). Issue the following command from the z/OS system console to start the Tivoli Enterprise Monitoring Server:

   ```
   S IBMDS
   ```

   Note: Use the stop command (P IBMDS) to stop the Tivoli Enterprise Monitoring Server.
2. Verify that the Tivoli Enterprise Monitoring Server has started successfully. You should see the following message displayed on the z/OS system console or in SYSLOG or in the RKLVLOG for the monitoring server (TEMS) started task procedure:

   ```
   KO4SRV032 Tivoli Enterprise Monitoring Server (TEMS) startup complete.
   ```
3. From the z/OS system console, issue the following command (shown using the default started task procedure name) to start the IBM Z OMEGAMON Network Monitor monitoring agent.

   ```
   S IBMN3
   ```

   Note: Use the stop command (P IBMN3) to stop the IBM Z OMEGAMON Network Monitor monitoring agent.
4. Verify that the IBM Z OMEGAMON Network Monitor Monitoring Agent has started successfully. You should see the following message displayed in the z/OS SYSLOG:

   ```
   IST1928I SNAMGMT CONNECTION TO KN3USER IS ACTIVE
   ```

   You should also see the following message displayed in the RKLVLOG for the IBM Z OMEGAMON Network Monitor monitoring agent:

   ```
   KN3PN001 IBM Z OMEGAMON Network Monitor INITIALIZATION COMPLETED
   ```
5. From the z/OS system console, issue the following command (shown using the default started task procedure name) to start the enhanced 3270UI.

   ```
   S IBMTOM
   ```

   Note: Use the stop command (P IBMTOM) to stop the enhanced 3270UI.

6. Verify that the enhanced 3270UI started successfully. You should see the following message displayed in the SYSPRINT log for the enhanced 3270UI:

```
KOBGW0000I: Enhanced 3270 User Interface address space initialized successfully
```

7. Verify that the enhanced 3270UI is configured correctly to collect the data that you want.
   a) Use this command to log on to the enhanced 3270UI from z/OS environment:

   ```
   LOGON APPLID(CTDOBAP)
   ```

   This command causes the enhanced 3270UI logon screen to be displayed.

   b) Log on to the enhanced 3270UI, using a valid user ID and password. If this log in fails, ensure that you completed the configuration required in "Completing the configuration" on page 42, especially those tasks under "Enable security" on page 55. The first screen you see is the Enterprise Summary workspace (KOBSTART), which serves as a "dashboard" for the IBM Z Monitoring Suite that use the enhanced 3270UI. Each agent has a subpanel contained within this main panel.

   c) Enter this command to display the Enterprise Network Workspaces popup options menu:.

   ```
   NETMENU
   ```

   The **Enterprise Networks Workspaces** pop-up window is displayed.

   d) Type **T** on the command line and press **Enter** to display the **Enterprise TCPIP Stack Performance Overview** workspace. In this workspace, you should see IP data.

   Validate that the values for the **System ID** and **TCPIP STC Name** are correct, that is, that they match the system ID of the system on which you configured the IBM Z OMEGAMON Network Monitor monitoring agent and the TCPIP STC entries for the TCP/IP stacks that the IBM Z OMEGAMON Network Monitor monitoring agent is configured to monitor.

   If you see no data, view the agent RKLVLOG and verify that the agent has successfully connected to its the monitoring server. Search for this connection message:

   ```
   Successfully connected to CMS system_id:CMS using ip.pipe:#x.xx.xx.xx.xxx.
   ```

   Where *system_id* is the name of the system on which your monitoring server is running and *x.xx.xx.xx.xxx* is the IP address of this system.

   If these values are incorrect, ensure that you performed the system setup tasks described in "Preparing your z/OS environment" on page 21. See the RKLVLOG for more information.

   e) Type NETMENU on the command line and press **Enter**.

   The **Enterprise Networks Workspaces** pop-up window is displayed.

   f) Type **M** on the command line and press **Enter** to display the **Enterprise Memory and CSM Storage Overview** workspace.

   Validate that you see information about memory and CSM storage. Validate that the values for the **System ID** and **TCPIP STC Name** are correct, that is, that they match the system ID of the system on which you configured the IBM Z OMEGAMON Network Monitor monitoring agent and the TCPIP STC entries for the TCP/IP stacks that the IBM Z OMEGAMON Network Monitor monitoring agent is configured to monitor.

   If these values are incorrect, ensure that you performed the system setup tasks described in "Preparing your z/OS environment" on page 21. See the RKLVLOG for more information.

   g) Type NETMENU on the command line and press **Enter**.

   The **Enterprise Networks Workspaces** pop-up window is displayed.

   h) Type **B** on the command line and press **Enter** to display the **Enterprise OSA Express Channels Overview** workspace.

   Validate that you see correct information about the OSA Express channels in your environment. Validate that the **System ID** is correct, that is, that it matches the system ID of the system on which

you configured the IBM Z OMEGAMON Network Monitor monitoring agent . Validate that the channel numbers displayed on this workspace reflect the correct OSA-Express devices connected to this system.

If you see no data, verify that the z/OS TCP/IP SNMP Subagent (OSNMPD by default) and the OSA Express subagent (IOBSNMP or IOASNMP by default) are started on the TCP/IP stacks that are connected to OSA-Express devices. Ensure that you performed the OSA setup task described in "Preparing your z/OS environment" on page 21. See the RKLVLOG for additional information.

Note: You can easily determine if the monitoring agent is online using the KOBMSNS Only Managed Systems workspace to determine if the IBM Z OMEGAMON Network Monitor monitoring agent is currently registered with the hub monitoring server. When the IBM Z OMEGAMON Network Monitor agent address space is active but shows the MS Online Status value as **N** (meaning it is offline), this usually means that a configuration error is preventing the monitoring services components from communicating with each other. It might also be that the IBM Z OMEGAMON Network Monitor agent address space had experienced an abend. More details about using this workspace and other troubleshooting scenarios are found in the *IBM Z OMEGAMON Network Monitor: Troubleshooting Guide*.

Results

For more information about the enhanced 3270UI, see the *Using* section of the *IBM Z OMEGAMON Network Monitor* documentation and the *Reference* section of the *IBM Z Monitoring and Tivoli Management Services on z/OS: Shared documentation*.

Appendix A. Reference

Reference material supplements the information provided in the planning, upgrading, configuring, monitoring, and troubleshooting documentation.

Overview of configuration parameters

IBM Z OMEGAMON Network Monitor uses parameters for setting and storing configuration values.

To set the values of these parameters, you use the PARMGEN configuration method. With the PARMGEN method, you edit a comprehensive list of parameters for configuring all installed products and components, and then submit a series of jobs to create a complete runtime environment with the parameter values you specified.

This guide is a reference for the IBM Z OMEGAMON Network Monitor parameters. Common information about using the PARMGEN configuration method is found in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: PARMGEN Reference*. Definitions of common parameters, such as those used by runtime environments (RTE parameters) and Tivoli Enterprise Monitoring Server (TEMS parameters), are found in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Parameter Reference*.

A great deal of information is available in this parameter reference about each parameter, including a description of the parameter, its name in both BATCH and PARMGEN configuration methods, where it is found in the Configuration Tool (name, panel, panel ID, and field), where it is stored, and related parameters (those that are part of the same PARMGEN group).

Attention: Do not attempt to do all configuration for this product using only this guide. This reference book must work in tandem with the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide* and the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Parameter Reference*.

Location of stored configuration parameters

Most configuration parameters are stored in KN3ENV or KN3SYSIN members, which contain environment and startup values, though some parameters are stored in other locations.

Most configuration parameters and their configured values are stored in the KN3ENV or KN3SYSIN members of the *&rhilev.&midlev.&rtename.*RKANPARU data set for each runtime environment, where *&rhilev* is the runtime high-level qualifier, *&midlev* is the mid-level qualifier, and *&rtename* is the name of the runtime environment.

The parameters that are stored in the KN3ENV member are environment variables, which determine the operating characteristics of the runtime environment in which products and components are configured. The parameters stored in the KN3SYSIN member are startup parameters, which determine the default startup values for each product or component. Some environment variables and startup parameters are stored in members other than KN3ENV and KN3SYSIN, or in data sets other than RKANPARU.

There are additional parameters that are neither environment variables not startup parameters, but must be included in the runtime libraries for the products and components to operate correctly.

Sample KN3ENV member

This sample KN3ENV member shows examples of the parameters that are environment variables.

The parameters stored in the KN3ENV member are environment variables, which determine the operating characteristics of the runtime environment in which products and components are configured. The sample that follows shows examples of these parameters as they are defined in a sample KN3ENV member.

Your KN3ENV member will be similar to this one, but might have more parameters or fewer parameters, depending on your configuration. This is just a sample.

```
KDE_TRANSPORT=\
     IP6.PIPE PORT:1918 USE:N\
     IP6.UDP PORT:1918 USE:N\
     IP.SPIPE PORT:3660 USE:N\
     IP6.SPIPE PORT:3660 USE:N\
     IP.PIPE PORT:1918\
     IP.UDP PORT:1918\
     SNA.PIPE PORT:135
 KDCFC_ALIAS=CTDN3NC
 KDCFC_MODE=CANCTDCS
 KBB_RAS1=ERROR
 KDC_DEBUG=N
 CT_CMSLIST=\
 IP.PIPE:NMPIPL16.TIVLAB.RALEIGH.IBM.COM;\
 IP.UDP:NMPIPL16.TIVLAB.RALEIGH.IBM.COM;\
 SNA:USIBMNT.CTDDSLB.CANCTDCS.SNASOCKETS;
 ** Global SAF class name:
 *RTE_SECURITY_CLASS=
 ** OMEGAMON XE on z/OS SAF Action class name override
 KN3_SECURITY_ACTION_CLASS=OMEGDEMO
 KN3_DXL_APPLID=\
 CNM01
 KN3_DXL_USERDATA=\

 CTIRA_IP_PORT=0
 LANG=en_US.ibm-037
 * If AUDIT_TRACE is not specified, AUDIT_TRACE=BASIC internal default is
 * set.  AUDIT_TRACE parameter is generated as commented out in
 * KN3ENV
 *AUDIT_TRACE=BASIC
 * If AUDIT_MAX_HIST is not specified, AUDIT_MAX_HIST=100 internal
 * default is set.  AUDIT_MAX_HIST parameter is generated as commented
 * out in KN3ENV
*AUDIT_MAX_HIST=100
*ITM_DOMAIN=
TEMA_SDA=Y
```

Sample KN3SYSIN member

This sample KN3SYSIN member shows in-context examples of the startup parameters.

The parameters stored in the KN3SYSIN member are startup parameters, which determine the default startup values for IBM Z OMEGAMON Network Monitor. The sample that follows shows examples of these parameters as they are defined in a sample KN3SYSIN member.

Your KN3SYSIN member will be similar to this one, but might have more parameters or fewer parameters, depending on your configuration. This is just a sample.

```
* STARTUP PARMS
INITIAL(KN3AGST)
OPSTART(KN3OPST)
INITLIST(KN3INIT)
LOADLIST(KRALLIST)
LOADLIST(KN3LLIST)
WTO(Y)
CONFIRM(0)
LGSA(Y)
LIMIT(24,X)
LIMIT(20,P)
TASKS(2)
LSRPOOL(32768,32)
RESERVE(2048,P)
RESERVE(2048,X)
SDUMP(Y)
MINIMUM(768000,X)
```

Configuring IBM Z OMEGAMON Network Monitor using the PARMGEN method

You configure IBM Z OMEGAMON Network Monitor by accepting or customizing the values of parameters that begin with KN3.

You configure the OMEGAMON XE component of the monitoring product to define enterprise-level entities, assign the current runtime environment to a Sysplex, install product-specific data on the Tivoli Enterprise Monitoring Server, and register the IBM Z OMEGAMON Network Monitor monitoring agent in the Tivoli Enterprise Monitoring Server address space. You also configure the persistent data store for the product historical data and allocate the data sets to store enterprise data. These parameters are specified in the KN3 section of the PARMGEN configuration profile.

Default values are provided for all required parameters and some optional ones. If you do not want to customize these parameters, and you do not want to enable optional features, you can complete the configuration by accepting these defaults. You can also specify custom values for optional parameters that have no defaults. You must specify values for these parameters in order to activate those features.

For guidance on setting parameter values, see the following sources of information:

- Comments in the configuration profiles and jobs
- Online help for the configuration profile

  If the supplied KCIRPLBS macro has been copied to your SYSPROC concatenation, you can enter TSO KCIRPLBS at the ISPF command line to run the help macro. Place the cursor anywhere on the line containing the parameter for which you want help text displayed, and press PF14.
- *IBM Tivoli OMEGAMON XE and IBM Tivoli Management Services on z/OS: PARMGEN Reference*
- *IBM Tivoli OMEGAMON XE and IBM Tivoli Management Services on z/OS: Common Parameter Reference*
- *IBM Z OMEGAMON Network Monitor: Parameter Reference.*

Before you configure the IBM Z OMEGAMON Network Monitor agent using the PARMGEN method, you should have completed the tasks listed in the complete the configuration section of the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide*.

Table 10. Tasks to complete before configuring IBM Z OMEGAMON Network Monitor

Configuration task	**Location of instructions**
Set up PARMGEN work libraries for the runtime environment	*IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: PARMGEN Reference*
Set up the PARMGEN configuration profile for the runtime environment	*IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: PARMGEN Reference*
Configure a Tivoli Enterprise Monitoring Server on z/OS	*IBM Tivoli Management Services on z/OS: Configuring the Tivoli Enterprise Monitoring Server on z/OS* and *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Parameter Reference*
(Optional) Configure the OMEGAMON enhanced 3270 user interface address space	*IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide* **Note:** You only need to configure one OMEGAMON enhanced 3270 user interface address space. If you have already configured this address space for another version 5.1.0 OMEGAMON monitoring agent on z/OS, you do not need to repeat this configuration step.

Tip: If you are enabling self describing agents, configure a stand-alone high-availability hub monitoring server. You can use a high-availability hub to apply maintenance or upgrades without recycling the hub. If

you have an existing static hub to which agents report, convert the hub to a remote and configure all the remotes to report to the new high-availability hub.

Configuring SAF security for Take Action commands
The security for Take Action commands provided with the IBM Z OMEGAMON Network Monitor is implemented through direct System Authorization Facility (SAF) calls and is based on profiles and resource names. Configure security before you can run these commands.

You must supply custom values for the security class and command-level control for Take Action commands.

IBM Z OMEGAMON Network Monitor agent Take Action commands cannot be successfully executed unless a security class is defined to the SAF security manager and the security class name configured in each runtime environment in which an IBM Z OMEGAMON Network Monitor monitoring agent is configured.

To secure Take Action commands, you must configure the global security parameter (RTE_SECURITY_CLASS). Optionally, you can use the SAF class name override parameter (KN3_SECURITY_ACTION_CLASS) to specify a separate class for securing individual Take Action commands. After each security class has been defined, profiles must be created to control access to individual commands and user IDs must be given UPDATE access to those profiles.

Default values

All components and the monitoring agent have default values defined for them.

Some parameters have only one default value, and some have more than one. For example, TMS:Engine (Tivoli Monitoring Services:Engine) sets this global default value for the KDS_TEMS_STORAGE_LIMIT_EXTEND parameter:

```
LIMIT(16,X)
```

However, the PARMGEN files override the TMS:Engine default and show a different default value for the Tivoli Enterprise Monitoring Server:

```
LIMIT(24,X)
```

When you edit a default value in a PARMGEN file, your edited value overrides the PARMGEN default value, which has already overridden the TMS:Engine default value (if a TMS:Engine default value exists). If you configured your environment using PARMGEN, the value for the KDS_TEMS_STORAGE_LIMIT_EXTEND parameter would be 24.

The IBM Z OMEGAMON Network Monitor monitoring agent KN3_X_AGT_STORAGE_LIMIT_EXTEND parameter has still a different default value.

```
LIMIT(24,X)
```

If the monitoring agent is configured in the TEMS address space, the TEMS value applies to both the TEMS and the monitoring agent, and the monitoring agent does not have its own value. If the monitoring agent is configured stand-alone, then the monitoring agent value for each parameter overrides the TME:Engine value, and the TEMS value has no effect on the monitoring agent.

If the hub monitoring server and the remote monitoring server reside on z/OS, they must also be modified to use LIMIT(24,X). Follow the process outlined in the *Configuring the Tivoli Enterprise Monitoring Server on z/OS* book and ensure that the KDS_TEMS_STORAGE_LIMIT_EXTEND parameter is set to greater than or equal to 24.

Default values for runtime environment and Tivoli Enterprise Monitoring Server parameters are documented in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Parameter Reference*. Default values for this monitoring agent are documented in this guide and are shown in the parameter maps (described in "Obtaining parameter reports" in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*).

Parameter names

Parameters can have different names, such as the Configuration Tool name, PARMGEN parameter name, or BATCH parameter name. Some parameters have **n** or **nn** in their names. Others have batch names designated NA.

Most parameters have several different names:

Parameter name
Name of the parameter as stored in a runtime library. Example: `MINIMUM (768000,X)`

Configuration Tool field name
Name of the field that identifies the parameter on an interactive panel. Example: Minimum extended storage

Batch parameter name
Name of the parameter in the batch parameter member. Example: `KN3_AGT_STOR_MIN_EXT`

PARMGEN name
Name of the parameter in the PARMGEN parameter list. Example: `KN3_AGT_STORAGE_MINIMUM_EXTEND`

Note: Batch parameter names and PARMGEN names are usually different. In this instance, they are similar.

This information unit refers to each parameter by the name that is suitable for the context. For a complete cross-reference of names for the runtime environment and Tivoli Enterprise Monitoring Server parameters, see *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Parameter Reference*. For information about the parameter names for this monitoring agent, see this guide.

Parameters with n or nn in their names

Some parameters include *n* or *nn* in their names. These names containing *n* or *nn* are not the actual names of these commands as you see them in the configuration profile. The *n* or *nn* means that you can have multiple instances of this parameter in your configuration profile. For example, you will most likely have multiple instances of the set of monitoring agent component override commands (for example, KN3_TCPX*nn*_OVRD_CONN or KN3_TCPX*nn*_OVRD_FTP) because you have one set of values for every instance in which you override the global (all stacks) collection values for a specific stack. Likewise, you might have multiple instances of the KN3_AGT_NONSTD*n*_DSN, KN3_AGT_NONSTD*n*_MBR, KN3_AGT_NONSTD*n*_PARM values if you defined several nonstandard parameters. If you cannot find a parameter by searching using its full name, try searching with a part of the name, omitting the numbers that define instance.

Parameters used by the PARMGEN configuration method

The comprehensive list of parameters for this monitoring agent are used by the PARMGEN configuration method are grouped logically in the configuration profile.

The PARMGEN configuration method is the preferred method for configuring the Tivoli Management Services on z/OS components and the OMEGAMON XE products.

With the PARMGEN configuration method, you edit a comprehensive list of parameters for configuring all installed products and components. You then submit a series of jobs to create a complete runtime environment with the parameter values you specified.

If you are an existing Configuration Tool user and already have an existing runtime environment that you want to convert to PARMGEN, you can do this. Refer to the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: PARMGEN Reference* for information about migrating to PARMGEN.

These parameters are found in the configuration profile, which can be generated from an existing RTE. If this is a new installation or if you do not want to base the configuration profile on an existing RTE, a default configuration profile is provided and can be edited. Refer to the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: PARMGEN Reference* to understand the other scenarios for using PARMGEN.

In the configuration profile, the OMEGAMON XE parameters are organized into the groups found in Table 11 on page 74:

Table 11. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile

PARMGEN classification	**Parameters in this group**	**Explanation**
Additional IBM Z OMEGAMON Network Monitor Agent settings	• "KN3_X_AGT_CONFIRM_SHUTDOWN" on page 202 • "KN3_X_AGT_KDC_DEBUG" on page 204 • "KN3_X_AGT_DEBUG_TRACE" on page 203 • "KN3_X_AGT_LGSA_VERIFY" on page 205 • "KN3_X_AGT_LSRPOOL_BUFFER_NUM" on page 206 • "KN3_X_AGT_LSRPOOL_BUFSIZE" on page 207 • "KN3_X_AGT_SDUMP_SVC_SYS1_DUMP" on page 208 • "KN3_X_AGT_STORAGE_LIMIT_EXTEND" on page 210 • "KN3_X_AGT_STORAGE_LIMIT_PRIMARY" on page 211 • "KN3_X_AGT_STORAGE_RESERVE_EXT" on page 212 • "KN3_X_AGT_STORAGE_RESERVE_PRI" on page 213 • "KN3_X_AGT_STORAGE_STGDEBUG" on page 214 • "KN3_X_AGT_TASKS_ATTACHED_NUM" on page 215 • "KN3_X_SECURITY_USER_EXIT" on page 219 • "KN3_X_SECURITY_RESOURCE_CLASS" on page 218	Specifies settings for initializing Tivoli Monitoring: Services (TMS: Engine). These values are usually found in the KN3SYSIN member in the *rhilev.midlev.rtename* . RKANPARU library and are usually updated only with the assistance of IBM Software Support.
Advanced Agent configuration values	• "KN3_AGT_FLUSH_LSR_BUFR_INT_HR" on page 91 • "KN3_AGT_FLUSH_LSR_BUFR_INT_MIN" on page 92 • "KN3_AGT_ICU_LANGUAGE_LOCALE" on page 93 • "KN3_AGT_KGL_WTO" on page 95 • "KN3_AGT_KLX_TCP_TOLERATERECYCLE" on page 97 • "KN3_AGT_STORAGE_DETAIL_INT_HR" on page 107 • "KN3_AGT_STORAGE_DETAIL_INT_MIN" on page 108 • "KN3_AGT_STORAGE_MINIMUM_EXTEND" on page 109 • "KN3_AGT_VIRTUAL_IP_ADDRESS" on page 115 • "KN3_AGT_VTAM_APPL_NCS" on page 118 • "KN3_AGT_WTO_MSG" on page 122	Specifies a wide range of essential agent configuration parameters, including parameters that define such values as where console messages are displayed, whether TCP/IP can be recycled, language of the interface, virtual addresses, and storage-related values.

Table 11. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile (continued)

PARMGEN classification	**Parameters in this group**	**Explanation**
Agent nonstandard parameters	• "KN3_AGT_NSNEWn_VALUE" on page 98 • "KN3_AGT_NONSTDn_DSN" on page 99 • "KN3_AGT_NONSTDn_MBR" on page 100 • "KN3_AGT_NONSTDn_PARM" on page 101 • "KN3_AGT_NSOLDn_VALUE" on page 101	Nonstandard parameters are customer-defined or hidden options that do not correspond to fields in the Configuration Tool interactive panels. This set of parameters defines the values required to establish a nonstandard parameter. Create these parameters under the guidance of IBM Software Support.
Agent parameters: TCP/IP information	• "KN3_SNA_VTAM_COLLECT_DATA" on page 129 • "KN3_SNA_VTAM_SNAC_SNACINTV" on page 130 • "KN3_SNMP_CONFIG_FILE" on page 131 • "KN3_TCP_ALLHPR" on page 132 • "KN3_TCP_COLLECT_STACK" on page 135 • "KN3_TCP_CONN" on page 136 • "KN3_TCP_CSM" on page 134 • "KN3_TCP_EEHPR" on page 137 • "KN3_TCP_FTP" on page 139 • "KN3_TCP_FTP_DSPINTV" on page 140 • "KN3_TCP_GLBS" on page 141 • "KN3_TCP_INTE" on page 143 • "KN3_TCP_INTS" on page 144 • "KN3_TCP_IPSEC" on page 145 • "KN3_TCP_OSA" on page 146 • "KN3_TCP_ROUTE_TBL" on page 148 • "KN3_TCP_ROUTE_TBL_FREQ" on page 149 • "KN3_TCP_SAMPLE_INTERVAL" on page 150 • "KN3_TCP_TN3270" on page 152 • "KN3_TCP_TN3270_DSPINTV" on page 153 • "KN3_TCP_VIO_UNIT" on page 154	Sets the global values for all configurable parameters unique to the IBM Z OMEGAMON Network Monitor monitoring agent.

Table 11. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile (continued)

PARMGEN classification	Parameters in this group	Explanation
Agent's Applids	• "KN3_AGT_VTAM_APPL_AA" on page 115 • "KN3_AGT_VTAM_APPL_KN3INVPO" on page 117 • "KN3_AGT_VTAM_APPL_NCS" on page 118 • "KN3_AGT_VTAM_APPL_OPERATOR" on page 119 • "KN3_AGT_VTAM_APPL_CNM_SPO" on page 116	Specifies the VTAM application IDs (applids) that the agent uses to define communication with the Tivoli Enterprise Monitoring Server. Applids are used for communication with the monitoring server except for KN3_AGT_VTAM_APPL_CNM_SPO, which is used to collect CNM data. These parameters are not used unless you are using SNA (instead of TCP/IP) to communicate with the monitoring server.
Agent's local TCP/IP information	• "KN3_AGT_TCP_HOST" on page 110 • "KN3_AGT_TCP_STC" on page 113 • "KN3_AGT_TCP_KDEB_INTERFACELIST" on page 111 (If the Agent requires network interface list support) • "KN3_AGT_PARTITION_NAME" on page 102 (If the Agent requires address translation support–optional)	Provides the TCP/IP information that the Tivoli Enterprise Monitoring Server uses to communicate with the monitoring agent.
Agent's local VTAM and logon information	• "KN3_AGT_VTAM_APPL_PREFIX" on page 119 • "KN3_AGT_VTAM_NODE" on page 120 •	Specifies the values used by the agent for defining VTAM definitions specific to the monitoring agent.
Agent's primary TEMS TCP/IP information	• "KN3_TEMS_TCP_HOST" on page 189 **Note:** KN3_TEMS_TCP_HOST and KN3_AGT_TCP_HOST must be the same value if KN3_TEMS_LOCAL _CONNECT_FLAG=Y (Agent connects to local TEMS).	Specifies the host name of the Tivoli Enterprise Monitoring Server specific to this monitoring agent. This field is required if you plan to have this server communicate with agents using TCP/IP.
Agent's Primary TEMS VTAM information:	• "KN3_TEMS_VTAM_LU62_DLOGMOD" on page 197 • "KN3_TEMS_VTAM_LU62_MODETAB" on page 198 • "KN3_TEMS_VTAM_NETID" on page 199 • "KN3_TEMS_VTAM_APPL_LLB_BROKER" on page 196	Specifies the VTAM information used by the Tivoli Enterprise Monitoring Server to communicate with the monitoring agent.

Table 11. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile (continued)

PARMGEN classification	Parameters in this group	Explanation
Audit parameters	• "KN3_AGT_AUDIT_ITM_DOMAIN" on page 86 • "KN3_AGT_AUDIT_MAX_HIST" on page 87 • "KN3_AGT_AUDIT_TRACE" on page 88	Specifies the amount of detail, maximum number of entries, and identifier for z/OS SAF tracing.
Define TCP monitoring systems member **Note:** Specify KN3_TCPXxx_* row for each TCP/IP monitored stack. Global default is $$$$ (monitor all TCP/IP stacks).	• "KN3_TCPX" on page 174 • "KN3_TCPXnn_OVRD_GLBS" on page 160 • "KN3_TCPXnn_OVRD_INTE" on page 163 • "KN3_TCPXnn_OVRD_INTS" on page 164 • "KN3_TCPXnn_OVRD_OSA" on page 167 • "KN3_TCPXnn_ROW" on page 175 • "KN3_TCPXnn_SYS_NAME" on page 176 • "KN3_TCPXnn_TCP_STC" on page 177 • "KN3_TCPXnn_TCPIP_PROFILES_DSN" on page 179 • "KN3_TCPXnn_OVRD_GLOBAL_FLAG" on page 162 • "KN3_TCPXnn_OVRD_COLLECT_STACK" on page 155 • "KN3_TCPXnn_OVRD_CONN" on page 157 • "KN3_TCPXnn_OVRD_IPSEC" on page 166 • "KN3_TCPXnn_OVRD_ROUTE_TBL" on page 168 • "KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ" on page 170 • "KN3_TCP_ROUTE_TBL" on page 148 • "KN3_TCP_ROUTE_TBL_FREQ" on page 149 • "KN3_TCPXnn_OVRD_FTP" on page 158 • "KN3_TCPXnn_OVRD_FTP_DSPINTV" on page 159 • "KN3_TCPXnn_OVRD_TN3270" on page 171 • "KN3_TCPXnn_OVRD_TN3270_DSPINTV" on page 172 • "KN3_TCPXnn_TCPIP_PROFILES_MBR" on page 180	Sets the stack-specific values that override the global parameters for all configurable parameters unique to the IBM Z OMEGAMON Network Monitor monitoring agent.
Define TN3270 Telnet session link user values	• "KN3_TN3270_DXL_APPLID" on page 200 • "KN3_TN3270_DXL_USERDATA" on page 201	Specifies the IBM Tivoli NetView for z/OS user ID and password that IBM Z OMEGAMON Network Monitor logs onto dynamically. The applid is the applid for the Tivoli NetView on z/OS application. The user data is the user ID and password that must be passed to NetView for z/OS to complete the login.

Table 11. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile (continued)

PARMGEN classification	Parameters in this group	Explanation
Enable self-describing agent processing	• “KN3_AGT_TEMA_SDA” on page 114	Specifies whether this monitoring agent plans to use the self-describing agent feature.
If the Agent requires address translation support	• “KN3_AGT_PARTITION_NAME” on page 102	Specifies the partition name that identifies the location of this TEMS (namespace) relative to the firewall(s) used for address translation.
If the Agent requires network interface list support	• “KN3_AGT_TCP_KDEB_INTERFACELIST” on page 111	Specifies a list of network interfaces you want the monitoring agent to use. This parameter is required for sites that are running multiple TCP/IP interfaces or network adapters on the same z/OS image.
Persistent datastore table space allocation overrides	• “KN3_PD” on page 123 • “KN3_PD_CYL” on page 124 • “KN3_PD_GRP” on page 125 • “KN3_PD_ROW” on page 127 • “KN3_X_PD_HISTCOLL_DATA_AGT_STC” on page 217 • “KN3_X_PD_HISTCOLL_DATA_TEMS_STC” on page 216	Specifies the information required for this monitoring agent to override the global RTE defaults for space allocation for the persistent data store libraries and for overhead information such as the product dictionary, table records, index records, and buffers to hold overflow data.

Table 11. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile (continued)

PARMGEN classification	**Parameters in this group**	**Explanation**
Protocol port numbers for Agent connection to TEMS	• "KN3_TEMS_TCP_PIPE_PORT_NUM" on page 190 • "KN3_TEMS_TCP_PIPES_PORT_NUM" on page 191 • "KN3_TEMS_TCP_PIPE6_PORT_NUM" on page 192 • "KN3_TEMS_TCP_PIPE6S_PORT_NUM" on page 193 • "KN3_TEMS_TCP_UDP_PORT_NUM" on page 194 • "KN3_TEMS_TCP_UDP6_PORT_NUM" on page 195	Specifies the port numbers used by the protocols specified under "Specify communication protocols preference for TEMS connection" for communication between the monitoring agent and Tivoli Enterprise Monitoring Server.
Secondary TEMS configuration	• "KN3_TEMS_BKUP1_NAME_NODEID" on page 181	Specifies the name of that server if you have defined a backup Tivoli Enterprise Monitoring Server. The BKUP1 values are found in the KN3ENV member in the *rhilev.midlev.rtename* . RKANPARU library to communicate with the backup Tivoli Enterprise Monitoring Server.
Secondary TEMS TCP/IP information	• "KN3_TEMS_BKUP1_TCP_HOST" on page 182	Specifies TCP/IP information for a backup Tivoli Enterprise Monitoring Server if you have defined a backup monitoring server. The BKUP1 values are found in the KN3ENV member in the *rhilev.midlev.rtename* . RKANPARU library to communicate with the backup Tivoli Enterprise Monitoring Server.

Table 11. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile (continued)

PARMGEN classification	Parameters in this group	Explanation
Secondary TEMS VTAM information:	• "KN3_TEMS_BKUP1_VTAM_APPL_LLB_BKR" on page 183 • "KN3_TEMS_BKUP1_VTAM_LU62_DLOGMOD" on page 184 • "KN3_TEMS_BKUP1_VTAM_NETID" on page 185	Specifies VTAM or SNA information for the backup Tivoli Enterprise Monitoring Server if you have defined a backup monitoring server. The BKUP1 values are found in the KN3ENV member in the *rhilev*.*midlev*.*rtename* . RKANPARU library to communicate with the backup Tivoli Enterprise Monitoring Server.
Specify communication protocols preference for TEMS connection	• "KN3_AGT_COMM_PROTOCOLn" on page 90	Details the protocol possibilities for communication between the monitoring agent and Tivoli Enterprise Monitoring Server in the order in which the protocols will be used.
Take Action commands security settings	• "KN3_AGT_PPI_RECEIVER" on page 104 • "KN3_AGT_PPI_SENDER" on page 105 • "KN3_SECURITY_ACTION_CLASS" on page 128	Defines the connection between IBM Z OMEGAMON Network Monitor and Tivoli NetView for z/OS if you use Tivoli NetView for z/OS and specifies whether to override at the agent the SAF security value specified for the runtime environment.
Values that describe the address space	• "KN3_AGT_CONFIGURATION_MODE" on page 89 • "KN3_AGT_STC" on page 106	Specifies the name of the address space where you are running in and the name of your agent PROC.

Table 11. IBM Z OMEGAMON Network Monitor parameters divided into the groups found in the configuration profile (continued)		
PARMGEN classification	**Parameters in this group**	**Explanation**
Values that describe the Primary TEMS the Agent will connect to	• "KN3_TEMS_LOCAL_CONNECT_FLAG" on page 187 • "KN3_TEMS_NAME_NODEID" on page 188	Defines the information required to connect to the local Tivoli Enterprise Monitoring Server.
VTAM Secondary Program Operator (SPO) for Communication Network Management (CNM) interface (optional)	• "KN3_AGT_VTAM_NODE_OMXE" on page 121 • "KN3_AGT_VTAM_APPL_CNM_SPO" on page 116	Defines how the IBM Z OMEGAMON Network Monitor monitoring agent communicates with the VTAM CNM interface to collect monitoring information.

Updating parameter values dynamically without rerunning PARMGEN or the Configuration Tool

You can enable or disable data collection on a per-component basis until the next agent recycle using z/OS MODIFY commands.

The IBM Z OMEGAMON Network Monitor monitoring agent is made up of components that map to data types. By default, each of the components is enabled with a default collection interval of 5 minutes.

You can enable or disable data collection by component, providing more granular control over which types of data are collected. These actions can be specified at the time you configure the IBM Z OMEGAMON Network Monitor monitoring agent or until the affected system or component is recycled using the z/OS MODIFY commands. After a recycle, these values must be set again if you specified them using the z/OS MODIFY commands.

The z/OS MODIFY command is issued when the IBM Z OMEGAMON Network Monitor monitoring agent is running. Then you can use the z/OS MODIFY command to initialize, start, stop, and display the status of components. The following components can be updated using the z/OS MODIFY commands:

- **CONN** for TCP/IP Connection and Application performance data. You can enable or disable collection of TCP/IP Connection and Application performance statistics by starting or stopping the CONN component. The default is to start this component.
- **CSM** for Communications Storage Manager data. You can enable or disable the Communications Storage Manager buffer reporting by starting or stopping the CSM component. The default is to start this component.
- **EEHPR** for Enterprise Extender and High Performance Routing data. You can enable or disable collection of Enterprise Extender and High Performance Routing statistics by starting or stopping the EEHPR component. The default is to start this component.
- **FTP** for FTP session and transfer data. You can enable or disable collection of FTP session and transfer data by starting or stopping the FTP component. Additionally, you can modify the display interval for FTP data. The default is to start this component.
- **GBLS** for TCP/IP Stack Layer statistics data collection. You can enable or disable collection of TCP/IP Stack layer statistics by starting or stopping the GBLS component. The default is to start this component.
- **INTS** for Interface Statistics data collection. You can enable or disable collection of interface statistics by starting or stopping the INTS component. The default is to start this component.

- **INTE** for interface Data Link Control (DLC) data collection. You can enable or disable collection of interface DLC statistics by starting or stopping the INTE component. The default is to start this component.
- **IPSec** for IPSec security extensions to the Internet Protocol. You can start or stop collection of IPSec data. The default is *not* to start this component.
- **OSA** for OSA devices. You can stop and start OSA-enabled data collection. The default is to start this component.
- **ROUTE** for gateways. You can enable or disable the collection of routing information (for example, the gateway table). The default is to start this component. Additionally, the Routing Table Collection Frequency allows you to collect data less frequently for this table.
- **TN3270** for TN3270 server session data. You can enable or disable collection of TN3270 server session data by starting or stopping the TN3270 component. Additionally, you can modify the display interval for TN3270 server session data. The default is to start this component.

See the "KN3FCCMD command reference" on page 220 for issues regarding the INSTALL, START, STOP, STATUS, and DEBUG commands on a per-component basis to change parameter values without rerunning PARMGEN. Remember that this update is temporary and is in effect only until a recycle, when the value reverts to the value that was configured using the PARMGEN method.

KN3 configuration parameters

The configuration parameters for the IBM Z OMEGAMON Network Monitor monitoring agent are grouped logically in the PARMGEN configuration file.

This section explains the parameters found in the IBM Z OMEGAMON Network Monitor section of the PARMGEN configuration profile. The prefix associated with IBM Z OMEGAMON Network Monitor is **KN3**.

The following parameters are grouped and presented in the order found in the configuration profile.

- **Values that describe the address space**
  - "KN3_AGT_CONFIGURATION_MODE" on page 89
  - "KN3_AGT_STC" on page 106
- **Specify communication protocols preference for TEMS connection**
  - "KN3_AGT_COMM_PROTOCOLn" on page 90
- **Protocol port numbers for Agent connection to TEMS**
  - "KN3_TEMS_TCP_PIPE_PORT_NUM" on page 190
  - "KN3_TEMS_TCP_PIPES_PORT_NUM" on page 191
  - "KN3_TEMS_TCP_PIPE6_PORT_NUM" on page 192
  - "KN3_TEMS_TCP_PIPE6S_PORT_NUM" on page 193
  - "KN3_TEMS_TCP_UDP_PORT_NUM" on page 194
  - "KN3_TEMS_TCP_UDP6_PORT_NUM" on page 195
- **Values that describe the Primary TEMS the Agent will connect to**
  - "KN3_TEMS_LOCAL_CONNECT_FLAG" on page 187
  - "KN3_TEMS_NAME_NODEID" on page 188
- **Agent's Primary TEMS TCP/IP information**
  - "KN3_TEMS_BKUP1_NAME_NODEID" on page 181
  - "KN3_TEMS_BKUP1_TCP_HOST" on page 182
  - "KN3_TEMS_BKUP1_VTAM_APPL_LLB_BKR" on page 183
  - "KN3_TEMS_BKUP1_VTAM_LU62_DLOGMOD" on page 184
  - "KN3_TEMS_BKUP1_VTAM_NETID" on page 185

- **Agent's primary TCP/IP information**

  Note: KN3_TEMS_TCP_HOST and KN3_AGT_TCP_HOST must be the same value if KN3_TEMS_LOCAL_CONNECT_FLAG=Y (Agent connects to local TEMS).

  - “KN3_TEMS_TCP_HOST” on page 189
- **Agent's local TCP/IP information**
  - “KN3_AGT_TCP_HOST” on page 110
  - “KN3_AGT_TCP_STC” on page 113
  - “KN3_AGT_TCP_KDEB_INTERFACELIST” on page 111 (If the Agent requires network interface list support)
  - “KN3_AGT_PARTITION_NAME” on page 102 (If the Agent requires address translation support–optional)
- **If the Agent requires network interface list support**
  - “KN3_AGT_TCP_KDEB_INTERFACELIST” on page 111
- **If the Agent requires address translation support**
  - “KN3_AGT_PARTITION_NAME” on page 102
- **Agent's Primary TEMS VTAM information**
  - “KN3_TEMS_VTAM_LU62_DLOGMOD” on page 197
  - “KN3_TEMS_VTAM_LU62_MODETAB” on page 198
  - “KN3_TEMS_VTAM_NETID” on page 199
  - “KN3_TEMS_VTAM_APPL_LLB_BROKER” on page 196
  -
- **Agent's local VTAM and logon information**
  - “KN3_AGT_VTAM_APPL_PREFIX” on page 119
  - “KN3_AGT_VTAM_NODE” on page 120
  -
- **Agent's Applids**
  - “KN3_AGT_VTAM_APPL_AA” on page 115
  - “KN3_AGT_VTAM_APPL_KN3INVPO” on page 117
  - “KN3_AGT_VTAM_APPL_NCS” on page 118
  - “KN3_AGT_VTAM_APPL_OPERATOR” on page 119
  -
- **VTAM Secondary Program Operator (SPO) for Communication Network Management (CNM) interface**
  - “KN3_AGT_VTAM_NODE_OMXE” on page 121
  - “KN3_AGT_VTAM_APPL_CNM_SPO” on page 116
  -
- **Advanced Agent configuration values**
  - “KN3_AGT_FLUSH_LSR_BUFR_INT_HR” on page 91
  - “KN3_AGT_FLUSH_LSR_BUFR_INT_MIN” on page 92
  - “KN3_AGT_ICU_LANGUAGE_LOCALE” on page 93
  - “KN3_AGT_KGL_WTO” on page 95
  - “KN3_AGT_KLX_TCP_TOLERATERECYCLE” on page 97
  - “KN3_AGT_STORAGE_DETAIL_INT_HR” on page 107

- "KN3_AGT_STORAGE_DETAIL_INT_MIN" on page 108
- "KN3_AGT_STORAGE_MINIMUM_EXTEND" on page 109
- "KN3_AGT_VIRTUAL_IP_ADDRESS" on page 115
- "KN3_AGT_VTAM_APPL_NCS" on page 118
- "KN3_AGT_WTO_MSG" on page 122

- **Take Action commands security settings**
  - "KN3_AGT_PPI_RECEIVER" on page 104
  - "KN3_AGT_PPI_SENDER" on page 105
- **Secondary TEMS configuration**
  - "KN3_TEMS_BKUP1_NAME_NODEID" on page 181
- **Secondary TEMS TCP/IP information**
  - "KN3_TEMS_BKUP1_TCP_HOST" on page 182
- **Secondary TEMS VTAM information**
  - "KN3_TEMS_BKUP1_VTAM_APPL_LLB_BKR" on page 183
  - "KN3_TEMS_BKUP1_VTAM_LU62_DLOGMOD" on page 184
  - "KN3_TEMS_BKUP1_VTAM_NETID" on page 185
- **Agent parameters: TCP/IP information**
  - "KN3_SNA_VTAM_COLLECT_DATA" on page 129
  - "KN3_SNA_VTAM_SNAC_SNACINTV" on page 130
  - "KN3_TCP_ALLHPR" on page 132
  - "KN3_TCP_COLLECT_STACK" on page 135
  - "KN3_TCP_CONN" on page 136
  - "KN3_TCP_CSM" on page 134
  - "KN3_TCP_EEHPR" on page 137
  - "KN3_TCP_FTP_DSPINTV" on page 140
  - "KN3_TCP_FTP" on page 139
  - "KN3_TCP_GLBS" on page 141
  - "KN3_TCP_INTE" on page 143
  - "KN3_TCP_IPSEC" on page 145
  - "KN3_TCP_INTS" on page 144
  - "KN3_TCP_OSA" on page 146
  - "KN3_TCP_ROUTE_TBL" on page 148
  - "KN3_TCP_ROUTE_TBL_FREQ" on page 149
  - "KN3_TCP_SAMPLE_INTERVAL" on page 150
  - "KN3_SNMP_CONFIG_FILE" on page 131
  - "KN3_TCP_TN3270" on page 152
  - "KN3_TCP_TN3270_DSPINTV" on page 153
  - "KN3_TCP_VIO_UNIT" on page 154
- **Define TCP monitoring systems member**

  Note: Specify KN3_TCPXxx_* row for each TCP/IP monitored system. The global default is $$$$ (monitored all TCP/IP stack).
  - "KN3_TCPX" on page 174
  - "KN3_TCPXnn_ROW" on page 175

  - “KN3_TCPXnn_SYS_NAME” on page 176
  - “KN3_TCPXnn_TCP_STC” on page 177
  - “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
  - “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
  - “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
  - “KN3_TCPXnn_OVRD_CONN” on page 157
  - “KN3_TCPXnn_OVRD_IPSEC” on page 166
  - “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168
  - “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
  - “KN3_TCP_ROUTE_TBL” on page 148
  - “KN3_TCP_ROUTE_TBL_FREQ” on page 149
  - “KN3_TCPXnn_OVRD_FTP” on page 158
  - “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
  - “KN3_TCPXnn_OVRD_TN3270” on page 171
  - “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
  - “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180
  - “KN3_TCPXnn_OVRD_OSA” on page 167
  - “KN3_TCPXnn_OVRD_GLBS” on page 160
  - “KN3_TCPXnn_OVRD_INTE” on page 163
  - “KN3_TCPXnn_OVRD_INTS” on page 164
- **Define TN3270 Telnet session link user values**
  - “KN3_TN3270_DXL_APPLID” on page 200
  - “KN3_TN3270_DXL_USERDATA” on page 201
- **Enable Self-Describing Agent processing**
  - “KN3_AGT_TEMA_SDA” on page 114
- **Audit parameters**
  - “KN3_AGT_AUDIT_TRACE” on page 88
  - “KN3_AGT_AUDIT_MAX_HIST” on page 87
  - “KN3_AGT_AUDIT_ITM_DOMAIN” on page 86
- **Persistent datastore table space allocation overrides**
  - “KN3_PD” on page 123
  - “KN3_PD_CYL” on page 124
  - “KN3_PD_GRP” on page 125
  - “KN3_PD_ROW” on page 127
  - “KN3_X_PD_HISTCOLL_DATA_AGT_STC” on page 217
  - “KN3_X_PD_HISTCOLL_DATA_TEMS_STC” on page 216
- **Additional IBM Z OMEGAMON Network Monitor Agent settings**
  - “KN3_X_AGT_CONFIRM_SHUTDOWN” on page 202
  - “KN3_X_AGT_KDC_DEBUG” on page 204
  - “KN3_X_AGT_DEBUG_TRACE” on page 203
  - “KN3_X_AGT_LGSA_VERIFY” on page 205
  - “KN3_X_AGT_LSRPOOL_BUFFER_NUM” on page 206
  - “KN3_X_AGT_LSRPOOL_BUFSIZE” on page 207

- "KN3_X_AGT_SDUMP_SVC_SYS1_DUMP" on page 208
- "KN3_X_AGT_STORAGE_LIMIT_EXTEND" on page 210
- "KN3_X_AGT_STORAGE_LIMIT_PRIMARY" on page 211
- "KN3_X_AGT_STORAGE_RESERVE_EXT" on page 212
- "KN3_X_AGT_STORAGE_RESERVE_PRI" on page 213
- "KN3_X_AGT_STORAGE_STGDEBUG" on page 214
- "KN3_X_AGT_TASKS_ATTACHED_NUM" on page 215
- "KN3_X_SECURITY_USER_EXIT" on page 219
- "KN3_X_SECURITY_RESOURCE_CLASS" on page 218

- **Agent nonstandard parameters**
  - "KN3_AGT_NSNEWn_VALUE" on page 98
  - "KN3_AGT_NONSTDn_DSN" on page 99
  - "KN3_AGT_NONSTDn_MBR" on page 100
  - "KN3_AGT_NONSTDn_PARM" on page 101
  - "KN3_AGT_NSOLDn_VALUE" on page 101

KN3_AGT_AUDIT_ITM_DOMAIN

Use the KN3_AGT_AUDIT_ITM_DOMAIN parameter to specify an identifier for associating audit records. This parameter defines the audit domain name.

The value that you specify on the KN3_AGT_AUDIT_ITM_DOMAIN parameter generates an AUDIT_ITM_DOMAIN parameter in the KN3ENV member.

Required or optional
Optional

Location where the parameter value is stored
In the KN3ENV member of the *rhilev.midlev.rtename*.RKANPARU library for the agent's runtime library.

Parameter name
ITM_DOMAIN=%KN3_AGT_AUDIT_ITM_DOMAIN%

Default value
None

Permissible values
Character string, maximum length 32

In the Configuration Tool (ICAT)

Panel name
SPECIFY ADVANCED AGENT CONFIGURATION VALUES

Panel ID
KAG62P5

Field
z/OS Audit collection values: Domain

Default value
None

Permissible values
Character string, maximum length 32.

Batch parameter name
KN3_AGT_AUDIT_ITM_DOMAIN

PARMGEN name
KN3_AGT_AUDIT_ITM_DOMAIN

PARMGEN classification
identifier to associate audit records

Description
This field specifies an identifier that can be used to associate audit records. It is used for commonly identifying agents that are associated with each other. For example, you could use this parameter to sort records by a particular customer. This field is also be used to create unique namespaces for RBAC.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_AGT_AUDIT_TRACE" on page 88
- "KN3_AGT_AUDIT_MAX_HIST" on page 87

KN3_AGT_AUDIT_MAX_HIST

Use the KN3_AGT_AUDIT_MAX_HIST parameter to specify the maximum in-memory cache entries. It is the maximum number of records kept in short-term memory for direct queries.

The value that you specify on the KN3_AGT_AUDIT_MAX_HIST parameter generates an AUDIT_MAX_HIST parameter in the KN3ENV member. If AUDIT_MAX_HIST is not specified, AUDIT_MAX_HIST=100 is the internal code default.

Required or optional
Optional

Location where the parameter value is stored
The AUDIT_MAX_HIST parameter in the *rhilev.rtename*.RKANPARU data set, member KN3ENV for the agent runtime environment.

Parameter name
`AUDIT_MAX_HIST=%KN3_AGT_AUDIT_MAX_HIST%`

Default value
None

Permissible values
10-1000

In the Configuration Tool (ICAT)

Panel name
SPECIFY ADVANCED AGENT CONFIGURATION VALUES

Panel ID
KAG62P5

Field
z/OS Audit collection values: Maximum in-memory cache entries

Default value
None

Permissible values
10-1000

Batch parameter name
KN3_AGT_AUDIT_MAX_HIST

PARMGEN name
KN3_AGT_AUDIT_MAX_HIST

PARMGEN classification
Audit trace

Description
The maximum number of records kept in short-term memory for direct queries.

Note: If AUDIT_MAX_HIST is not specified in the KN3ENV member, the internal default AUDIT_MAX_HIST=100 is set. The AUDIT_MAX_HIST parameter is generated as commented out in KN3ENV.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_AGT_AUDIT_TRACE" on page 88
- "KN3_AGT_AUDIT_ITM_DOMAIN" on page 86

KN3_AGT_AUDIT_TRACE

Use the KN3_AGT_AUDIT TRACE parameter to indicate the trace level to pass messages.

The value that you specify on the KN3_AGT_AUDIT_TRACE parameter generates an AUDIT_TRACE parameter in the KN3ENV member.

Required or optional
Optional

Location where the parameter value is stored
In the KN3ENV member of the *rhilev.rtename*. RKANPARU library

Parameter name
AUDIT_TRACE=%KN3_AGT_AUDIT_TRACE%

Default value
None

Permissible values
M, B, D, or X, where:

- `M=Minimum`
- `B=Basic`
- `D=Detail`
- `X=Disabled`

In the Configuration Tool (ICAT)

Panel name
SPECIFY ADVANCED AGENT CONFIGURATION VALUES

Panel ID
KAG62P5

Field
z/OS Audit collection values: Enable/Disable z/OS audit collection

Default value
NOne

Permissible values
M, B, D, or X, where:

- `M=Minimum`
- `B=Basic`
- `D=Detail`
- `X=Disabled`

Batch parameter name
KN3_AGT_AUDIT TRACE

PARMGEN name
KN3_AGT_AUDIT TRACE

PARMGEN classification
Audit trace

Description
This indicates the trace level to pass messages. Message trace levels, from low to high, are:

- `X=Disabled`
- `M=Minimum`
- `B=Basic`
- `D=Detail`

Note: If AUDIT_TRACE is not specified in the KN3ENV member, then the internal default AUDIT_TRACE=BASIC is set. The AUDIT_TRACE parameter is generated as commented out in KN3ENV.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_AGT_AUDIT_MAX_HIST" on page 87
- "KN3_AGT_AUDIT_ITM_DOMAIN" on page 86

KN3_AGT_CONFIGURATION_MODE

Use the KN3_AGT_CONFIGURATION_MODE parameter to specify how you want to run the monitoring agent you are defining, in the agent address space or the server address space.

Required or optional
Required

Location where parameter value is stored
The parameter value is not stored, but is used for internal processing.

Parameter name
N/A

Default value
STANDALONE

Permissible values
STANDALONE or TEMS

In the Configuration Tool (ICAT)

Panel name
CONFIGURE IBM Z OMEGAMON Network Monitor

Panel ID
KN341MCU

Field
Configure IBM Z OMEGAMON Network Monitor

This value is set when you select Option 3 on this panel and complete the resulting set of panels. If you choose Option 3 then the value for this parameter is set to **AGTCMS**, which is strongly recommended (meaning that the agent runs in its own address space). If you choose PF5 Advanced on Panel KN341MCU, then the value for this parameter will be set to **CMS**, which means that the agent runs in the run in the monitoring server (CMS) address space.

Default value
No default

Permissible values
One of the following:

- STANDALONE

- CMS
- AGTCMS

Batch parameter name
KN3_AGT_CONFIG

PARMGEN name
KN3_AGT_CONFIGURATION_MODE

PARMGEN classification
Values that describe the address space

Description

Agent configuration option

This parameter specifies how you want to run the monitoring agent you are defining.

When defining an agent, you have the option to run the agent in an agent address space or in the server address space. For performance reasons, you should run the agent in an agent address space. If you plan to run the agent in the server address space, the runtime environment must contain a server.

To run the agent in an agent address space, choose Option 3 (AGTCMS) in the Configuration Tool, which is the preferred configuration or specify STANDALONE in PARMGEN. Otherwise, by choosing PF5 Advanced from the KN341MCU panel (the Mainframe Networks main menu panel), you specify CMS in the Configuration Tool or TEMS in PARMGEN to run the agent in the server. The procedures outlined in *IBM Tivoli IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* assumes that you are running the recommended configuration for this agent, which is running in the agent address space.

Related parameters

- "KN3_AGT_STC" on page 106

KN3_AGT_COMM_PROTOCOLn

Use the KN3_AGT_COMM_PROTOCOLn parameter to specify the communication protocol for the TEMS connection. Valid values are IPPIPE, IP, SNA, IP6PIPE, IP6, IPSPIPE, and IP6SPIPE. When communication with the TEMS is initiated, the agent first tries protocol 1, then goes to protocol 2, and so on, in case of failure.

Note: Update the corresponding KN3_TEMS_TCP_*_PORT_NUM parameter for each KN3_AGT_COMM_PROTOCOLx parameter enabled. For example, if KN3_AGT_COMM_PROTOCOL1="IPPIPE", set the corresponding KN3_TEMS_TCP_PIPE_PORT_NUM parameter. If KN3_TEMS_COMM_PROTOCOL2="IP" (for IP.UDP), set the corresponding KN3_TEMS_TCP_UDP_PORT_NUM parameter.

Required or optional
Required

Location where the parameter value is stored
In the KN3ENV member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
N/A

Default value
None

Permissible values
`IP.PIPE`, `IP.UDP`, `IP6.PIPE`, `IP6.UDP`, `IP.SPIPE`, `IP6.SPIPE`, and `SNA.PIPE`

In the Configuration Tool (ICAT)

Panel name
SPECIFY AGENT ADDRESS SPACE PARAMETERS

Panel ID
KAG62P2

Field
Specify the communication protocols in priority sequence.

- IP.PIPE
- IP.UDP
- IP6.PIPE
- IP6.UDP
- IP.SPIPE
- IP6.SPIPE
- SNA.PIPE

Default value
None

Permissible values
1 - 7

Batch parameter name
KN3_AGT_COMM_PRO*n*

PARMGEN name
KN3_AGT_COMM_PROTOCOL*n*

PARMGEN classification
Specify communication protocols preference for TEMS connection

Description

Agent Communication protocol *n*

This parameter specifies the communication protocol to be supported by the monitoring agent, where *n* corresponds to a number between 1 and 7 to indicate the priority sequence for the communication protocols.

In the Configuration Tool (ICAT), the seven fields corresponding to the communication protocols that can be supported are shown, and you can set the priority sequence for these protocols by assigning each field a value from 1 to 7, with 1 as the highest priority and 7 as the lowest. Leave blank any fields that represent unsupported communication protocols.

The protocols, both supported and unsupported, are listed along with assigned port numbers in the KN3ENV member, as shown in the Example section. Unused protocols are indicated by USE:N. Supported protocols are listed in priority order.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters
None

KN3_AGT_FLUSH_LSR_BUFR_INT_HR

Use the KN3_AGT_FLUSH_LSR_BUFR_INT_HR parameter to specify the interval to force all deferred VSAM writes to DASD.

Required or optional
Required

Location where the parameter value is stored
In the KN3AGST member in the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
EVERY **HH**:MM:SS FLUSH (Flush VSAM buffers interval - hours)

Default value
0 hours, 30 minutes

Permissible values
0 - 24

In the Configuration Tool (ICAT)

Panel name
Specify Advanced Agent Configuration Values

Panel ID
KAG62P5

Field
Flush VSAM buffers: Hours

Default value
0 hours, 30 minutes, 0 seconds (seconds is not configurable)

Permissible values
0 - 24

Batch parameter name
KN3_AGT_FLUSH_INT_HR

PARMGEN name
KN3_AGT_FLUSH_LSR_BUFR_INT_HR

PARMGEN classification
Advanced Agent configuration values

Description

Flush VSAM buffers interval - hours

This parameter specifies the interval to force all deferred VSAM writes to DASD. The interval values are written as part of the third EVERY command in the KN3AGST member in the *rhilev.midlev.rtename*.RKANCMDU library. The default is 0 hours (hh) and 30 minutes (mm).

Related parameters

- “KN3_AGT_FLUSH_LSR_BUFR_INT_MIN” on page 92
- “KN3_AGT_ICU_LANGUAGE_LOCALE” on page 93
- “KN3_AGT_KGL_WTO” on page 95
- “KN3_AGT_KLX_TCP_TOLERATERECYCLE” on page 97
- “KN3_AGT_STORAGE_DETAIL_INT_HR” on page 107
- “KN3_AGT_STORAGE_DETAIL_INT_MIN” on page 108
- “KN3_AGT_STORAGE_MINIMUM_EXTEND” on page 109
- “KN3_AGT_VIRTUAL_IP_ADDRESS” on page 115
- “KN3_AGT_VTAM_APPL_NCS” on page 118
- “KN3_AGT_WTO_MSG” on page 122

KN3_AGT_FLUSH_LSR_BUFR_INT_MIN

Use the KN3_AGT_FLUSH_LSR_BUFR_INT_MIN parameter to specify the interval to force all deferred VSAM writes to DASD.

Required or optional
Required

Location where the parameter value is stored
In the KN3AGST member in the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
EVERY HH:**MM**:SS FLUSH (Flush VSAM buffers interval - mins)

Default value
0 hours 30 minutes

Permissible values
0 - 60

In the Configuration Tool (ICAT)

Panel name
Specify Advanced Agent Configuration Values

Panel ID
KAG62P5

Field
Flush VSAM buffers: Minutes

Default value
0 hours 30 minutes 0 seconds (seconds is not configurable)

Permissible values
0 - 60

Batch parameter name
KN3_AGT_FLUSH_INT_MIN

PARMGEN name
KN3_AGT_FLUSH_LSR_BUFR_INT_MIN

Description

Flush VSAM buffers interval - mins

This parameter specifies the interval to force all deferred VSAM writes to DASD. The interval values are written as part of the third EVERY command in: *rhilev*.*midlev*.*rtename*.RKANCMDU(KN3AGST) The default is 0 hours (hh) and 30 minutes (mm).

Related parameters

- “KN3_AGT_FLUSH_LSR_BUFR_INT_HR” on page 91
- “KN3_AGT_ICU_LANGUAGE_LOCALE” on page 93
- “KN3_AGT_KGL_WTO” on page 95
- “KN3_AGT_KLX_TCP_TOLERATERECYCLE” on page 97
- “KN3_AGT_STORAGE_DETAIL_INT_HR” on page 107
- “KN3_AGT_STORAGE_DETAIL_INT_MIN” on page 108
- “KN3_AGT_STORAGE_MINIMUM_EXTEND” on page 109
- “KN3_AGT_VIRTUAL_IP_ADDRESS” on page 115
- “KN3_AGT_VTAM_APPL_NCS” on page 118
- “KN3_AGT_WTO_MSG” on page 122

KN3_AGT_ICU_LANGUAGE_LOCALE

Use the KN3_AGT_ICU_LANGUAGE_LOCALE parameter to specify the language and codeset (system's locale) that you want the monitoring agent to use.

Required or optional
Required

Location where the parameter value is stored
Generated in the KN3ENV member in the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name
LANG= (Language locale of z/OS system)

In the Configuration Tool (ICAT)

Panel name
Specify Advanced Agent Configuration Values

Panel ID
KAG62P5

Field
Language locale

Default value
1 (English - United States)

Permissible values

- **1** (English - United States)
- **2** (English - United Kingdom)
- **3** (German - Germany)
- **4** (German - Switzerland)
- **5** (French - Belgium)
- **6** (French - France)
- **7** (French - Switzerland)
- **8** (Spanish - Spain)
- **9** (Italian - Italy)
- **10** (Portuguese - Portugal)
- **11** (Portuguese - Brazil)
- **12** (Norwegian - Norway)
- **13** (Swedish - Sweden)
- **14** (Danish - Denmark)
- **15** (Finnish - Finland)
- **16** (Japanese - Japan)
- **17** (French - Canada)
- **18** (Traditional Chinese - Taiwan)
- **19** (Simplified Chinese - China)
- **20** (Albanian - Albania)
- **21** (Bulgarian - Bulgaria)
- **22** (Czech - Slovenia)
- **23** (Dutch - Belgium)
- **24** (Dutch - Netherlands)
- **25** (Greek - Greece)
- **26** (Hebrew - Israel)
- **27** (Korean - Korea)
- **28** (Lithuanian - Lithuania)
- **29** (Macedonian - Macedonia)
- **30** (Romanian - Romania)
- **31** (Russian - Russia)
- **32** (Serbian - Serbia)
- **33** (Slovak - Slovakia)
- **34** (Slovenian - Slovenia)

- **35** (Thai - Thailand)
- **36** (Turkish - Turkey)

Batch parameter name
KN3_AGT_ICU_LANG

PARMGEN name
KN3_AGT_ICU_LANGUAGE_LOCALE

PARMGEN classification
Advanced Agent configuration values

Description
Language and region for the z/OS system.

This parameter specifies the language and codeset (system's locale) that you want the monitoring agent to use. The language locale value is used for National Language support. This field requires the numeric value (1-36) representing the Language and Region in the table that follows. As an example, specify 1 for "English - United States". The country and character set that this language represents (for example, country is en_US and character set is ibm-037) make up the LANG= environmental variable value generated in the KN3ENV member in the *rhilev*.*midlev*.*rtename*.RKANPARU library. For English - United States, LANG=en_US.ibm-037 is generated in KN3ENV.

From the Configuration Tool panel, press F1 (Help) and select **Language locale** for a list of the possible values. If you accept the default value of `1 (English - United States)`, the Configuration Tool generates this environment variable in KN3ENV:

```
LANG=en_US.ibm-037
```

If the z/OS UNIX System Services (USS) codepage (`en_US.ibm-1047`) is required, you can specify either `en_US.ibm-1047` or `1A` in the Language locale field on the Configuration Tool panel. In batch mode, you can specify either of these values:

```
KN3_AGT_ICU_LANG     en_US.ibm-1047
KN3_AGT_ICU_LANG     1
```

In PARMGEN mode, you can specify either of these values for the USS codepage:

```
KN3_AGT_ICU_LANGUAGE_LOCALE       en_US.ibm-1047
```

The USS codepage (`en_US.ibm-1047`) is required for agent autonomy and for private situation XML files.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters
None

KN3_AGT_KGL_WTO

Use the KPP_AGT_ICU_LANGUAGE_LOCALE parameter to activate write-to-operator messages for a particular agent.

Required or optional
Required

Location where the parameter value is stored
In the KN3ENV member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name
KGL_WTO= (Enable agent WTO messages)

Default value
YES

Permissible values
YES or NO

In the Configuration Tool (ICAT)

Panel name
Specify Agent Advanced Configuration Values

Panel ID
KAG62P5

Field
Enable startup console messages

Default value
N

Permissible values
Y, N

Batch parameter name
KN3_AGT_KGL_WTO

PARMGEN name
KN3_AGT_KGL_WTO

PARMGEN classification
Advanced agent configuration values

Description
Enable agent WTO messages

Specify **Y** to this parameter if you want a SYSLOG message on the console to indicate when the monitoring agent finishes initializing. You can use this message in an automation script. See the automation package for your site for further instructions on how to capture the monitoring agent startup automation message IDs. If you specify **Y**, the KGL_WTO=YES parameter is added to the *rhilev.midlev.rtename*.RKANPARU(KN3ENV) member. The default is **N** for the Configuration Tool and **YES** for PARMGEN.

Note: The existence of the KGL_WTO= parameter triggers the startup console messages. Therefore this parameter must not be present in the KN3ENV member if you do not want this feature enabled. When it is enabled after configuration, the parameter is added to the KN3ENV member. If you want to turn it off again, you must regenerate the Configuration Tool N3#3*xxx* job created in the monitoring agent "Create runtime members" step to refresh KN3ENV, where *xxx* is the JCL suffix. If you configured using PARMGEN, you can edit the configuration profile and recycle the monitoring agent.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_AGT_FLUSH_LSR_BUFR_INT_HR" on page 91
- "KN3_AGT_FLUSH_LSR_BUFR_INT_MIN" on page 92
- "KN3_AGT_KLX_TCP_TOLERATERECYCLE" on page 97
- "KN3_AGT_ICU_LANGUAGE_LOCALE" on page 93
- "KN3_AGT_STORAGE_DETAIL_INT_HR" on page 107
- "KN3_AGT_STORAGE_DETAIL_INT_MIN" on page 108
- "KN3_AGT_STORAGE_MINIMUM_EXTEND" on page 109
- "KN3_AGT_VIRTUAL_IP_ADDRESS" on page 115
- "KN3_AGT_VTAM_APPL_NCS" on page 118
- "KN3_AGT_WTO_MSG" on page 122

KN3_AGT_KLX_TCP_TOLERATERECYCLE

Use the KN3_AGT_KLX_TCP_TOLERATERECYCLE parameter to determine whether the monitoring agent address space reconnects to its TCP/IP stack without being recycled after the stack is recycled.

Required or optional
Optional

Location where the parameter value is stored
In the KN3INTCP member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name
`TCP/IP_USERID='&tcpip_stc' TOLERATERECYCLE` (Reconnect after TCP/IP recycle)

Default value
N

Permissible values
Y or N

In the Configuration Tool (ICAT)

Panel name
Specify Advanced Agent Configuration Values

Panel ID
KAG62P5

Field
Reconnect after TCP/IP recycle

Default value
N

Permissible values
Y, N

Batch parameter name
KN3_AGT_KLX_TCP_RECYCLE

PARMGEN name
KN3_AGT_KLX_TCP_TOLERATERECYCLE

PARMGEN classification
Advanced Agent configuration values

Description

Reconnect after TCP/IP recycle

The parameter determines whether the monitoring agent address space reconnects to its TCP/IP stack without being recycled after the stack is recycled. Set this parameter to **Y** to allow the monitoring agent address space to reconnect to the z/OS Communications Server without having to subsequently recycle the address space. When this parameter is set to **Y**, the "TOLERATERECYCLE" keyword is added in the KN3INTCP member of the RKANPARU library. The parameter line is generated as: `TCP/IP_USERID=&tcp_userid TOLERATERECYCLE`.

If this parameter is set to **N**, when the z/OS Communications Server is recycled, the monitoring agent address space must also be recycled to establish connectivity to TCP/IP. The default is **N** for the Configuration Tool and **TOLERATERECYCLE** (meaning yes) for PARMGEN.

Note: This parameter may be specified only when the monitoring agent is reporting to Tivoli Enterprise Monitoring Server V6.2.0 and later versions.

Related parameters
None

KN3_AGT_NSNEWn_VALUE

Use the KN3_AGT_NSNEWn_VALUE parameter to specify the value for a nonstandard parameter.

Required or optional
Optional

Attention: Use extreme caution in specifying nonstandard parameters. No error-checking is provided at present. Syntax is not validated. The presence of the data set and member specified is not validated. If faulty syntax or other errors cause your edits to fail, no warning or error message is issued. Use this facility only under the guidance of IBM Software Support.

Location where the parameter value is stored
Data set, member, and parameter specified in the “KN3_AGT_NONSTDn_MBR” on page 100, “KN3_AGT_NONSTDn_DSN” on page 99, and “KN3_AGT_NONSTDn_PARM” on page 101 parameters, respectively.

In the Configuration Tool (ICAT)

Panel name
Specify Nonstandard Parameters

Panel ID
KAGPNST*n*

Field
New Value

Default value
None

Permissible values
Character string, maximum length 50

Batch parameter name
KN3_NSNEW*n*_VALUE

PARMGEN name
KN3_NSNEW*n*_VALUE

PARMGEN Classification
Agent nonstandard parameters

Description
Value for a nonstandard parameter (a parameter that is not presented in a Configuration Tool interactive panel). In specifying the value, be sure to include format characters. For example, if the format in the runtime member is `parameter=value`, precede the value with an equal sign; or if the format is `parameter(value)`, surround the value with parentheses. If you want to delete an existing parameter that is specified in “KN3_AGT_NONSTDn_PARM” on page 101, leave the value of the corresponding KN3_NSNEW*nn*_VALUE parameter blank.

Each KN3_NSNEW*nn*_VALUE parameter has a unique name, in which *nn* represents a number between 1 and 6, corresponding to the number set for “KN3_AGT_NONSTDn_PARM” on page 101.

For more information about specifying nonstandard parameters, see the "Parameters" section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*.

Related parameters

- “KN3_AGT_NONSTDn_DSN” on page 99
- “KN3_AGT_NONSTDn_MBR” on page 100
- “KN3_AGT_NONSTDn_PARM” on page 101
- “KN3_AGT_NSOLDn_VALUE” on page 101

KN3_AGT_NONSTDn_DSN

Use the KN3_AGT_NONSTDn_DSN parameter to specify the low-level qualifier of the data set containing the member with the parameter to be added, replaced, or deleted by specifying a nonstandard parameter.

Required or optional
Optional

Attention: Use extreme caution in specifying nonstandard parameters. No error-checking is provided at present. Syntax is not validated. The presence of the data set and member specified is not validated. If faulty syntax or other errors cause your edits to fail, no warning or error message is issued. Use this facility only under the guidance of IBM Software Support.

Location where the parameter value is stored
Member specified in the “KN3_AGT_NONSTDn_MBR” on page 100 parameter

In the Configuration Tool (ICAT)

Panel name
Specify Nonstandard Parameters

Panel ID
KAGPNST*n*

Field
Low-level dataset qualifier

Default value
None

Permissible values
Character string, maximum length 8

Batch parameter name
KN3_AGT_NONSTDn_DSN

PARMGEN name
KN3_AGT_NONSTDn_DSN

PARMGEN Classification
Agent nonstandard parameters

Description

Low-level dataset qualifier

This parameter specifies the low-level qualifier of the data set containing the member with the parameter to be added, replaced, or deleted by specifying a nonstandard parameter (a parameter that is not presented in a Configuration Tool interactive panel). Each “KN3_AGT_NONSTDn_DSN” on page 99 parameter has a unique name, in which *n* represents a number between 1 and 6, corresponding to the number set for “KN3_AGT_NONSTDn_PARM” on page 101.

For more information about specifying nonstandard parameters, see the "Parameters" section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*.

Related parameters

- “KN3_AGT_NSNEWn_VALUE” on page 98
- “KN3_AGT_NONSTDn_MBR” on page 100
- “KN3_AGT_NONSTDn_PARM” on page 101
- “KN3_AGT_NSOLDn_VALUE” on page 101

KN3_AGT_NONSTDn_MBR

Use the KN3_AGT_NONSTDn_MBR parameter to specify the name of the name of the KN3_AGT_NONSTDn_DSN data set member that contains the parameter to be added, replaced, or deleted by specifying a nonstandard parameter.

Required or optional
Optional

Attention: Use extreme caution in specifying nonstandard parameters. No error-checking is provided at present. Syntax is not validated. The presence of the data set and member specified is not validated. If faulty syntax or other errors cause your edits to fail, no warning or error message is issued. Use this facility only under the guidance of IBM Software Support.

Location where the parameter value is stored
Member specified in this parameter, in the data set specified in the “KN3_AGT_NONSTDn_DSN” on page 99 parameter

In the Configuration Tool (ICAT)

Panel name
Specify Nonstandard Parameters

Panel ID
KAGPNST*n*

Field
Member

Default value
None

Permissible values
Character string, maximum length 8

Batch parameter name
KN3_NONSTD*nn*_MBR

PARMGEN name
KN3_NONSTD*nn*_MBR

PARMGEN Classification
Agent nonstandard parameters

Description
Name of the “KN3_AGT_NONSTDn_DSN” on page 99 data set member that contains the parameter to be added, replaced, or deleted by specifying a nonstandard parameter (a parameter that is not presented in a Configuration Tool interactive panel). The asterisk (*****) wildcard character can be used as a suffix in column 4, 5, 6, 7, or 8 of the member name (provided that column is the final one in the name).

Each KN3_NONSTD*nn*_MBR parameter has a unique name, in which *nn* represents a number between 1 and 6, corresponding to the number set for “KN3_AGT_NONSTDn_PARM” on page 101.

For more information about specifying nonstandard parameters, see the "Parameters" section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*.

Related parameters

- “KN3_AGT_NSNEWn_VALUE” on page 98
- “KN3_AGT_NONSTDn_DSN” on page 99
- “KN3_AGT_NONSTDn_PARM” on page 101
- “KN3_AGT_NSOLDn_VALUE” on page 101

KN3_AGT_NONSTDn_PARM

Use the KN3_AGT_NONSTDn_PARM parameter to specify the name of the configuration parameter to be added, replaced, or deleted.

Required or optional
Optional

Attention: Use extreme caution in specifying nonstandard parameters. No error-checking is provided at present. Syntax is not validated. The presence of the data set and member specified is not validated. If faulty syntax or other errors cause your edits to fail, no warning or error message is issued. Use this facility only under the guidance of IBM Software Support.

Location where the parameter value is stored
Data set and member specified in the “KN3_AGT_NONSTDn_MBR” on page 100 and “KN3_AGT_NONSTDn_DSN” on page 99 parameters, respectively

In the Configuration Tool (ICAT)

Panel name
Specify Nonstandard Parameters

Panel ID
KAGPNST*n*

Field
Parameter

Default value
None

Permissible values
Character string, maximum length 40

Batch parameter name
KN3_AGT_NONSTDn_PARM

PARMGEN name
KN3_AGT_NONSTDn_PARM

PARMGEN Classification
Agent nonstandard parameters

Description
Name of the configuration parameter to be added, replaced, or deleted. You can specify up to 6 *nonstandard* parameters (parameters that are not presented in the Configuration Tool interactive panels). Each nonstandard parameter has a unique name in which *nn* represents a number between 1 and 6.

For more information about specifying nonstandard parameters, see the "Parameters" section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*.

Related parameters

- “KN3_AGT_NSNEWn_VALUE” on page 98
- “KN3_AGT_NONSTDn_DSN” on page 99
- “KN3_AGT_NONSTDn_MBR” on page 100
- “KN3_AGT_NSOLDn_VALUE” on page 101

KN3_AGT_NSOLDn_VALUE

Use the KN3_AGT_NSOLDn_VALUE parameter to specify the existing value to be replaced or deleted in the parameter definition corresponding to KN3_AGT_NONSTDN_PARM.

Required or optional
Optional

Attention: Use extreme caution in specifying nonstandard parameters. No error-checking is provided at present. Syntax is not validated. The presence of the data set and member specified is not validated. If faulty syntax or other errors cause your edits to fail, no warning or error message is issued. Use this facility only under the guidance of IBM Software Support.

Location where the parameter value is stored
Replaced in the data set, member, and parameter specified in the "KN3_AGT_NONSTDn_MBR" on page 100, "KN3_AGT_NONSTDn_DSN" on page 99, and "KN3_AGT_NONSTDn_PARM" on page 101 parameters, respectively.

In the Configuration Tool (ICAT)

Panel name
Specify Nonstandard Parameters

Panel ID
KAGPNST*n*

Field
Old Value (if replacing)

Default value
None

Permissible values
Character string, maximum length 50

Batch parameter name
KN3_AGT_NSOLDn_VALUE

PARMGEN name
KN3_AGT_NSOLDn_VALUE

PARMGEN Classification
Agent nonstandard parameters

Description
Existing value to be replaced or deleted in the parameter definition corresponding to "KN3_AGT_NONSTDn_PARM" on page 101. The character string that you specify must match exactly the existing value for the parameter in the runtime member, or the value is not replaced. For example, if the format in the runtime member is `parameter=value`, precede the value with an equal sign; or if the format is `parameter(value)`, surround the value with parentheses.

Each KN3_NSOLD*nn*_VALUE parameter has a unique name, in which *nn* represents a number between 1 and 6, corresponding to the number set for "KN3_AGT_NONSTDn_PARM" on page 101.

For more information about specifying nonstandard parameters, see the "Parameters" section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*.

Related parameters

- "KN3_AGT_NSNEWn_VALUE" on page 98
- "KN3_AGT_NONSTDn_DSN" on page 99
- "KN3_AGT_NONSTDn_MBR" on page 100
- "KN3_AGT_NONSTDn_PARM" on page 101

KN3_AGT_PARTITION_NAME

Use the KN3_AGT_PARTITION_NAME parameter to specify the partition name that identifies the location of this monitoring server (TEMS namespace) relative to the firewalls used for address translation.

Required or optional
Optional

Location where the parameter value is stored
In the KN3ENV member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
KDC_PARTITION= (Agent IP.PIPE partition name)

Default value
None

Permissible values
Character string, maximum length 32

In the Configuration Tool (ICAT)

Panel name
SPECIFY AGENT IP.PIPE CONFIGURATION VALUES

Panel ID
KAG62P2C

Field
Partition name

Default value
None

Permissible values
Character string, maximum length 32

Batch parameter name
KN3_AGT_PIPE_NAME

PARMGEN name
KN3_AGT_PARTITION_NAME

PARMGEN classification
If the Agent requires address translation support

Description

Agent IP.PIPE partition name

This parameter specifies the partition name that identifies the location of this monitoring server (TEMS namespace) relative to the firewalls used for address translation.

Note: The Tivoli Enterprise Monitoring Server that this monitoring agent connects to must have a corresponding partition reference entry.

This parameter is put into the partition table that contains labels and associated socket addresses that are provided by the firewall administrator.

The labels in the partition table are configured into and used by IBM products on an external network, outside a firewall, during the Tivoli Enterprise Monitoring Server (TEMS) connection establishment phase. The first part of this connection establishment is the lb lookup, which requires that the location brokers return the socket address of the monitoring agent.

The partition table is used by the brokers, matching a partition name for a client to the labels in the partition table. On a match, the associated socket address in the partition table is returned to the client outside the firewall. This socket address is used by the IBM products to traverse the firewall and connect to the monitoring server.

Each entry consists of a label or partition name, a protocol (IP for UDP or IP.PIPE for TCP), and a host name or dotted-decimal IP address. The well-known port (Hub port) must be authorized by the firewall administrator.

- If UDP is the protocol configured in the partition table, then a range of (UDP) ports must be authorized by the firewall administrator (in addition to the well-known port).
- If TCP is the protocol, no additional ports other than the well-known TEMS port need be authorized.

Related parameters
None

KN3_AGT_PPI_RECEIVER

Use the KN3_AGT_PPI_RECEIVER parameter to specify the Program to Program Interface (PPI) values that enable the monitoring agent to forward Take Action commands to IBM Tivoli NetView for z/OS V5.2, or later.

Required or optional
Required if the monitoring agent will be forwarding Take Action commands to the IBM Tivoli NetView for z/OS Program-to-Program Interface (PPI).

Location where the parameter value is stored
In the KN3ENV member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
KGLHC_PPI_RECEIVER= (NetView for z/OS PPI receiver)

Default value
This value defaults to the IBM Tivoli NetView for z/OS PPI receiver used by the server if one is configured in this RTE. Otherwise, specify the default of **CNMPCMDR**.

Permissible values
Character string, maximum length 8

In the Configuration Tool (ICAT)

Panel name
Specify Advanced Agent Configuration Values

Panel ID
KAG62P5

Field
NetView PPI receiver

Default value
This value defaults to the IBM Tivoli NetView for z/OS PPI receiver used by the server if one is configured in this RTE. Otherwise, specify the default of **CNMPCMDR**.

Permissible values
Character string, maximum length 8

Batch parameter name
KN3_AGT_PPI_RECEIVER

PARMGEN name
KN3_AGT_PPI_RECEIVER

PARMGEN classification
Take Action commands security settings

Description
NetView for z/OS PPI receiver

The parameter specifies the Program to Program Interface (PPI) values that enable the monitoring agent to forward Take Action commands to IBM Tivoli NetView for z/OS V5.2, or later. The Tivoli Enterprise Portal user ID is passed to Tivoli NetView for z/OS.

Specify the name of the PPI receiver on IBM Tivoli NetView for z/OS that will receive Take Action commands. If the specified name is invalid or the receiver is not active on Tivoli NetView for z/OS, default (MGCR) command routing is performed. The value should be a 1-8 character, unique identifier for the receiver program. It can contain alphabetic characters A-Z or a-z, numeric characters 0-9, and the following special characters:

- dollar sign ($)
- percent sign (%)
- ampersand (&)
- number sign (#)

This value must match the *xyz* value coded on statement `AUTOTASK.?APSERV.InitCmd = APSERV xyz`" in the Tivoli NetView DSIPARM initialization member, CNMSTYLE. The Configuration Tool generates the KGLHC_PPI_RECEIVER parameter in the KN3ENV member of the *rhilev.midlev.rtename*.RKANPARU library. This value defaults to the Tivoli NetView for z/OS PPI receiver used by the Server if one is configured in this RTE. Otherwise, specify the default of CNMPCMDR. See the Tivoli NetView for z/OS online help for command APSERV for more details.

To enable this function, specify a value on the KN3_AGT_PPI_RECEIVER parameter. Ensure that the parameter is not commented out and the value is enclosed in double quotation marks (""). To disable this function, simply comment out the parameter with asterisks ('**').

For complete instructions, see the "Configuring NetView authorization of z/OS commands" section of *IBM Tivoli Monitoring: Configured Tivoli Enterprise Monitoring Server on z/OS*.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_AGT_PPI_SENDER" on page 105

KN3_AGT_PPI_SENDER

Use the KN3_AGT_PPI_SENDER parameter to specify the Program to Program Interface (PPI) values that enable the monitoring agent to forward Take Action commands to IBM Tivoli NetView for z/OS V5.2, or later.

Required or optional
Required if the monitoring agent will be forwarding Take Action commands to the IBM Tivoli NetView for z/OS Program-to-Program Interface (PPI).

Location where the parameter value is stored
In the KN3ENV member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
KGLHC_PPI_SENDER (Agent PPI sender)

Default value
None

Permissible values
Character string, maximum length 8

In the Configuration Tool (ICAT)

Panel name
Specify Advanced Agent Configuration Values

Panel ID
KAG62P5

Field
Agent PPI sender

Default value
None

Permissible values
Character string, maximum length 8

Batch parameter name
KN3_AGT_PPI_SENDER

PARMGEN name
KN3_AGT_PPI_SENDER

PARMGEN classification
Take Action commands security settings

Description
Agent PPI sender

The parameter specifies the Program to Program Interface (PPI) values that enable the monitoring agent to forward Take Action commands to IBM Tivoli NetView for z/OS V5.2, or later. The Tivoli Enterprise Portal user ID gets passed to IBM Tivoli NetView for z/OS.

Specify the optional name of the PPI sender. The value should be a 1-8 character, unique identifier for the sender program. It can contain alphabetic characters A-Z or a-z, numeric characters 0-9, and the following special characters: dollar sign ('$'), percent sign ('%'), ampersand ('&'), at sign ('@'), and number sign ('#'). This name should not conflict with any NetView for z/OS domain name, as it is used in logging the command and command response in the NetView for z/OS log. If a value is specified on this field, the Configuration Tool generates the KGLHC_PPI_SENDER parameter in the KN3ENV member of the *rhilev.midlev.rtename*.RKANPARU library. If a value is not specified on this field, the default is the current monitoring agent jobname that is the source of the command.

For complete instructions, see the "Configuring NetView authorization of z/OS commands" section of *IBM Tivoli Monitoring: Configured Tivoli Enterprise Monitoring Server on z/OS*.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_AGT_PPI_RECEIVER" on page 104

KN3_AGT_STC

Use the KN3_AGT_STC parameter to specify the started task name for the agent.

Required or optional
Required if you configure the monitoring agent in its own address space

Location where the parameter value is stored
Value becomes the name of the monitoring agent started task procedure member in the *rhilev.midlev.rtename*.RKANSAMU library for stand-alone agents.

Parameter name
N/A

Default value
CANSN3

Permissible values
Character string, maximum length 8

In the Configuration Tool (ICAT)

Panel name
SPECIFY AGENT ADDRESS SPACE PARAMETERS

Panel ID
KAG62P2

Field
Agent started task

Default value
CANSN3

Permissible values
Character string, maximum length 8

Batch parameter name
KN3_AGT_STC

PARMGEN name
KN3_AGT_STC

PARMGEN classification
Values that describe the address space

Description

Agent started task name

This parameter specifies the started task name for the agent. This started task must be copied to your system procedure library. The default is **CANSN3**.

The Configuration Tool created started task procedures in *rhilev*.*midlev*.*rtename*.RKANSAMU that you must copy to your started task library. If you have configured an agent address space, copy the IBM Z OMEGAMON Network Monitor monitoring agent started task (the default name is CANSN3) from *rhilev*.*midlev*.*rtename*.RKANSAMU to your started task library (PROCLIB). If you have configured the agent in the TEMS address space, then the TEMS started task procedure will be updated in *rhilev*.*midlev*.*rtename*.RKANSAMU (the default name is CANSDSST) and this started task must be copied to your started task library (PROCLIB).

Note: You might also use the sample system copy JCL to copy the system procedures and the VTAM major node members from the *rhilev*.*midlev*.*rtename*.RKANSAMU library to the system libraries (if applicable). The sample JCL can be generated from the RTE Utility option using the Configuration Tool.

See the "Copy the started task procedures to your procedure library" task in the *IBM Tivoli IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

You will also need this value when you customize the KN3UAUTH job. When you edit this job, you change **agentproc** to the started procedure name for the IBM Z OMEGAMON Network Monitor monitoring agent. See "Define monitoring agent access to the NMI" in the *IBM Tivoli IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide*.

Related parameters
None

KN3_AGT_STORAGE_DETAIL_INT_HR

Use the KN3_AGT_STORAGE_DETAIL_INT_HR parameter to set the interval to monitor storage.

Required or optional
Required

Location where the parameter value is stored
Part of the second EVERY command in the KN3AGST member of the *rhilev*.*midlev*.*rtename*.RKANCMDU library

Parameter name
EVERY **HH**:MM:SS STORAGE D (Storage detail logging interval - hours)

Default value
0

Permissible values
0 - 24

In the Configuration Tool (ICAT)

Panel name
Specify Advanced Agent Configuration Values

Panel ID
KAG62P5

Field
Storage detail logging: Hours

Default value
0

Permissible values
0 - 24

Batch parameter name
KN3_AGT_STOR_DTL_INT_HR

PARMGEN name
KN3_AGT_STORAGE_DETAIL_INT_HR

PARMGEN classification
Advanced Agent configuration values

Description

Storage detail logging interval - hours

This parameters sets the interval to monitor storage. The interval values are written as part of the second EVERY command in: *rhilev*.*midlev*.*rtename*.RKANCMDU(KN3AGST) The default is **0** hours (hh) and **60** minutes (mm).

Related parameters

- “KN3_AGT_FLUSH_LSR_BUFR_INT_HR” on page 91
- “KN3_AGT_FLUSH_LSR_BUFR_INT_MIN” on page 92
- “KN3_AGT_ICU_LANGUAGE_LOCALE” on page 93
- “KN3_AGT_KGL_WTO” on page 95
- “KN3_AGT_KLX_TCP_TOLERATERECYCLE” on page 97
- “KN3_AGT_STORAGE_DETAIL_INT_MIN” on page 108
- “KN3_AGT_STORAGE_MINIMUM_EXTEND” on page 109
- “KN3_AGT_VIRTUAL_IP_ADDRESS” on page 115
- “KN3_AGT_VTAM_APPL_NCS” on page 118
- “KN3_AGT_WTO_MSG” on page 122

KN3_AGT_STORAGE_DETAIL_INT_MIN

Use the KN3_AGT_STORAGE_DETAIL_INT_MIN parameter to set the interval to monitor storage.

Required or optional
Required

Location where the parameter value is stored
Part of the second EVERY command in the KN3AGST member of the *rhilev*.*midlev*.*rtename*.RKANCMDU library

Parameter name
EVERY HH:**MM**:SS STORAGE D (Storage detail logging interval - minutes)

Default value
60

Permissible values
0 - 60

In the Configuration Tool (ICAT)

Panel name
Specify Advanced Agent Configuration Values

Panel ID
KAG62P5

Field
Storage detail logging: Minutes

Default value
60

Permissible values
0 - 60

Batch parameter name
KN3_AGT_STOR_DTL_INT_MIN

PARMGEN name
KN3_AGT_STORAGE_DETAIL_INT_MIN

PARMGEN classification
Advanced Agent configuration values

Description

Storage detail logging interval - minutes

This parameters sets the interval to monitor storage. The interval values are written as part of the second EVERY command in: *rhilev*.*midlev*.*rtename*.RKANCMDU(KN3AGST) The default is **0** hours (hh) and **60** minutes (mm).

Related parameters

- “KN3_AGT_FLUSH_LSR_BUFR_INT_HR” on page 91
- “KN3_AGT_FLUSH_LSR_BUFR_INT_MIN” on page 92
- “KN3_AGT_ICU_LANGUAGE_LOCALE” on page 93
- “KN3_AGT_KGL_WTO” on page 95
- “KN3_AGT_KLX_TCP_TOLERATERECYCLE” on page 97
- “KN3_AGT_STORAGE_DETAIL_INT_HR” on page 107
- “KN3_AGT_STORAGE_MINIMUM_EXTEND” on page 109
- “KN3_AGT_VIRTUAL_IP_ADDRESS” on page 115
- “KN3_AGT_VTAM_APPL_NCS” on page 118
- “KN3_AGT_WTO_MSG” on page 122

KN3_AGT_STORAGE_MINIMUM_EXTEND

Use the KN3_AGT_STORAGE_MINIMUM_EXTEND parameter to specify the amount of virtual storage the monitoring agent must acquire to run at your site.

Required or optional
Required

Location where the parameter value is stored
In the KN3SYSIN member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name
`MINIMUM (768000,X)` (Minimum extended storage)

Default value
768000

Permissible values
0 - 9999999

In the Configuration Tool (ICAT)

Panel name
Specify Advanced Agent Configuration Values

Panel ID
KAG62P5

Field
Minimum extended storage

Default value
768000

Permissible values
0 - 9999999

Batch parameter name
KN3_AGT_STOR_MIN_EXT

PARMGEN name
KN3_AGT_STORAGE_MINIMUM_EXTEND

PARMGEN classification
Advanced Agent configuration values

Description

Minimum extended storage

This parameter specifies the amount of virtual storage the monitoring agent must acquire to run at your site. The default is **768000**.

Related parameters

- “KN3_AGT_FLUSH_LSR_BUFR_INT_HR” on page 91
- “KN3_AGT_FLUSH_LSR_BUFR_INT_MIN” on page 92
- “KN3_AGT_ICU_LANGUAGE_LOCALE” on page 93
- “KN3_AGT_KGL_WTO” on page 95
- “KN3_AGT_KLX_TCP_TOLERATERECYCLE” on page 97
- “KN3_AGT_STORAGE_DETAIL_INT_HR” on page 107
- “KN3_AGT_STORAGE_DETAIL_INT_MIN” on page 108
- “KN3_AGT_VIRTUAL_IP_ADDRESS” on page 115
- “KN3_AGT_VTAM_APPL_NCS” on page 118
- “KN3_AGT_WTO_MSG” on page 122

KN3_AGT_TCP_HOST

Use the KN3_AGT_TCP_HOST parameter to specify the hostname of the system that the agent is running on.

Required or optional
Optional. This field is required if you plan to have this agent communicate with Tivoli Enterprise Monitoring Server using TCP/IP.

Location where the parameter value is stored
KDCSSITE member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
N/A

Default value
Value set for the RTE_TCP_HOST parameter for the runtime environment

Permissible values
Character string, maximum length 32

In the Configuration Tool (ICAT)

Panel name

- SPECIFY AGENT IP.UDP CONFIGURATION VALUES (KAG62P2B)
- SPECIFY AGENT IP.PIPE CONFIGURATION VALUES (KAG62P2C)

Panel ID

- KAG62P2B (IP.UDP)
- KAG62P2C (IP.PIPE)

Field
Network address (Hostname)

Default value
Value set for the RTE_TCP_HOST parameter for the runtime environment

Permissible values
Character string, maximum length 32

Batch parameter name
KN3_AGT_TCP_HOST

PARMGEN name
KN3_AGT_TCP_HOST

PARMGEN classification
Agent's local TCP/IP information

Description

Agent TCP/IP hostname

This parameter specifies the hostname of the system that the agent is running on. This value is the TCP/IP host name or dotted decimal IP address of the z/OS system where the hub monitoring server is installed.

To obtain the host name or IP address, enter `TSO HOMETEST` at the command line. If the z/OS domain name resolver configuration specifies a search path that includes the target domain suffix, specify only the first qualifier of the host name. (Example: `sys` is the first qualifier of the fully qualified host name `sys.ibm.com`.) Otherwise, specify the fully qualified host name.

This field is required if you plan to have this agent communicate with the server using TCP/IP.

Related parameters
None

KN3_AGT_TCP_KDEB_INTERFACELIST

Use the KN3_AGT_TCP_KDEB_INTERFACELIST parameter to specify a list of network interfaces you want the monitoring agent to use.

Required or optional
Optional

Location where the parameter value is stored
In the KN3ENV member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name

```
KDEB_INTERFACELIST=(%KN3_AGT_TCP_KDEB_INTERFACELIST)
```

Default value
None

Permissible values
Character string, maximum length 44

In the Configuration Tool (ICAT)

Panel name

- SPECIFY AGENT IP.UDP CONFIGURATION VALUES (KAG62P2B)
- SPECIFY AGENT IP.PIPE CONFIGURATION VALUES (KAG62P2C)

Panel ID

- KAG62P2B (for IP.UDP)
- KAG62P2C (for IP.PIPE)

Field
Network interface list

Default value
None

Permissible values
Character string, maximum length 44

Batch parameter name
KN3_AGT_TCP_KDEBLST

PARMGEN name
KN3_AGT_TCP_KDEB_INTERFACELIST

PARMGEN classification
If the Agent requires network interface list support

Description
TCP/IP network interface list

This parameter specifies a list of network interfaces you want the monitoring agent to use. This parameter is required for sites that are running multiple TCP/IP interfaces or network adapters on the same z/OS image.

Setting this parameter allows you to direct the monitoring agent to connect to a specific TCP/IP local interface. Specify the network adapters as one or more of the following values:

- A fully-qualified hostname, for example `sys.ibm.com`
- The first qualifier of the fully-qualified hostname, for example `sys` from `sys.ibm.com`
- An IPv4 address in dotted decimal notation, for example `9.67.1.100`

If your site supports DNS, you can enter the short hostname or an IP address. If your site does not support DNS, you must enter the fully qualified hostname. This field is only applicable for networks with multiple interface cards for which a specific output network interface list is required.

If an interface address or a list of interface addresses is specified, the Configuration Tool generates the KDEB_INTERFACELIST parameter in the KN3ENV member of the *rhilev.midlev.rtename*.RKANPARU library.

Note: This value defaults to the IPv4 network interface list setting used by the Tivoli Enterprise Monitoring Server if one is configured in this RTE. Also, separate the entries using a blank space between interface addresses. For example:

```
==> 129.0.131.214 SYS1 SYS.IBM.COM
```

In addition, special considerations apply when specifying *!<&value>* or * for this field. Type `README COM` on the command line when you are in the Configuration Tool to see more information about network interface list considerations and usage.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters
The following parameters in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Parameter Reference Guide*:

- KDS_TEMS_TYPE
- KDS_TEMS_HA_TYPE
- KDS_TEMS_TCP_KDEB_INTERFACELIST

KN3_AGT_TCP_STC

Use the KN3_AGT_TCP_STC parameter to specify the name of the TCP/IP started task running on the monitoring agent host.

Required or optional

Optional. Required if you plan to have this agent communicate with Tivoli Enterprise Monitoring Server using TCP/IP.

Location where the parameter value is stored

In the KN3INTCP member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name

TCP/IP_USERID='*' (TCP/IP started task)

Default value

*

Permissible values

Character string, maximum length 8

In the Configuration Tool (ICAT)

Panel name

- SPECIFY AGENT IP.UDP CONFIGURATION VALUES (KAG62P2B)
- SPECIFY AGENT IP.PIPE CONFIGURATION VALUES (KAG62P2C)

Panel ID

- KAG62P2B (IP.UDP)
- KAG62P2C (IP.PIPE)

Field

Started task

Default value

*

Permissible values

Character string, maximum length 8

Batch parameter name

KN3_AGT_TCP_STC

PARMGEN name

KN3_AGT_TCP_STC

PARMGEN classification

Agent's local TCP/IP information

Description

TCP/IP started task

This parameter specifies the name of the TCP/IP started task running on the monitoring agent host. This a required field if you plan to have this agent communicate with the server using TCP/IP.

This parameter identifies the TCP/IP stack to be used. If the LPAR contains a single TCP/IP stack, accept the default value of an asterisk (*), which uses the first TCP/IP stack that was started. If the LPAR contains more than one TCP/IP stack, specify the started task name of the TCP/IP stack you want to use.

Alternatively, you can specify the number sign (#), which is translated to a blank and allows the TCP/IP environment to choose the stack to use, either through TCP/IP definitions or through the use of the SYSTCPD DD statement.

Whichever method is used to select a TCP/IP stack in a multi-stack environment, the Tivoli Management Services components continue to use that stack, even if a different stack becomes the

primary stack. Therefore, in a multi-stack environment, it is best to specify the started task name of the TCP/IP stack to be used, rather than specifying a wildcard or a blank.

Related parameters

- "KN3_AGT_TCP_HOST" on page 110
- "KN3_AGT_KLX_TCP_TOLERATERECYCLE" on page 97

KN3_AGT_TEMA_SDA

Use the KN3_AGT_TEMA_SDA parameter to enable or disable self-describing agent processing. By default, the TEMA_SDA KN3ENV parameter is initially enabled (set to **Yes**).

Required or optional
Required

Location where the parameter value is stored
The KN3ENV member in the *rhilev.rtename*.RKANPARU library.

Parameter name
TEMA_SDA=%KN3_AGT_TEMA_SDA%

Default value
Y

Permissible values
Y or N

In the Configuration Tool (ICAT)

Panel name
SPECIFY ADVANCED AGENT CONFIGURATION VALUES

Panel ID
KAG62P5

Field
Enable Self-Describing Agent processing

Default value
Y

Permissible values
Y or N

Batch parameter name
KN3_AGT_TEMA_SDA

PARMGEN name
KN3_AGT_TEMA_SDA

PARMGEN classification
Enable Self-Describing Agent processing

Description
This parameter indicates whether the agent has enabled the self-describing agent (SDA) function in the agent address space.

Related parameters
The following parameters in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Parameter Reference Guide*:

- GBL_HFS_JAVA_DIRn
- GBL_DSN_SYS1_SBPXEXEC
- RTE_USS_RTEDIR
- KDS_KMS_SDA
- KDS_TEMA_SDA

KN3_AGT_VIRTUAL_IP_ADDRESS

Use the KN3_AGT_VIRTUAL_IP_ADDRESS parameter to set this parameter to the type of VIPA defined for this z/OS system.

.

Required or optional
Required

Location where the parameter value is stored
The parameter value is not stored, but is used for internal processing.

Parameter name
AGVIPA (VIPA type for the z/OS system)

Default value
N

Permissible values
S (static), D (dynamic), or N (none)

In the Configuration Tool (ICAT)

Panel name
Specify Advanced Agent Configuration Values

Panel ID
KAG62P5

Field
Virtual IP Address (VIPA) type

Default value
N

Permissible values
S (static), D (dynamic), or N (none)

Batch parameter name
KN3_AGT_VIPA

PARMGEN name
KN3_AGT_VIRTUAL_IP_ADDRESS

PARMGEN classification
Advanced Agent configuration values

Description

VIPA type for the z/OS system

Set this parameter to the type of VIPA defined for this z/OS system. If the monitoring agent address space is a VIPA-defined application, specify if the VIPA definition is Static or Dynamic. If VIPA is in use, the VIPA name is resolvable through the Domain Name Server (DNS).

Note: The IP.PIPE protocol is required when dynamic VIPA is in use.

Related parameters
None

KN3_AGT_VTAM_APPL_AA

Use the KN3_AGT_VTAM_APPL_AA parameter to specify the Alert Adapter application identifier for the agent address space.

Required or optional
Required

Location where the parameter value is stored
In the VTAM major node (CTDN3N is the default) member of the of the *rhilev.midlev.rtename*.RKANSAMU library

Parameter name
N/A

Default value
CTDN3AA

Permissible values
A valid applid name no longer than 8 characters in length

In the Configuration Tool (ICAT)

Panel name
SPECIFY VTAM APPLID VALUES

Panel ID
KAG62P6

Field
VTAM applid for Alert Adapter

Default value
CTDN3AA

Permissible values
A valid applid name no longer than 8 characters in length

Batch parameter name
KN3_AGT_VTM_APPL_AA

PARMGEN name
KN3_AGT_VTAM_APPL_AA

Description

VTAM applid for Alert Adapter

This parameter specifies the Alert Adapter application identifier for the agent address space. This value is normally specified in "KN3_AGT_VTAM_APPL_PREFIX" on page 119, with the characters **AA** appended to it.

Related parameters
None

KN3_AGT_VTAM_APPL_CNM_SPO

Use the KN3_AGT_VTAM_APPL_CNM_SPO parameter to specify the applid for VTAM Secondary Program Operator.

Required or optional
Required

Location where the parameter value is stored
In the CTDN3N member of the of the *rhilev.midlev.rtename*.RKANSAMU library

Parameter name
N3APLSPV (OMEGAMON XE CNM application ID)

Default value
CTDN3SP

Permissible values
A character string no more than 8 characters in length

In the Configuration Tool (ICAT)

Panel name
SPECIFY VTAM APPLID VALUES

Panel ID
KN341P6

Field
CNM application

Default value
CTDN3SP

Permissible values
A character string no more than 8 characters in length

Batch parameter name
KN3_AGT_VTM_APPL_SPO

PARMGEN name
KN3_AGT_VTAM_APPL_CNM_SPO

PARMGEN classification
VTAM Secondary Program Operator (SPO) for Communication Network Management (CNM) interface

Description

OMEGAMON XE CNM application ID

This parameter specifies the applid for VTAM Secondary Program Operator. This parameter also supports the product's console facility.

As a VTAM Secondary Program Operator, the product can issue VTAM commands and receive the VTAM responses. Each panel has a PF key that enables a user to access the product's console.

Note: To support the product's console facility, one applid is needed for the VTAM Secondary Program Operator and one virtual session applid is needed for each user accessing the VTAM Console.

Related parameters

- "KN3_AGT_VTAM_NODE_OMXE" on page 121

KN3_AGT_VTAM_APPL_KN3INVPO

Use the KN3_AGT_VTAM_APPL_KN3INVPO parameter to specify the VPO VTAM application identifier for the agent address space.

Required or optional
Required

Location where the parameter value is stored
In the CTDN3N member of the of the *rhilev.midlev.rtename*.RKANSAMU library

Parameter name
N/A

Default value
CTDN3VP

Permissible values
A valid applid name no longer than 8 characters in length

In the Configuration Tool (ICAT)

Panel name
SPECIFY VTAM APPLID VALUES

Panel ID
KAG62P6

Field
TMS:Engine VTAM program operator

Default value
CTDN3VP

Batch parameter name
KN3_AGT_VTM_APPL_VPO

PARMGEN name
KN3_AGT_VTAM_APPL_KN3INVPO

PARMGEN classification
Agent applids

Description

VTAM applid for VPO interface

This parameter specifies the VPO VTAM application identifier for the agent address space. This value is normally specified in "KN3_AGT_VTAM_APPL_PREFIX" on page 119, with the characters VP appended to it.

Related parameters
None

KN3_AGT_VTAM_APPL_NCS

Use the KN3_AGT_VTAM_APPL_NCS parameter to specify the Network Computing System (NCS) application identifier for the agent address space.

Required or optional
Required

Location where the parameter value is stored
In the CTDN3N member of the of the *rhilev*.*midlev*.*rtename*.RKANSAMU library

Parameter name
N/A

Default value
CTDN3NC

Permissible values
A valid node name no more than 8 characters in length

In the Configuration Tool (ICAT)

Panel name
SPECIFY VTAM APPLID VALUES

Panel ID
KAG62P6

Field
Agent to TEMS connection

Default value
CTDN3NC

Batch parameter name
KN3_AGT_VTM_APPL_NCS

PARMGEN name
KN3_AGT_VTAM_APPL_NCS

PARMGEN classification
Agent applids

Description

Agent to server connection applid

This parameter specifies the Network Computing System (NCS) application identifier for the agent address space. This value is normally specified in "KN3_AGT_VTAM_APPL_PREFIX" on page 119, with the characters **NC** appended to it.

Related parameters

- "KN3_AGT_VTAM_APPL_PREFIX" on page 119

KN3_AGT_VTAM_APPL_OPERATOR

Use the KN3_AGT_VTAM_APPL_OPERATOR parameter to specify the operator VTAM application identifier for the agent address space.

Required or optional
Required

Location where the parameter value is stored
In the CTDN3N member of the of the *rhilev*.*midlev*.*rtename*.RKANSAMU library

Parameter name
N/A

Default value
CTDN3OR

Permissible values
A valid applid name no longer than 8 characters in length

In the Configuration Tool (ICAT)

Panel name
SPECIFY VTAM APPLID VALUES

Panel ID
KAG62P6

Field
TMS:Engine (non-CUA)

Default value
CTDN3OR

Batch parameter name
KN3_AGT_VTM_APPL_OPR

PARMGEN name
KN3_AGT_VTAM_APPL_OPERATOR

PARMGEN classification
Agent applids

Description

VTAM applid for non-CUA operator

This parameter specifies the operator VTAM application identifier for the agent address space. This is normally the value specified in "KN3_AGT_VTAM_APPL_PREFIX" on page 119, with the characters OR appended to it.

Related parameters
None

KN3_AGT_VTAM_APPL_PREFIX

Use the KN3_AGT_VTAM_APPL_PREFIX parameter to build the VTAM applids for the agent.

Required or optional
Required for SNA communications

Location where the parameter value is stored
The VTAMLST definition is created in the *rhilev*.*midlev*.*rtename*.RKANSAMU library. Copy this definition to your SYS1.VTAMLST library.

Parameter name
VTAMLST

Default value
CTDN3

Permissible values
A character string of up to 6 characters

In the Configuration Tool (ICAT)

Panel name
Specify Configuration Values/ RTE: *rtename*

Panel ID
KAG62P2A

Field
Applid prefix

Default value
CTDN3

Permissible values
A character string of up to 6 characters

Batch parameter name
KN3_AGT_VTM_APPL_PREF

PARMGEN name
KN3_AGT_VTAM_APPL_PREFIX

PARMGEN classification
Agent applids

Description
Agent Applid prefix

This parameter is a prefix that is used to build the VTAM applids for the agent. This is a required field if you plan to have the monitoring agent communicate with the server using VTAM.

This parameter specifies the applid prefix to establish the VTAM node and applid list. The product creates a customized VTAMLST definition in the *rhilev.midlev.rtename*.RKANSAMU library, which you then copy to your SYS1.VTAMLST library after the Configuration Tool work is complete. The default is **CTDN3**.

Note:

1. Each product requires its own set of IDs. Make sure that the product identifiers are unique. Type `README APP` on the command line from the Configuration Tool to get more information about how the Configuration Tool processes VTAM applids. Use the **F6=Applids** key to specify the VTAM major node and applid values.
2. If System Variable support is enabled, type `README SYS` on the command line from the Configuration Tool to get more information on how the Configuration Tool processes VTAM applids using MVS system symbols.
3. Do not confuse this value with "KN3_AGT_VTAM_NODE" on page 120, the value for specifying the VTAM major node.

Related parameters

- "KN3_AGT_VTAM_NODE" on page 120

KN3_AGT_VTAM_NODE

Use the KN3_AGT_VTAM_NODE parameter to specify the name that will be used to build the VTAM node entry for the agent.

Required or optional
Required for SNA communications

Location where the parameter value is stored
In the CTDN3N member of the *rhilev.midlev.rtename*.RKANSAMU library

Parameter name
XN3APLN

Default value
CTDN3N

Permissible values
A valid node name no more than 8 characters in length

In the Configuration Tool (ICAT)

Panel name
Specify VTAM Applid Values

Panel ID
KN341P6

Field
Major Node

Default value
CTDN3N

Permissible values
A valid node name no more than 8 characters in length

Batch parameter name
KN3_AGT_VTM_NODE

PARMGEN name
KN3_AGT_VTAM_NODE

PARMGEN classification
Agent's local VTAM and logon information

Description

Agent node name

This parameter specifies the name that will be used to build the VTAM node entry for the agent. This is a required field if you plan to have the agent communicate with the server using VTAM.

Specify the name of the VTAM major node name that contains all the VTAM APPLID definitions for IBM Z OMEGAMON Network Monitor. This member must be moved to your VTAMLST concatenation. The name of this major node is also the name used to activate the VTAM APPLIDs. The default is **CTDN3N**.

Related parameters
In the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS Common Parameter Reference*, the following parameter:

- RTE_AGT_GBL_MAJOR_NODE

KN3_AGT_VTAM_NODE_OMXE

Use the KN3_AGT_VTAM_NODE_OMXE parameter to specify the name that will be used to build the VTAM node entry for the agent.

Required or optional
Required

Location where the parameter value is stored
In the CTDN3N member of the of the *rhilev.midlev.rtename*.RKANSAMU library

Parameter name
N3APLN (Agent node name)

Default value
CTDN3N

Permissible values
A valid node name no more than 8 characters in length

In the Configuration Tool (ICAT)

Panel name

- Specify Agent SNA Configuration Values (KAG62P2A)
- Specify VTAM Applid Values (KN341P6)

Panel ID

- KAG62P2A (Specify Agent SNA Configuration Values)
- KN341P6 (Specify VTAM Applid Values)

Field
Major Node

Default value
CTDN3N

Permissible values
A valid node name no more than 8 characters in length

Batch parameter name
KN3_AGT_VTM_NODE_OMXE

PARMGEN name
KN3_AGT_VTAM_NODE_OMXE

PARMGEN classification
VTAM Secondary Program Operator (SPO) for Communication Network Management (CNM) interface

Description

Agent node name

This parameter specifies the name that will be used to build the VTAM node entry for the agent.

Specify the name of the VTAM major node name that contains all the VTAM APPLID definitions for IBM Z OMEGAMON Network Monitor. This member must be moved to your VTAMLST concatenation. The name of this major node is also the name used to activate the VTAM APPLIDs. The default is **CTDN3N**.

Related parameters

- "KN3_AGT_VTAM_APPL_CNM_SPO" on page 116

KN3_AGT_WTO_MSG

Use the KN3_AGT_WTO_MSG parameter to specify whether you want the monitoring agent address space to issue Write To Operator (WTO) messages.

Required or optional
Required

Location where the parameter value is stored
In the KN3SYSIN member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
`WTO(N)` (Enable WTO messages)

Default value
N

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
SPECIFY CONFIGURATION VALUES / RTE: *rtename*

Panel ID
KAG62P5

Field
Enable WTO messages

Default value
N

Permissible values
Y, N

Batch parameter name
KN3_AGT_WTO_MSG

PARMGEN name
KN3_AGT_WTO_MSG

PARMGEN classification
Advanced Agent configuration values

Description
Enable WTO messages

Specify **Y** as the value for this parameter if you want the monitoring agent address space to issue Write To Operator (WTO) messages. WTOs write information and exception condition messages to the operator consoles. Alert messages are always written to the consoles. The default is **N.**

Example: To see this parameter specified in the context of the KN3SYSIN member, see "Sample KN3SYSIN member" on page 70.

Related parameters

- "KN3_AGT_FLUSH_LSR_BUFR_INT_HR" on page 91
- "KN3_AGT_FLUSH_LSR_BUFR_INT_MIN" on page 92
- "KN3_AGT_ICU_LANGUAGE_LOCALE" on page 93
- "KN3_AGT_KGL_WTO" on page 95
- "KN3_AGT_STORAGE_DETAIL_INT_HR" on page 107
- "KN3_AGT_STORAGE_DETAIL_INT_MIN" on page 108
- "KN3_AGT_STORAGE_MINIMUM_EXTEND" on page 109
- "KN3_AGT_VIRTUAL_IP_ADDRESS" on page 115
- "KN3_AGT_VTAM_APPL_NCS" on page 118

KN3_PD

The KN3_PD parameter specifies the beginning and ending syntax markers for the KN3_PD_* group of parameters.

Required or optional
Not a parameter. KN3_PD is a syntax marker in the configuration profile that marks the beginning and end of the KN3_PD_* block of values.

Location where the parameter value is stored
The KN3AL member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
NA

Default value
BEGIN

Permissible values
BEGIN, END

In the Configuration Tool (ICAT)
This value cannot be updated using the Configuration Tool.

Batch parameter name
KN3_PD

PARMGEN name
KN3_PD

PARMGEN classification
Persistent datastore table space allocation overrides

Description

Specifies the beginning and ending syntax markers for the KN3_PD_* group of parameters.

Related parameters

- “KN3_PD_CYL” on page 124
- “KN3_PD_GRP” on page 125
- “KN3_PD_ROW” on page 127

In the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS Common Parameter Reference*:

- RTE_PDS_HILEV
- RTE_PDS_KPDPROC_PREFIX
- RTE_PDS_BACKUP_FLAG
- RTE_PDS_BATCHINIT_FLAG
- RTE_PDS_EXPORT_FLAG
- RTE_PDS_EXTRACT_FLAG
- RTE_PDS_FILE_COUNT
- RTE_PDS_SMS_VOLUME
- RTE_PDS_SMS_UNIT
- RTE_PDS_SMS_STORCLAS
- RTE_PDS_SMS_MGMTCLAS
- KPP_PD_HISTCOLL_DATA_IN_AGT_STC
- KPP_PD_HISTCOLL_DATA_IN_TEMS_STC

KN3_PD_CYL

Use the KN3_PD_CYL parameter to specify the space allocation for the persistent data store libraries and for overhead information such as the product dictionary, table records, index records, and buffers to hold overflow data when the libraries are full.

Required or optional
Optional

Location where the parameter value is stored
The KN3AL member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
DSG3390 (Datastore group space)

Default value
The Configuration Tool computes this value using a formula using the SIZE, WINDOW, and UNIT TYPE values. The default in batch mode is 290. The default in interactive mode and PARMGEN is 420.

Permissible values
1 - 9999

In the Configuration Tool (ICAT)

Panel name
Modify and Review Datastore Specifications

Panel ID
KPD62PP3

Field
Est Cyl Space

Default value
The Configuration Tool computes this value using a formula using the SIZE, WINDOW, and UNIT TYPE values. The default in batch mode is 290. The default in interactive and PARMGEN mode is 261.

Permissible values
1 - 9999

Batch parameter name
KN3_PD_CYL

PARMGEN name
KN3_PD_CYL

PARMGEN classification
Persistent datastore table space allocation overrides

Description

Datastore group space

The parameter specifies the space allocation for the persistent data store libraries and for overhead information such as the product dictionary, table records, index records, and buffers to hold overflow data when the libraries are full. Allocate enough storage so that maintenance procedures are run only once a day. For more information about maintaining the persistent data store, see the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide*.

Related parameters

- "KN3_PD" on page 123
- "KN3_PD_GRP" on page 125
- "KN3_PD_ROW" on page 127

In the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS Common Parameter Reference*:

- RTE_PDS_HILEV
- RTE_PDS_KPDPROC_PREFIX
- RTE_PDS_BACKUP_FLAG
- RTE_PDS_BATCHINIT_FLAG
- RTE_PDS_EXPORT_FLAG
- RTE_PDS_EXTRACT_FLAG
- RTE_PDS_FILE_COUNT
- RTE_PDS_SMS_VOLUME
- RTE_PDS_SMS_UNIT
- RTE_PDS_SMS_STORCLAS
- RTE_PDS_SMS_MGMTCLAS
- KPP_PD_HISTCOLL_DATA_IN_AGT_STC
- KPP_PD_HISTCOLL_DATA_IN_TEMS_STC

KN3_PD_GRP

Use the KN3_PD_GRP parameter to specify the name of a single persistent data store group.

Required or optional
Optional

Location where the parameter value is stored
The KN3PG member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name
PDV1GRP (Datastore group name)

Default value
KN3

Permissible values
Character string, maximum length 8

In the Configuration Tool (ICAT)

Panel name
Modify and Review Datastore Specifications

Panel ID
KPD62PP3

Field
Datastore group name

Default value
KN3

Permissible values
Character string, maximum length 8

Batch parameter name
KN3_PD_GRP

PARMGEN name
KN3_PD_GRP

PARMGEN classification
Persistent datastore table space allocation overrides

Description

Datastore group name

This parameter specifies the name of a single persistent data store group. **KN3** is the name of the default group. Each group contains the number of data sets specified in the Group Count field. The default for the Group Count field is 3, the minimum.

Related parameters

- “KN3_PD” on page 123
- “KN3_PD_CYL” on page 124
- “KN3_PD_ROW” on page 127

In the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS Common Parameter Reference*:

- RTE_PDS_HILEV
- RTE_PDS_KPDPROC_PREFIX
- RTE_PDS_BACKUP_FLAG
- RTE_PDS_BATCHINIT_FLAG
- RTE_PDS_EXPORT_FLAG
- RTE_PDS_EXTRACT_FLAG
- RTE_PDS_FILE_COUNT
- RTE_PDS_SMS_VOLUME
- RTE_PDS_SMS_UNIT
- RTE_PDS_SMS_STORCLAS

- RTE_PDS_SMS_MGMTCLAS
- KPP_PD_HISTCOLL_DATA_IN_AGT_STC
- KPP_PD_HISTCOLL_DATA_IN_TEMS_STC

KN3_PD_ROW

Use the KN3_PD_ROW parameter to specify the beginning or end of a single persistent datastore group for the server product.

Required or optional
Optional

Location where the parameter value is stored
The KN3PG member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name
PDV1R0W (Row begin group end indicator)

Default value
BEGIN

Permissible values
BEGIN, END

In the Configuration Tool (ICAT)
This value cannot be updated using the Configuration Tool.

Batch parameter name
KN3_PD_ROW

PARMGEN name
KN3_PD_ROW

PARMGEN classification
Persistent datastore table space allocation overrides

Description

Row begin group end indicator

This parameter indicates the beginning or end of a single persistent datastore group for the server product. If the value is BEGIN, then the variables up to either the next BEGIN or the next END contain all the information required to construct the group information for a single group. If no value is specified, the default is BEGIN.

Related parameters

- “KN3_PD” on page 123
- “KN3_PD_CYL” on page 124
- “KN3_PD_GRP” on page 125

In the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS Common Parameter Reference*:

- RTE_PDS_HILEV
- RTE_PDS_KPDPROC_PREFIX
- RTE_PDS_BACKUP_FLAG
- RTE_PDS_BATCHINIT_FLAG
- RTE_PDS_EXPORT_FLAG
- RTE_PDS_EXTRACT_FLAG
- RTE_PDS_FILE_COUNT
- RTE_PDS_SMS_VOLUME
- RTE_PDS_SMS_UNIT

- RTE_PDS_SMS_STORCLAS
- RTE_PDS_SMS_MGMTCLAS
- KPP_PD_HISTCOLL_DATA_IN_AGT_STC
- KPP_PD_HISTCOLL_DATA_IN_TEMS_STC

KN3_SECURITY_ACTION_CLASS

Use the KN3_SECURITY_ACTION_CLASS parameter to override the RTE_SECURITY_CLASS value that is specified for the runtime environment, allowing the use of a separate security class to control command-level security for IBM Z OMEGAMON Network Monitor monitoring agent Take Action commands.

Required or optional
Optional

Location where the parameter value is stored
In the KN3ENV member in the *&rhilev*.*&rte*.RKANPARU library

Parameter name
KN3_SECURITY_ACTION_CLASS

Default value
None

Permissible values
Any value that is consistent with the definition rules dictated by the security manager.

In the Configuration Tool (ICAT)

Panel name
Specify Configuration Parameters (Page 1)

Panel ID
KN341P2

Field
SAF class name override

Default value
None

Permissible values
Any value that is consistent with the definition rules dictated by the security manager.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Batch parameter name
KN3_SECURITY_ACTION_CLASS

PARMGEN name
KN3_SECURITY_ACTION_CLASS

PARMGEN classification
Agent parameters: Security

Description

SAF class name override

To create resource profiles to control IBM Z OMEGAMON Monitor for z/OS Take Action commands, you must know the resource names of the commands. In addition, if you are using the SAF class name override parameter KN3_SECURITY_ACTION_CLASS to override the SAF security class name for Take Action commands, you must also create resource profiles for the override class.

Related parameters

- RTE_SECURITY_CLASS (see the *IBM Tivoli OMEGAMON XE and Tivoli Management Services: Common Parameter Reference*).

KN3_SNA_VTAM_COLLECT_DATA

Use the KN3_SNA_VTAM_COLLECT_DATA parameter to specify whether to collect data for VTAM buffer pools, applications, extents, and address spaces.

Required or optional
Required

Location where the parameter value is stored
In the KN3AGOPS member in the *rhilev*.*midlev*.*rtename*.RKANCMDU library

Parameter name
KN3FCCMD START SNAC (Collect SNA and VTAM data)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P5

Field
Buffer Pool/VTAM Environment Data Collection

Batch parameter name
KN3_VTAM_DATA

PARMGEN name
KN3_SNA_VTAM_COLLECT_DATA

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Collect SNA and VTAM data

The parameter determines whether to collect data for VTAM buffer pools, applications, extents, and address spaces. **Y** indicates VTAM data will be collected (the default). **N** indicates VTAM data will not be collected. If you specify **Y**, you will see an additional configuration panel when using the Configuration Tool. You may not start or modify the collection of VTAM buffer pools or VTAM address space data using the KN3FCCMD START SNAC command unless you indicate Y for this parameter. For more information about this command, see the "KN3FCCMD and KONFCCMD command reference" appendix in the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide*.

Related parameters

- "KN3_SNA_VTAM_SNAC_SNACINTV" on page 130
- "KN3_SNMP_CONFIG_FILE" on page 131
- "KN3_TCP_ALLHPR" on page 132
- "KN3_TCP_COLLECT_STACK" on page 135
- "KN3_TCP_CONN" on page 136
- "KN3_TCP_CSM" on page 134
- "KN3_TCP_EEHPR" on page 137
- "KN3_TCP_FTP_DSPINTV" on page 140
- "KN3_TCP_FTP" on page 139
- "KN3_TCP_GLBS" on page 141
- "KN3_TCP_INTE" on page 143

- “KN3_TCP_IPSEC” on page 145
- “KN3_TCP_INTS” on page 144
- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153
- “KN3_TCP_VIO_UNIT” on page 154

KN3_SNA_VTAM_SNAC_SNACINTV

Use the KN3_SNA_VTAM_SNAC_SNACINTV parameter to specify how often VTAM buffer pool and VTAM address space performance data is collected.

Required or optional
Required

Location where the parameter value is stored
In the KN3AGOPS member in the *rhilev*.*midlev*.*rtename*.RKANCMDU library

Parameter name
SNACINTV(&N3SNAINT) (SNA data collection interval)

Data collection interval is defined as the number of minutes between SNA data collection samples.

Default value
5

Permissible values
1-60

In the Configuration Tool (ICAT)

Panel name
Specify VTAM Applid Values

Panel ID
KN341P6

Field
SNA data collection interval

Default value
5 minutes

Permissible values
A valid data set name no longer than 54 characters

Batch parameter name
KN3_SNA_COLL_INTERVAL

PARMGEN name
KN3_SNA_VTAM_SNAC_SNACINTV

PARMGEN classification
Agent parameters: TCP/IP Information

Description

SNA data collection interval

The parameter determines how often VTAM buffer pool and VTAM address space performance data is collected. A value of “1” means that SNA data is collected every minute. This value is expressed as a whole number from 1 to 60, indicating the collection interval in minutes. The default is 5 minutes.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_GLBS” on page 141
- “KN3_TCP_INTE” on page 143
- “KN3_TCP_IPSEC” on page 145
- “KN3_TCP_INTS” on page 144
- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153
- “KN3_TCP_VIO_UNIT” on page 154

KN3_SNMP_CONFIG_FILE

Use the KN3_SNMP_CONFIG_FILE parameter to specify the name of the data set containing configuration entries for the SNMP manager functions within TCP/IP data collection.

Required or optional
Required

Location where the parameter value is stored
In the CANSN3 member in the *rhilev*.*midlev*.*rtename*.RKANSAMU library and in the KN3SNMP member of the *rhilev*.*midlev*.*rtename*.RKANSAMU library

Parameter name
KN3SNMP

Default value
USER.PARMLIB(KN3SNMP)

Permissible values
A valid data set name no longer than 54 characters

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P4

Field
SNMP Configuration file USER.PARMLIB(KN3SNMP)

Default value
USER.PARMLIB(KN3SNMP)

Permissible values
A valid data set name no longer than 54 characters

Batch parameter name
KN3_SNMP_CONFIG_FILE

PARMGEN name
KN3_SNMP_CONFIG_FILE

Description

SNMP configuration file

This parameter specifies the name of the data set containing configuration entries for the SNMP manager functions within TCP/IP data collection. Specify either the name of a sequential data set or the name of a partitioned data set and the name of the member containing SNMP configuration entries. As an example, the data set name has a format such as USER.SNMP, if the data set has physical sequential organization, or a format such as `USER.PARMLIB(KN3SNMP)`, if the data set has partitioned organization and the KN3SNMP member contains SNMP configuration entries.

For more information about defining the entries in this data set, see the KN3SNMP sample file in RKANSAMU or the "Format of the SNMP configuration file" section of the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide*. KN3SNMP sample member is created in RKANSAMU when the Configuration Tool "Create Runtime Members" step is run.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_FTP” on page 139
- “KN3_TCP_GLBS” on page 141
- “KN3_TCP_INTE” on page 143
- “KN3_TCP_IPSEC” on page 145
- “KN3_TCP_INTS” on page 144
- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153
- “KN3_TCP_VIO_UNIT” on page 154

KN3_TCP_ALLHPR

Use the KN3_TCP_ALLHPR parameter to specify if High Performance routing statistics is collected for all connections or only Enterprise Extender connections.

Required or optional
Required

Location where the parameter value is stored
In the KN3AGOPT member in the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
KN3FCCMD START EEHPR ALLHPR(N) (All Performance HPR data)

Default value
ALLHPR(N)

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P5

Field
All High Performance Routing Connections

Default value
N

Permissible values
Y, N

Batch parameter name
KN3_ALL_HPR

PARMGEN name
KN3_TCP_ALLHPR

PARMGEN classification
Agent parameters: TCP/IP Information

Description

All Performance HPR data

This parameter determines if High Performance routing statistics is collected for all connections or only Enterprise Extender connections. **Y** indicates that performance data for all High Performance Routing connections is collected, regardless of whether this data flows over Enterprise Extender connections. **N** indicates that performance data will be collected only for High Performance Routing connections that flow data over Enterprise Extender connections (the default).

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP” on page 139
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_GLBS” on page 141
- “KN3_TCP_INTE” on page 143
- “KN3_TCP_INTS” on page 144
- “KN3_TCP_IPSEC” on page 145
- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148

- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153
- “KN3_TCP_VIO_UNIT” on page 154

KN3_TCP_CSM

Use the KN3_TCP_CSM parameter to specify whether to collect Communications Storage Manager buffer reporting data.

Required or optional
Required

Location where parameter value is stored
The KN3AGOPT member of the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
`KN3FCCMD START CSM` (Collect CSM data)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P5

Field
CSM Buffer Reporting

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_TCP_CSM

PARMGEN name
KN3_TCP_CSM

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Collect CSM data

This parameter determines whether to collect Communications Storage Manager buffer reporting data. **Y** indicates Communications Storage Manager buffer reporting data will be collected (the default). **N** indicates Communications Storage Manager buffer reporting data will not be collected.By default, this data will be collected.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132

KN3_TCP_COLLECT_STACK

Use the KN3_TCP_COLLECT_STACK parameter to specify whether to monitor this stack.

Required or optional
Required

Location where parameter value is stored
In the KN3TCPMO member in the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name
`N3STACK COLLECT(Y)` (Monitor stack function)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
TCP/IP Monitored Systems Info

Panel ID
KN341PPI

Field
Do you want to monitor this stack?

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_TCP_STACK

PARMGEN name
KN3_TCP_COLLECT_STACK

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Monitor stack function

This parameter determines whether to monitor this stack. **Y** indicates this stack will be monitored. **N** indicates this stack will not be monitored. The default is **Y**.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_FTP” on page 139
- “KN3_TCP_GLBS” on page 141
- “KN3_TCP_INTE” on page 143
- “KN3_TCP_INTS” on page 144
- “KN3_TCP_IPSEC” on page 145
- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153
- “KN3_TCP_VIO_UNIT” on page 154
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155

KN3_TCP_CONN

Use the KN3_TCP_CONN parameter to specify whether to collect TCP/IP Connection and Application performance statistics globally.

Required or optional
Required

Location where parameter value is stored
In the KN3AGOPT member of the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
`KN3FCCMD START CONN` (Collect TCP/IP Connections)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
TCP/IP Monitored Systems Info

Panel ID
KN341P4

Field
TCP/IP Connection and Application Performance Statistics Collection

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_TCP_CON

PARMGEN name
KN3_TCP_CONN

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Collect TCP/IP Connections

This parameter determines whether to collect TCP/IP Connection and Application performance statistics globally. By default, this data will be collected.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_FTP” on page 139
- “KN3_TCP_GLBS” on page 141
- “KN3_TCP_INTE” on page 143
- “KN3_TCP_INTS” on page 144
- “KN3_TCP_IPSEC” on page 145
- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153
- “KN3_TCP_VIO_UNIT” on page 154
- “KN3_TCPXnn_OVRD_CONN” on page 157

KN3_TCP_EEHPR

Use the KN3_TCP_EEHPR parameter to specify whether to collect Enterprise Extender and High Performance Routing or EEHPR statistics globally.

Required or optional
Required

Location where parameter value is stored
In the KN3AGOPT member in the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
KN3FCCMD START EEHPR (Collect EEHPR data)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P5

Field
Enterprise Extender and High Performance Routing Statistics Collection

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_TCP_HPR

PARMGEN name
KN3_TCP_EEHPR

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Collect EEHPR data

This parameter determines whether to collect Enterprise Extender and High Performance Routing or EEHPR statistics globally. By default, this data will be collected.

See also "KN3_TCP_ALLHPR" on page 132. You specify this parameter with the ALLHPR parameter, which indicates whether the monitoring agent will collect all High Performance Routing (HPR) connections or only those connections that flow over Enterprise Extender (EE) connections. ALLHPR (N) indicates that the monitoring agent is to collect data on HPR connections that flow over EE connections. ALLHPR (Y) indicates that the monitoring agent is to collect data on all HPR connections, not just those that flow over EE connections.

Related parameters

- "KN3_SNA_VTAM_COLLECT_DATA" on page 129
- "KN3_SNA_VTAM_SNAC_SNACINTV" on page 130
- "KN3_SNMP_CONFIG_FILE" on page 131
- "KN3_TCP_ALLHPR" on page 132
- "KN3_TCP_COLLECT_STACK" on page 135
- "KN3_TCP_CONN" on page 136
- "KN3_TCP_CSM" on page 134
- "KN3_TCP_FTP_DSPINTV" on page 140
- "KN3_TCP_FTP" on page 139
- "KN3_TCP_GLBS" on page 141
- "KN3_TCP_INTE" on page 143
- "KN3_TCP_INTS" on page 144
- "KN3_TCP_IPSEC" on page 145

- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153
- “KN3_TCP_VIO_UNIT” on page 154

KN3_TCP_FTP

Use the KN3_TCP_FTP parameter to specify whether to collect FTP data globally.

Required or optional
Required

Location where parameter value is stored
In the KN3AGOPT member of the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
KN3FCCMD START FTP (Collect FTP data)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P4

Field
FTP Data Collection

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_TCP_FTP

PARMGEN name
KN3_TCP_FTP

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Collect FTP data

This parameter determines whether to collect FTP data globally. By default, this data will be collected.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132

KN3_TCP_FTP_DSPINTV

Use the KN3_TCP_FTP_DSPINTV parameter to specify the FTP display interval.

Required or optional
Optional

Location where parameter value is stored
In the KN3AGOPT member of the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
`KN3FCCMD START FTP DSPINTV(&N3FTPDSP)` (TCP/IP sample FTP interval)

`DSPINTV` is defined as the number of hours of data that is displayed.

Default value
2

Permissible values
A whole number between 1 and 24.

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P4

Field
FTP Data Display Interval

Default value
2

Permissible values
A whole number between 1 and 24.

Batch parameter name
KN3_TCP_FTP_INTERVAL

PARMGEN name
KN3_TCP_FTP_DSPINTV

PARMGEN classification
Agent parameters: TCP/IP Information

Description

TCP/IP sample FTP interval

This parameter specifies the FTP display interval. The value is in hours from 1 to 24. This value must be a whole number. The default is 2 hours.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP” on page 139
- “KN3_TCP_GLBS” on page 141
- “KN3_TCP_INTE” on page 143
- “KN3_TCP_INTS” on page 144
- “KN3_TCP_IPSEC” on page 145
- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153
- “KN3_TCP_VIO_UNIT” on page 154
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159

KN3_TCP_GLBS

Use the KN3_TCP_GLBS parameter to specify whether to collect TCP/IP Stack Layer Statistics data for the system.

Required or optional
Required

Location where the parameter value is stored
In the KN3AGOPT member in the *rhilev*.*midlev*.*rtename*.RKANCMDU library

Parameter name
KN3FCCMD START GLBS (Collect TCP/IP Stack Layer Data)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN342PPK

Field
TCP/IP Stack Layer Statistics Collection

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_TCP_GST_COLL

PARMGEN name
KN3_TCP_GLBS

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Collect TCP/IP Stack Layer Data

This parameter determines whether to collect TCP/IP Stack Layer Statistics data for the system. This parameter is global for the entire system. **Y** (the default) indicates that TCP/IP Stack Layer Statistics data will be collected on this system. **N** indicates that TCP/IP Stack Layer Statistics data will not be collected on this system.

Related parameters

- "KN3_SNA_VTAM_COLLECT_DATA" on page 129
- "KN3_SNA_VTAM_SNAC_SNACINTV" on page 130
- "KN3_SNMP_CONFIG_FILE" on page 131
- "KN3_TCP_ALLHPR" on page 132
- "KN3_TCP_COLLECT_STACK" on page 135
- "KN3_TCP_CONN" on page 136
- "KN3_TCP_CSM" on page 134
- "KN3_TCP_EEHPR" on page 137
- "KN3_TCP_FTP_DSPINTV" on page 140
- "KN3_TCP_FTP" on page 139
- "KN3_TCP_INTE" on page 143
- "KN3_TCP_INTS" on page 144
- "KN3_TCP_IPSEC" on page 145
- "KN3_TCP_OSA" on page 146
- "KN3_TCP_ROUTE_TBL" on page 148
- "KN3_TCP_ROUTE_TBL_FREQ" on page 149
- "KN3_TCP_SAMPLE_INTERVAL" on page 150
- "KN3_TCP_TN3270" on page 152
- "KN3_TCP_TN3270_DSPINTV" on page 153
- "KN3_TCP_VIO_UNIT" on page 154
- "KN3_TCPXnn_OVRD_GLBS" on page 160

KN3_TCP_INTE

Use the KN3_TCP_INTE parameter to specify whether to collect Interface Data Link Control (DLC) Statistics read and write queue data.

Required or optional
Required

Location where the parameter value is stored
In the KN3AGOPT member in the *rhilev*.*midlev*.*rtename*.RKANCMDU library

Parameter name
`KN3FCCMD START INTE` (Collect DLC Data)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN322PPK

Field
Interface Data Link Control Statistics Collection

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_TCP_IEX_COLL

PARMGEN name
KN3_TCP_INTE

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Collect DLC Data

The parameter determines whether to collect Interface DLC Statistics read and write queue data. This global parameter is for the entire system. **Y** (the default) indicates Interface DLC Statistics data will be collected on this system. **N** indicates Interface DLC Statistics data will not be collected on this system.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_FTP” on page 139

KN3_TCP_INTS

Use the KN3_TCP_INTS parameter to specify whether to collect Interface Statistics data for the system.

Required or optional
Required

Location where the parameter value is stored
In the KN3AGOPT member in the *rhilev*.*midlev*.*rtename*.RKANCMDU library

Parameter name
KN3FCCMD START INTS (Collect Interface Statistics Data)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN342PPK

Field
Interface Statistics Collection

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_TCP_IST_COLL

PARMGEN name
KN3_TCP_INTS

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Collect Interface Statistics Data

The parameter determines whether to collect Interface Statistics data for the system. This is a global parameter for the entire system. **Y** (the default) indicates that Interface Statistics data will be collected on this system. **N** indicates Interface Statistics data will not be collected on this system.

Note: It is recommended (but not required) that you turn on Interface Statistics collection if Routing Table Collection is active.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_FTP” on page 139
- “KN3_TCP_GLBS” on page 141
- “KN3_TCP_INTE” on page 143
- “KN3_TCP_IPSEC” on page 145
- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153
- “KN3_TCP_VIO_UNIT” on page 154
- “KN3_TCPXnn_OVRD_INTS” on page 164

KN3_TCP_IPSEC

Use the KN3_TCP_IPSEC parameter to specify whether to collect IPSec security data.

Required or optional
Required

Location where parameter value is stored
In the KN3AGOPT data set in the *rhilev.midlev.rtename*.RKANCMDU member

Parameter name
`KN3FCCMD START IPSEC` (Collect IPSEC Data)

Default value
N

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P4

Field
IP Filters and IPSec Tunnels Statistics Collection

Default value
N

Permissible values
Y, N

Batch parameter name
KN3_TCP_IPSEC

PARMGEN name
KN3_TCP_IPSEC

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Collect IPSEC data

This parameter determines whether to collect IPSec security data. **Y** indicates IPSec Security data will be collected. **N** indicates IPSec Security data will not be collected (the default).

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_FTP” on page 139
- “KN3_TCP_GLBS” on page 141
- “KN3_TCP_INTE” on page 143
- “KN3_TCP_INTS” on page 144
- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153
- “KN3_TCP_VIO_UNIT” on page 154
- “KN3_TCPXnn_OVRD_IPSEC” on page 166

KN3_TCP_OSA

Use the KN3_TCP_OSA parameter to specify whether to collect OSA data for the system.

Required or optional
Required

Location where the parameter value is stored
In the KN3AGOPT member in the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
`KN3FCCMD START OSA` (Collect OSA Data)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN342PPK

Field
OSA Statistics Collection

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_TCP_OSA_COLL

PARMGEN name
KN3_TCP_OSA

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Collect OSA Data

This parameter determines whether to collect OSA data for the system. This global parameter is for the entire system. **Y** (the default) indicates that OSA data will be collected on this system. **N** indicates that OSA data will not be collected on this system.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_FTP” on page 139
- “KN3_TCP_GLBS” on page 141
- “KN3_TCP_INTE” on page 143
- “KN3_TCP_INTS” on page 144
- “KN3_TCP_IPSEC” on page 145
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153
- “KN3_TCP_VIO_UNIT” on page 154

- “KN3_TCPXnn_OVRD_OSA” on page 167

KN3_TCP_ROUTE_TBL

Use the KN3_TCP_ROUTE_TBL parameter to specify whether to collect Gateways and Device routing table data globally.

Required or optional
Optional

Location where parameter value is stored
In the KN3AGOPT member of the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
KN3FCCMD START ROUTE (Collect routing table data)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P4

Field
Routing Table Statistics Collection

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_TCP_RTC

PARMGEN name
KN3_TCP_ROUTE_TBL

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Collect routing table data

This parameter determines whether to collect Gateways and Device routing table data globally. **Y** indicates SNMP routing data will be collected (the default). **N** indicates SNMP routing data will not be collected.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140

KN3_TCP_ROUTE_TBL_FREQ

Use the KN3_TCP_ROUTE_TBL_FREQ parameter to specify how often the routing table information will be collected.

Required or optional
Optional

Location where parameter value is stored
In the KN3AGOPT member in the *rhilev*.*midlev*.*rtename*.RKANCMDU library

Parameter name
`KN3FCCMD START ROUTE FREQ(&N3TCPRTF)` (Routing table data frequency)

Frequency (FREQ) is defined as the number of collection intervals before the routing information will be collected.

Default value
10

Permissible values
A whole number between 1 and 99.

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P4

Field
Routing table collection frequency

Default value
10

Permissible values
A whole number between 1 and 99.

Batch parameter name
KN3_TCP_RTF

PARMGEN name
KN3_TCP_ROUTE_TBL_FREQ

PARMGEN classification
Agent parameters: TCP/IP Information

Description

Routing table data frequency

This parameter determines how often the routing table information will be collected. Use this parameter to collect the data less often, which will reduce the overall CPU consumption while still making the data available. A value of 1 means that routing information will be collected every collection cycle. The global default value of 10 indicates that the data would be collected once every 10 collection cycles. The specification should be a whole number within the range of 1 through 99.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_FTP” on page 139
- “KN3_TCP_GLBS” on page 141
- “KN3_TCP_INTE” on page 143
- “KN3_TCP_INTS” on page 144
- “KN3_TCP_IPSEC” on page 145
- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153
- “KN3_TCP_VIO_UNIT” on page 154
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170

KN3_TCP_SAMPLE_INTERVAL

Use the KN3_TCP_SAMPLE_INTERVAL parameter to specify the TCP/IP sample interval.

Required or optional
Required

Location where parameter value is stored
In the KN3AGST member of the *rhilev*.*midlev*.*rtename*.RKANCMDU library

Parameter name
`KN3FCCMD START TCPC TCPCINTV(&N3TCPINT)` (TCP/IP Sample Interval)

TCPCINTV is the TCP/IP data sampling interval. This value controls the frequency of data sampling for data collected using SNMP as well as data collected from the NMI for the CONN, CSM, EEHPR, and IPSEC components.

Default value
5

Permissible values
The value is in minutes from 1 to 60.

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P2

Field
TCP/IP Sample Interval

Default value
5

Permissible values
The value is in minutes from 1 to 60.

Batch parameter name
KN3_TCP_SAMP_INTERVAL

PARMGEN name
KN3_TCP_SAMPLE_INTERVAL

PARMGEN classification
Agent parameters: TCP/IP Information

Description

TCP/IP Sample Interval

This parameter specifies the TCP/IP sample interval. The value is in minutes from 1 to 60. The default value is **5** minutes. This value controls the frequency at which the Tivoli OMEGAMON XE software monitors your TCP/IP stack. On the sample interval, Tivoli OMEGAMON XE software gathers TCP/IP performance data. The Tivoli OMEGAMON XE software requests information from the IBM SNMP agent. SNMP retrieves the information stored in its Management Information Base, MIB, and returns it to the Tivoli OMEGAMON XE software.

Related parameters

- "KN3_SNA_VTAM_COLLECT_DATA" on page 129
- "KN3_SNA_VTAM_SNAC_SNACINTV" on page 130
- "KN3_SNMP_CONFIG_FILE" on page 131
- "KN3_TCP_ALLHPR" on page 132
- "KN3_TCP_COLLECT_STACK" on page 135
- "KN3_TCP_CONN" on page 136
- "KN3_TCP_CSM" on page 134
- "KN3_TCP_EEHPR" on page 137
- "KN3_TCP_FTP_DSPINTV" on page 140
- "KN3_TCP_FTP" on page 139
- "KN3_TCP_GLBS" on page 141
- "KN3_TCP_INTE" on page 143
- "KN3_TCP_INTS" on page 144
- "KN3_TCP_IPSEC" on page 145
- "KN3_TCP_OSA" on page 146
- "KN3_TCP_ROUTE_TBL" on page 148
- "KN3_TCP_ROUTE_TBL_FREQ" on page 149
- "KN3_TCP_TN3270" on page 152
- "KN3_TCP_TN3270_DSPINTV" on page 153
- "KN3_TCP_VIO_UNIT" on page 154

KN3_TCP_TN3270

Use the KN3_TCP_TN3270 parameter to specify whether to collect TN3270 data for all TN3270 servers running on this system.

Required or optional
Required

Location where parameter value is stored
In the KN3AGOPT member of the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
`KN3FCCMD START TN3270` (Collect TN3270 data)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P4

Field
TN3270 Server Statistics Collection

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_TCP_TNC

PARMGEN name
KN3_TCP_TN3270

Description

Collect TN3270 data

This parameter determines whether to collect TN3270 data for all TN3270 servers running on this system. **Y** (the default) indicates TN3270 data will be collected. N indicates TN3270 data will not be collected. Only TN3270 connections which started within the display interval will be seen in the real time data displays.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_FTP” on page 139
- “KN3_TCP_GLBS” on page 141

- "KN3_TCP_INTE" on page 143
- "KN3_TCP_INTS" on page 144
- "KN3_TCP_IPSEC" on page 145
- "KN3_TCP_OSA" on page 146
- "KN3_TCP_ROUTE_TBL" on page 148
- "KN3_TCP_ROUTE_TBL_FREQ" on page 149
- "KN3_TCP_SAMPLE_INTERVAL" on page 150
- "KN3_TCP_TN3270_DSPINTV" on page 153
- "KN3_TCP_VIO_UNIT" on page 154
- "KN3_TCPXnn_OVRD_TN3270" on page 171

KN3_TCP_TN3270_DSPINTV

Use the KN3_TCP_TN3270_DSPINTV parameter to specify the TN3270 display interval.

Required or optional
Optional

Location where parameter value is stored
In the KN3AGOPT member of the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
`KN3FCCMD START TN3270 DSPINTV(&N3OTND)` (TCP/IP sample TN3270 interval)

`DSPINTV` specifies the number of hours of data that is displayed.

Default value
2 hours

Permissible values
1 to 24 hours

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P4

Field
TN3270 Data Display Interval

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_TCP_TNC_INTERVAL

PARMGEN name
KN3_TCP_TN3270_DSPINTV

Description

TCP/IP sample TN3270 interval

This parameter specifies the TN3270 display interval. The value is in hours from 1 to 24. This value must be a whole number. The default is **2 hours.**

Related parameters

- "KN3_SNA_VTAM_COLLECT_DATA" on page 129
- "KN3_SNA_VTAM_SNAC_SNACINTV" on page 130

- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_FTP” on page 139
- “KN3_TCP_GLBS” on page 141
- “KN3_TCP_INTE” on page 143
- “KN3_TCP_INTS” on page 144
- “KN3_TCP_IPSEC” on page 145
- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_TCP_SAMPLE_INTERVAL” on page 150
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_VIO_UNIT” on page 154
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172

KN3_TCP_VIO_UNIT

Use the KN3_TCP_VIO_UNIT parameter to specify the TCP/IP virtual input/output (VIO) unit name for your site.

Required or optional
Optional

Location where parameter value is stored
In the KN3AGST member in the *rhilev*.*midlev*.*rtename*.RKANCMDU library

Parameter name
`KN3FCCMD START TCPC TCPCVIOU(VIO)` (TCPIP VIO unit)

Default value
VIO

Permissible values
A string of up to 8 characters.

In the Configuration Tool (ICAT)

Panel name
Specify Component Configuration

Panel ID
KN341P2

Field
Specify your site's VIO unit name

Default value
VIO

Permissible values
A string of up to 8 characters.

Batch parameter name
KN3_TCP_VIO_UNIT

PARMGEN name
KN3_TCP_VIO_UNIT

PARMGEN classification
Agent parameters: TCP/IP Information

Description

TCPIP VIO unit

This parameter provides the TCP/IP virtual input/output (VIO) unit name for your site. The VIO unit is used to allocate temporary data sets. The default is **VIO**.

Related parameters

- “KN3_SNA_VTAM_COLLECT_DATA” on page 129
- “KN3_SNA_VTAM_SNAC_SNACINTV” on page 130
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_ALLHPR” on page 132
- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCP_CONN” on page 136
- “KN3_TCP_CSM” on page 134
- “KN3_TCP_EEHPR” on page 137
- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCP_FTP” on page 139
- “KN3_TCP_GLBS” on page 141
- “KN3_TCP_INTE” on page 143
- “KN3_TCP_INTS” on page 144
- “KN3_TCP_IPSEC” on page 145
- “KN3_TCP_OSA” on page 146
- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCP_ROUTE_TBL_FREQ” on page 149
- “KN3_SNMP_CONFIG_FILE” on page 131
- “KN3_TCP_TN3270” on page 152
- “KN3_TCP_TN3270_DSPINTV” on page 153

KN3_TCPXnn_OVRD_COLLECT_STACK

Use the KN3_TCPXnn_OVRD_COLLECT_STACK parameter to whether to monitor this stack.

Required or optional
Optional unless you want to override the global value for this parameter. See “KN3_TCP_COLLECT_STACK” on page 135.

Location where the parameter value is stored
In the KN3TCPMO member in the *rhilev.midlev.rtename*.RKANSAMU library

Parameter name
smf_ID stack_name COLLECT(Y) (Monitor stack option)

Default value
The global value. See. “KN3_TCP_COLLECT_STACK” on page 135.

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
CHANGE TCP/IP MONITORED SYSTEMS INFO / RTE: *rtename*

Panel ID
KN341PPI

Field
Do you want to monitor this stack?

Default value
The global value. See. “KN3_TCP_COLLECT_STACK” on page 135.

Permissible values
Y, N

Batch parameter name
KN3_TCPX_OSTACK

PARMGEN name
KN3_TCPXnn_OVRD_COLLECT_STACK

PARMGEN classification
Define TCP monitoring systems member

Description

Monitor stack option

The parameter determines whether to monitor this stack. **Y** (the default) indicates this stack will be monitored. N indicates this stack will not be monitored.

Related parameters

- “KN3_TCP_COLLECT_STACK” on page 135
- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163
- “KN3_TCPXnn_OVRD_INTS” on page 164
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176
- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_CONN” on page 157
- “KN3_TCPXnn_OVRD_IPSEC” on page 166
- “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_OVRD_CONN

Use the KN3_TCPXnn_OVRD_CONN parameter to override the global TCP/IP Connection collection setting.

Required or optional

Optional unless you want to override the global value for this parameter. See “KN3_TCP_CONN” on page 136.

Location where the parameter value is stored

In the KN3AGOPT member in the *rhilev.midlev.rtename*.RKANPARU library

Parameter name

`KN3FCCMD START CONN TCPNAME(`*`tcpip_proc_name`*`)` (Collection Override for TCP connections)

`TCPNAME` identifies which TCP/IP address spaces this applies to. `tcpip_proc_name` is the name of a TCP/IP address space in your environment.

Default value

The global value. See “KN3_TCP_CONN” on page 136.

Permissible values

Y, N

In the Configuration Tool (ICAT)

Panel name

TCP/IP Monitored Systems Info

Panel ID

KN341PPI

Field

TCP/IP Connection Collection Override

Default value

The global value. See “KN3_TCP_CONN” on page 136.

Permissible values

Y, N

Batch parameter name

KN3_TCPX_OTCPC

PARMGEN name

KN3_TCPXnn_OVRD_CONN

PARMGEN classification

Define TCP monitoring systems member

Description

Collection Override for TCP connections

This parameter overrides the global TCP/IP Connection collection setting. This parameter determines whether to collect TCP/IP Connection and Application performance statistics for this address space.

Related parameters

- “KN3_TCP_CONN” on page 136
- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163
- “KN3_TCPXnn_OVRD_INTS” on page 164
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176

- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
- “KN3_TCPXnn_OVRD_IPSEC” on page 166
- “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_OVRD_FTP

Use the KN3_TCPXnn_OVRD_FTP parameter to override the global FTP data collection setting.

Required or optional
Optional unless you want to override the global value for this parameter. See “KN3_TCP_FTP” on page 139.

Location where the parameter value is stored
In the KN3AGOPT member in the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
`KN3FCCMD START FTP TCPNAME(`*`tcpip_proc_name`*`)` (Collection Override for FTP data)

`TCPNAME` identifies which TCP/IP address spaces this applies to. *`tcpip_proc_name`* is the name of a TCP/IP address space in your environment.

Default value
The global value. See “KN3_TCP_FTP” on page 139.

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
TCP/IP Monitored Systems Info2

Panel ID
KN341PPJ

Field
FTP Collection Override

Default value
The global value. See “KN3_TCP_FTP” on page 139.

Permissible values
Y, N

Batch parameter name
KN3_TCPX_OFTPC

PARMGEN name
KN3_TCPXnn_OVRD_FTP

Description

Collection Override for FTP data

This parameter overrides the global FTP data collection setting. This parameter determines whether to collect FTP data for this address space.

Related parameters

- "KN3_TCP_FTP" on page 139
- "KN3_TCPX" on page 174
- "KN3_TCPXnn_OVRD_GLBS" on page 160
- "KN3_TCPXnn_OVRD_INTE" on page 163
- "KN3_TCPXnn_OVRD_INTS" on page 164
- "KN3_TCPXnn_OVRD_OSA" on page 167
- "KN3_TCPXnn_ROW" on page 175
- "KN3_TCPXnn_SYS_NAME" on page 176
- "KN3_TCPXnn_TCP_STC" on page 177
- "KN3_TCPXnn_TCPIP_PROFILES_DSN" on page 179
- "KN3_TCPXnn_OVRD_GLOBAL_FLAG" on page 162
- "KN3_TCPXnn_OVRD_COLLECT_STACK" on page 155
- "KN3_TCPXnn_OVRD_CONN" on page 157
- "KN3_TCPXnn_OVRD_IPSEC" on page 166
- "KN3_TCPXnn_OVRD_ROUTE_TBL" on page 168
- "KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ" on page 170
- "KN3_TCPXnn_OVRD_FTP_DSPINTV" on page 159
- "KN3_TCPXnn_OVRD_TN3270" on page 171
- "KN3_TCPXnn_OVRD_TN3270_DSPINTV" on page 172
- "KN3_TCPXnn_TCPIP_PROFILES_MBR" on page 180

KN3_TCPXnn_OVRD_FTP_DSPINTV

Use the KN3_TCPXnn_OVRD_FTP_DSPINTV parameter to override the global FTP Display Interval setting.

Required or optional

Optional unless you want to override the global value for this parameter. See "KN3_TCP_FTP_DSPINTV" on page 140.

Location where the parameter value is stored

In the KN3AGOPT data set of the *rhilev.midlev.rtename*.RKANPARU member

Parameter name

`KN3FCCMD START FTP TCPNAME(`*`tcpip_proc_name`*`) DSPINTV(&N3OFTPD)` (Override TCP/IP FTP display interval)

`TCPNAME` identifies which TCP/IP address spaces this applies to. `tcpip_proc_name` is the name of a TCP/IP address space in your environment. `DSPINTV` is defined as the number of hours of data that is available to be displayed.

Default value

The global value. See "KN3_TCP_FTP_DSPINTV" on page 140

Permissible values

A whole number between 1 and 24

In the Configuration Tool (ICAT)

Panel name

TCP/IP Monitored Systems Info2

Panel ID

KN341PPJ

Field

Override TCP/IP FTP display interval

Default value
The global value. See “KN3_TCP_FTP_DSPINTV” on page 140.

Permissible values
A whole number between 1 and 24

Batch parameter name
KN3_TCPX_FTP_INT_SPEC

PARMGEN name
KN3_TCPXnn_OVRD_FTP_DSPINTV

PARMGEN classification
Define TCP monitoring systems member

Description

Override TCP/IP FTP display interval

This optional setting will override the global FTP Display Interval setting. The FTP data may be collected with a display interval of 1 hour to 24 hours. The specification should be a whole number within the range of 1 through 24, which will indicate the display interval in hours.

Related parameters

- “KN3_TCP_FTP_DSPINTV” on page 140
- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163
- “KN3_TCPXnn_OVRD_INTS” on page 164
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176
- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
- “KN3_TCPXnn_OVRD_CONN” on page 157
- “KN3_TCPXnn_OVRD_IPSEC” on page 166
- “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_OVRD_GLBS

Use the KN3_TCPXnn_OVRD_GLBS parameter specify whether to override the global TCP/IP Stack Layer Statistics Collection setting for this address space.

Required or optional
Optional unless you want to override the global value for this parameter. See “KN3_TCP_GLBS” on page 141.

Location where the parameter value is stored
In the KN3AGOPT member in the *rhilev.midlev.rtename*.RKANSAMU library

Parameter name
KN3FCCMD START GST TCPNAME(*tcpip_proc_name*) (Collection Override for Stack Layer)

TCPNAME identifies which TCP/IP address spaces this applies to. tcpip_proc_name is the name of a TCP/IP address space in your environment.

Default value
The global default. See "KN3_TCP_GLBS" on page 141.

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
ADD TCP/IP MONITORED SYSTEMS INFO3 / RTE: *rtename*

Panel ID
KN342PPK

Field
Stack Layer Collection Override

Default value
The global default. See "KN3_TCP_GLBS" on page 141.

Permissible values
Y, N

Batch parameter name
KN3_TCPX_OGLSTK

PARMGEN name
KN3_TCPXnn_OVRD_GLBS

PARMGEN classification
Define TCP monitoring systems member

Description

Collection Override for Stack Layer

The parameter determines whether to override the global TCP/IP Stack Layer Statistics Collection setting for this address space. **Y** indicates TCP/IP Stack Layer data will be collected for this address space. **N** indicates TCP/IP Stack Layer data will not be collected for this address space.

Related parameters

- "KN3_TCP_GLBS" on page 141
- "KN3_TCPX" on page 174
- "KN3_TCPXnn_OVRD_INTE" on page 163
- "KN3_TCPXnn_OVRD_INTS" on page 164
- "KN3_TCPXnn_OVRD_OSA" on page 167
- "KN3_TCPXnn_ROW" on page 175
- "KN3_TCPXnn_SYS_NAME" on page 176
- "KN3_TCPXnn_TCP_STC" on page 177
- "KN3_TCPXnn_TCPIP_PROFILES_DSN" on page 179
- "KN3_TCPXnn_OVRD_GLOBAL_FLAG" on page 162
- "KN3_TCPXnn_OVRD_COLLECT_STACK" on page 155
- "KN3_TCPXnn_OVRD_CONN" on page 157
- "KN3_TCPXnn_OVRD_IPSEC" on page 166
- "KN3_TCPXnn_OVRD_ROUTE_TBL" on page 168
- "KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ" on page 170

- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_OVRD_GLOBAL_FLAG

Use the KN3_TCPXnn_OVRD_GLOBAL_FLAG parameter to override stack-specific options.

Required or optional
Required for PARMGEN configuration. Set internally when using the Configuration Tool.

Location where the parameter value is stored
The parameter value is not stored, but is used for internal processing.

Parameter name
N30GBL (Override for stack specific options)

Default value
N

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
Specify TCP/IP Monitored Systems Information

Panel ID
KN341PP1

Field
Global override

Default value
This value is set internally in the Configuration Tool depending on whether you set any overrides.

Permissible values
Y, N

Batch parameter name
KN3_TCPX_OGBL

PARMGEN name
KN3_TCPX_OVRD_GLOBAL_FLAG

PARMGEN classification
Define TCP monitoring systems member

Description

Override for stack specific options

This parameter specifies the override for stack specific options. **Y** is an indication that an override has been specified for this address space. The override may negate the global specifications for one or more of the following: TCP/IP connection collection, FTP data collection, FTP display interval, TN3270 data collection, or TN3270 display interval. **N** is an indication that no overrides have been specified for this address space.

Related parameters

- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163

- "KN3_TCPXnn_OVRD_INTS" on page 164
- "KN3_TCPXnn_ROW" on page 175
- "KN3_TCPXnn_SYS_NAME" on page 176
- "KN3_TCPXnn_TCP_STC" on page 177
- "KN3_TCPXnn_TCPIP_PROFILES_DSN" on page 179
- "KN3_TCPXnn_OVRD_COLLECT_STACK" on page 155
- "KN3_TCPXnn_OVRD_CONN" on page 157
- "KN3_TCPXnn_OVRD_IPSEC" on page 166
- "KN3_TCPXnn_OVRD_ROUTE_TBL" on page 168
- "KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ" on page 170
- "KN3_TCPXnn_OVRD_FTP" on page 158
- "KN3_TCPXnn_OVRD_FTP_DSPINTV" on page 159
- "KN3_TCPXnn_OVRD_TN3270" on page 171
- "KN3_TCPXnn_OVRD_TN3270_DSPINTV" on page 172
- "KN3_TCPXnn_TCPIP_PROFILES_MBR" on page 180

KN3_TCPXnn_OVRD_INTE

Use the KN3_TCPXnn_OVRD_INTE parameter to specify whether to override the global Interface Data Link Control (DLC) Collection read and write queue data for interfaces that are defined to this address space.

Required or optional
Optional unless you want to override the global value for this parameter. See "KN3_TCP_INTE" on page 143.

Location where the parameter value is stored
In the KN3AGOPT member in the *rhilev.midlev.rtename*.RKANSAMU library

Parameter name
`KN3FCCMD START INTE TCPNAME(`*`tcpip_proc_name`*`)` (Collection Override for Interface DLC)

`TCPNAME` identifies the TCP/IP address spaces to which this parameter applies. `tcpip_proc_name` is the name of a TCP/IP address space in your environment.

Default value
The global default. See "KN3_TCP_INTE" on page 143.

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
ADD TCP/IP MONITORED SYSTEMS INFO3 / RTE: *rtename*

Panel ID
KN342PPK

Field
Interface DLC Collection Override

Default value
The global default. See "KN3_TCP_INTE" on page 143.

Permissible values
Y, N

Batch parameter name
KN3_TCPX_OIESTK

PARMGEN name
KN3_TCPXnn_OVRD_INTE

PARMGEN classification
Define TCP monitoring systems member

Description

Collection Override for Interface DLC

This parameter determines whether to override the global Interface DLC Collection read and write queue data for interfaces that are defined for this address space. **Y** indicates that Interface DLC read and write queue data settings for this address space will be collected. **N** indicates Interface DLC read and write queue data settings for this address space will not be collected.

Related parameters

- “KN3_TCP_INTE” on page 143
- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTS” on page 164
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176
- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
- “KN3_TCPXnn_OVRD_CONN” on page 157
- “KN3_TCPXnn_OVRD_IPSEC” on page 166
- “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_OVRD_INTS

Use the KN3_TCPXnn_OVRD_INTS parameter to specify whether to override the global interface collection setting for this address space.

Required or optional
Optional unless you want to override the global value for this parameter. See “KN3_TCP_INTS” on page 144.

Location where the parameter value is stored
In the KN3AGOPT member in the *rhilev.midlev.rtename*.RKANSAMU library

Parameter name
`KN3FCCMD START INTS TCPNAME(`*`tcpip_proc_name`*`)` (Collection Override for Interfaces)

`TCPNAME` identifies the TCP/IP address spaces to which this parameter applies. *`tcpip_proc_name`* is the name of a TCP/IP address space in your environment.

Default value
The global value. See “KN3_TCP_INTS” on page 144.

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
ADD TCP/IP MONITORED SYSTEMS INFO3 / RTE: *rtename*

Panel ID
KN342PPK

Field
Interface Collection Override

Default value
The global value. See “KN3_TCP_INTS” on page 144.

Permissible values
Y, N

Batch parameter name
KN3_TCPX_OISSTK

PARMGEN name
KN3_TCPXnn_OVRD_INTS

PARMGEN classification
Define TCP monitoring systems member

Description

Collection Override for Interfaces

The parameter determines whether to override the global interface collection setting for this address space. **Y** indicates interface data will be collected for this address space. **N** indicates interface data will not be collected for this address space.

Related parameters

- “KN3_TCP_INTS” on page 144
- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176
- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
- “KN3_TCPXnn_OVRD_CONN” on page 157
- “KN3_TCPXnn_OVRD_IPSEC” on page 166
- “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_OVRD_IPSEC

Use the KN3_TCPXnn_OVRD_IPSEC parameter to specify whether to collect IP Security and tunnel data for this address space.

Required or optional
Optional unless you want to override the global value for this parameter. See “KN3_TCP_IPSEC” on page 145.

Location where the parameter value is stored
In the KN3AGOPT member in the *rhilev*.*midlev*.*rtename*.RKANCMDU library

Parameter name
`KN3FCCMD START IPSEC TCPNAME(`*`tcpip_proc_name`*`)` (Collection Override for IPSEC)

`TCPNAME` identifies which TCP/IP address spaces this applies to. `tcpip_proc_name` is the name of a TCP/IP address space in your environment.

Default value
The global value. See “KN3_TCP_IPSEC” on page 145.

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
TCP/IP Monitored Systems Info

Panel ID
KN341PPI

Field
IP Filters and IPSec Tunnels Collection Override

Default value
The global value. See “KN3_TCP_IPSEC” on page 145.

Permissible values
Y, N

Batch parameter name
KN3_TCPX_OIPSEC

PARMGEN name
KN3_TCPXnn_OVRD_IPSEC

PARMGEN classification
Define TCP monitoring systems member

Description

Collection Override for IPSEC

The parameter determines whether to collect IP Security and tunnel data for this address space. **Y** indicates IP Security data will be collected. **N** indicates IP Security data will not be collected. Leaving the field blank indicates that IP Security Data collection will use the default.

Related parameters

- “KN3_TCP_IPSEC” on page 145
- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163
- “KN3_TCPXnn_OVRD_INTS” on page 164
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176

- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
- “KN3_TCPXnn_OVRD_CONN” on page 157
- “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_OVRD_OSA

Use the KN3_TCPXnn_OVRD_OSA parameter to specify whether to override the global OSA Collection setting for this address space.

Required or optional
Optional unless you want to override the global value for this parameter. See “KN3_TCP_OSA” on page 146.

Location where the parameter value is stored
In the KN3AGOPT member in the *rhilev*.*midlev*.*rtename*.RKANSAMU library

Parameter name
`KN3FCCMD START OSA TCPNAME (`*`tcpip_proc_name`*`)` (Collection Override for OSA)

`TCPNAME` identifies which TCP/IP address spaces this applies to. `tcpip_proc_name` is the name of a TCP/IP address space in your environment.

Default value
The global default. See “KN3_TCP_OSA” on page 146.

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
ADD TCP/IP MONITORED SYSTEMS INFO3 / RTE: *rtename*

Panel ID
KN342PPK

Field
OSA Collection Override

Default value
The global default. See “KN3_TCP_OSA” on page 146.

Permissible values
Y, N

Batch parameter name
KN3_TCPX_OSASTK

PARMGEN name
KN3_TCPXnn_OVRD_OSA

PARMGEN classification
Define TCP monitoring systems member

Description

Collection Override for OSA

The parameter determines whether to override the global OSA Collection setting for this address space. **Y** indicates OSA data will be collected for this address space. **N** indicates OSA data will not be collected for this address space.

Related parameters

- “KN3_TCP_OSA” on page 146
- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163
- “KN3_TCPXnn_OVRD_INTS” on page 164
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176
- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
- “KN3_TCPXnn_OVRD_CONN” on page 157
- “KN3_TCPXnn_OVRD_IPSEC” on page 166
- “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_OVRD_ROUTE_TBL

Use the KN3_TCPXnn_OVRD_ROUTE_TBL parameter to specify whether to collect routing table data for this address space.

Required or optional

Optional unless you want to override the global value for this parameter. See “KN3_TCP_ROUTE_TBL” on page 148.

Location where the parameter value is stored

In the KN3AGOPT member of the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name

`KN3FCCMD START ROUTE TCPNAME(`*`tcpip_proc_name`*`) (Collection Override for routing table)`

`TCPNAME` identifies which TCP/IP address spaces this applies to. `tcpip_proc_name` is the name of a TCP/IP address space in your environment.

Default value

The global value. See “KN3_TCP_ROUTE_TBL” on page 148.

Permissible values

Y, N

In the Configuration Tool (ICAT)

Panel name
TCP/IP Monitored Systems Info

Panel ID
KN341PPI

Field
Routing Table Collection Override

Default value
The global value. See “KN3_TCP_ROUTE_TBL” on page 148.

Permissible values
Y, N

Batch parameter name
KN3_TCPX_ORTC

PARMGEN name
KN3_TCPXnn_OVRD_ROUTE_TBL

PARMGEN classification
Define TCP monitoring systems member

Description

Collection Override for routing table

This parameter determines whether to collect routing table data for this address space. **Y** indicates SNMP routing data will be collected for this address space. **N** indicates SNMP routing data will not be collected for this address space. Leaving the field blank indicates that Routing Table Data Collection will use the global default.

Related parameters

- “KN3_TCP_ROUTE_TBL” on page 148
- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_OVRD_INTS” on page 164
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176
- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
- “KN3_TCPXnn_OVRD_CONN” on page 157
- “KN3_TCPXnn_OVRD_IPSEC” on page 166
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ

Use the KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ parameter to override the global routing table collection frequency.

Required or optional
Optional unless you want to override the global value for this parameter. See "KN3_TCP_ROUTE_TBL_FREQ" on page 149.

Location where the parameter value is stored
In the KN3AGOPT member of the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
`KN3FCCMD START ROUTE TCPNAME(`*`tcpip_proc_name`*`) FREQ (&N3OTCPRF)` (Override routing table data frequency)

`TCPNAME` identifies which TCP/IP address spaces this applies to. `tcpip_proc_name` is the name of a TCP/IP address space in your environment. `FREQ` is the number of collection intervals before the routing information will be collected.

Default value
The global value. See "KN3_TCP_ROUTE_TBL_FREQ" on page 149.

Permissible values
A whole number within the range of 1 through 99.

In the Configuration Tool (ICAT)

Panel name
TCP/IP Monitored Systems Info

Panel ID
KN341PPI

Field
Routing Table Collection Frequency

Default value
The global value. See "KN3_TCP_ROUTE_TBL_FREQ" on page 149.

Permissible values
A whole number within the range of 1 through 99

Batch parameter name
KN3_TCPX_ORTF

PARMGEN name
KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ

PARMGEN classification
Define TCP monitoring systems member

Description

Override routing table data frequency

This optional setting will override the global routing table collection frequency. This setting determines how often the routing information ia collected. This setting allows you to collect the data less often, which reduces the overall CPU consumption while still making the data available. A value of 1 means that the routing information will be collected every collection cycle. The global default value of 10 indicates that the data is collected once every 10 collection cycles. The specification should be a whole number within the range of 1 through 99.

Related parameters

- "KN3_TCP_ROUTE_TBL_FREQ" on page 149
- "KN3_TCPX" on page 174
- "KN3_TCPXnn_OVRD_GLBS" on page 160
- "KN3_TCPXnn_OVRD_INTE" on page 163

- "KN3_TCPXnn_OVRD_INTS" on page 164
- "KN3_TCPXnn_OVRD_OSA" on page 167
- "KN3_TCPXnn_ROW" on page 175
- "KN3_TCPXnn_SYS_NAME" on page 176
- "KN3_TCPXnn_TCP_STC" on page 177
- "KN3_TCPXnn_TCPIP_PROFILES_DSN" on page 179
- "KN3_TCPXnn_OVRD_GLOBAL_FLAG" on page 162
- "KN3_TCPXnn_OVRD_COLLECT_STACK" on page 155
- "KN3_TCPXnn_OVRD_CONN" on page 157
- "KN3_TCPXnn_OVRD_IPSEC" on page 166
- "KN3_TCPXnn_OVRD_ROUTE_TBL" on page 168
- "KN3_TCPXnn_OVRD_FTP" on page 158
- "KN3_TCPXnn_OVRD_FTP_DSPINTV" on page 159
- "KN3_TCPXnn_OVRD_TN3270" on page 171
- "KN3_TCPXnn_OVRD_TN3270_DSPINTV" on page 172
- "KN3_TCPXnn_TCPIP_PROFILES_MBR" on page 180

KN3_TCPXnn_OVRD_TN3270

Use the KN3_TCPXnn_OVRD_TN3270 parameter to specify whether to override the global TN3270 Server Statistics Collection setting for the TN3270 server running on this system.

Required or optional

Optional unless you want to override the global value for this parameter. See "KN3_TCP_TN3270" on page 152.

Location where the parameter value is stored

In the KN3AGOPT member in the *rhilev*.*midlev*.*rtename*.RKANSAMU library

Parameter name

`KN3FCCMD START TN3270 TCPNAME(`*`tcpip_proc_name`*`)` (Collection Override for TN3270 data)

`TCPNAME` identifies which TCP/IP address spaces this applies to. `tcpip_proc_name` is the name of a TCP/IP address space in your environment. `FREQ` is the number of collection intervals before the routing information will be collected.

Default value

The global value. See "KN3_TCP_TN3270" on page 152.

Permissible values

Y, N

In the Configuration Tool (ICAT)

Panel name

TCP/IP Monitored Systems Info

Panel ID

KN341PPJ

Field

TN3270 Collection Override

Default value

The global value. See "KN3_TCP_TN3270" on page 152.

Permissible values

Y, N

Batch parameter name
KN3_TCPX_OTNC

PARMGEN name
KN3_TCPXnn_OVRD_TN3270

PARMGEN classification
Define TCP monitoring systems member

Description

Collection Override for TN3270 data

The parameter determines whether to override the global TN3270 Server Statistics Collection setting for the TN3270 server running on this system. **Y** indicates TN3270 data will be collected for the TN3270 server running on this system. **N** indicates TN3270 data will not be collected for the TN3270 server running on this system.

Related parameters

- “KN3_TCP_TN3270” on page 152
- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163
- “KN3_TCPXnn_OVRD_INTS” on page 164
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176
- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
- “KN3_TCPXnn_OVRD_CONN” on page 157
- “KN3_TCPXnn_OVRD_IPSEC” on page 166
- “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_OVRD_TN3270_DSPINTV

Use the KN3_TCPXnn_OVRD_TN3270_DSPINTV parameter to specify how long TN3270 server statistics will be displayed on the Tivoli Enterprise Portal for the TN3270 server running on this system.

Required or optional
Optional unless you want to override the global value for this parameter. See “KN3_TCP_TN3270_DSPINTV” on page 153.

Location where the parameter value is stored
In the KN3AGOPS member in the *rhilev.midlev.rtename*.RKANSAMU library

Parameter name
`KN3FCCMD START TN3270 TCPNAME(`*`tcpip_proc_name`*`) DSPINTV(&N3OTND)` (Override TN3270 data display interval)

TCPNAME identifies which TCP/IP address spaces this applies to. `tcpip_proc_name` is the name of a TCP/IP address space in your environment. DSPINTV specifies the number of hours of data that is displayed.

Default value
The global value. See "KN3_TCP_TN3270_DSPINTV" on page 153.

Permissible values
1-24

In the Configuration Tool (ICAT)

Panel name
TCP/IP Monitored Systems Info

Panel ID
KN341PPJ

Field
TN3270 Display Interval Override

Default value
The global value. See "KN3_TCP_TN3270_DSPINTV" on page 153.

Permissible values
1-24

Batch parameter name
KN3_TCPX_TNC_INT_SPEC

PARMGEN name
KN3_TCPXnn_OVRD_TN3270_DSPINTV

PARMGEN classification
Define TCP monitoring systems member

Description

Override TN3270 data display interval

This parameter determines how long TN3270 server statistics will be displayed for the TN3270 server running on this system. This value is expressed as a whole number in hours from 1 to 24. The global default is **2 hours**.

Related parameters

- "KN3_TCP_TN3270_DSPINTV" on page 153
- "KN3_TCPX" on page 174
- "KN3_TCPXnn_OVRD_GLBS" on page 160
- "KN3_TCPXnn_OVRD_INTE" on page 163
- "KN3_TCPXnn_OVRD_INTS" on page 164
- "KN3_TCPXnn_OVRD_OSA" on page 167
- "KN3_TCPXnn_ROW" on page 175
- "KN3_TCPXnn_SYS_NAME" on page 176
- "KN3_TCPXnn_TCP_STC" on page 177
- "KN3_TCPXnn_TCPIP_PROFILES_DSN" on page 179
- "KN3_TCPXnn_OVRD_GLOBAL_FLAG" on page 162
- "KN3_TCPXnn_OVRD_COLLECT_STACK" on page 155
- "KN3_TCPXnn_OVRD_CONN" on page 157
- "KN3_TCPXnn_OVRD_IPSEC" on page 166
- "KN3_TCPXnn_OVRD_ROUTE_TBL" on page 168
- "KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ" on page 170

- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPX

The KN3_TCPX syntax marker indicates the beginning and end of the KN3_TCPX_* block of values.

Required or optional
Not a parameter. KN3_TCPX is a syntax marker in the configuration profile (either your *rte_name* or CFGUSR) file that marks the beginning and end of the KN3_TCPX_* block of values.

Location where the parameter value is stored
The parameter value is not stored, but is used for internal processing.

Parameter name
N3SNAINT (Row begin group end indicator)

Default value
BEGIN

Permissible values
BEGIN, END

In the Configuration Tool (ICAT)
This value cannot be defined using the Configuration Tool.

Batch parameter name
KN3_TCPX

PARMGEN name
KN3_TCPX

PARMGEN classification
Define TCP monitoring systems member

Description

Beginning and ending syntax markers for the KN3_TCPX group of parameters.

Related parameters

- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163
- “KN3_TCPXnn_OVRD_INTS” on page 164
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176
- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
- “KN3_TCPXnn_OVRD_CONN” on page 157
- “KN3_TCPXnn_OVRD_IPSEC” on page 166
- “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159

- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_ROW

Use the KN3_TCPXnn_ROW parameter to indicate the beginning or end of a single KN3TCP entry.

Required or optional
Optional

Location where the parameter value is stored
The parameter value is not stored, but is used as a syntax marker.

Parameter name
N3SNAINT (Row begin group end indicator)

Default value
BEGIN

Permissible values
BEGIN, END

In the Configuration Tool (ICAT)
This value cannot be defined using the Configuration Tool.

Batch parameter name
KN3_TCPX_ROW

PARMGEN name
KN3_TCPXnn_ROW

PARMGEN classification
Define TCP monitoring systems member

Description

Row begin group end indicator

This parameter indicates the beginning or end of a single KN3TCP entry.

If the variable value is BEGIN, the variables up to either the next BEGIN or the next END contain all the information necessary to construct the information for a single KN3TCP entry.

The default, if no value is specified, is **BEGIN**.

Related parameters

- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163
- “KN3_TCPXnn_OVRD_INTS” on page 164
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176
- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
- “KN3_TCPXnn_OVRD_CONN” on page 157
- “KN3_TCPXnn_OVRD_IPSEC” on page 166
- “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168

- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_SYS_NAME

Use the KN3_TCPXnn_SYS_NAME parameter to specify the name of the system to be monitored.

Required or optional
Required

Location where the parameter value is stored
In the KN3TCPMO member in the *rhilev.midlev.rtename*.RKANPARU library and in the KN3AGOPT member in the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
Depends on whether your use global defaults or stack-specific values

- `N3SYSNAM`
- `TCPNAME(&N3SYSNAM)`

(System name)

Default value
$$$$

Permissible values
A string up to 4 characters in length

In the Configuration Tool (ICAT)

Panel name

- *action* TCP/IP MONITORED SYSTEMS INFO / RTE: *rtename*, where *action* is ADD, COPY, UPDATE, DELETE, or VIEW (KN341PPI OR KN341PPJ)
- SPECIFY TCP/IP MONITORING SYSTEMS INFORMATION (KN341PP1)

Panel ID

- KN341PP1 (global or stack specific)
- KN341PPI (stack specific)
- KN341PPJ (stack specific)

Field
Sys

Default value
$$$$

Permissible values
A string up to 4 characters in length

Batch parameter name
KN3_TCPX_SYS_NAME

PARMGEN name
KN3_TCPXnn_SYS_NAME

PARMGEN classification
Define TCP monitoring systems member

Description

System name

This parameter specifies the name of the system to be monitored. The default is four dollar signs (**$$$$**). Whenever no specific entry exists in the table for a detected TCP/IP address space, the configuration options provided in the $$$$ entry will be used. The four dollar signs (**$$$$**) and eight dollar signs (**$$$$$$$$**) are reserved combinations that cannot be deleted and represent the global system-wide values.

Related parameters

- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163
- “KN3_TCPXnn_OVRD_INTS” on page 164
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176
- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
- “KN3_TCPXnn_OVRD_CONN” on page 157
- “KN3_TCPXnn_OVRD_IPSEC” on page 166
- “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_TCP_STC

Use the KN3_TCPXnn_TCP_STC parameter to specify the name of the TCP/IP address space on the monitored system.

Required or optional
Required

Location where the parameter value is stored
In the KN3TCPMO member in the *rhilev.midlev.rtename*.RKANPARU library and in the KN3AGOPT member in the *rhilev.midlev.rtename*.RKANCMDU library

Parameter name
`TCPNAME(&N3TCPAS)` (TCP/IP address space name)

Default value
$$$$$$$$, indicating that all TCP/IP address spaces will be monitored

Permissible values
A string of up to 8 characters

In the Configuration Tool (ICAT)

Panel name

- *action* TCP/IP MONITORED SYSTEMS INFO / RTE: *rtename*, where *action* is ADD, COPY, UPDATE, DELETE, or VIEW (KN341PPI OR KN341PPJ)
- SPECIFY TCP/IP MONITORING SYSTEMS INFORMATION (KN341PP1)

Panel ID

- KN341PP1 (global)
- KN341PPI (stack-specific)
- KN341PPJ (stack-specific)

Field
TCP/IP address space

Default value
$$$$$$$$, indicating that all TCP/IP address spaces will be monitored

Permissible values
A string of up to 8 characters

Batch parameter name
KN3_TCPX_ADDR_SPACE

PARMGEN name
KN3_TCPXnn_TCP_STC

PARMGEN classification
Define TCP monitoring systems member

Description

TCP/IP address space name

This parameter specifies the name of the TCP/IP address space on the monitored system. The default is eight dollar signs (**$$$$$$$$**). A maximum of eight (8) TCP/IP address spaces can be monitored using global override specifications. The four dollar signs (**$$$$**) and eight dollar signs (**$$$$$$$$**) are reserved combinations that cannot be deleted and represent the global system-wide values.

Related parameters

- “KN3_TCPX” on page 174
- “KN3_TCPXnn_OVRD_OSA” on page 167
- “KN3_TCPXnn_OVRD_GLBS” on page 160
- “KN3_TCPXnn_OVRD_INTE” on page 163
- “KN3_TCPXnn_OVRD_INTS” on page 164
- “KN3_TCPXnn_ROW” on page 175
- “KN3_TCPXnn_SYS_NAME” on page 176
- “KN3_TCPXnn_TCP_STC” on page 177
- “KN3_TCPXnn_TCPIP_PROFILES_DSN” on page 179
- “KN3_TCPXnn_OVRD_GLOBAL_FLAG” on page 162
- “KN3_TCPXnn_OVRD_COLLECT_STACK” on page 155
- “KN3_TCPXnn_OVRD_CONN” on page 157
- “KN3_TCPXnn_OVRD_IPSEC” on page 166
- “KN3_TCPXnn_OVRD_ROUTE_TBL” on page 168
- “KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ” on page 170
- “KN3_TCPXnn_OVRD_FTP” on page 158
- “KN3_TCPXnn_OVRD_FTP_DSPINTV” on page 159
- “KN3_TCPXnn_OVRD_TN3270” on page 171
- “KN3_TCPXnn_OVRD_TN3270_DSPINTV” on page 172
- “KN3_TCPXnn_TCPIP_PROFILES_MBR” on page 180

KN3_TCPXnn_TCPIP_PROFILES_DSN

Use the KN3_TCPXnn_TCPIP_PROFILES_DSN parameter to specify the name of the TCP/IP profile data set.

Required or optional
Required

Location where the parameter value is stored
In the KN3TCPMO member in the *rhilev*.*midlev*.*rtename*.RKANSAMU library

Parameter name
N3PFLDSN (TCP/IP profile dataset name)

Default value
TCPIP.PROFILE.TCPIP

Permissible values
A string of up to 44 characters

In the Configuration Tool (ICAT)

Panel name
action TCP/IP MONITORED SYSTEMS INFO / RTE: *rtename*, where *action* is ADD, COPY, UPDATE, DELETE, or VIEW

Panel ID

- KN341PPI
- KN341PPJ

Field
TCP/IP profile data set name

Note: This is the one of only two global parameter that can be changed on the stack-specific Configuration Tool panels. The other parameter is the member name for this data set if it is a partitioned data set, the `Member name` field in the Configuration Tool or the "KN3_TCPXnn_TCPIP_PROFILES_MBR" on page 180 parameter.

Default value
TCPIP.PROFILE.TCPIP

Permissible values
A string of up to 44 characters

Batch parameter name
KN3_TCPX_PROF_DATASET

PARMGEN name
KN3_TCPXnn_TCPIP_PROFILES_DSN

PARMGEN classification
Define TCP monitoring systems member

Description

TCP/IP profile dataset name

The parameter specifies the name of the TCP/IP profile data set. This parameter can be either a partitioned data set or a sequential data set. The default is **TCPIP.PROFILE.TCPIP**. If you specify a partitioned data set, then you must supply a member name. See "KN3_TCPXnn_TCPIP_PROFILES_MBR" on page 180.

Related parameters

- "KN3_TCPX" on page 174
- "KN3_TCPXnn_OVRD_OSA" on page 167
- "KN3_TCPXnn_OVRD_GLBS" on page 160
- "KN3_TCPXnn_OVRD_INTE" on page 163

- "KN3_TCPXnn_OVRD_INTS" on page 164
- "KN3_TCPXnn_ROW" on page 175
- "KN3_TCPXnn_SYS_NAME" on page 176
- "KN3_TCPXnn_TCP_STC" on page 177
- "KN3_TCPXnn_OVRD_GLOBAL_FLAG" on page 162
- "KN3_TCPXnn_OVRD_COLLECT_STACK" on page 155
- "KN3_TCPXnn_OVRD_CONN" on page 157
- "KN3_TCPXnn_OVRD_IPSEC" on page 166
- "KN3_TCPXnn_OVRD_ROUTE_TBL" on page 168
- "KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ" on page 170
- "KN3_TCPXnn_OVRD_FTP" on page 158
- "KN3_TCPXnn_OVRD_FTP_DSPINTV" on page 159
- "KN3_TCPXnn_OVRD_TN3270" on page 171
- "KN3_TCPXnn_OVRD_TN3270_DSPINTV" on page 172
- "KN3_TCPXnn_TCPIP_PROFILES_MBR" on page 180

KN3_TCPXnn_TCPIP_PROFILES_MBR

Use the KN3_TCPXnn_TCPIP_PROFILES_MBR parameter to specify the member name of the TCP/IP profiles in the TCP/IP profile data set.

Required or optional
Optional. This field is required if the TCP/IP profile data set is a partitioned data store.

Location where the parameter value is stored
In the KN3TCPMO member in the *rhilev.midlev.rtename*.RKANSAMU library

Parameter name
N3PFLMEM (TCP/IP Profile member name)

Default value
No default

Permissible values
A character string of up to 8 characters

In the Configuration Tool (ICAT)

Panel name
action TCP/IP MONITORED SYSTEMS INFO / RTE: *rtename*, where *action* is ADD, COPY, UPDATE, DELETE, or VIEW

Panel ID

- KN341PPI
- KN341PPJ

Field
Member name

Note: This is the one of only two global parameter that can be changed on the stack-specific Configuration Tool panels. The other parameter is the name of the TCP/IP profile data set, the `TCP/IP profile data set name` field in the Configuration Tool or the "KN3_TCPXnn_TCPIP_PROFILES_DSN" on page 179 parameter.

Default value
No default

Permissible values
A character string of up to 8 characters

Batch parameter name
KN3_TCPX_PROF_MEMBER

PARMGEN name
KN3_TCPXnn_TCPIP_PROFILES_MBR

PARMGEN classification
Define TCP monitoring systems member

Description

TCP/IP Profile member name

The parameter specifies the member name of the TCP/IP profiles in the TCP/IP profile data set. This value is required if you specify a partitioned data set. It is not used if you specify a sequential data set. See also "KN3_TCPXnn_TCPIP_PROFILES_DSN" on page 179.

Related parameters

- "KN3_TCPX" on page 174
- "KN3_TCPXnn_OVRD_OSA" on page 167
- "KN3_TCPXnn_OVRD_GLBS" on page 160
- "KN3_TCPXnn_OVRD_INTE" on page 163
- "KN3_TCPXnn_OVRD_INTS" on page 164
- "KN3_TCPXnn_ROW" on page 175
- "KN3_TCPXnn_SYS_NAME" on page 176
- "KN3_TCPXnn_TCP_STC" on page 177
- "KN3_TCPXnn_TCPIP_PROFILES_DSN" on page 179
- "KN3_TCPXnn_OVRD_GLOBAL_FLAG" on page 162
- "KN3_TCPXnn_OVRD_COLLECT_STACK" on page 155
- "KN3_TCPXnn_OVRD_CONN" on page 157
- "KN3_TCPXnn_OVRD_IPSEC" on page 166
- "KN3_TCPXnn_OVRD_ROUTE_TBL" on page 168
- "KN3_TCPXnn_OVRD_ROUTE_TBL_FREQ" on page 170
- "KN3_TCPXnn_OVRD_FTP" on page 158
- "KN3_TCPXnn_OVRD_FTP_DSPINTV" on page 159
- "KN3_TCPXnn_OVRD_TN3270" on page 171
- "KN3_TCPXnn_OVRD_TN3270_DSPINTV" on page 172

KN3_TEMS_BKUP1_NAME_NODEID

Use the KN3_TEMS_BKUP1_NAME_NODEID parameter to specify the backup monitoring server values for configuring an agent for your site.

Required or optional
Optional

Location where the parameter value is stored
In the KN3ENV member in the *rhilev.midlev.rtename*.RKANPARU library to communicate with the backup Tivoli Enterprise Monitoring Server

Parameter name
N/A

Default value
No default

Permissible values
A string of up to 32 case-sensitive characters

In the Configuration Tool (ICAT)

Panel name
SPECIFY AGENT SECONDARY TEMS VALUES

Panel ID
KAG62P8

Field
Backup TEMS name

Default value
No default

Permissible values
A string of up to 32 case-sensitive characters

Batch parameter name
KN3_CMSB_NAME

PARMGEN name
KN3_TEMS_BKUP1_NAME_NODEID

PARMGEN classification
Secondary TEMS VTAM information

Description

Server that the monitoring agent will connect to if the primary Tivoli Enterprise Monitoring Server (monitoring server) fails.

This parameter specifies backup monitoring server values for configuring an agent for your site. This name must match the name of a non-z/OS monitoring server, or the CMS_NODEID parameter value, in the KDSENV member of the *rhilev.midlev.rtename*.RKANPARU library for a z/OS TEMS. If the parameter value contains the SMFID, you must enter the z/OS system's SMFID in place of this literal.

Note: The value of this field is case-sensitive for both z/OS and non-z/OS monitoring server names.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters
None

KN3_TEMS_BKUP1_TCP_HOST

Use the KN3_TEMS_BKUP1_TCP_HOST to specify the TCP/IP hostname identifier for the backup Tivoli Enterprise Monitoring Server that this agent should try to connect to if the primary server is unavailable.

Required or optional
Optional. Required field if you plan to have this monitoring agent communicate with the backup server using TCP/IP.

Location where the parameter value is stored
In the KN3ENV member in the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
`CT_CMSLIST=\` (Agent backup Server TCP/IP hostname)

Default value
No default

Permissible values
A string of up to 32 characters

In the Configuration Tool (ICAT)

Panel name
SPECIFY AGENT SECONDARY TEMS VALUES

Panel ID
KAG62P8

Field
Network address (Hostname of Secondary TEMS)

Default value
No default

Permissible values
A string of up to 32 characters

Batch parameter name
KN3_CMSB_TCP_HOST

PARMGEN name
KN3_TEMS_BKUP1_TCP_HOST

PARMGEN classification
Secondary TEMS TCP/IP information

Description

Agent backup Server TCP/IP hostname

This parameter specifies the TCP/IP hostname identifier for the backup Tivoli Enterprise Monitoring Server that this agent should try to connect to if the primary server is unavailable. This is a required field if you plan to have this agent communicate with the backup server using TCP/IP.

Specify the network address of the system on which the secondary monitoring server that this monitoring agent connects to is running. A network address may be specified as one of the following values:

1. A fully-qualified hostname (for example: `sys.ibm.com`)
2. The first qualifier of the fully-qualified hostname (for example: `sys` for `sys.ibm.com`)
3. An IPv4 address in dotted decimal notation (for example: `9.67.1.100`)

If the secondary monitoring server is running on a z/OS platform, you can find this value by issuing the `TSO HOMETEST` command from the system where the secondary monitoring server is running. If you will specify the hostname value for network address, use the first qualifier of the fully qualified hostname if the z/OS domain name resolver configuration specifies a search path that would include the target domain suffix. Otherwise, specify the fully-qualified hostname when using a Domain Name Server (DNS). If you will specify the IP address value for network address, use the assigned IPv4 address written in dotted decimal notation. This scheme is numeric and consists of four groups separated by a period (.).

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_TEMS_BKUP1_NAME_NODEID" on page 181
- "KN3_TEMS_BKUP1_VTAM_APPL_LLB_BKR" on page 183
- "KN3_TEMS_BKUP1_VTAM_LU62_DLOGMOD" on page 184
- "KN3_TEMS_BKUP1_VTAM_NETID" on page 185

KN3_TEMS_BKUP1_VTAM_APPL_LLB_BKR

Use the KN3_TEMS_BKUP1_VTAM_APPL_LLB_BKR parameter to identify the Local Location Broker that is to be used for VTAM-type communication to the backup server.

Required or optional
Optional. This is a required field if this monitoring agent needs to communicate with the backup server using VTAM protocol.

Location where the parameter value is stored
In the KN3ENV member in the *rhilev.midlev.rtename*.RKANPARU library if you use SNA to communicate with the backup Tivoli Enterprise Monitoring Server

Parameter name
N/A

Default value
No default

Permissible values
A string of up to 8 characters

In the Configuration Tool (ICAT)

Panel name
Specify Agent Secondardy TEMS Values

Panel ID
KAG62P8

Field
Local location broker applid

Default value
No default

Default value
No default

Permissible values
A string of up to 8 characters

Batch parameter name
KN3_CMSB_VTM_APPL_LLB

PARMGEN name
KN3_TEMS_BKUP1_VTAM_APPL_LLB_BKR

PARMGEN classification
Secondary TEMS VTAM information

Description

Backup Server Location Broker applid

This parameter identifies the Local Location Broker that is to be used for VTAM-type communication to the backup server. Enter the Local Location Broker applid of the secondary Tivoli Enterprise Monitoring Server that this agent communicates with. This is a required field if this agent needs to communicate with the backup server using SNA protocol. This field is not required if you use TCP/IP for communication with the backup monitoring server.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters
None

KN3_TEMS_BKUP1_VTAM_LU62_DLOGMOD

Use the KN3_TEMS_BKUP1_VTAM_LU62_DLOGMOD parameter to specify the name of the LU6.2 LOGMODE that was defined for the backup server.

Required or optional
Optional. This is a required field if you plan to have the backup server communicate with monitoring agents using VTAM.

Location where the parameter value is stored
In the KN3ENV member in the *rhilev.midlev.rtename*.RKANPARU library if you use SNA to communicate with the backup Tivoli Enterprise Monitoring Server

Parameter name
N/A

Default value
CANCTDCS

Permissible values
A string of up to 8 characters

In the Configuration Tool (ICAT)

Panel name
Specify Agent Secondard TEMS Values

Panel ID
KAG62P8

Field
LU6.2 logmode

Default value
CANCTDCS

Permissible values
A string of up to 8 character

Batch parameter name
KN3_CMSB_VTM_LU62_LOG

PARMGEN name
KN3_TEMS_BKUP1_VTAM_LU62_DLOGMOD

PARMGEN classification
Secondary TEMS VTAM information

Description

Agent backup Server LU6.2 logmode

This parameter specifies the name of the LU6.2 LOGMODE that was defined for the backup server. The default is CANCTDCS. This is a required field if you plan to have the backup server communicate with agents using SNA. This field is not needed if you use TCP/IP for communication with the backup monitoring server.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters
None

KN3_TEMS_BKUP1_VTAM_NETID

Use the KN3_TEMS_BKUP1_VTAM_NETID parameter to identify your SNA network.

Required or optional
Optional. This is a required field if you plan to have the backup server communicate with monitoring agents using VTAM.

Location where the parameter value is stored
In the KN3ENV member in the *rhilev*.*midlev*.*rtename*.RKANPARU library if you use SNA to communicate with the backup Tivoli Enterprise Monitoring Server

Parameter name
N/A

Default value
No default

Permissible values
A string of up to 8 characters

In the Configuration Tool (ICAT)

Panel name
Specify Agent Secondard TEMS Values

Panel ID
KAG62P8

Field
Network ID

Default value
No default

Permissible values
A string of up to 8 characters

Batch parameter name
KN3_CMSB_VTM_NETID

PARMGEN name
KN3_TEMS_BKUP1_VTAM_NETID

PARMGEN classification
Secondary TEMS VTAM information

Description

Agent backup Sever Network ID

This parameter identifies your SNA network. You can locate this value on the NETID parameter within the VTAMLST startup member, ATCSTR*nn*. This is a required field if you plan to have the backup server communicate with monitoring agents using SNA. This field is not needed if you use TCP/IP for communication with the backup monitoring server.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters
None

KN3_TEMS_HUB_TCP_HOST

Use the KN3_TEMS_HUB_TCP_HOST parameter to specify the hostname or IP address of the system where the primary Tivoli Enterprise Monitoring Server (local or remote) is running.

Required or optional
Optional. Required for remote Tivoli Enterprise Monitoring Servers that use TCP/IP for communications with the hub monitoring server

Location where the parameter value is stored
In the KDCSSITE member in the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name
AGL0CCN (Connect agent to local TEMS)

Default value
None

Permissible values
Character string, maximum length 32

In the Configuration Tool (ICAT)

Panel name
Specify Agent Primary TEMS Values

Panel ID
KAG62P1

Field
Network Address (Hostname of the primary TEMS)

Default value
None

Permissible values
Character string, maximum length 32

Batch parameter name
KN3_CMS_HUB_TCP_HOST

PARMGEN name
KN3_TEMS_HUB_TCP_HOST

PARMGEN classification
Values that describe the Primary TEMS the Agent will connect to

Description

Hostname of the primary TEMS

This parameter specifies the hostname or IP address of the system where the primary Tivoli Enterprise Monitoring Server (local or remote) is running. The value specified for this parameter must match the value set for the KDS_TEMS_TCP_HOST parameter in the runtime environment where the hub is configured, or the value set for an equivalent parameter of a distributed hub.

Related parameters

- "KN3_TEMS_LOCAL_CONNECT_FLAG" on page 187
- "KN3_TEMS_NAME_NODEID" on page 188

KN3_TEMS_LOCAL_CONNECT_FLAG

Use the KN3_TEMS_LOCAL_CONNECT_FLAG parameter to specify how you want to connect the agent you are defining.

Required or optional
Optional

Location where the parameter value is stored
The parameter value is not stored, but is used for internal processing.

Parameter name
AGL0CCN (Connect agent to local TEMS)

Default value
Y

Permissible values
Y, N

In the Configuration Tool (ICAT)

Panel name
SPECIFY AGENT ADDRESS SPACE PARAMETERS

Panel ID
KAG62P2

Field
Connect to TEMS in this RTE

Default value
Y

Permissible values
Y, N

Batch parameter name
KN3_CMS_LOCAL_CONNECT

PARMGEN name
KN3_TEMS_LOCAL_CONNECT_FLAG

PARMGEN classification
Values that describe the Primary TEMS the Agent will connect to

Description

Connect agent to local TEMS

This parameter specifies how you want to connect the agent you are defining. When defining an agent, you have the option to connect the agent to a local server or a remote server. When connecting to a local server you are connecting the agent to the server in this runtime environment.

Specify **Y** to connect the agent to the server in this RTE. Otherwise, specify **N** to have the agent connect to a remote server.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_TEMS_NAME_NODEID" on page 188

KN3_TEMS_NAME_NODEID

Use the KN3_TEMS_NAME_NODEID parameter to specify the primary Tivoli Enterprise Monitoring Server values for configuring an agent for your site.

Required or optional
Optional

Location where the parameter value is stored
In the KN3ENV member in the *rhilev.midlev.rtename*.RKANPARU library

Parameter name

```
CT_CMSLIST=\
CIDSCELL
```

(TEMS name)

Default value
No default

Permissible values
A string of up to 8 case-sensitive characters defining the nodeid of the server to which you are connecting the agent

In the Configuration Tool (ICAT)

Panel name
Specify Agent Primary TEMS Values

Panel ID
KAG62P1

Field
TEMS Name

This value is created if you specify use of a local Tivoli Enterprise Monitoring Server (TEMS) on the same system where you created the runtime environment (RTE). This field is prefilled if you specified a local monitoring server on z/OS and cannot be changed.

Default value
No default

Permissible values
A string of up to 8 case-sensitive characters defining the nodeid of the server to which you are connecting the agent

Batch parameter name
KN3_CMS_NAME

PARMGEN name
KN3_TEMS_NAME_NODEID

PARMGEN classification
Values that describe the Primary TEMS the Agent will connect to

Description

Primary monitoring server that this monitoring agent connects to

This parameter specifies the primary Tivoli Enterprise Monitoring Server values for configuring an agent for your site. This name must match the name of a non-z/OS monitoring server, or the CMS_NODEID parameter value, in the KDSENV member of the *rhilev.midlev.rtename*.RKANPARU library for a z/OS TEMS. If the parameter value contains the SMFID, you must enter the z/OS system's SMFID in place of this literal.

Note: The value of this field is case-sensitive for both z/OS and non-z/OS monitoring server names.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters
None

KN3_TEMS_TCP_HOST

Use the KN3_TEMS_TCP_HOST parameter to specify the agent's primary TEMS TCP/IP information.

Required or optional
This is a required field if you plan to have this agent communicate with Tivoli Enterprise Monitoring Server using TCP/IP.

Location where the parameter value is stored
In the KN3ENV member in the *rhilev.midlev.rtename*.RKANPARU library

Parameter name

```
CT_CMSLIST=%KN3_TEMS_TCP_HOST
```

Default value
Value set for the RTE_TCP_HOST parameter for the runtime environment

Permissible values
Character string, maximum length 32

In the Configuration Tool (ICAT)

Panel name
Specify Agent Primary TEMS Values

Panel ID
KAG62P1

Field
Network Address

Default value
Value set for the RTE_TCP_HOST parameter for the runtime environment

Permissible values
Character string, maximum length 32

Batch parameter name
KN3_CMS_TCP_HOST

PARMGEN name
KN3_TEMS_TCP_HOST

PARMGEN classification
Agent's Primary TEMS TCP/IP information

Description

Server hostname

This parameter specifies the server hostname. To obtain the host name or IP address, enter TSO HOMETEST at the command line. If the z/OS domain name resolver configuration specifies a search path that includes the target domain suffix, specify only the first qualifier of the host name. (Example: `sys` is the first qualifier of the fully qualified host name `sys.ibm.com`.) Otherwise, specify the fully qualified host name.

This is a required field if you plan to have this server communicate with agents using TCP/IP.

Attention: "KN3_TEMS_TCP_HOST" on page 189 and "KN3_AGT_TCP_HOST" on page 110 must be the same value if "KN3_TEMS_LOCAL_CONNECT_FLAG" on page 187=Y (that is, if the agent connects to local monitoring server).

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_AGT_TCP_HOST" on page 110
- "KN3_TEMS_TCP_HOST" on page 189

KN3_TEMS_TCP_PIPE_PORT_NUM

Use the KN3_TEMS_TCP_PIPE_PORT_NUM parameter to specify the IP.PIPE port number that you want to use.

Required or optional

Required if you specified a value of IPPIPE as one of the "KN3_AGT_COMM_PROTOCOLn" on page 90 protocol parameters

Location where the parameter value is stored

The KN3ENV member of the *rhilev.rte*.RKANPARU library

Parameter name

`IP.PIPE PORT:` (Agent IP.PIPE port number)

Default value

1918

Permissible values

1 - 65535

In the Configuration Tool (ICAT)

Panel name

- Specify Agent Primary TEMS Values (KAG62P1 for a non-local TEMS)
- Specify IP.PIPE Communication Protocol (KDS62PPD for a local TEMS)

Panel ID

- KAG62P1 for a non-local TEMS
- KDS62PPD for a local TEMS

Field

Port number (IP.PIPE)

Default value

1918

Permissible values

1 - 65535

Batch parameter name

KN3_CMS_TCP_PIPE_PORT

PARMGEN name
KN3_TEMS_TCP_PIPE_PORT_NUM

PARMGEN classification
Protocol port numbers for Agent connection to TEMS

Description

Agent IP.PIPE port number

This parameter specifies the IP.PIPE port number that you want to use. This port number is used by the non-secure Network Computing System (NCS) IP.PIPE protocol. The default is **1918**.

Note: Port numbers for non-secure IP.PIPE protocol and IP.UDP protocol must match.

Related parameters

- "KN3_TEMS_TCP_PIPES_PORT_NUM" on page 191
- "KN3_TEMS_TCP_PIPE6_PORT_NUM" on page 192
- "KN3_TEMS_TCP_PIPE6S_PORT_NUM" on page 193
- "KN3_TEMS_TCP_UDP_PORT_NUM" on page 194
- "KN3_TEMS_TCP_UDP6_PORT_NUM" on page 195

KN3_TEMS_TCP_PIPES_PORT_NUM

Use the KN3_TEMS_TCP_PIPES_PORT_NUM parameter to specify the IP.SPIPE port number that you want to use.

Required or optional
Required if you specified a value of IPSPIPE in one of the "KN3_AGT_COMM_PROTOCOLn" on page 90 protocol parameters.

Location where the parameter value is stored
The KDSENV member of the *rhilev.rte*.RKANPARU library

Parameter name
`IP.SPIPE PORT:` (Agent IP.SPIPE port number)

Default value
3660

Permissible values
1 - 65535

In the Configuration Tool (ICAT)

Panel name

- Specify Agent Primary TEMS Values (KAG62P1 for a non-local TEMS)
- Specify IP.PIPE Communication Protocol (KDS62PPD for a local TEMS)

Panel ID

- KAG62P1 for a non-local TEMS
- KDS62PPD for a local TEMS

Field
Port number (Secure IP.PIPE)

Default value
3660

Permissible values
1 - 65535

Batch parameter name
KN3_CMS_TCP_PIPES_PORT

PARMGEN name
KN3_TEMS_TCP_PIPES_PORT_NUM

PARMGEN classification
Protocol port numbers for Agent connection to TEMS

Description

Agent IP.SPIPE port number

This parameter specifies the IP.SPIPE port number that you want to use. This port number is used by the secure Network Computing System (NCS) IP.PIPE protocol. The default is 3660.

Note: Port numbers for non-secure IP6.PIPE and IP.UDP protocols must match.

This parameter is required if you specified a value of IPSPIPE in one of the KN3_AGT_COMM_PRO*n* protocol parameters.

Related parameters

- “KN3_TEMS_TCP_PIPE_PORT_NUM” on page 190
- “KN3_TEMS_TCP_PIPE6_PORT_NUM” on page 192
- “KN3_TEMS_TCP_PIPE6S_PORT_NUM” on page 193
- “KN3_TEMS_TCP_UDP_PORT_NUM” on page 194
- “KN3_TEMS_TCP_UDP6_PORT_NUM” on page 195

KN3_TEMS_TCP_PIPE6_PORT_NUM

Use the KN3_TEMS_TCP_PIPE6_PORT_NUM parameter to specify the IP6.PIPE port number that you want to use.

Required or optional
Required if you specified a value of IP6PIPE in one of the “KN3_AGT_COMM_PROTOCOLn” on page 90 protocol parameters.

Location where the parameter value is stored
The KN3ENV member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name
`PORT: IP6.PIPE PORT:` (Agent IP6.PIPE port number)

Default value
No default

Permissible values
1 - 65535

In the Configuration Tool (ICAT)

Panel name

- Specify Agent Primary TEMS Values (KAG62P1 for a non-local TEMS)
- Specify IP.PIPE Communication Protocol (KDS62PPD for a local TEMS)

Panel ID

- KAG62P1 for a non-local TEMS
- KDS62PPD for a local TEMS

Field
Port number (IP.PIPE for IPV6)

Default value
No default

Permissible values
1 - 65535

Batch parameter name
KN3_CMS_TCP_PIPE6_PORT

PARMGEN name
KN3_TEMS_TCP_PIPE6_PORT_NUM

PARM

PARMGEN classification
Protocol port numbers for Agent connection to TEMS

Description

Agent IP6.PIPE port number

This parameter specifies the IP6.PIPE port number that you want to use. This port number is used by the non-secure Network Computing System (NCS) IP.PIPE protocol. The default is **1918**.

Note: Port numbers for non-secure IP6.PIPE and IP.UDP protocols must match.

This parameter is required if you specified a value of IP6PIPE in one of the KN3_AGT_COMM_PRO*n* protocol parameters.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_TEMS_TCP_PIPE_PORT_NUM" on page 190
- "KN3_TEMS_TCP_PIPES_PORT_NUM" on page 191
- "KN3_TEMS_TCP_PIPE6S_PORT_NUM" on page 193
- "KN3_TEMS_TCP_UDP_PORT_NUM" on page 194
- "KN3_TEMS_TCP_UDP6_PORT_NUM" on page 195

KN3_TEMS_TCP_PIPE6S_PORT_NUM

Use the KN3_TEMS_TCP_PIPE6S_PORT_NUM parameter to specify the IP6.SPIPE port number that you want to use.

Required or optional
Required if you specified a value of IP6SPIPE in one of the "KN3_AGT_COMM_PROTOCOLn" on page 90 protocol parameters.

Location where the parameter value is stored
The KN3ENV member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
`IP6.SPIPE: PORT:` (Agent IP.PIPE port number)

Default value
3660

Permissible values
1 - 65535

In the Configuration Tool (ICAT)

Panel name

- Specify Agent Primary TEMS Values (KAG62PI1 for a non-local TEMS)
- Specify IP.PIPE Communication Protocol (KDS62PPD for a local TEMS)

Panel ID

- KAG62P1 for a non-local TEMS
- KDS62PPD for a local TEMS

Field
Port number (Secure IP.PIPE for IPV6)

Default value
3660

Permissible values
1 - 65535

Batch parameter name
KN3_CMS_TCP_PIPE6S_PORT

PARMGEN name
KN3_TEMS_TCP_PIPE6S_PORT_NUM

Description

Agent IP6.SPIPE port number

This parameter specifies the IP6.SPIPE port number that you want to use. This port number is used by the secure Network Computing System (NCS) IP.PIPE protocol. The default is 3660.

Note: Port numbers for non-secure IP.PIPE and IP.UDP protocols must match.

This parameter is required if you specified a value of IP6.SPIPE in one of the KN3_AGT_COMM_PRO*n* protocol parameters.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_TEMS_TCP_PIPE_PORT_NUM" on page 190
- "KN3_TEMS_TCP_PIPES_PORT_NUM" on page 191
- "KN3_TEMS_TCP_PIPE6_PORT_NUM" on page 192
- "KN3_TEMS_TCP_PIPE6S_PORT_NUM" on page 193
- "KN3_TEMS_TCP_UDP_PORT_NUM" on page 194
- "KN3_TEMS_TCP_UDP6_PORT_NUM" on page 195

KN3_TEMS_TCP_UDP_PORT_NUM

Use the KN3_TEMS_TCP_UDP_PORT_NUM parameter to specify the IP.UDP port number that you want to use.

Use the KN3_TEMS_TCP_UDP_PORT_NUM parameter to specify the IP.UDP port number that you want to use.

Required or optional
Required if you specified a value of IP in one of the "KN3_AGT_COMM_PROTOCOLn" on page 90 protocol parameters.

Location where the parameter value is stored
The KN3ENV member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name
`IP.UDP PORT:` (Agent IP.UDP port number)

Default value
1918

Permissible values
1 - 65535

In the Configuration Tool (ICAT)

Panel name

- Specify Agent Primary TEMS Values (KAG62P1 for a non-local TEMS)
- Specify IP.PIPE Communication Protocol (KDS62PPD for a local TEMS)

Panel ID

- KAG62P1 for a non-local TEMS
- KDS62PPD for a local TEMS

Field
Port number (IP.UDP)

Default value
1918

Permissible values
1 - 65535

Batch parameter name
KN3_CMS_TCP_UDP_PORT

PARMGEN name
KN3_TEMS_TCP_UDP_PORT_NUM

Description

Agent IP.UDP port number

This parameter specifies the IP.UDP port number that you want to use. This port number is used by the non-secure Network Computing System (NCS) IP (UDP) protocol. The default is **1918**.

Note: Port numbers for non-secure IP.PIPE protocol and IP.UDP protocol must match.

This parameter is required if you specified a value of IP in one of the KN3_AGT_COMM_PRO*n* protocol parameters.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_TEMS_TCP_PIPE_PORT_NUM" on page 190
- "KN3_TEMS_TCP_PIPES_PORT_NUM" on page 191
- "KN3_TEMS_TCP_PIPE6S_PORT_NUM" on page 193
- "KN3_TEMS_TCP_UDP6_PORT_NUM" on page 195

KN3_TEMS_TCP_UDP6_PORT_NUM

Use the KN3_TEMS_TCP_UDP6_PORT_NUM parameter to specify the IP6.UDP port number that you want to use.

Required or optional
Required if you specified a value of IP6 in one of the "KN3_AGT_COMM_PROTOCOLn" on page 90 protocol parameters.

Location where the parameter value is stored
The KN3ENV member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name
`IP6.UDP PORT:` (Agent IP.UDP port number)

Default value
No default

Permissible values
1 - 65535

In the Configuration Tool (ICAT)

Panel name

- Specify Agent Primary TEMS Values (KAG62P1 for a non-local TEMS)
- Specify IP.PIPE Communication Protocol (KDS62PPD for a local TEMS)

Panel ID

- KAG62P1 for a non-local TEMS
- KDS62PPD for a local TEMS

Field
Port number (IP6.UDP)

Default value
No default

Permissible values
1 - 65535

Batch parameter name
KN3_CMS_TCP_UDP6_PORT

PARMGEN name
KN3_TEMS_TCP_UDP6_PORT_NUM

Description

Agent IP6.UDP port number for IPv6

This parameter specifies the IP6.UDP port number that you want to use. This port number is used by the non-secure Network Computing System (NCS) IP (UDP) protocol. The default is **1918**.

Note: Port numbers for non-secure IP.PIPE protocols must match.

This parameter is required if you specified a value of IP6 in one of the KN3_AGT_COMM_PRO*n* protocol parameters.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_TEMS_TCP_PIPE_PORT_NUM" on page 190
- "KN3_TEMS_TCP_PIPES_PORT_NUM" on page 191
- "KN3_TEMS_TCP_PIPE6_PORT_NUM" on page 192
- "KN3_TEMS_TCP_PIPE6S_PORT_NUM" on page 193
- "KN3_TEMS_TCP_UDP_PORT_NUM" on page 194

KN3_TEMS_VTAM_APPL_LLB_BROKER

Use the KN3_TEMS_VTAM_APPL_LLB_BROKER parameter to identify which Local Location Broker is to be used for VTAM-type communication.

Required or optional
Required if you use SNA to communicate with the Tivoli Enterprise Monitoring Server

Location where the parameter value is stored
The KN3ENV member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name

```
CT_CMSLIST=%KN3_TEMS_VTAM_APPL_LLB_BROKER
```

Default value
CTDDSLB

Permissible values
A string of up to 8 characters

In the Configuration Tool

Panel name
Specify Agent Primary TEMS Values

Panel ID
KAG62P1

Field
Local Location Broker applid

Default value
CTDDSLB

Permissible values
A string of up to 8 characters

Batch parameter name
KN3_CMS_VTM_APPL_LLB

PARMGEN name
KN3_TEMS_VTAM_APPL_LLB_BROKER

PARMGEN classification
Agent's Primary TEMS VTAM information

Description

Local Location Broker applid

This parameter identifies which Local Location Broker is to be used for VTAM-type communication.

This is a required field if you use SNA to communicate with the Tivoli Enterprise Monitoring Server.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters
None

KN3_TEMS_VTAM_LU62_DLOGMOD

Use the KN3_TEMS_VTAM_LU62_DLOGMOD parameter to specify the name of the LU6.2 LOGMODE that was defined for the server.

Required or optional
Required if you use SNA to communicate with the Tivoli Enterprise Monitoring Server

Location where the parameter value is stored
The CTDN3N member of the *rhilev*.*midlev*.*rtename*.RKANSAMU library

Parameter name

```
CT_CMSLIST=\
CIDSMODE
```

(LU6.2 LOGMODE)

Default value
CANCTDCS

Permissible values
Character string, maximum length 8

In the Configuration Tool (ICAT)

Panel name
Specify Agent Primary TEMS Values

Panel ID
KAG62P1

Field
LU6.2 logmode

Default value
CANCTDCS

Permissible values
Character string, maximum length 8

Batch parameter name
KN3_CMS_VTM_LU62_LOG

PARMGEN name
KN3_TEMS_VTAM_LU62_DLOGMOD

PARMGEN classification
Agent's Primary TEMS VTAM information

Description

LU6.2 LOGMODE

This parameter specifies the name of the LU6.2 LOGMODE that was defined for the server. This is a required field if you plan to have the server communicate with agents using VTAM. The IBM default is **CANCTDCS**.

Related parameters
None

KN3_TEMS_VTAM_LU62_MODETAB

Use the KN3_TEMS_VTAM_LU62_MODETAB parameter to specify the name of the LOGMODE table containing the LU6.2 LOGMODE definition.

Required or optional
Required if you use SNA to communicate with the Tivoli Enterprise Monitoring Server

Location where the parameter value is stored
The CTDN3N member of the *rhilev*.*midlev*.*rtename*.RKANSAMU library

Parameter name

```
CT_CMSLIST=%KN3_TEMS_VTAM_LU62_MODETAB
```

Default value
KDSMTAB1

Permissible values
Character string, maximum length 8

In the Configuration Tool (ICAT)

Panel name
Specify Agent Primary TEMS Values

Panel ID
KAG62P1

Field
LOGMODE table name

Default value
KDSMTAB1

Permissible values
Character string, maximum length 8

Batch parameter name
KN3_CMS_VTM_LU62_LOGTAB

PARMGEN name
KN3_TEMS_VTAM_LU62_MODETAB

PARMGEN classification
Agent's Primary TEMS VTAM information

Description

LOGMODE table name

This parameter specifies the name of the LOGMODE table containing the LU6.2 LOGMODE definition. This is a required field if you plan to have the server communicate with agents using SNA.

Related parameters
None

KN3_TEMS_VTAM_NETID

Use the KN3_TEMS_VTAM_NETID parameter to specify the identifier of your VTAM network.

Required or optional
Required if you use SNA to communicate with the Tivoli Enterprise Monitoring Server

Location where the parameter value is stored
The KN3ENV member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name

```
CT_CMSLIST=%KN3_TEMS_VTAM_NETID
```

Default value
Value set for the RTE_VTAM_NETID or RTE_SYSV_VTAM_NETID parameter

Permissible values
Character string, maximum length 8

In the Configuration Tool (ICAT)

Panel name
Specify Agent Primary TEMS Values

Panel ID
KAG62P1

Field
Network ID

Default value
Value set for the RTE_VTAM_NETID or RTE_SYSV_VTAM_NETID parameter

Permissible values
Character string, maximum length 8

Batch parameter name
KN3_CMS_VTM_NETID

PARMGEN name
KN3_TEMS_VTAM_NETID

PARMGEN classification
Agent's Primary TEMS VTAM information

Description

Network ID

This parameter specifies the identifier of your VTAM network. You can locate this value on the NETID parameter within the VTAMLST startup member (ATCSTR*nn*). This is a required field if you plan to have this server communicate to agents using VTAM.

Related parameters
None

KN3_TN3270_DXL_APPLID

Use the KN3_TN3270_DXL_APPLID parameter to specify the IBM Tivoli NetView for z/OS APPLID that the IBM Z OMEGAMON Network Monitor monitoring agent will dynamically log on to.

Required or optional
Optional. Required if you want to use the IBM Tivoli NetView for z/OS packet trace feature.

Location where the parameter value is stored
In the KN3ENV member in the *rhilev.midlev.rtename*.RKANPARU library

Parameter name

```
KN3_DXL_APPLID=\
N3APPL
```

(Specify NetView APPLID)

Default value
CNM01

Permissible values
A character string with a maximum length of 8.

In the Configuration Tool (ICAT)

Panel name
Specify Dynamic Terminal Integration Parameters

Panel ID
KN341PT1

Field
NetView APPLID

Default value
CNM01

Permissible values
A character string with a maximum length of 8.

Batch parameter name
KN3_TN3270_APPLID

PARMGEN name
KN3_TN3270_DXL_APPLID

PARMGEN classification
Define TN3270 Telnet session link user values

Description

Specify NetView APPLID

The parameter specifies the IBM Tivoli NetView for z/OS APPLID that the OMEGAMON XE for Mainframe Networks monitoring agent will dynamically log on to. The NetView instance specified must run on the same system as the OMEGAMON XE for Mainframe Networks monitoring agent. The Configuration Tool generated the KN3_DLX_APPLID parameter in the KN3ENV member of the *rhilev.midlev.rtename*.RKANPARU library. The default is **CNM01**. The field is a character string with a maximum length of 8.

Example: To see this parameter specified in the context of the KN3ENV member, see "Sample KN3ENV member" on page 69.

Related parameters

- "KN3_TN3270_DXL_USERDATA" on page 201

KN3_TN3270_DXL_USERDATA

Use the KN3_TN3270_DXL_USERDATA parameter to specify the data to be passed to the IBM Tivoli NetView for z/OS program during logon.

Required or optional
Optional. Required if you want to use the IBM Tivoli NetView for z/OS packet trace feature.

Location where parameter value is stored
In the KN3ENV member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name

```
KN3_DXL_USERDATA=\
N3USDTA
```

(TN3270 User Data Field)

Default value
None

Permissible values
A character string with a maximum length of 109 in the format userid/password

In the Configuration Tool (ICAT)

Panel name
Specify Dynamic Terminal Integration Parameters

Panel ID
KN341PT1

Field
User data

Default value
None

Permissible values
A character string with a maximum length of 109 in the format userid/password

Batch parameter name
KN3_TN3270_USER_DATA

PARMGEN name
KN3_TN3270_DXL_USERDATA

PARMGEN classification
Define TN3270 Telnet session link user values

Description

TN3270 User Data Field

This parameter specifies the data to be passed to the IBM Tivoli NetView for z/OS program during logon. The Configuration Tool generates the KN3_DLX_USERDATA parameter in the KN3ENV member of the *rhilev.midlev.rtename*.RKANPARU library. If no user data is specified, the default value is a null string. This option may be used to specify the NetView OPERATOR ID and PASSWORD in NetView for z/OS if the LOGONPW option is enabled in NetView. The field is a character string with a maximum length of 109 in the format userid/password. This is an optional field. However, if you provide an operator ID in this field, the NetView operator ID you provide should not be configured to be a receiver of unsolicited messages. For more information about the format of this field, see the "Logging on to NetView from a 3270 session" topic in the *IBM Tivoli NetView for z/OS: User's Guide*.

Example: To see this parameter specified in the context of the KN3ENV member, see “Sample KN3ENV member” on page 69.

Related parameters

- “KN3_TN3270_DXL_APPLID” on page 200

KN3_X_AGT_CONFIRM_SHUTDOWN

Use the KN3_X_AGT_CONFIRM_SHUTDOWN parameter to specify the maximum number of seconds between two successive SHUTDOWN commands or MVS STOP (P) commands to terminate the IBM Z OMEGAMON Network Monitor address space.

Required or optional
Required

Location where parameter value is stored
In the KN3SYSIN member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
CONFIRM(&XN3FIRM) (Confirm shutdown option)

Default value
0

Permissible values
0 to 15

In the Configuration Tool
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See "Parameter names" on page 73.

PARMGEN name
KN3_X_AGT_CONFIRM_SHUTDOWN

PARMGEN classification
Additional agent settings

Description

Confirm shutdown option

This parameter sets the maximum number of seconds between two successive SHUTDOWN commands or MVS STOP (P) commands to terminate the IBM Z OMEGAMON Network Monitor address space.

CONFIRM(0) allows TMS:Engine shutdown to begin immediately without an additional, confirming SHUTDOWN command.

CONFIRM(n) prevents accidental shutdowns by requiring you to confirm the command by entering it a second time within the specified number of seconds.

For example, CONFIRM(15) requires you enter SHUTDOWN twice within 15 seconds to terminate the address space.

The default for IBM Z OMEGAMON Network Monitor CONFIRM is 0 which is also the Tivoli Enterprise Monitoring Server default.

Example: To see this parameter specified in the context of the KN3SYSIN member, see "Sample KN3SYSIN member" on page 70.

Related parameters

- "KN3_X_AGT_KDC_DEBUG" on page 204
- "KN3_X_AGT_DEBUG_TRACE" on page 203
- "KN3_X_AGT_LGSA_VERIFY" on page 205
- "KN3_X_AGT_LSRPOOL_BUFFER_NUM" on page 206
- "KN3_X_AGT_LSRPOOL_BUFSIZE" on page 207
- "KN3_X_AGT_SDUMP_SVC_SYS1_DUMP" on page 208
- "KN3_X_AGT_STORAGE_LIMIT_EXTEND" on page 210

- “KN3_X_AGT_STORAGE_LIMIT_PRIMARY” on page 211
- “KN3_X_AGT_STORAGE_RESERVE_EXT” on page 212
- “KN3_X_AGT_STORAGE_RESERVE_PRI” on page 213
- “KN3_X_AGT_STORAGE_STGDEBUG” on page 214
- “KN3_X_AGT_TASKS_ATTACHED_NUM” on page 215
- “KN3_X_SECURITY_RESOURCE_CLASS” on page 218
- “KN3_X_SECURITY_USER_EXIT” on page 219

KN3_X_AGT_DEBUG_TRACE

Use the KN3_X_AGT_DEBUG_TRACE parameter to specify whether TMS:Engine debugging services are to be activated.

Required or optional
Optional

Location where parameter value is stored
In the KN3SYSIN member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
DEBUG(&XN3DEBG) (TMS:Engine Debugging Services)

Default value
N

Permissible values
Y, N

In the Configuration Tool
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See “Parameter names” on page 73.

PARMGEN name
KN3_X_AGT_DEBUG_TRACE

PARMGEN classification
Additional agent settings

Description

TMS:Engine Debugging Services

Attention: Do not modify this parameter except under the guidance of IBM Software Support.

This parameter specifies whether TMS:Engine debugging services are to be activated.

N means that basic debugging information will not be recorded.

Y means that basic debugging information will be recorded.

DEBUG and STGDEBUG may affect each other. If DEBUG(Y) is specified and STGDEBUG is omitted, basic storage debugging is turned on, causing an increase in storage use.

STGDEBUG must also be specified after DEBUG in the initialization deck for proper functioning of these turned on, causing an increase in storage use. DEBUG will override STGDEBUG if it follows STGDEBUG.

The default for IBM Z OMEGAMON Network Monitor DEBUG is **N**.

Related parameters

- “KN3_X_AGT_CONFIRM_SHUTDOWN” on page 202

KN3_X_AGT_KDC_DEBUG

Use the KN3_X_AGT_KDC_DEBUG parameter to instruct the data communications layer to report communications problems using a minimal, summary format.

Required or optional
Optional

Location where parameter value is stored
In the KN3ENV member in the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
KDC_DEBUG=(&XN3DBUG) (TCP/IP communication trace debug)

Default value
N

Permissible values
Y, N, D, M, A

In the Configuration Tool
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See "Parameter names" on page 73.

PARMGEN name
KN3_X_AGT_KDC_DEBUG

PARMGEN classification
Additional agent settings

Description

TCP/IP communication trace debug

Attention: Do not modify this parameter except under the guidance of IBM Software Support.

TCP/IP communication trace debug

Set this parameter to **Y** if you want KDC_DEBUG=Y as the override setting in RKANPARU(KN3ENV) member. Otherwise, the default setting of KDC_DEBUG=N is used. This default parameter instructs the data communications layer to report communications problems using a minimal, summary format. This parameter is intended for stable applications in production.

Note that the default KDC_DEBUG=N generates standard RAS1 trace data in the Agent RKLVLOG, in addition to the summary information diagnosing possible timeout conditions.

The following settings report on data communications problems:

- KDC_DEBUG=**N**: minimal tracing (default)
- KDC_DEBUG=**Y**: full-packet tracing
- KDC_DEBUG=**D**: KDC_DEBUG=Y plus STATE & FLOW tracing
- KDC_DEBUG=**M**: KDC_DEBUG=D plus INPUT & OUTPUT HELPs tracing
- KDC_DEBUG=**A**: KDC_DEBUG=M plus all format tracing

Note: Do not set KDC_DEBUG=A unless directed to by IBM Software Support.

Related parameters

- "KN3_X_AGT_CONFIRM_SHUTDOWN" on page 202
- "KN3_X_AGT_DEBUG_TRACE" on page 203
- "KN3_X_AGT_LGSA_VERIFY" on page 205
- "KN3_X_AGT_LSRPOOL_BUFFER_NUM" on page 206
- "KN3_X_AGT_LSRPOOL_BUFSIZE" on page 207
- "KN3_X_AGT_SDUMP_SVC_SYS1_DUMP" on page 208
- "KN3_X_AGT_STORAGE_LIMIT_EXTEND" on page 210
- "KN3_X_AGT_STORAGE_LIMIT_PRIMARY" on page 211
- "KN3_X_AGT_STORAGE_RESERVE_EXT" on page 212
- "KN3_X_AGT_STORAGE_RESERVE_PRI" on page 213
- "KN3_X_AGT_STORAGE_STGDEBUG" on page 214
- "KN3_X_AGT_TASKS_ATTACHED_NUM" on page 215
- "KN3_X_SECURITY_RESOURCE_CLASS" on page 218
- "KN3_X_SECURITY_USER_EXIT" on page 219

KN3_X_AGT_LGSA_VERIFY

Use the KN3_X_AGT_LGSA_VERIFY parameter to specify whether TMS:Engine checks that the $GSA address is available.

Required or optional
Required

Location where parameter value is stored
In the KN3SYSIN member of the *rhilev.midlev.rtename*.RKANPAU library

Parameter name
LGSA(&XN3LGSA) (Verify $GSA address availability)

Default value
Y

Permissible values
Y, N

In the Configuration Tool
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See "Parameter names" on page 73.

PARMGEN name
KN3_X_AGT_LGSA_VERIFY

PARMGEN classification
Additional agent settings

Description

Verify $GSA address availability

Attention: Do not modify this parameter except under the guidance of IBM Software Support.

This parameter determines whether TMS:Engine checks that the $GSA address is available. Y, N are the only options.

Y means you want to check if available.

N means you do not want to check if available.

The default for IBM Z OMEGAMON Network Monitor LGSA is **Y**, which is also the Tivoli Enterprise Monitoring Server default value.

Example: To see this parameter specified in the context of the KN3SYSIN member, see "Sample KN3SYSIN member" on page 70.

Related parameters

- "KN3_X_AGT_CONFIRM_SHUTDOWN" on page 202
- "KN3_X_AGT_KDC_DEBUG" on page 204
- "KN3_X_AGT_DEBUG_TRACE" on page 203
- "KN3_X_AGT_LSRPOOL_BUFFER_NUM" on page 206
- "KN3_X_AGT_LSRPOOL_BUFSIZE" on page 207
- "KN3_X_AGT_SDUMP_SVC_SYS1_DUMP" on page 208
- "KN3_X_AGT_STORAGE_LIMIT_EXTEND" on page 210
- "KN3_X_AGT_STORAGE_LIMIT_PRIMARY" on page 211
- "KN3_X_AGT_STORAGE_RESERVE_EXT" on page 212
- "KN3_X_AGT_STORAGE_RESERVE_PRI" on page 213
- "KN3_X_AGT_STORAGE_STGDEBUG" on page 214
- "KN3_X_AGT_TASKS_ATTACHED_NUM" on page 215
- "KN3_X_SECURITY_RESOURCE_CLASS" on page 218
- "KN3_X_SECURITY_USER_EXIT" on page 219

KN3_X_AGT_LSRPOOL_BUFFER_NUM

Use the KN3_X_AGT_LSRPOOL_BUFFER_NUM parameter to specify the number of virtual storage buffers to be allocated for the specified buffer pool in the VSAM resource pool.

Required or optional
Required

Location where parameter value is stored
In the KN3SYSIN member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
LSRPOOL(&XN3BNUM,*number*) (Number of buffers)

Default value
32

Permissible values
3 - 65535 (to the maximum amount of available virtual storage in the monitoring agent address space)

In the Configuration Tool
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See "Parameter names" on page 73.

PARMGEN name
KN3_X_AGT_LSRPOOL_BUFFER_NUM

PARMGEN classification
Additional agent settings

Description

Number of buffers

This parameter specifies the number of virtual storage buffers to be allocated for buffer pool "n" in the VSAM resource pool. You must specify a size for each buffer pool individually. You cannot string the definitions because they must be specified individually.

Permissible values: 3-65535.

This parameter has size of buffers and number of buffer and is specified as LSRPOOL(32768,32).

The default for IBM Z OMEGAMON Network Monitor LSRPOOL buffer number is 32.

Example: To see this parameter specified in the context of the KN3SYSIN member, see "Sample KN3SYSIN member" on page 70.

Related parameters

- "KN3_X_AGT_CONFIRM_SHUTDOWN" on page 202
- "KN3_X_AGT_KDC_DEBUG" on page 204
- "KN3_X_AGT_DEBUG_TRACE" on page 203
- "KN3_X_AGT_LGSA_VERIFY" on page 205
- "KN3_X_AGT_LSRPOOL_BUFSIZE" on page 207
- "KN3_X_AGT_SDUMP_SVC_SYS1_DUMP" on page 208
- "KN3_X_AGT_STORAGE_LIMIT_EXTEND" on page 210
- "KN3_X_AGT_STORAGE_LIMIT_PRIMARY" on page 211
- "KN3_X_AGT_STORAGE_RESERVE_EXT" on page 212
- "KN3_X_AGT_STORAGE_RESERVE_PRI" on page 213
- "KN3_X_AGT_STORAGE_STGDEBUG" on page 214
- "KN3_X_AGT_TASKS_ATTACHED_NUM" on page 215
- "KN3_X_SECURITY_RESOURCE_CLASS" on page 218
- "KN3_X_SECURITY_USER_EXIT" on page 219

KN3_X_AGT_LSRPOOL_BUFSIZE

Use the KN3_X_AGT_LSRPOOL_BUFSIZE parameter to specify the size in bytes of each virtual storage buffer in the specified buffer pool in the VSAM resource pool.

Required or optional
Required

Location where parameter value is stored
In the KN3SYSIN member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
LSRPOOL(&&XN3BSIZ,*number*) (Size of virtual storage buffer in pool)

Default value
32768

Permissible values
512, 1024, 2048, 8192, 12288, 16384, 20480, 24576, 28672, or 32768

In the Configuration Tool
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See "Parameter names" on page 73.

PARMGEN name
KN3_X_AGT_LSRPOOL_BUFSIZE

PARMGEN classification
Additional agent settings

Description

Size of virtual storage buffer in pool

This parameter specifies the size in bytes of each virtual storage buffer in buffer pool "n" in the VSAM resource pool. You must specify a size for each buffer pool individually. You cannot string the definitions because they must be specified individually.

Permissible values are one of the following: 512, 1024, 2048, 8192, 12288, 16384, 20480, 24576, 28672, or 32768.

This parameter has size of buffers and number of buffer and specified as LSRPOOL(32768,32).

The default for IBM Z OMEGAMON Network Monitor LSRPOOL buffer size is 32768.

Example: To see this parameter specified in the context of the KN3SYSIN member, see "Sample KN3SYSIN member" on page 70.

Related parameters

- "KN3_X_AGT_CONFIRM_SHUTDOWN" on page 202
- "KN3_X_AGT_KDC_DEBUG" on page 204
- "KN3_X_AGT_DEBUG_TRACE" on page 203
- "KN3_X_AGT_LGSA_VERIFY" on page 205
- "KN3_X_AGT_LSRPOOL_BUFFER_NUM" on page 206
- "KN3_X_AGT_SDUMP_SVC_SYS1_DUMP" on page 208
- "KN3_X_AGT_STORAGE_LIMIT_EXTEND" on page 210
- "KN3_X_AGT_STORAGE_LIMIT_PRIMARY" on page 211
- "KN3_X_AGT_STORAGE_RESERVE_EXT" on page 212
- "KN3_X_AGT_STORAGE_RESERVE_PRI" on page 213
- "KN3_X_AGT_STORAGE_STGDEBUG" on page 214
- "KN3_X_AGT_TASKS_ATTACHED_NUM" on page 215
- "KN3_X_SECURITY_RESOURCE_CLASS" on page 218
- "KN3_X_SECURITY_USER_EXIT" on page 219

KN3_X_AGT_SDUMP_SVC_SYS1_DUMP

Use the KN3_X_AGT_SDUMP_SVC_SYS1_DUMP parameter to specify whether SVC dumps are generated.

Required or optional
Required

Location where parameter value is stored
In the KN3SYSIN member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
SDUMP(&XN3DSVC) (Generate SVC dump)

Default value
Y

Permissible values
Y, N, S ,M

In the Configuration Tool
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See "Parameter names" on page 73.

PARMGEN name
KN3_X_AGT_SDUMP_SVC_SYS1_DUMP

PARMGEN classification
Additional agent settings

Description

Generate SVC dump

This parameter determines whether SVC dumps are generated.

Y directs the SVC dump to a system dump data set (SYS1.DUMPxx). Before you specify Y as the value of this parameter, ensure that the TMS:Engine job step is APF-authorized and that the SYS1.DUMPxx data sets are large enough to hold the contents of the TMS:Engine address space.

N directs formatted dumps to the RKLVSNAP data set. Avoid formatted dumps if possible because they disable the TMS:Engine address space for a longer time than either SVC dumps or SYSMDUMPs, and are more difficult to analyze.

S directs summary dumps to the RKLVSNAP data set. A summary dump consistes of an ABEND summary and dispatcher summary and does not provide enough information for reliable problem analysis. Use this setting for specific testing purposes only.

M directs ABEND dumps to the data set with the SYSMDUMP DD name. This type of dump is not formatted by the operating system and must be analyzed with IPCS. Only the first dump taken is captured in the SYSMDUMP data set unless JCL specifies DISP=MOD. TMS:Engine automatically initializes the SYSMDUMP data set with an end-of-file mark.

The default for IBM Z OMEGAMON Network Monitor SDUMP is **Y**.

Example: To see this parameter specified in the context of the KN3SYSIN member, see "Sample KN3SYSIN member" on page 70.

Related parameters

- "KN3_X_AGT_CONFIRM_SHUTDOWN" on page 202
- "KN3_X_AGT_KDC_DEBUG" on page 204
- "KN3_X_AGT_DEBUG_TRACE" on page 203
- "KN3_X_AGT_LGSA_VERIFY" on page 205
- "KN3_X_AGT_LSRPOOL_BUFFER_NUM" on page 206
- "KN3_X_AGT_LSRPOOL_BUFSIZE" on page 207
- "KN3_X_AGT_STORAGE_LIMIT_EXTEND" on page 210
- "KN3_X_AGT_STORAGE_LIMIT_PRIMARY" on page 211

- “KN3_X_AGT_STORAGE_RESERVE_EXT” on page 212
- “KN3_X_AGT_STORAGE_RESERVE_PRI” on page 213
- “KN3_X_AGT_STORAGE_STGDEBUG” on page 214
- “KN3_X_AGT_TASKS_ATTACHED_NUM” on page 215
- “KN3_X_SECURITY_RESOURCE_CLASS” on page 218
- “KN3_X_SECURITY_USER_EXIT” on page 219

KN3_X_AGT_STORAGE_LIMIT_EXTEND

Use the KN3_X_AGT_STORAGE_LIMIT_EXTEND parameter to specify the maximum size for the TMS:Engine primary storage (above-the-line) request.

Required or optional
Required

Location where parameter value is stored
In the KN3SYSIN data set of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
`LIMIT(&XN3ELIM,X)`

Default value
24

Permissible values
A power of 2 between 16 and 25.

In the Configuration Tool (ICAT)
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See “Parameter names” on page 73.

PARMGEN name
KN3_X_AGT_STORAGE_LIMIT_EXTEND

PARMGEN classification
Additional agent settings

Description

Extended maximum storage request

This parameter specifies the maximum size for the TMS:Engine primary storage (above-the-line) request. The maximum extended storage request size is specified as a power of 2. The minimum extended storage size is 16, which specifies a limit of 64K. The maximum is 25, which specifies a limit of 32 MB.

The default for IBM Z OMEGAMON Network Monitor extended storage is 24, which specifies a limit of 4 MB.

Example: To see this parameter specified in the context of the KN3SYSIN member, see “Sample KN3SYSIN member” on page 70.

Related parameters

- “KN3_X_AGT_CONFIRM_SHUTDOWN” on page 202
- “KN3_X_AGT_KDC_DEBUG” on page 204
- “KN3_X_AGT_DEBUG_TRACE” on page 203
- “KN3_X_AGT_LGSA_VERIFY” on page 205
- “KN3_X_AGT_LSRPOOL_BUFFER_NUM” on page 206

- "KN3_X_AGT_LSRPOOL_BUFSIZE" on page 207
- "KN3_X_AGT_SDUMP_SVC_SYS1_DUMP" on page 208
- "KN3_X_AGT_STORAGE_LIMIT_EXTEND" on page 210
- "KN3_X_AGT_STORAGE_LIMIT_PRIMARY" on page 211
- "KN3_X_AGT_STORAGE_RESERVE_EXT" on page 212
- "KN3_X_AGT_STORAGE_RESERVE_PRI" on page 213
- "KN3_X_AGT_STORAGE_STGDEBUG" on page 214
- "KN3_X_AGT_TASKS_ATTACHED_NUM" on page 215
- "KN3_X_SECURITY_RESOURCE_CLASS" on page 218
- "KN3_X_SECURITY_USER_EXIT" on page 219

KN3_X_AGT_STORAGE_LIMIT_PRIMARY

Use the KN3_X_AGT_STORAGE_LIMIT_PRIMARY parameter to specify the maximum size for the TMS:Engine primary storage request.

Required or optional
Required

Location where parameter value is stored
In the KN3SYSIN member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
`LIMIT(&XN3PLIM,P)` (Primary maximum storage request)

Default value
20

Permissible values
A power of two between 16 and 25

In the Configuration Tool
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See "Parameter names" on page 73.

PARMGEN name
KN3_X_AGT_STORAGE_LIMIT_PRIMARY

PARMGEN classification
Additional agent settings

Description

Primary maximum storage request

This parameter specifies the maximum size for the TMS:Engine primary storage request. The maximum primary storage request size is specified as a power of 2. The minimum primary storage size is 16, which specifies a limit of 64K. The maximum is 25, which specifies a limit of 32 MB

The default for IBM Z OMEGAMON Network Monitor primary storage is **20**, which specifies a limit of 1 MB.

Example: To see this parameter specified in the context of the KN3SYSIN member, see "Sample KN3SYSIN member" on page 70.

Related parameters

- "KN3_X_AGT_CONFIRM_SHUTDOWN" on page 202
- "KN3_X_AGT_KDC_DEBUG" on page 204

- “KN3_X_AGT_DEBUG_TRACE” on page 203
- “KN3_X_AGT_LGSA_VERIFY” on page 205
- “KN3_X_AGT_LSRPOOL_BUFFER_NUM” on page 206
- “KN3_X_AGT_LSRPOOL_BUFSIZE” on page 207
- “KN3_X_AGT_SDUMP_SVC_SYS1_DUMP” on page 208
- “KN3_X_AGT_STORAGE_LIMIT_EXTEND” on page 210
- “KN3_X_AGT_STORAGE_RESERVE_EXT” on page 212
- “KN3_X_AGT_STORAGE_RESERVE_PRI” on page 213
- “KN3_X_AGT_STORAGE_STGDEBUG” on page 214
- “KN3_X_AGT_TASKS_ATTACHED_NUM” on page 215
- “KN3_X_SECURITY_RESOURCE_CLASS” on page 218
- “KN3_X_SECURITY_USER_EXIT” on page 219

KN3_X_AGT_STORAGE_RESERVE_EXT

Use the KN3_X_AGT_STORAGE_RESERVE_EXT parameter to specify the number of kilobytes of extended (above-the-line) storage to set aside for other routines that might perform their own GETMAINs in this address space.

Required or optional
Required

Location where parameter value is stored KN3SYSIN
In the KN3SYSIN member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
RESERVE(&XAGERES,X) (Extended 31-bit region reserve)

Default value
2048

Permissible values
0 to 9999

In the Configuration Tool
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See “Parameter names” on page 73.

PARMGEN name
KN3_X_AGT_STORAGE_RESERVE_EXT

PARMGEN classification
Additional agent settings

Description

Extended 31-bit region reserve

This parameter specifies the number of kilobytes of extended (above-the-line) storage to set aside for other routines that might perform their own GETMAINs in this address space. If your RESERVE value is too small, you might encounter IST566I messages from VTAM or S80A, S878, S066, S40D, or S0F9 abends.

The default for IBM Z OMEGAMON Network Monitor primary storage reserve is **2048** KB.

Example: To see this parameter specified in the context of the KN3SYSIN member, see “Sample KN3SYSIN member” on page 70.

Related parameters

- “KN3_X_AGT_CONFIRM_SHUTDOWN” on page 202
- “KN3_X_AGT_KDC_DEBUG” on page 204
- “KN3_X_AGT_DEBUG_TRACE” on page 203
- “KN3_X_AGT_LGSA_VERIFY” on page 205
- “KN3_X_AGT_LSRPOOL_BUFFER_NUM” on page 206
- “KN3_X_AGT_LSRPOOL_BUFSIZE” on page 207
- “KN3_X_AGT_SDUMP_SVC_SYS1_DUMP” on page 208
- “KN3_X_AGT_STORAGE_LIMIT_PRIMARY” on page 211
- “KN3_X_AGT_STORAGE_RESERVE_PRI” on page 213
- “KN3_X_AGT_STORAGE_STGDEBUG” on page 214
- “KN3_X_AGT_TASKS_ATTACHED_NUM” on page 215
- “KN3_X_SECURITY_RESOURCE_CLASS” on page 218
- “KN3_X_SECURITY_USER_EXIT” on page 219

KN3_X_AGT_STORAGE_RESERVE_PRI

Use the KN3_X_AGT_STORAGE_RESERVE_PRI parameter to specify the number of KB of primary (below-the-line) storage to set aside for other routines (for example, ACF2 and RACF) that might perform their own GETMAINs in this address space.

Required or optional
Required

Location where parameter value is stored
In the KN3SYSIN member of the *rhilev*.*midlev*.*rtename*.RKANPARU library

Parameter name
RESERVE(&XN3PRES,P) (Primary 24-bit region reserve)

Default value
2048

Permissible values
0 to 9999

In the Configuration Tool
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See “Parameter names” on page 73.

PARMGEN name
KN3_X_AGT_STORAGE_RESERVE_PRI

PARMGEN classification
Additional agent settings

Description

Primary 24-bit region reserve

This parameter specifies the number of KB of primary (below-the-line) storage to set aside for other routines (for example, ACF2 and RACF) that might perform their own GETMAINs in this address space. ACF2 and RACF use approximately 1 KB of primary storage per logged-on user. If your RESERVE value is too small, you might encounter IST566I messages from VTAM or S80A, S878, S066, S40D, or S0F9 abends.

The default for IBM Z OMEGAMON Network Monitor primary storage reserve is **2048** KB.

Example: To see this parameter specified in the context of the KN3SYSIN member, see "Sample KN3SYSIN member" on page 70.

Related parameters

- "KN3_X_AGT_CONFIRM_SHUTDOWN" on page 202
- "KN3_X_AGT_KDC_DEBUG" on page 204
- "KN3_X_AGT_DEBUG_TRACE" on page 203
- "KN3_X_AGT_LGSA_VERIFY" on page 205
- "KN3_X_AGT_LSRPOOL_BUFFER_NUM" on page 206
- "KN3_X_AGT_LSRPOOL_BUFSIZE" on page 207
- "KN3_X_AGT_SDUMP_SVC_SYS1_DUMP" on page 208
- "KN3_X_AGT_STORAGE_LIMIT_PRIMARY" on page 211
- "KN3_X_AGT_STORAGE_RESERVE_EXT" on page 212
- "KN3_X_AGT_STORAGE_STGDEBUG" on page 214
- "KN3_X_AGT_TASKS_ATTACHED_NUM" on page 215
- "KN3_X_SECURITY_RESOURCE_CLASS" on page 218
- "KN3_X_SECURITY_USER_EXIT" on page 219

KN3_X_AGT_STORAGE_STGDEBUG

Use the KN3_X_AGT_STORAGE_STGDEBUG parameter to specify whether TMS:Engine storage debugging services are to be activated.

Required or optional
Optional

Location where parameter value is stored
The KN3SYSIN member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
STGDEBUG(&XN3STDB) (Storage Debugging Services)

Default value
N

Permissible values
Y, N, X

In the Configuration Tool
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See "Parameter names" on page 73.

PARMGEN name
KN3_X_AGT_STORAGE_STGDEBUG

PARMGEN classification
Additional agent settings

Description

Storage Debugging Services

This parameter specifies whether TMS:Engine storage debugging services are to be activated.

N means that storage debugging information will not be recorded.

Y means that basic storage debugging information will be recorded.

X means that extended storage debugging information will be recorded.

DEBUG and STGDEBUG can affect each other. If DEBUG(Y) is specified and STGDEBUG is omitted, basic storage debugging is turned on, causing an increase in storage use.

STGDEBUG must also be specified after DEBUG in the initialization deck for proper functioning of these turned on, causing an increase in storage use. DEBUG will override STGDEBUG if it follows STGDEBUG.

The default for IBM Z OMEGAMON Network Monitor STGDEBUG is **N**. This parameter is usually omitted from the KN3SYSIN member.

Related parameters

- “KN3_X_AGT_CONFIRM_SHUTDOWN” on page 202
- “KN3_X_AGT_KDC_DEBUG” on page 204
- “KN3_X_AGT_DEBUG_TRACE” on page 203
- “KN3_X_AGT_LGSA_VERIFY” on page 205
- “KN3_X_AGT_LSRPOOL_BUFFER_NUM” on page 206
- “KN3_X_AGT_LSRPOOL_BUFSIZE” on page 207
- “KN3_X_AGT_SDUMP_SVC_SYS1_DUMP” on page 208
- “KN3_X_AGT_STORAGE_LIMIT_EXTEND” on page 210
- “KN3_X_AGT_STORAGE_LIMIT_PRIMARY” on page 211
- “KN3_X_AGT_STORAGE_RESERVE_EXT” on page 212
- “KN3_X_AGT_STORAGE_RESERVE_PRI” on page 213
- “KN3_X_AGT_TASKS_ATTACHED_NUM” on page 215
- “KN3_X_SECURITY_RESOURCE_CLASS” on page 218
- “KN3_X_SECURITY_USER_EXIT” on page 219

KN3_X_AGT_TASKS_ATTACHED_NUM

Use the KN3_X_AGT_TASKS_ATTACHED_NUM parameter to specify the number of general-purpose subtasks to be attached in the TMS:Engine address space.

Required or optional
Required

Location where parameter value is stored
In the KN3SYSIN member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
TASKS(&XN3TASK) (Default number of available processors)

Default value
1

Permissible values
Do not modify this parameter except under the guidance of IBM Software Support.

In the Configuration Tool
This value cannot be updated using the Configuration Tool. It is set internally and could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See “Parameter names” on page 73.

PARMGEN name
KN3_X_AGT_TASKS_ATTACHED_NUM

PARMGEN classification
Additional agent settings

Description

Default number of available processors

Attention: Do not modify this parameter except under the guidance of IBM Software Support.

This parameter specifies the number of general-purpose subtasks to be attached in the TMS:Engine address space. If TMS:Engine is running on a multiprocessor, the TASKS default increases both throughput and CPU usage. Reducing the number of tasks decreases both throughput and CPU usage.

The default for IBM Z OMEGAMON Network Monitor TASKS is **1**.

Example: To see this parameter specified in the context of the KN3SYSIN member, see "Sample KN3SYSIN member" on page 70.

Related parameters

- "KN3_X_AGT_CONFIRM_SHUTDOWN" on page 202
- "KN3_X_AGT_KDC_DEBUG" on page 204
- "KN3_X_AGT_DEBUG_TRACE" on page 203
- "KN3_X_AGT_LGSA_VERIFY" on page 205
- "KN3_X_AGT_LSRPOOL_BUFFER_NUM" on page 206
- "KN3_X_AGT_LSRPOOL_BUFSIZE" on page 207
- "KN3_X_AGT_SDUMP_SVC_SYS1_DUMP" on page 208
- "KN3_X_AGT_STORAGE_LIMIT_EXTEND" on page 210
- "KN3_X_AGT_STORAGE_LIMIT_PRIMARY" on page 211
- "KN3_X_AGT_STORAGE_RESERVE_EXT" on page 212
- "KN3_X_AGT_STORAGE_RESERVE_PRI" on page 213
- "KN3_X_AGT_STORAGE_STGDEBUG" on page 214
- "KN3_X_SECURITY_RESOURCE_CLASS" on page 218
- "KN3_X_SECURITY_USER_EXIT" on page 219

KN3_X_PD_HISTCOLL_DATA_TEMS_STC

Use the KN3_X_PD_HISTCOLL_DATA_TEMS_STC parameter to specify whether historical collection is being performed by the monitoring agent address space.

Required or optional
Optional

Location where parameter value is stored
The parameter value is not stored, but is used for internal processing.

Parameter name
NA

Default value
N

Permissible values
Y, N

In the Configuration Tool
This value cannot be updated using the Configuration Tool.

Batch parameter name
NA

PARMGEN name
KN3_X_PD_HISTCOLL_DATA_TEMS_STC

PARMGEN classification
Persistent datastore

Description

This parameter indicates whether historical collection is being performed by the monitoring agent address space. **Y** means that this agent address space is collecting historical data. N means that the agent address space is not collecting historical data. The default in **N**.

This parameter determines whether historical data collection takes place on the Tivoli Enterprise Monitoring Server or on the monitoring agents where the monitoring agent is running in the monitoring server address space (which is the recommended configuration for this monitoring agent). The KPDPG, KPDPCTL, KPDPCTL2, and KPDDEFIN members of the *rhilev*.*midlev*.*rtename*.RKANPARU library are updated with KN3*-specific parameters when this flag is set.

Related parameters

- “KN3_AGT_CONFIGURATION_MODE” on page 89
- “KN3_PD_CYL” on page 124
- “KN3_PD_GRP” on page 125
- “KN3_PD_ROW” on page 127
- “KN3_X_PD_HISTCOLL_DATA_AGT_STC” on page 217

KN3_X_PD_HISTCOLL_DATA_AGT_STC

Use the KN3_X_PD_HISTCOLL_DATA_AGT_STC parameter to specify historical collection is being performed by the Tivoli Enterprise Monitoring Server address space.

Required or optional
Optional

Location where parameter value is stored
This parameter is used for internal processing to enable a flag to be set if persistent datastore configuration is being set for the product. When this flag is set, the KN3PG, KN3AL, KN3PCTL, KN3PCTL2 and KN3DEFIN members are created in *rhilev*.*midlev*.*rtename*.RKANPARU library.

Parameter name
NA

Default value
Y

Permissible values
Y, N

In the Configuration Tool
This value cannot be updated using the Configuration Tool.

Batch parameter name
NA

PARMGEN name
KN3_X_PD_HISTCOLL_DATA_AGT_STC

PARMGEN classification
Persistent datastore

Description

This parameter indicates whether historical collection is being performed by the Tivoli Enterprise Monitoring Server address space. **Y** means that the monitoring server address space is collecting historical data. **N** means that the monitoring server address space is not collecting historical data/ The default in **N**

This parameter defines the started task name for historical data collection when this collection takes place on the Tivoli Enterprise Monitoring Server and the monitoring agent is running in the monitoring server address space (which is the recommended configuration for this monitoring agent). **Y** means that the monitoring server is collecting historical data. The KPDPG, KP3AL,KN3PCTL, KPDPCTL2, and KPDDEFIN members of the *rhilev.midlev.rtename*.RKANPARU library are created when this flag is set.

Related parameters

- "KN3_AGT_CONFIGURATION_MODE" on page 89
- "KN3_PD_CYL" on page 124
- "KN3_PD_GRP" on page 125
- "KN3_PD_ROW" on page 127
- "KN3_X_PD_HISTCOLL_DATA_TEMS_STC" on page 216

KN3_X_SECURITY_RESOURCE_CLASS

Use the KN3_X_SECURITY_RESOURCE_CLASS parameter to specify a value in the KN3INNAM member in *rhilev.midlev.rtename*.RKANPARU that contains protected class lists information.

Required or optional
Optional

Location where parameter value is stored
In the KN3INNAM member of the *rhilev.midlev.rtename*.RKANPARU library

Parameter name
`EXIT="&XN3SCLA"` (External security classes)

Default value
blank (no value specified)

Permissible values
A character string up to 8 characters in length

In the Configuration Tool
The monitoring agent cannot set this value using the Configuration Tool. This value is defined using the common parameter RTE_SECURITY_USER_LOGON and set on panel KCIPRT1. The monitoring agent sets this value internally . This value could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
NA

See "Parameter names" on page 73.

PARMGEN name
KN3_X_SECURITY_RESOURCE_CLASS

PARMGEN classification
Additional agent settings

Description

External security classes

This parameter specifies a value in the KN3INNAM member in *rhilev.midlev.rtename*.RKANPARU that contains protected class lists information. This parameter is used by external security packages to construct the correct resource validation request. This value is the same as the value set using the RTE_SECURITY_USER_LOGON parameters. This value is passed to the IBM Z OMEGAMON Network Monitor monitoring agent by the Configuration Tool.

The default for IBM Z OMEGAMON Network Monitor CLASSES is "".

Example: `CLASSES="  "`

Related parameters

- RTE_SECURITY_USER_LOGON in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Parameter Reference*
- “KN3_X_AGT_CONFIRM_SHUTDOWN” on page 202
- “KN3_X_AGT_KDC_DEBUG” on page 204
- “KN3_X_AGT_DEBUG_TRACE” on page 203
- “KN3_X_AGT_LGSA_VERIFY” on page 205
- “KN3_X_AGT_LSRPOOL_BUFFER_NUM” on page 206
- “KN3_X_AGT_LSRPOOL_BUFSIZE” on page 207
- “KN3_X_AGT_SDUMP_SVC_SYS1_DUMP” on page 208
- “KN3_X_AGT_STORAGE_LIMIT_EXTEND” on page 210
- “KN3_X_AGT_STORAGE_LIMIT_PRIMARY” on page 211
- “KN3_X_AGT_STORAGE_RESERVE_EXT” on page 212
- “KN3_X_AGT_STORAGE_RESERVE_PRI” on page 213
- “KN3_X_AGT_STORAGE_STGDEBUG” on page 214
- “KN3_X_AGT_TASKS_ATTACHED_NUM” on page 215
- “KN3_X_SECURITY_USER_EXIT” on page 219

KN3_X_SECURITY_USER_EXIT

Use the KN3_X_SECURITY_USER_EXIT parameter to specify a load module name of an exit routine that will be invoked to provide validation.

Required or optional
Optional

Location where parameter value is stored
This value is set internally for the monitoring agent. The value comes from a common parmeter set on Configuration Tool panel KCIPRT1. It is passed to the monitoring agent in sample job KLV@VSM in *rhilev.midlev.rtename*.RKANSAMU. This sample job must be run to create the external security exit.

Parameter name
EXIT="&XN3SUEX" (External security exit)

Default value
blank (no value specified)

Permissible values
A character string up to 8 characters in length

In the Configuration Tool
The monitoring agent cannot set this value using the Configuration Tool. This value could be updated using nonstandard parameters. However, this workaround is not recommended.

Batch parameter name
KN3_X_SECURITY_USER_EXIT

PARMGEN name
KN3_X_SECURITY_USER_EXIT

PARMGEN classification
Additional agent settings

Description

External security exit

This parameter specifies a load module name of an exit routine that will be invoked to provide validation.

The default for IBM Z OMEGAMON Network Monitor EXIT is "".

Example: EXIT=" "

Related parameters

- “KN3_X_AGT_CONFIRM_SHUTDOWN” on page 202
- “KN3_X_AGT_KDC_DEBUG” on page 204
- “KN3_X_AGT_DEBUG_TRACE” on page 203
- “KN3_X_AGT_LGSA_VERIFY” on page 205
- “KN3_X_AGT_LSRPOOL_BUFFER_NUM” on page 206
- “KN3_X_AGT_LSRPOOL_BUFSIZE” on page 207
- “KN3_X_AGT_SDUMP_SVC_SYS1_DUMP” on page 208
- “KN3_X_AGT_STORAGE_LIMIT_EXTEND” on page 210
- “KN3_X_AGT_STORAGE_LIMIT_PRIMARY” on page 211
- “KN3_X_AGT_STORAGE_RESERVE_EXT” on page 212
- “KN3_X_AGT_STORAGE_RESERVE_PRI” on page 213
- “KN3_X_AGT_STORAGE_STGDEBUG” on page 214
- “KN3_X_AGT_TASKS_ATTACHED_NUM” on page 215
- “KN3_X_SECURITY_RESOURCE_CLASS” on page 218

KN3FCCMD command reference

KN3FCCMD commands enable or disable data collection by component, providing more granular control over which types of data are collected.

This section is a reference for the KN3FCCMD z/OS MODIFY commands that are supported by the IBM Z OMEGAMON Network Monitor monitoring agent. This chapter provides an explanation of the KN3FCCMD commands.

Introduction to the KN3FCCMD commands

The z/OS MODIFY KN3FCCMD commands enable or disable data collection by component, providing more granular control over which types of data are collected. These components are supported. The commands use this syntax.

The IBM Z OMEGAMON Network Monitor monitoring agent is made up of components that map to data types. By default, each of the components is enabled. The default collection interval is 5 minutes.

You can enable or disable data collection by component, providing more granular control over which types of data are collected. These actions can be specified at the time you configure the IBM Z OMEGAMON Network Monitor monitoring agent (the preferred method) or through the z/OS MODIFY command. The z/OS MODIFY command is issued when the IBM Z OMEGAMON Network Monitor monitoring agent is running. Then you can use the z/OS MODIFY command to initialize, start, stop, and display the status of components.

This section shows you how to use the z/OS MODIFY command with the following components:

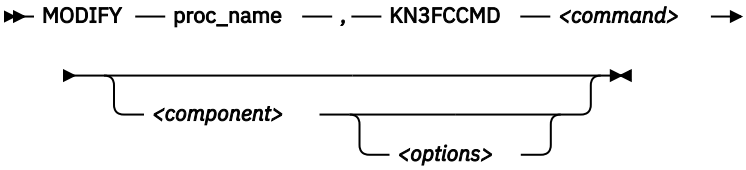
- **CONN** for TCP/IP Connection and Application performance data. You can enable or disable collection of TCP/IP Connection and Application performance statistics by starting or stopping the CONN component. The default is to start this component.
- **CSM** for Communications Storage Manager data. You can enable or disable the Communications Storage Manager buffer reporting by starting or stopping the CSM component. The default is to start this component.
- **EEHPR** for Enterprise Extender and High Performance Routing data. You can enable or disable collection of Enterprise Extender and High Performance Routing statistics by starting or stopping the EEHPR component. The default is to start this component.

- **FTP** for FTP session and transfer data. You can enable or disable collection of FTP session and transfer data by starting or stopping the FTP component. Additionally, you can modify the display interval for FTP data. The default is to start this component.
- **GLBS** for TCP/IP Stack Layer statistics data collection. You can enable or disable collection of TCP/IP Stack layer statistics by starting or stopping the GLBS component. The default is to start this component.
- **INTS** for Interface Statistics data collection. You can enable or disable collection of interface statistics by starting or stopping the INTS component. The default is to start this component.
- **INTE** for interface Data Link Control (DLC) data collection. You can enable or disable collection of interface DLC statistics by starting or stopping the INTE component. The default is to start this component.
- **IPSec** for IPSec security extensions to the Internet Protocol. You can start or stop collection of IPSec data. The default is **not** to start this component.
- **OSA** for OSA devices. You can stop and start OSA-enabled data collection. The default is to start this component.
- **ROUTE** for gateways. You can enable or disable the collection of routing information (for example, the gateway table). The default is to start this component. Additionally, the Routing Table Collection Frequency allows you to collect data less frequently for this table.
- **TN3270** for TN3270 server session data. You can enable or disable collection of TN3270 server session data by starting or stopping the TN3270 component. Additionally, you can modify the display interval for TN3270 server session data. The default is to start this component.

On a more global level, you can start or stop collection of TCP/IP data by starting and stopping the **TCPC** task. Starting TCPC will initiate data collection for ALL enabled components. Stopping the TCPC task will disable ALL data.

For a more complete view of these data types and the workspaces associated with them, see *IBM Z OMEGAMON Network Monitor: User's Guide*.

The general syntax for KN3FCCMD commands issued as a z/OS MODIFY command is:



Where:

proc_name
Is the name of the started procedure for your monitoring agent.

component
Is the component in the monitoring agent to take action on.

command
Is the action to be taken. STATUS, HELP, INSTALL, START and STOP are supported commands.

options
Are one or more arguments that provide further information about the action to be taken against the component.

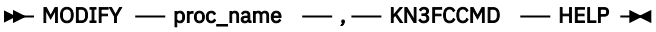
Command responses are written to the RKLVLOG but are buffered in memory and might not be written immediately. To immediately view the command responses, enter the following command, where IBMN3 is the name of the IBM Z OMEGAMON Network Monitor started procedure. This command causes the buffered output to be written to RKLVLOG:

```
F IBMN3,FLUSH
```

KN3FCCMD HELP

The KN3FCCMD HELP command displays the actions and options provided on the KN3FCCMD commands.

Format



Purpose

Displays the actions and options provided on the KN3FCCMD commands.

Usage

Sample output of this command follows.

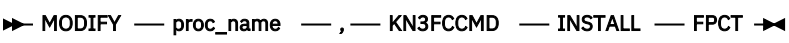
```
KLVOP191    'KN3FCCMD HELP'
KN3FC005 --------+-----------------------------------------------------------+
KN3FC005 COMMAND | DESCRIPTION                                               |
KN3FC005 --------+-----------------------------------------------------------+
KN3FC005 STATUS  | DISPLAY STATUS INFORMATION ABOUT INSTALLED COMPONENTS      |
KN3FC005 HELP    | HELP INFORMATION FOR KN3FCCMD                             |
KN3FC005 INSTALL | INSTALL COMPONENT(S) FOR PRODUCT ENVIRONMENT              |
KN3FC005 START   | START INSTALLED COMPONENTS                                |
KN3FC005 STOP    | STOP INSTALLED COMPONENTS                                 |
KN3FC005 SEND    | SEND COMMAND MESSAGES                                     |
KN3FC005 --------+-----------------------------------+-----------------------+
KN3FC005 OPTION  | DESCRIPTION                       | COMMANDS              |
KN3FC005 --------+-----------------------------------+-----------------------+
KN3FC005 CONN    | NMI TCP CONN/APPL DATA COLLECTION | START,STOP            |
KN3FC005 OSA     | OSA SNMP DATA COLLECTION          | START,STOP            |
KN3FC005 INTS    | INTS SNMP DATA COLLECTION         | START,STOP            |
KN3FC005 INTE    | INTE SNMP DATA COLLECTION         | START,STOP            |
KN3FC005 GLBS    | GLBS SNMP DATA COLLECTION         | START,STOP            |
KN3FC005 CSM     | NMI CSM DATA COLLECTION           | START,STOP            |
KN3FC005 DBUG    | EXTENDED DIAGNOSTICS MODE         | START,STOP,STATUS     |
KN3FC005 EEHPR   | NMI EE/HPR DATA COLLECTION        | START,STOP            |
KN3FC005 FPON    | OMEGAMON PRODUCT FEATURES         | INSTALL,STATUS        |
KN3FC005 FPCT    | CMS DATA SERVER FEATURES          | INSTALL,STATUS        |
KN3FC005 FTP     | NMI FTP DATA COLLECTION           | START,STOP            |
KN3FC005 IPSEC   | NMI IPSEC DATA COLLECTION         | START,STOP            |
KN3FC005 ROUTE   | SNMP ROUTE DATA COLLECTION        | START,STOP            |
KN3FC005 SEVT    | VTAM ENVIRONMENT FEATURES         | INSTALL,STATUS        |
KN3FC005 SEMV    | MVS ENVIRONMENT FEATURES          | INSTALL,STATUS        |
KN3FC005 SNAC    | SNA STATISTICS COLLECTOR          | START,STATUS          |
KN3FC005 TCPC    | TCP/IP STATISTICS COLLECTOR       | INSTALL,START,        |
KN3FC005         |                                   | STOP,STATUS           |
KN3FC005 TN3270  | NMI TN3270 DATA COLLECTION        | START,STOP            |
KN3FC005 TRACE   | DIAGNOSTICS TRACE FACILITY        | START,STOP,STATUS     |
KN3FC005 TRAP    | DIAGNOSTICS TRAP FACILITY         | START,STOP,STATUS     |
KN3FC005 ZERT    | NMI ZERT DATA COLLECTION          | START,STOP            |
KN3FC005 --------+-----------------------------------+-----------------------+
KN3FC005 PARM    | DESCRIPTION                       | OPTION                |
KN3FC005 --------+-----------------------------------+-----------------------+
KN3FC005 ALLHPR  | Y=ALL HPR CONNECTIONS             | EEHPR                 |
KN3FC005         | N=HPR FLOWING OVER EE CONNECTIONS |                       |
KN3FC005 APP     | DIAGNOSTICS FOR APPLICATIONS      | DBUG                  |
KN3FC005 BASE    | DIAGNOSTICS FOR BASE COLLECTOR    | DBUG                  |
KN3FC005 COMM    | DIAGNOSTICS FOR COMMON FUNCTIONS  | DBUG                  |
KN3FC005 CSM     | DIAGNOSTICS FOR CSM               | DBUG                  |
KN3FC005 DSPINTV | NMI DATA DISPLAY INTERVAL SUBCMD  | FTP, TN3270           |
KN3FC005 EEHPR   | DIAGNOSTICS FOR EE AND HPR        | DBUG                  |
KN3FC005 FREQ    | ROUTE COLLECTION FREQUENCY SUBCMD | ROUTE                 |
KN3FC005 FTP     | DIAGNOSTICS FOR FTP               | DBUG                  |
KN3FC005 HASH    | DIAGNOSTICS FOR HASH FUNCTIONS    | DBUG                  |
KN3FC005 INIT    | DIAGNOSTICS FOR INITIALIZATION    | DBUG                  |
KN3FC005 IPSEC   | DIAGNOSTICS FOR IPSEC             | DBUG                  |
KN3FC005 SNA     | DIAGNOSTICS FOR SNA MANAGEMENT    | DBUG                  |
KN3FC005 MAX     | MAXIMUM DIAGNOSTICS LEVEL         | DBUG                  |
KN3FC005 MID     | MEDIUM  DIAGNOSTICS LEVEL         | DBUG                  |
KN3FC005 MIN     | MINIMUM DIAGNOSTICS LEVEL         | DBUG                  |
KN3FC005 SNAC    | DIAGNOSTICS FOR SNAC              | DBUG                  |
KN3FC005 SNMP    | DIAGNOSTICS FOR SNMP              | DBUG                  |
KN3FC005 SYSTCP  | DIAGNOSTICS FOR REAL-TIME TCP/IP  | DBUG                  |
KN3FC005         | NETWORK MONITORING NMI            | DBUG                  |
KN3FC005 SNACINTV| SNA COLLECTOR INTERVAL            | SNAC                  |
KN3FC005 TCON    | DIAGNOSTICS FOR TCP CONNECTIONS   | DBUG                  |
```

```
KN3FC005 TCPC    | DIAGNOSTICS FOR TCPC               | DBUG                   |
KN3FC005 TCPCINTV| TCP/IP COLLECTOR INTERVAL          | TCPC                   |
KN3FC005 TCPCTCPC| TCP/IP COLLECTOR NAME/PROFILE/COM  | TCPC                   |
KN3FC005 TCPCVIOU| TCP/IP COLLECTOR DYNALLOC VIOUNIT  | TCPC                   |
KN3FC005 TCPNAME | TCP/IP STACK SUBCMD                | TCPC                   |
KN3FC005 TLIS    | DIAGNOSTICS FOR TCP LISTENERS      | DBUG                   |
KN3FC005 TSTO    | DIAGNOSTICS FOR TCP STORAGE        | DBUG                   |
KN3FC005 TN32    | DIAGNOSTICS FOR TN3270             | DBUG                   |
KN3FC005 UDP     | DIAGNOSTICS FOR UDP CONNECTIONS    | DBUG                   |
KN3FC005 GGS     | DIAGNOSTICS FOR PROTOCOL STATS     | DBUG                   |
KN3FC005 GIF     | DIAGNOSTICS FOR TCP INTERFACES     | DBUG                   |
KN3FC005 --------+------------------------------------+------------------------+
```

KN3FCCMD INSTALL FPCT

The KN3FCCMD INSTALL FPCT command initializes the Tivoli Enterprise Portal data server features in the monitoring agent address space

Format



Purpose

Initializes the Tivoli Enterprise Portal data server features in the monitoring agent address space. This component is installed during monitoring agent initialization.

Usage

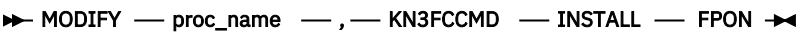
Sample output of this command follows.

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD INSTALL FPCT'
KN3FC015 FPCT COMPONENT FUNCTIONS INSTALLATION COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD INSTALL FPON

The KN3FCCMD INSTALL FPON command initializes the OMEGAMON product features in the monitoring agent address space.

Format



Purpose

Initializes the OMEGAMON product features in the monitoring agent address space. This component is installed during monitoring agent initialization.

Usage

Sample output of this command follows:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD INSTALL FPON'
KN3FC010 FPON COMPONENT FUNCTIONS INSTALLATION COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD INSTALL SEMV

The KN3FCCMD INSTALL SEMV command initializes the MVS environment features in the monitoring agent address space.

Format

Purpose

Initializes the MVS environment features in the monitoring agent address space. This component is installed during monitoring agent initialization.

Usage

Sample output of this command follows:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD INSTALL SEMV'
KN3FC025 SEMV MVS ENVIRONMENT INSTALLATION COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD INSTALL SEVT

The KN3FCCMD INSTALL SEVT command initializes the VTAM environment features in the monitoring agent address space.

Format

Purpose

Initializes the VTAM environment features in the monitoring agent address space. This component is installed during monitoring agent initialization.

Usage

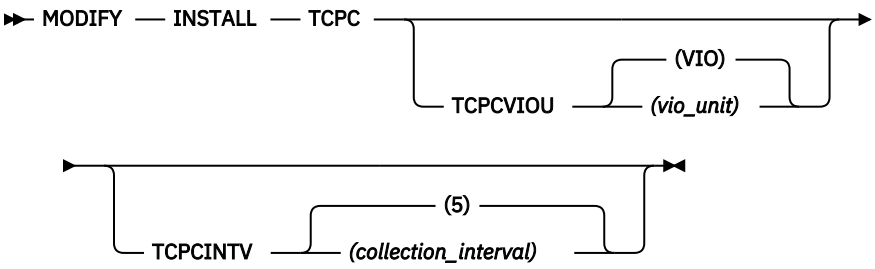
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD INSTALL SEMV'
KN3FC020 SEVT VTAM ENVIRONMENT INSTALLATION COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD INSTALL TCPC

The KN3FCCMD INSTALL TCPC command initializes the TCP/IP and VTAM statistics collector.

Format



Where:

TCPCVIOU
Is the VIO unit name

vio_unit
Is used for the allocation of temporary data sets. The default is VIO.

TCPCINTV
Is the TCP/IP sample interval.

collection_interval
Is the TCP/IP data sampling interval. The value is specified in minutes with a valid range of 1 to 60 and the default value is 5 minutes. This controls the frequency of data sampling for data collected using SNMP as well as data collected from the NMI for the CONN, CSM, EEHPR, and IPSEC components.

Purpose

Initializes the TCP/IP and VTAM statistics collector. This component is installed during monitoring agent initialization.

After you stop collection of TCP/IP and VTAM statistics, you must issue the following command to have collection started again:

```
MODIFY proc_name,KN3FCCMD START TCPC
```

If you want to change the value for either TCPCVIOU or TCPCINTV when you start TCPC collection, you must issue these commands:

```
MODIFY proc_name,KN3FCCMD INSTALL TCPC TCPCVIOU(vio_unit) TCPCINTV(collection_interval)
MODIFY proc_name,KN3FCCMD START TCPC
```

Usage

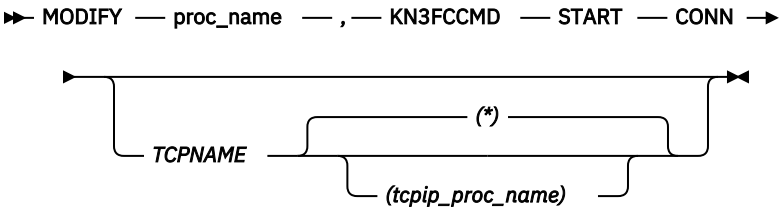
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START TCPC'
KN3CT000 TCP/IP STATISTICS COLLECTOR INITIALIZATION COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START CONN

The KN3FCCMD START CONN command starts the monitoring of connections and applications.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this command applies to.

*****
Indicates that this applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Starts the monitoring of connections and applications.

The following attribute groups and workspaces are affected by this command:

Table 12. Attribute groups and workspaces affected by the KN3FCCMD START CONN command

Workspace name	Attribute group name	Attribute group name prefix
Active TN3270 Server Connections for Selected Port	TN3270 Server Sess Avail	KN3TNA
Application Connections	TCPIP Connections	KN3TCN
Application Details	TCPIP Applications	KN3TAP
Application TCP Connections	TCPIP Details	KN3TCP
Application TCP Listeners	TCP Listener	KN3TCL
Application UDP Endpoints	UDP Connections	KN3UDP
Applications	TCPIP Applications	KN3TAP
Connections	TCPIP Connections	KN3TCN
EE Connection Summary	• EE Connections Details • HPR Connections • UDP Connections	• KN3EED • KN3HPR • KN3UDP
Enterprise Applications Health	TCPIP Applications	KN3TAP
Enterprise Connections Find	TCPIP Details	KN3TCP
Enterprise Connections Health	TCPIP Details	KN3TCP
Enterprise TN3270 Find	TN3270 Server Sess Avail	KN3TNA
Enterprise TN3270 Server Overview	TCP Listener	KN3TCL
FTP Sessions Details	• FTP Session • TCPIP Details	• KN3FSE • KN3TCP
FTP Transfer Details	• TCPIP FTP • TCPIP Details	• KN3FTP • KN3TCP
TCP Connections	TCPIP Details	KN3TCP
TCP Connection Details	TCPIP Details	KN3TCP
TCP Connections Link	TCPIP Details	KN3TCP
TCP Listeners	TCP Listener	KN3TCL
TN3270 Active Server Session Summary for Remote IP	TN3270 Server Sess Avail	KN3TNA

Table 12. Attribute groups and workspaces affected by the KN3FCCMD START CONN command (continued)		
Workspace name	**Attribute group name**	**Attribute group name prefix**
TN3270 Server Session Availability	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Details	• TN3270 Response Time Buckets • TN3270 Server Sess Avail	• KN3TNB • KN3TNA
TN3270 Server Session Pair	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Summary for Remote IP	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Summary for SNA Name	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Sessions	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Sessions for Remote IP	• TCPIP Address Space • TN3270 Server Sess Avail	• KN3TAS • KN3TNA
TN3270 Server Sessions for SNA Name	• TCPIP Address Space • TN3270 Server Sess Avail	• KN3TAS • KN3TNA
UDP Endpoints	UDP Connections	KN3UDP

Usage

Sample output of this command using the default value of all TCP/IP address spaces is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START CONN'
KN3C111I START FOR COMPONENT CONN ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

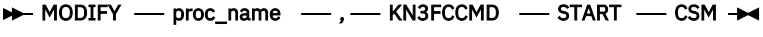
Sample output of this command using a specific TCP/IP address space is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START CONN TCPNAME(TCPIP)'
KN3C111I START FOR COMPONENT CONN ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START CSM

The KN3FCCMD START CSM command starts the monitoring of the Communication Storage Manager.

Format



Purpose

Starts monitoring of the Communication Storage Manager.

The following attribute groups and workspaces are affected by this command:

Table 13. Attribute groups and workspaces affected by the KN3FCCMD START CSM command		
Workspace name	**Attribute group name**	**Attribute group name prefix**
CSM Buffer Pools	CSM Storage Attributes	KN3CSM
CSM Storage by Owner Summary workspace	KN3 CSM Storage by Owner Attributes	KN3CSO

Usage

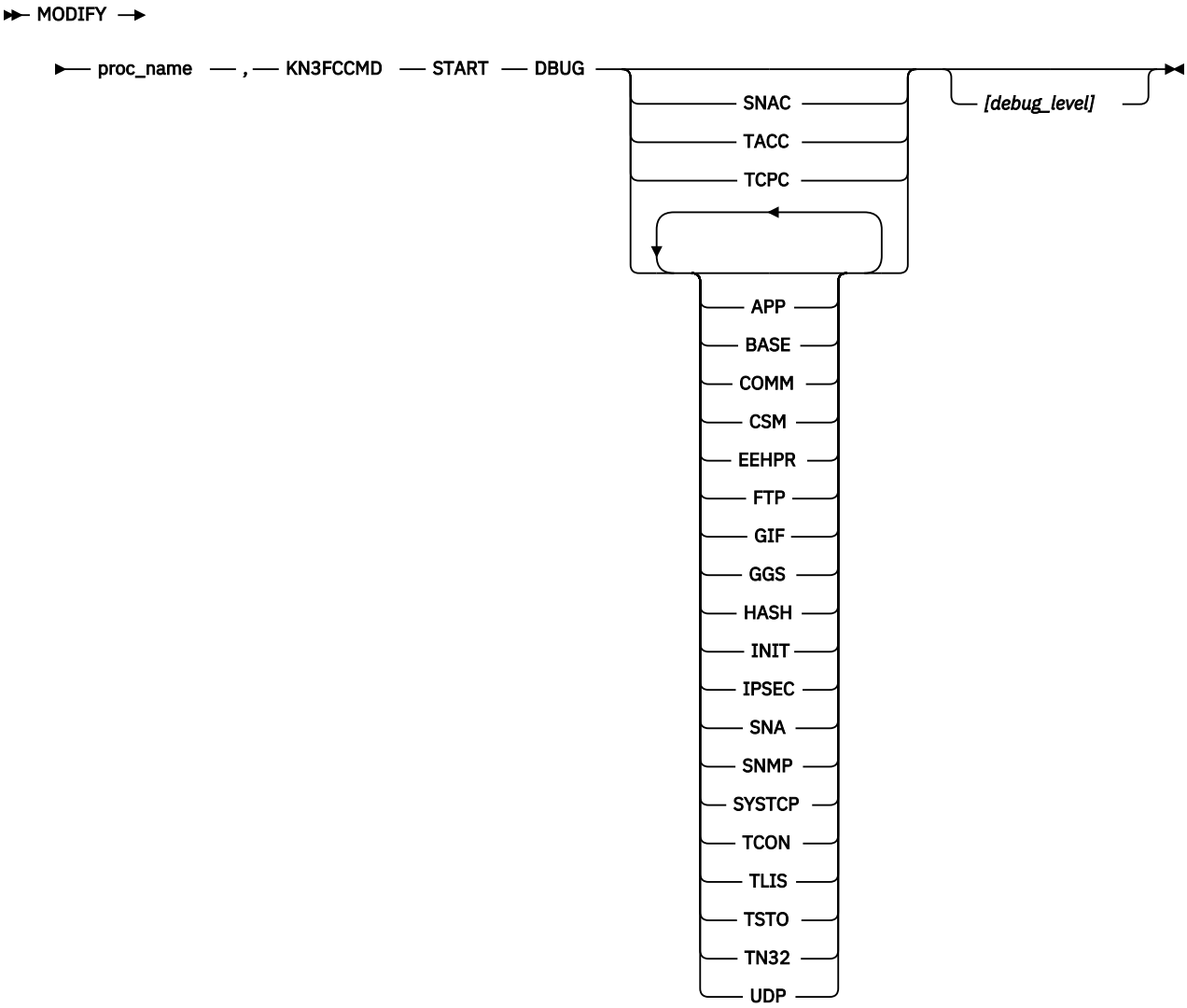
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START CSM'
KN3C112I START FOR COMPONENT CSM ACCEPTED.
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START DBUG

The KN3FCCMD START DBUG command starts the writing of trace messages for the TCP/IP and VTAM statistics collector to the log files.

Format



Where:

SNAC
Means write trace records for SNA Statistics collection.

TACC
Means write trace records for the product-specific Take Action commands issued by the IBM Z OMEGAMON Network Monitor command handler.

TCPC
Means write trace records for TCP/IP Statistics collections. Turning on all of the TCPC component may result in large amounts of trace data being written to the monitoring agent's job logs. To focus on the problem that you are experiencing, IBM Software Support may ask you to specify additional parameters to only write a subset of the trace records for TCP/IP Statistics collection. Table 14 on page 229 describes those additional parameters:

Table 14. Components available from subset trace records

Component	Description
APP	TCP/IP Application table
BASE	Base data collection in the KN3ACTC4 task
COMM	Common functions
CSM	CSM Storage table
EEHPR	Enterprise Extender and High Performance Routing tables
FTP	FTP sessions and transfers tables
GIF	Interface data
GGS	Stack Layer data
HASH	Hash functions
INIT	Initialization and control
IPSEC	IP filters and IP security tables
SNA	VTAM Summary Statistics table
SNMP	SNMP data collection
SYSTCP	Functions that access the real-time TCP/IP network management interface (NMI) and pass the retrieved data to the FTP and TN3270 data collection routines. For more information about the real-time interface, see the *IBM z/OS Communications Server: IP Programmer's Guide and Reference*.
TCON	TCPIP Details table and TCP Connections data stored in the TCPIP Connections table
TLIS	TCP Listener table and TCP Listener data stored in the TCPIP Connections table
TSTO	TCPIP Memory Statistics table
TN32	TN3270 Server Sessions Avail and TN3270 Response Time Buckets tables
UDP	UDP Connections table and UDP Connections data stored in the TCPIP Connections table
ZERT	zERT Summary data collection

debug_level
Is one of the following:

Debug level identifier	Meaning
MIN	Trace data is captured only when an error is detected.
MID	"Medium-detail" debugging messages are captured. These messages are used by IBM Software Support to diagnose software problems.
MAX	All trace data is captured. These messages are used by IBM Software Support to diagnose software problems.

Purpose

Starts the writing of trace messages for the TCP/IP and VTAM statistics collector to the log files. Additional trace messages will be written to sysout or spool data sets to facilitate investigation of a problem. IBM Software Support might request that you issue this command and then provide a copy of the log files. When the STOP command is issued, the component and subcomponents will capture trace information only when there is an error (MIN level).

Attention: Issuing the KN3FCCMD START DBUG command with the debug level set at MAX may result in the rapid filling of all spool volumes. When all spool volumes fill, system failure may occur.

Usage

These usages notes apply:

- You must specify a component before specifying a subcomponent. If you specify a subcomponent without a component, Message KN3FC004 is issued.
- When no subcomponent is specified when component is specified, the specified *debug_level* is applied to all subcomponents of the selected component.
- When all TCPC subcomponents are enabled at the MAX debug level (either as part of one command or cumulative), warning message KN3C143W is issued indicating that a significant amount of trace data may be written to the job log.
- When multiple subcomponent identifiers are specified, they are separated by spaces.
- All components/subcomponents are started at the MIN debug level by default when the agent is started.
- Multiple subcomponents may be specified on one command with different levels for trace defined for each component. Each START DBUG command has a cumulative effect.

Examples illustrating these usage points follow. These examples assume the default MIN level debug setting.

1. This command:

   ```
   MODIFY procname,KN3FCCMD START DBUG TCPC BASE TN32 MAX
   ```

   Results in the trace levels for the BASE and TN32 subcomponents of TCPC being set at MAX debug level. All other subcomponents of TCPC are still at the MIN debug level, and the SNAC component is at MIN debug level.

   Here is sample output for this command:

   ```
   KLVOP191 REPLY FROM *MASTER*:
   KLVOP191    'KN3FCCMD START DBUG TCPC BASE TN32 MAX'
   KN3C070I DBUG EXTENDED DIAGNOSTICS MODE STARTED
   KN3FC000 KN3FCCMD PROCESSING COMPLETE
   KLVOP191 REPLY FROM *MASTER*:
   KLVOP191    'KN3FCCMD STATUS DBUG'
   KN3AHFD3 (TCPC, BASE) KN3AHFD3 EXIT
   KN3C074I DBUG EXTENDED DIAGNOSTICS MODE IS ACTIVE
   KN3C200I FOR TCPC COMPONENT, MAXIMUM TRACING IS ENABLED FOR SUBCOMPONENTS:
   KN3C201I TN32 BASE
   ```

```
KN3C204I DBUG STATUS DISPLAY COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

2. This command:

```
MODIFY procname,KN3FCCMD START DBUG TCPC TN32 MID
```

Results in the trace levels for the TN32 subcomponent being set to MID, but the trace level for the BASE subcomponent is still at MAX. All other TCPC subcomponents and the SNAC component are set at MIN by default.

Here is sample output for this command:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START DBUG TCPC TN32 MID'
KN3C070I DBUG EXTENDED DIAGNOSTICS MODE STARTED
KN3FC000 KN3FCCMD PROCESSING COMPLETE
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STATUS DBUG'
KN3C074I DBUG EXTENDED DIAGNOSTICS MODE IS ACTIVE
KN3C200I FOR TCPC COMPONENT, MAXIMUM TRACING IS ENABLED FOR SUBCOMPONENTS:
KN3C201I BASE
KN3C200I FOR TCPC COMPONENT, MEDIUM TRACING IS ENABLED FOR SUBCOMPONENTS:
KN3C201I TN32
KN3C204I DBUG STATUS DISPLAY COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

3. This command:

```
MODIFY procname,KN3FCCMD START DBUG TCPC MAX
```

Results in the trace levels for all TCPC subcomponents being set to MAX. The trace level for the SNAC component is still set at MIN.

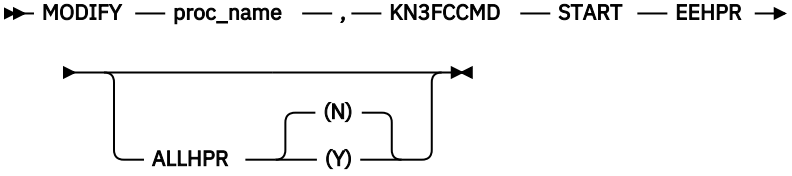
Here is sample output for this command:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START DBUG TCPC MAX'
KN3C070I DBUG EXTENDED DIAGNOSTICS MODE STARTED
KN3C143W MAX DEBUG LEVEL SET FOR COMPONENT TCPC
KN3FC000 KN3FCCMD PROCESSING COMPLETE
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STATUS DBUG'
KN3C074I DBUG EXTENDED DIAGNOSTICS MODE IS ACTIVE
KN3C202I MAXIMUM TRACING FOR COMPONENT TCPC IS ENABLED
KN3C204I DBUG STATUS DISPLAY COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START EEHPR

The KN3FCCMD START EEHPR command starts the monitoring of Enterprise Extender and High Performance Routing connections.

Format



Where:

ALLHPR

Is an optional parameter that specifies whether the monitoring agent will collect all High Performance Routing (HPR) connections or only those connections that flow over Enterprise Extender (EE) connections.

(N)
Indicates that the monitoring agent is to collect data on HPR connections that flow over EE connections.

(Y)
Indicates that the monitoring agent is to collect data on all HPR connections, not just those that flow over EE connections.

Purpose

Starts the monitoring of Enterprise Extender and High Performance Routing connections.

The following attribute groups and workspaces are affected by this command:

Table 15. Attribute groups and workspaces affected by the KN3FCCMD START EEHPR command

Workspace name	Attribute group name	Attribute group name prefix
EE Connection Summary	EE Connections Details	KN3EED
	HPR Connections	KN3HPR
	UDP Connections	KN3UDP
Enterprise EE Connections Overview	EE Connections Details	KN3EED
Enterprise HPR Connections Overview	HPR Connections	KN3HPR
EE Connections	EE Connections	KN3EEC
	EE Connections Details	KN3EED
HPR Connection Details	HPR Connections	KN3HPR
HPR Connections	HPR Connections	KN3HPR

Usage

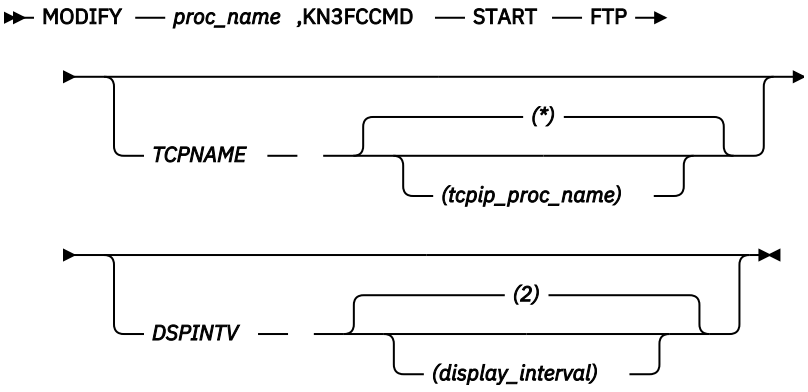
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191 'KN3FCCMD START EEHPR ALLHPR(Y)'
KN3C112I START FOR COMPONENT EEHPR ACCEPTED. ALLHRP:Y
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START FTP

The KN3FCCMD START FTP command starts the monitoring of FTP sessions and transfers.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this applies to.

*****
Indicates that this command applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

DSPINTV
Specifies the number of hours of data that is displayed.

2
Is the default number of hours of data that is displayed.

display_interval
Is a value you specify for the DSPINTV parameter. The value must be a valid number in the range 1-24.

Purpose

Starts the monitoring of FTP sessions and transfers. The TCPNAME option identifies which TCP/IP address spaces this applies to. The DSPINTV option specifies the number of hours of data that is displayed.

The following attribute groups and workspaces are affected by this command:

Table 16. Attribute groups and workspaces affected by the KN3FCCMD START FTP command

Workspace name	Attribute group name	Attribute group name prefix
Active FTP Sessions	FTP Sessions Attributes	KN3FSE
Enterprise FTP Sessions Find		
FTP Sessions		
FTP Sessions for Selected File transfer		
Active FTP Transfers	TCPIP FTP Attributes	KN3FTP
Enterprise FTP Transfers Find		
FTP Transfers		
FTP Transfers for Session		
FTP Transfers for Selected FTP Session	TCPIP FTP	KN3FTP
Enterprise FTP Sessions Overview	FTP Sessions Attributes	KN3FSE
	TCPIP FTP Attributes	KN3FTP
FTP Session Details	FTP Sessions Attributes	KN3FSE
	TCPIP Details	KN3TCP
FTP Transfer Details	FTP Sessions Attributes	KN3FSE
	TCPIP Details	KN3TCP

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START FTP'
KN3C110I START FOR COMPONENT FTP ACCEPTED. TCPNAME: * DSPINTV: 2
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START FTP DSPINTV(1)'
KN3C110I START FOR COMPONENT FTP ACCEPTED. TCPNAME: * DSPINTV: 1
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

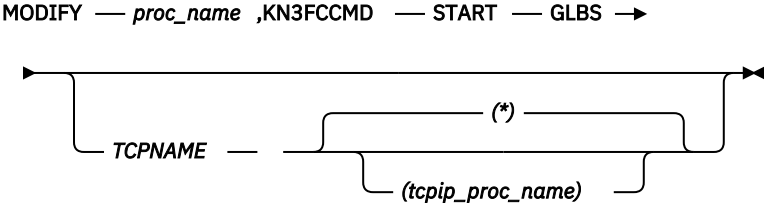
Sample output 3:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START FTP  TCPNAME(TCPIP)'
KN3C110I START FOR COMPONENT FTP ACCEPTED. TCPNAME: TCPIP DSPINTV: 2
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START GLBS

The KN3FCCMD START GLBS command starts TCP/IP stack layer statistics data collection.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this applies to.

*****
Indicates that this command applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Starts TCP/IP stack layer statistics data collection. The following attribute groups and workspaces are affected by this command:

Table 17. Attribute groups and workspaces affected by the KN3FCCMD START GLBS command

Workspace name	Attribute group name	Attribute group name prefix
Address Space	TCPIP Address Space	KN3TAS
ICMP Statistics	KN3 ICMP Global Counters	KN3GCG
	KN3 ICMP Type Counters	KN3GCT
IP Statistics	KN3 IP Counter Statistics	KN3GIC
	KN3 IP General Statistics	KN3GIG
TCP Statistics	KN3 TCP Counter Statistics	KN3GTC

Table 17. Attribute groups and workspaces affected by the KN3FCCMD START GLBS command (continued)		
Workspace name	**Attribute group name**	**Attribute group name prefix**
TCP/IP Stack Layers	KN3 TCPIP Stack Layer	KN3TSL
TCP/IP Stack Layers History	KN3 TCPIP Stack Layer	KN3TSL
TCP/IP Summary	KN3 TCPIP Address Space	KN3TAS
TCP/IP Summary History	KN3 TCPIP Address Space	KN3TAS
UDP Statistics	KN3 UDP Counter Statistics	KN3GUC

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START GLBS'
KN3C111I START FOR COMPONENT GLBS ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

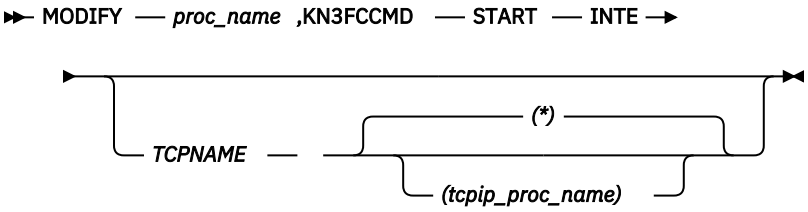
Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START GLBS TCPNAME(TCPIP)'
KN3C111I START FOR COMPONENT GLBS ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START INTE

The KN3FCCMD START INTE command starts interface data link control (DLC) data collection.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this applies to.

*****
Indicates that this command applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Starts interface data link control (DLC) data collection.

The following attribute groups and workspaces are affected by this command:

Table 18. Attribute groups and workspaces affected by the KN3FCCMD START INTE command		
Workspace name	**Attribute group name**	**Attribute group name prefix**
Data Link Control (DLC) Read and Write Queue Statistics	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
Enterprise HiperSockets Interfaces Overview	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise Interfaces Overview	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise OSA Interfaces Overview	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START INTE
KN3C111I START FOR COMPONENT INTE ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

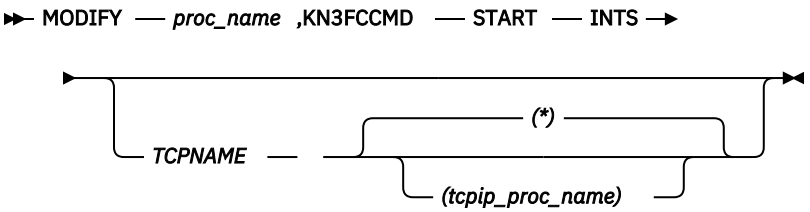
Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START INTE TCPNAME(TCPIP)'
KN3C111I START FOR COMPONENT INTE ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START INTS

The KN3FCCMD START INTS command starts interface statistics data collection.

Format



Where:

TCPNAME

Identifies which TCP/IP address spaces this applies to.

*****

Indicates that this command applies to all TCP/IP address spaces.

tcpip_proc_name

Is the name of a TCP/IP address space in your environment.

Purpose

Starts Interface Statistics data collection. The following attribute groups and workspaces are affected by this command:

Table 19. Attribute groups and workspaces affected by the KN3FCCMD START INTS command

Workspace name	Attribute group name	Attribute group name prefix
Enterprise HiperSockets Interfaces Overview	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise Interfaces Overview	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise OSA Interfaces Overview	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Gateways and Devices	TCPIP Devices	KN3TDV
Interface Statistics	KN3 Interface Statistics	KN3IFS
Interface Statistics History	KN3 Interface Statistics	KN3IFS
Interface Status	KN3 Interfaces	KN3IFE
Interfaces	Interfaces	KN3TIF
Interfaces History	Interfaces	KN3TIF

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START INTS
KN3C111I START FOR COMPONENT INTS ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

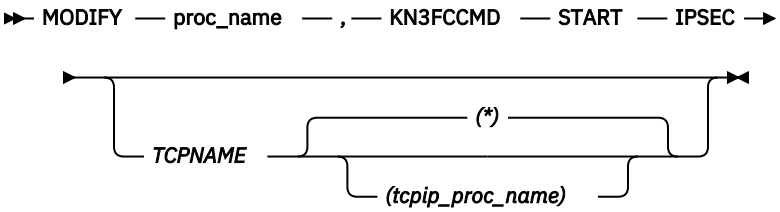
Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START INTS TCPNAME(TCPIP)'
KN3C111I START FOR COMPONENT INTS ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START IPSEC

The KN3FCCMD START IPSEC command starts collection of IPSEC data.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this command applies to.

*****
Indicates that this applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Starts collection of IPSec data.

The following attribute groups and workspaces are affected by this command:

Table 20. Attribute groups and workspaces affected by the KN3FCCMD START IPSEC command

Workspace name	Attribute group name	Attribute group name prefix
Current IP Filters	Current IP Filters	KN3IFC
Current IP Filters by Destination Address		
Current IP Filters by Filter Rule Definition Name		
Current IP Filters in Scan Order		
Dynamic IP Tunnels	Dynamic IP Tunnels	KN3ITD
Dynamic IP Tunnels by Destination Address		
Dynamic IP Tunnels by Filter Rule Definition Name		
Dynamic IP Tunnels by Tunnel ID		
Dynamic IP Tunnels with Byte Rate < 2048		
Dynamic IP Tunnel Statistics	IPSec Status	KN3ISS

Table 20. Attribute groups and workspaces affected by the KN3FCCMD START IPSEC command (continued)		
Workspace name	**Attribute group name**	**Attribute group name prefix**
IKE Tunnels	IKE Tunnels	KN3ITI
IKE Tunnels by Security Endpoint		
IKE Tunnels by Tunnel ID		
IKE Tunnels with Byte Rate < 1024		
Manual IP Tunnels	Manual IP Tunnels	KN3ITM
Manual IP Tunnels by Tunnel ID		

Usage

Sample output of this command using the default value of all TCP/IP address spaces is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START IPSEC'
KN3C110I START FOR COMPONENT IPSEC ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

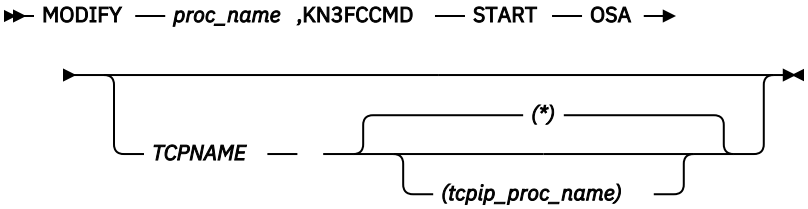
Sample output of this command using a specific TCP/IP address space is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START IPSEC  TCPNAME(TCPIP)'
KN3C110I START FOR COMPONENT IPSEC ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START OSA

The KN3FCCMD START OSA command starts collection of OSA data.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this applies to.

*****
Indicates that this command applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Starts OSA data collection. The TCPNAME option identifies which TCP/IP address spaces this applies to.

The following attribute groups and workspaces are affected by this command:

Table 21. Attribute groups and workspaces affected by the KN3FCCMD START OSA command

Workspace name	Attribute group name	Attribute group name prefix
Enterprise OSA-Express Channels Overview	OSA-Express Channels	KN3TCH
Enterprise OSA-Express Ports Overview	OSA-Express3 Ports Errors	KN3THE
	OSA-Express Ports	KN3TPO
	OSA 10 Gigabit Ports Errors	KN3TTE
	OSA 10 Gigabit Ports Summary	KN3TTS
OSA Channels	OSA-Express Channels	KN3TCH
OSA Ports	OSA-Express Ports	KN3TPO
OSA LPARs	OSA-Express LPARs	KN3TLP
OSA-Express2 10 Gigabit Port Errors	OSA-Express Channels	KN3TCH
OSA-Express2 10 Gigabit Port Control	OSA 10 Gigabit Ports Control	KN3TTC
OSA-Express2 10 Gigabit Ports Summary	OSA 10 Gigabit Ports Summary	KN3TTS
OSA-Express2 10 Gigabit Port Throughput Detail	OSA 10 Gigabit Ports Throughput	KN3TTT
OSA-Express3 Port Control	OSA-Express3 Ports Control	KN3THC
OSA-Express3 Port Errors	OSA-Express3 Ports Errors	KN3THE
OSA-Express3 Ports Summary	OSA-Express3 Ports Summary	KN3THS
OSA-Express3 Port Throughput Detail	OSA-Express3 Ports Throughput	KN3THT

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START OSA'
KN3C111I START FOR COMPONENT OSA ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

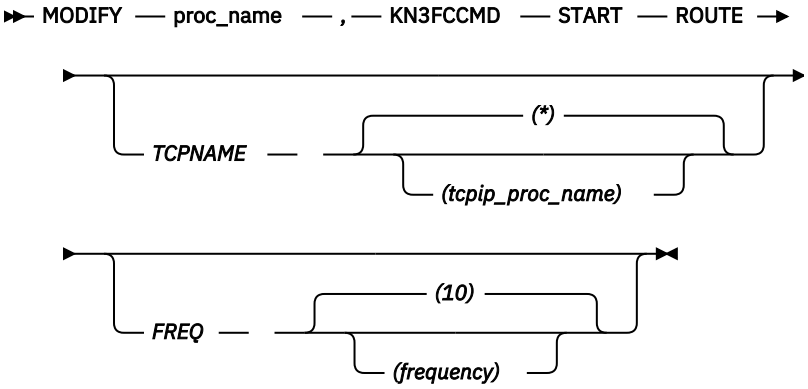
Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START OSA TCPNAME(TCPIP)'
KN3C111I START FOR COMPONENT OSA ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START ROUTE

The KN3FCCMD START ROUTE command starts the monitoring of routing information, which is displayed in Tivoli Enterprise Portal in the Gateways view of the Gateways and Devices workspace.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this applies to.

*****
Indicates that this command applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

FREQ
Is the number of collection intervals before the routing information will be collected. The value must be a valid number in the range of 1 to 99.

10
The default collection interval. With a default 5 minute collection interval, routing information would be collected approximately every 50 minutes.

frequency
Is specified as the number of collection intervals before the routing information will be collected. The value must be a valid number in the range of 1 to 99. An example would be a frequency of 2 with a 15-minute collection interval.

Purpose

Starts the monitoring of routing information, which is displayed in Tivoli Enterprise Portal in the Gateways view of the Gateways and Devices workspace. The TCPNAME option identifies which TCP/IP address spaces this command applies to. The FREQ option allows you to collect routing information less frequently than the rest of the resources because gateway tables can be large and do not change very often.

The following attribute groups and workspaces are affected by this command:

Table 22. Attribute groups and workspaces affected by the KN3FCCMD START ROUTE command

Workspace name	Attribute group name	Attribute group name prefix
Gateways and Devices	TCPIP Gateways	KN3TGA

Usage

Sample output using default of all TCP/IP address spaces:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START ROUTE'
KN3C120I START FOR COMPONENT ROUTE ACCEPTED. TCPNAME: * FREQ: 10
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

Sample output with a specific TCP/IP address space named:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START ROUTE TCPNAME(TCPIP)'
KN3C120I START FOR COMPONENT ROUTE ACCEPTED. TCPNAME: TCPIP FREQ: 10
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

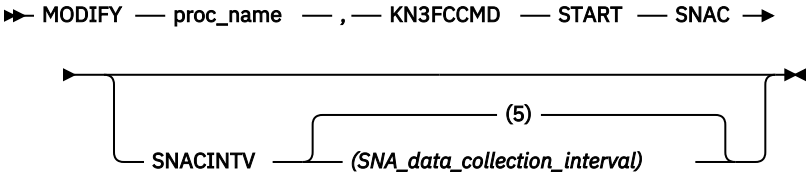
Sample output with frequency interval specified:

```
KN3FC000 KN3FCCMD PROCESSING COMPLETE
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START ROUTE FREQ(5)'
KN3C120I START FOR COMPONENT ROUTE ACCEPTED. TCPNAME: * FREQ: 5
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START SNAC

The KN3FCCMD START SNAC command starts the monitoring of the SNA data collector and determines how often data will be collected.

Format



Where:

SNACINTV
Is the SNA data collection interval. The default is 5 minutes.

SNA_data_collection_interval
Is the number of minutes between SNA data collection samples. This value is specified in minutes with a valid range of 1 to 60.

Purpose

Starts the monitoring of the SNA data collector and determines how often data will be collected.

When the user specifies **Y** for the Buffer Pool/VTAM Environment Data Collection parameter in the SPECIFY COMPONENT CONFIGURATION (Page 3) panel when using the Configuration Tool to configure IBM Z OMEGAMON Network Monitor, the KN3FCCMD START SNAC command is added to member KN3AGOPS of the RKANCMDU dataset. This command starts the monitoring of the SNA data collector and determines how often data will be collected. In order to collect data using the SNA collector the user must specify **Y** for Buffer Pool/VTAM Environment Data Collection.

If the SNA collector is active, the KN3FCCMD START SNAC command may be used to change the collection interval dynamically when the command is issued using the SNACINTV keyword.

The following attribute groups and workspaces are affected by this command:

Table 23. Attribute groups and workspaces affected by the KN3FCCMD START SNAC command		
Workspace name	**Attribute group name**	**Attribute group name prefix**
Address Space	VTAM Address Space	KN3VAS
	VTAM I/O	KN3VIO
	VTAM Storage	KN3VIO
VTAM Buffer Pools Summary	VTAM Buffer Pools	KN3BPD
VTAM Buffer Pool Details	VTAM Buffer Pools	
VTAM Buffer Pool Extents	VTAM Buffer Pool Extents	KN3BPE
VTAM Buffer Usage By Address Space	VTAM Buffer Usage By Address Space	KN3BPS
VTAM Buffer Usage By Application for Address Space	VTAM Buffer by Application	KN3BPA
VTAM Buffer Usage By Category	VTAM Buffer Usage By Category	KN3BPG
VTAM SIO	VTAM I/O	KN3VIO
VTAM Storage	VTAM I/O	KN3VIO
VTAM Summary	VTAM Summary Statistics	KN3SNA

Usage

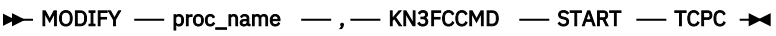
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START SNAC SNACINTV(1)'
KN3C112I START FOR COMPONENT SNAC ACCEPTED.
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START TCPC

The KN3FCCMD START TCPC command starts the monitoring of TCP/IP and VTAM statistics.

Format



Purpose

Starts the monitoring of TCP/IP and VTAM statistics.

After you stop monitoring TCP/IP and VTAM statistics, issue the following commands to restart collection:

```
MODIFY proc_name,KN3FCCMD INSTALL TCPC
   TCPCVIOU(vio_unit)
   TCPCINTV(collection_interval)
MODIFY proc_name,KN3FCCMD START TCPC
```

After you stop collection of TCP/IP and VTAM statistics, you must issue the following command to have collection started again:

```
MODIFY proc_name,KN3FCCMD START TCPC
```

If you want to change the value for either TCPCVIOU or TCPCINTV when you start TCPC collection, you must issue these commands:

```
MODIFY proc_name,KN3FCCMD INSTALL TCPC TCPCVIOU(vio_unit) TCPCINTV(collection_interval)
MODIFY proc_name,KN3FCCMD START TCPC
```

The following attribute groups and workspaces are affected by this command:

Table 24. Attribute groups and workspaces affected by the KN3FCCMD START TCPC command

Workspace name	Attribute group name	Attribute group name prefix
Active FTP Sessions	FTP Sessions	KN3FSE
Active TN3270 Server Connections for Selected Port	TN3270 Server Sess Avail	KN3TNA
Active FTP Transfers	TCPIP FTP	KN3FTP
Address Space	TCPIP Address Space	KN3TAS
Application Connections	TCPIP Connections	KN3TCN
Application Details	TCPIP Applications	KN3TAP
Application TCP Connections	TCPIP Details	KN3TCP
Application TCP Listeners	TCP Listener	KN3TCL
Application UDP Endpoints	UDP Connections	KN3UDP
Applications	TCPIP Applications	KN3TAP
Command Log	KN3 Take Action Command Attributes	KN3CTA
	KN3 Take Action Command Response Attributes	KN3RTA
Connections	TCPIP Connections	KN3TCN
CSM Buffer Pools	CSM Storage	KN3CSM
Current IP Filters	Current IP Filters	KN3IFC
Current IP Filters by Destination Address		
Current IP Filters by Filter Rule Definition Name		
Current IP Filters in Scan Order		
Data Link Control (DLC) Read and Write Queue Statistics	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
Dynamic IP Tunnel Statistics	IPSec Status	KN3ISS

Table 24. Attribute groups and workspaces affected by the KN3FCCMD START TCPC command (continued)

Workspace name	Attribute group name	Attribute group name prefix
Dynamic IP Tunnels	Dynamic IP Tunnels	KN3ITD
Dynamic IP Tunnels by Destination Address		
Dynamic IP Tunnels by Filter Rule Definition Name		
Dynamic IP Tunnels by Tunnel ID		
Dynamic IP Tunnels with Byte Rate < 2048		
EE Connection Summary	EE Connection Details	KN3EED
	HPR Connections	KN3HPR
	UDP Connections	KN3UDP
EE Connection Details	EE Connection Details	KN3EED
EE Connections	EE Connection	KN3EEC
Enterprise Applications Health	TCPIP Applications	KN3TAP
Enterprise Connections Find	TCPIP Details	KN3TCP
Enterprise Connections Health	TCPIP Details	KN3TCP
Enterprise FTP Sessions Find	FTP Sessions	KN3FSE
Enterprise FTP Sessions Overview	FTP Sessions	KN3FSE
	TCPIP FTP	KN3FTP
Enterprise FTP Transfers Find	TCPIP FTP	KN3FTP
Enterprise HiperSockets Interfaces Overview	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise Interfaces Overview	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise OSA-Express Channels Overview	OSA-Express Channels	KN3TCH

Table 24. Attribute groups and workspaces affected by the KN3FCCMD START TCPC command (continued)

Workspace name	Attribute group name	Attribute group name prefix
Enterprise OSA-Express Ports Overview	OSA-Express3 Ports Errors	KN3THE
	OSA-Express Ports	KN3TPO
	OSA 10 Gigabit Ports Errors	KN3TTE
	OSA 10 Gigabit Ports Summary	KN3TTS
Enterprise OSA Interfaces Overview	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise TN3270 Find	TN3270 Server Sess Avail	KN3TNA
FTP Session Details	FTP Sessions	KN3FSE
	TCPIP Details	KN3TCP
FTP Sessions	FTP Sessions	KN3FSE
FTP Sessions for selected file transfer	FTP Sessions	KN3FSE
FTP Transfer Details	TCPIP FTP	KN3FTP
	TCPIP Details	KN3TCP
FTP Transfers	TCPIP FTP	KN3FTP
FTP Transfers for link selected	TCPIP FTP	KN3FTP
FTP Transfers for Session	TCPIP FTP	KN3FTP
Gateways and Devices	TCPIP Devices	KN3TDV
	TCPIP Gateways	KN3TGA
HPR Connections	HPR Connections	KN3HPR
ICMP Statistics	KN3 ICMP Global Counters	KN3GCG
	KN3 ICMP Type Counters	KN3GCT
Interface Statistics	KN3 Interface Statistics	KN3IFS
Interface Statistics History	KN3 Interface Statistics	KN3IFS
Interface Status	KN3 Interface Status	KN3IFE
Interfaces	Interfaces	KN3TIF
Interfaces History		
IP Statistics	KN3 IP Counter Statistics	KN3GIC
	KN3 IP General Statistics	KN3GIG

Table 24. Attribute groups and workspaces affected by the KN3FCCMD START TCPC command (continued)

Workspace name	Attribute group name	Attribute group name prefix
IKE Tunnels	IKE Tunnels	KN3ITI
IKE Tunnels by Security Endpoint		
IKE Tunnels by Tunnel ID		
IKE Tunnels with Byte Rate < 1024		
IKE Tunnels Statistics	IPSec Status	KN3ISS
IPSec Status		
Manual IP Tunnels	Manual IP Tunnels	KN3ITM
Manual IP Tunnels by Tunnel ID		
NetView for z/OS: Packet Trace – Start	KN3 DWL to 3270	KN3DWL3270
NetView for z/OS: Packet Trace – Stop	KN3 DWL to 3270	KN3DWL3270
OSA Channels	OSA-Express Channels	KN3TCH
OSA-Express2 10 Gigabit Port Errors	OSA 10 Gigabit Ports Errors	KN3TTE
OSA-Express2 10 Gigabit Port Control	OSA 10 Gigabit Ports Control	KN3TTC
OSA-Express2 10 Gigabit Ports Summary	OSA 10 Gigabit Ports Summary	KN3TTS
OSA-Express2 10 Gigabit Port Throughput Detail	OSA 10 Gigabit Ports Throughput	KN3TTT
OSA-Express3 Port Control	OSA-Express3 Ports Control	KN3THC
OSA-Express3 Port Errors	OSA-Express3 Ports Errors	KN3THE
OSA-Express3 Ports Summary	OSA-Express3 Ports Summary	KN3THS
OSA-Express3 Port Throughput Detail	OSA-Express3 Ports Throughput	KN3THT
OSA LPARs	OSA-Express LPARs	KN3TLP
OSA Port Interfaces	OSA Port Interfaces	KN3TIF
OSA Ports	OSA-Express Ports	KN3TPO
TCP Connection Details	TCPIP Details	KN3TCP
TCP Connections	TCPIP Details	KN3TCP
TCP Connections Link	TCPIP Details	KN3TCP
TCP Listeners	TCP Listener	KN3TCL
TCP Statistics	KN3 TCP Counter Statistics	KN3GTC

Table 24. Attribute groups and workspaces affected by the KN3FCCMD START TCPC command (continued)

Workspace name	Attribute group name	Attribute group name prefix
TCP/IP Memory Statistics	TCPIP Memory Statistics	KN3TPV
TCP/IP Stack Layers	TCPIP Stack Layer	KN3TSL
TCP/IP Stack Layers History	TCPIP Stack Layer	KN3TSL
TCP/IP Summary	TCPIP Address Space	KN3TAS
TCP/IP Summary History	TCPIP Address Space	KN3TAS
TN3270 Active Server Session Summary for Remote IP	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Availability	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Pair	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Summary for Remote IP		
TN3270 Server Session Summary for SNA Name		
TN3270 Server Sessions for Remote IP		
TN3270 Server Sessions for SNA Name		
TN3270 Server Session Details	TN3270 Server Sess Avail	KN3TNA
	TN3270 Response Time Buckets	KN3TNB
TN3270 Server Sessions	TN3270 Server Sess Avail	KN3TNA
UDP Endpoints	UDP Connections	KN3UDP
UDP Statistics	KN3 UDP Counter Statistics	KN3GUC

Usage

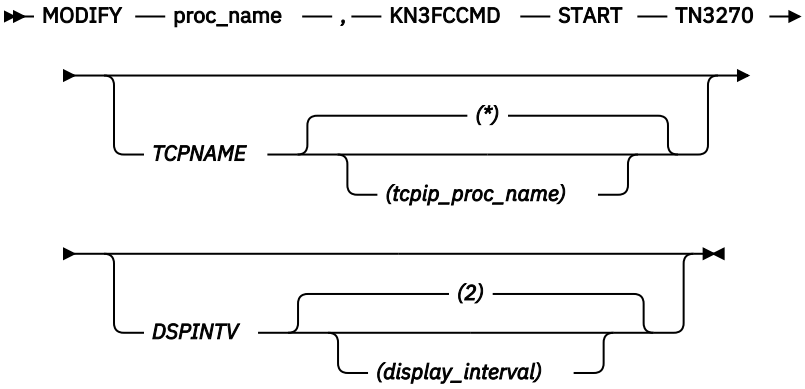
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START TCPC'
KN3CT100 TCP/IP SERVICE THREAD INITIALIZATION COMPLETE
KN3CT000 TCP/IP STATISTICS COLLECTOR INITIALIZATION COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
KN3FC095 TCPC COLLECTOR STATUS IS ACTIVE
KN3FC095 KONAYTGA ADDRESS IS D1D3098, KONAYFCV ADDRESS IS D1D1E20
KN3FC095 SAMPLE INTERVAL IS 1 MINUTES
KN3FC095 NUMBER OF TIMES COLLECTOR HAS ABENDED IS 0
KN3FC095 TCPC COLLECTION IS ACTIVE FOR TCPC, CONN, OSA, INTS, INTE, GLBS, FTP
KN3FC095 TCPC COLLECTION IS ACTIVE FOR TN3270, ROUTE
KN3FC095 FTP DISPLAY INTERVAL IS 2 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL IS 2 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY IS ONCE EVERY 10 INTERVALS
KN3FC095 VTAM COLLECTION IS ACTIVE FOR SNA, CSM, EEHPR
KN3FC095 TCPC STATUS DISPLAY COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START TN3270

The KN3FCCMD START TN3270 command starts the monitoring of TN3270 data.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this applies to.

*****
Indicates that this command applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

DSPINTV
Specifies the number of hours of data that is displayed.

2
Is the default number of hours of data that is displayed.

display_interval
Is a value you specify for the DSPINTV parameter. The value must be a valid number in the range 1-24.

Purpose

Starts the monitoring of TN3270 server sessions. The TCPNAME option identifies which TCP/IP address spaces this applies to. The DSPINTV option specifies the number of hours of data that is displayed.

The following attribute groups and workspaces are affected by this command:

Table 25. Attribute groups and workspaces affected by the KN3FCCMD START TN3270 command

Workspace name	Attribute group name	Attribute group name prefix
Active TN3270 Server Connections for Selected Port workspace	TN3270 Server Sess Avail	KN3TNA
Enterprise TN3270 Find workspace	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Availability	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Sessions	TN3270 Server Sess Avail	KN3TNA
TN3270 Active Server Session Summary for Remote IP	TN3270 Server Sess Avail	KN3TNA

Table 25. Attribute groups and workspaces affected by the KN3FCCMD START TN3270 command (continued)		
Workspace name	**Attribute group name**	**Attribute group name prefix**
TN3270 Server Session Details	TN3270 Server Sess Avail	KN3TNA
	TN3270 Response Time Buckets	KN3TNB
TN3270 Server Session Pair	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Summary for Remote IP	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Summary for SNA Name	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Sessions for Remote IP	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Sessions for SNA Name	TN3270 Server Sess Avail	KN3TNA

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START TN3270'
KN3C110I START FOR COMPONENT TN3270 ACCEPTED. TCPNAME: * DSPINTV: 2
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START TN3270 DSPINTV(1)'
KN3C110I START FOR COMPONENT TN3270 ACCEPTED. TCPNAME: * DSPINTV: 1
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

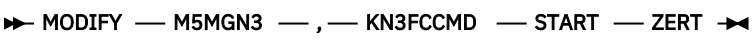
Sample output 3:

```
Sample output #3:
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START TN3270 TCPNAME(TCPIP)'
KN3C110I START FOR COMPONENT TN3270 ACCEPTED. TCPNAME: TCPIP DSPINTV: 2
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD START ZERT

The KN3FCCMD START ZERT command starts the monitoring of zERT summary data. The zERT summary data collection is started and stopped with the ZERT keyword on the KN3FCCMD modify command. By default, zERT summary data collection is enabled when the Network Monitor Agent is started.

Format



Where:

M5MGN3
is the name of the Network Monitor Started Task address space.

An example invocation of this command is:

```
F M5MGN3,KN3FCCMD START ZERT
```

Purpose

Starts monitoring of zERT sessions.

The following attribute groups and workspaces are affected by this command:

Table 26. Attribute groups and workspaces affected by the KN3FCCMD START ZERT command

Workspace name	Attribute group name	Attribute group name prefix
zERT ALL Sessions	zERT Common Session Data	KN3ZCM
zERT SSH Sessions	zERT SSH Session Data	KN3ZSH
zERT TLS Sessions	zERT TLS Session Data	KN3ZTL
zERT IPSec Sessions	zERT IPSec Session Data	KN3ZIP
zERT Session Distinguished Names	zERT DNs Session Data	KN3ZDN

Usage

Sample output from this command:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START zERT'
KN3C110I START FOR COMPONENT zERT ACCEPTED.
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

Notes

Since zERT summary data collection is part of the TCP/IP component data collection of the Network Monitor, KN3FCCMD START TCPC and KN3FCCMD STOP TCPC will start and stop zERT data collection along with all other TCP/IP component data collection.

The KN3FCCMD STATUS TCPC modify command will show whether zERT summary data collection is active.

The KN3FCCMD HELP modify command will show help information for the ZERT keyword of the modify command.

The KN3FCCMD START DBUG modify command is updated to support a ZERT keyword for starting trace against ZERT summary data collection.

The KN3FCCMD STOP DBUG modify command is updated to support a ZERT keyword for stopping trace against zERT summary data collection.

KN3FCCMD STATUS DBUG

The KN3FCCMD STATUS DBUG command displays the current settings of the extended diagnostics component.

Format

Purpose

Display the current settings of the extended diagnostics component.

Usage

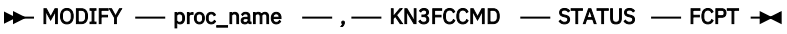
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STATUS DBUG'
KN3FC074 DBUG EXTENDED DIAGNOSTICS MODE IS INACTIVE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STATUS FCPT

The KN3FCCMD STATUS FCPT command displays the status of the Tivoli Enterprise Portal data server features.

Format



Purpose

Displays the status of the Tivoli Enterprise Portal data server features.

Usage

Sample output of this command is provided in the following section:

```
KLVOP191    'KN3FCCMD STATUS FPCT'
KN3FC017 KONAYFCV AT 0D1D1E20
KN3FC017 FPCT COMPONENT FUNCTIONS INSTALLED
KN3FC017 FUNCTION PACKAGE KN3AZCFV LOADED AT 0D1517D8
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STATUS FPON

The KN3FCCMD STATUS FPON command displays the status of the OMEGAMON product features.

Format

Purpose

Displays the status of the OMEGAMON product features.

Usage

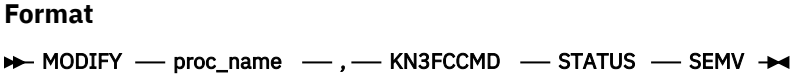
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STATUS FPON'
KN3FC012 KONAYFCV AT 0D1D1E20
KN3FC012 FPON COMPONENT FUNCTIONS INSTALLED
KN3FC012 FUNCTION PACKAGE KN3AZOFV LOADED AT 0D15BF08
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STATUS SEMV

The KN3FCCMD STATUS SEMV command displays the status of the MVS environment features.

Format



Purpose

Displays the status of the MVS environment features.

Usage

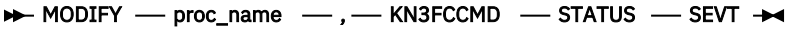
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STATUS SEMV'
KN3FC027 KONAYFCV AT 0D1D1E20
KN3FC027 SEMV MVS ENVIRONMENT INSTALLED
KN3FC027 MVS DICTIONARY KN3AZD2C LOADED AT 90780B9C
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STATUS SEVT

The KN3FCCMD STATUS SEVT command displays the status of the VTAM environment features.

Format



Purpose

Displays the status of the VTAM environment features.

Usage

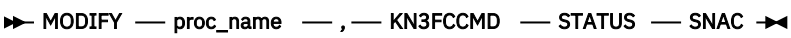
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STATUS SEVT'
KN3FC023 KONAYFCV AT 0D1D1E20
KN3FC023 SEVT VTAM ENVIRONMENT INSTALLED
KN3FC023 VTAM DICTIONARY KN3AZD1E LOADED AT 90781C7C
KN3FC023 SRT HASH FLAG IS 40
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STATUS SNAC

The KN3FCCMD STATUS SNAC command displays the status of the SNA data collector.

Format



Purpose

Displays the status of the SNA data collector.

Usage

Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STATUS SNAC'
KN3C130I SNA COLLECTOR STATUS IS ACTIVE
KN3C131I KONAYPWK ADDRESS IS 4CB000, KONAYACT ADDRESS IS EB41300
KN3C132I MONITORING VTAM ADDRESS SPACE NAMED VTAM
KN3C133I SNA COLLECTION INTERVAL IS 1
KN3C134I ACB PREFIX IS OVTAMC, PMI ACB NAME IS N341N3SP
KN3C136I SAMPLE INTERVAL IS 6000 HUNDREDTH SECONDS
KN3C138I CYCLE COUNT IS 15
KN3C141I SNA COLLECTOR STATUS DISPLAY COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STATUS TCPC

The KN3FCCMD STATUS TCPC command displays the status of the TCP/IP and VTAM statistics component.

Format

Purpose

Displays the status of the TCP/IP and VTAM statistics component.

Usage

Sample output of this command is provided in the following section:

```
KN3FC095 TCPC COLLECTOR STATUS IS ACTIVE
KN3FC095 KONAYTGA ADDRESS IS 108C9D20, KONAYFCV ADDRESS IS 108C8560
KN3FC095 SAMPLE INTERVAL IS 1 MINUTES
KN3FC095 NUMBER OF TIMES COLLECTOR HAS ABENDED IS 0
KN3FC095 TCPC COLLECTION IS ACTIVE FOR TCPC, CONN, OSA, INTS, INTE, GLBS, FTP
KN3FC095 TCPC COLLECTION IS ACTIVE FOR TN3270, ROUTE
KN3FC095 FTP DISPLAY INTERVAL IS 2 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL IS 2 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY IS ONCE EVERY 10 INTERVALS
KN3FC095 TCPC COLLECTION FROM TCPIP IS ACTIVE FOR TCPC, CONN, OSA, INTS, INTE, GLBS,
KN3FC095 TCPC COLLECTION FROM TCPIP IS ACTIVE FOR  FTP, TN3270, ROUTE
KN3FC095 FTP DISPLAY INTERVAL FOR TCPIP IS 24 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL FOR TCPIP IS 24 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY FOR TCPIP IS ONCE EVERY 15 INTERVALS
KN3FC095 VTAM COLLECTION IS ACTIVE FOR SNA, CSM, EEHPR
KN3FC095 EEHPR OPTIONS: ALLHPR(Y)
KN3FC095 TCPC STATUS DISPLAY COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

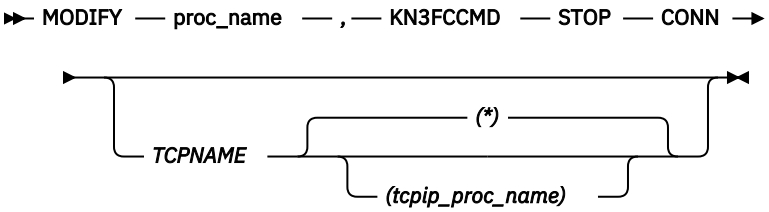
Sample output for a system with three TCP/IP address spaces:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191 'KN3FCCMD STATUS TCPC'
KN3FC095 TCPC COLLECTOR STATUS IS ACTIVE
KN3FC095 KONAYTGA ADDRESS IS D4320C0, KONAYFCV ADDRESS IS D430E48
KN3FC095 SAMPLE INTERVAL IS 5 MINUTES
KN3FC095 NUMBER OF TIMES COLLECTOR HAS ABENDED IS 0
KN3FC095 TCPC COLLECTION IS ACTIVE FOR TCPC, CONN, OSA, INTS, INTE, GLBS, FTP
KN3FC095 TCPC COLLECTION IS ACTIVE FOR TN3270, ROUTE
KN3FC095 FTP DISPLAY INTERVAL IS 2 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL IS 2 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY IS ONCE EVERY 10 INTERVALS
KN3FC095 TCPC COLLECTION FROM TCPIP IS ACTIVE FOR TCPC, CONN, OSA, INTS, INTE, GLBS,
KN3FC095 TCPC COLLECTION FROM TCPIP IS ACTIVE FOR  FTP, TN3270, ROUTE
KN3FC095 FTP DISPLAY INTERVAL FOR TCPIP IS 2 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL FOR TCPIP IS 2 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY FOR TCPIP IS ONCE EVERY 10 INTERVALS
KN3FC095 TCPC COLLECTION FROM TCPIPB IS ACTIVE FOR TCPC, CONN, OSA, INTS, INTE, GLBS,
KN3FC095 TCPC COLLECTION FROM TCPIPB IS ACTIVE FOR  FTP, TN3270, ROUTE
KN3FC095 FTP DISPLAY INTERVAL FOR TCPIPB IS 2 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL FOR TCPIPB IS 2 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY FOR TCPIPB IS ONCE EVERY 10 INTERVALS
KN3FC095 TCPC COLLECTION FROM TCPIPC IS ACTIVE FOR TCPC, CONN, OSA, INTS, INTE, GLBS,
KN3FC095 TCPC COLLECTION FROM TCPIPC IS ACTIVE FOR  FTP, TN3270, ROUTE
KN3FC095 FTP DISPLAY INTERVAL FOR TCPIPC IS 2 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL FOR TCPIPC IS 2 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY FOR TCPIPC IS ONCE EVERY 10 INTERVALS
KN3FC095 VTAM COLLECTION IS ACTIVE FOR SNA, CSM, EEHPR
KN3FC095 EEHPR options: ALLHPR(Y)
KN3FC095 TCPC STATUS DISPLAY COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP CONN

The KN3FCCMD STOP CONN command stops the monitoring of connections and applications.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this command applies to.

*****
Indicates that this applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Stops the monitoring of connections and applications.

The following attribute groups and workspaces are affected by this command:

Table 27. Attribute groups and workspaces affected by the KN3FCCMD STOP CONN command

Workspace name	Attribute group name	Attribute group name prefix
Active TN3270 Server Connections for Selected Port	TN3270 Server Sess Avail	KN3TNA
Application Connections	TCPIP Connections	KN3TCN
Application Details	TCPIP Applications	KN3TAP
Application TCP Connections	TCPIP Details	KN3TCP
Application TCP Listeners	TCP Listener	KN3TCL
Application UDP Endpoints	UDP Connections	KN3UDP
Applications	TCPIP Applications	KN3TAP
Connections	TCPIP Connections	KN3TCN
EE Connection Summary	• EE Connections Details • HPR Connections • UDP Connections	• KN3EED • KN3HPR • KN3UDP
Enterprise Applications Health	TCPIP Applications	KN3TAP
Enterprise Connections Find	TCPIP Details	KN3TCP
Enterprise Connections Health	TCPIP Details	KN3TCP

Table 27. Attribute groups and workspaces affected by the KN3FCCMD STOP CONN command (continued)		
Workspace name	**Attribute group name**	**Attribute group name prefix**
Enterprise TN3270 Find	TN3270 Server Sess Avail	KN3TNA
Enterprise TN3270 Server Overview	TCP Listener	KN3TCL
FTP Sessions Details	• FTP Session • TCPIP Details	• KN3FSE • KN3TCP
FTP Transfer Details	• TCPIP FTP • TCPIP Details	• KN3FTP • KN3TCP
TCP Connections	TCPIP Details	KN3TCP
TCP Connection Details	TCPIP Details	KN3TCP
TCP Connections Link	TCPIP Details	KN3TCP
TCP Listeners	TCP Listener	KN3TCL
TN3270 Active Server Session Summary for Remote IP	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Availability	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Details	• TN3270 Response Time Buckets • TN3270 Server Sess Avail	• KN3TNB • KN3TNA
TN3270 Server Session Pair	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Summary for Remote IP	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Summary for SNA Name	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Sessions	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Sessions for Remote IP	• TCPIP Address Space • TN3270 Server Sess Avail	• KN3TAS • KN3TNA
TN3270 Server Sessions for SNA Name	• TCPIP Address Space • TN3270 Server Sess Avail	• KN3TAS • KN3TNA
UDP Endpoints	UDP Connections	KN3UDP

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP CONN'
KN3C115I STOP FOR COMPONENT CONN ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

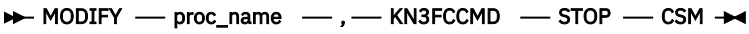
Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP  CONN TCPNAME(TCPIP)'
KN3C115I STOP FOR COMPONENT CONN ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP CSM

The KN3FCCMD STOP CSM command stops the monitoring of Communications Storage Manager.

Format



Purpose

Stops the monitoring of Communications Storage Manager.

The following attribute groups and workspaces are affected by this command:

Table 28. Attribute groups and workspaces affected by the KN3FCCMD STOP CSM command

Workspace name	Attribute group name	Attribute group name prefix
CSM Buffer Pools	CSM Storage Attributes	KN3CSM
CSM Storage by Owner Summary workspace	KN3 CSM Storage by Owner Attributes	KN3CSO

Usage

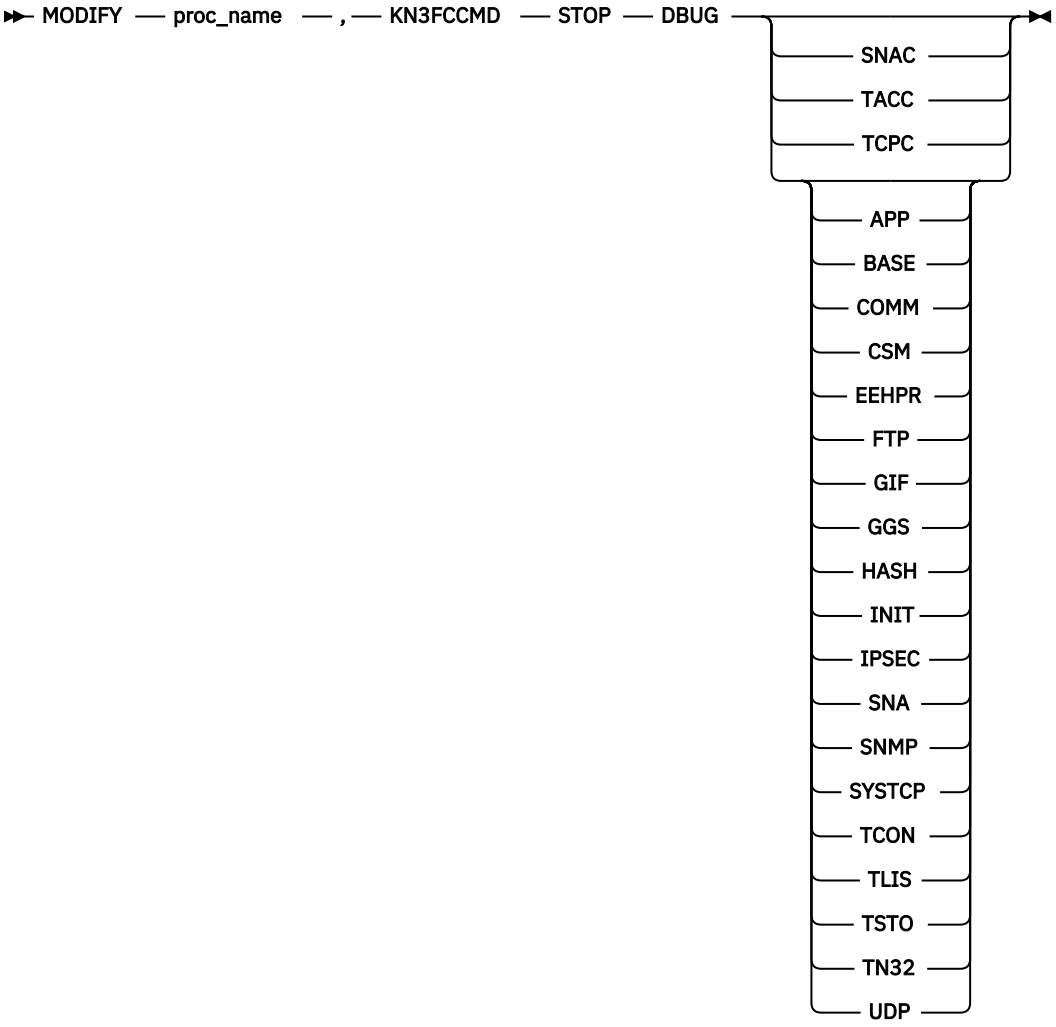
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP CSM'
KN3C116I STOP FOR COMPONENT CSM ACCEPTED.
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP DBUG

The KN3FCCMD STOP DBUG command stops the writing of trace messages for the TCP/IP and VTAM statistics collector to the log files.

Format



Where:

SNAC
Means to stop writing trace records for SNA Statistics collection.

TACC
Means to stop writing trace records for the product-specific Take Action commands issued by the IBM Z OMEGAMON Network Monitor command handler.

TCPC
Means to stop writing trace records for TCP/IP Statistics collections. Any of the following TCPC components can be stopped. Table 29 on page 258describes those additional parameters:

Table 29. Components available from subset trace records

Component	Description
APP	TCP/IP Application table
BASE	Base data collection in the KN3ACTC4 task
COMM	Common functions

Table 29. Components available from subset trace records (continued)	
Component	**Description**
CSM	CSM Storage table
EEHPR	Enterprise Extender and High Performance Routing tables
FTP	FTP sessions and transfers tables
GIF	Interface data
GGS	Stack Layer data
HASH	Hash functions
INIT	Initialization and control
IPSEC	IP filters and IP security tables
SNA	VTAM Summary Statistics table
SNMP	SNMP data collection
SYSTCP	Functions that access the real-time TCP/IP network management interface (NMI) and pass the retrieved data to the FTP and TN3270 data collection routines. For more information about the real-time interface, see the *IBM z/OS Communications Server: IP Programmer's Guide and Reference*.
TCON	TCPIP Details table and TCP Connections data stored in the TCPIP Connections table
TLIS	TCP Listener table and TCP Listener data stored in the TCPIP Connections table
TSTO	TCPIP Memory Statistics table
TN32	TN3270 Server Sessions Avail and TN3270 Response Time Buckets tables
UDP	UDP Connections table and UDP Connections data stored in the TCPIP Connections table

Purpose

Stops the writing of trace messages for the TCP/IP and VTAM statistics collector to the log files.

Usage

These usages notes apply:

- You must specify a component before specifying a subcomponent. If you specify a subcomponent without a component, Message KN3FC004 is issued.
- When all TCPC subcomponents are enabled at the MAX debug level (either as part of one command or cumulative), warning message KN3C143W is issued indicating that a significant amount of trace data may be written to the job log.
- When multiple subcomponent identifiers are specified, they are separated by spaces.
- All components/subcomponents are started at the MIN debug level by default when the agent is started. When the STOP command is issued, the component and subcomponents will capture trace information only when there is an error (MIN level).

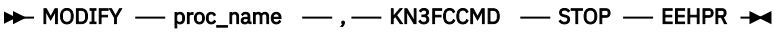
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP DBUG TCPC'
KN3FC072 DBUG EXTENDED DIAGNOSTICS MODE STOPPED
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP EEHPR

The KN3FCCMD STOP DBUG command stops the writing of Enterprise Extender and High Performance Routing connections.

Format



Purpose

Stops the writing of Enterprise Extender and High Performance Routing connections.

The following attribute groups and workspaces are affected by this command:

Table 30. Attribute groups and workspaces affected by the KN3FCCMD STOP EEHPR command

Workspace name	Attribute group name	Attribute group name prefix
EE Connection Summary	EE Connections Details	KN3EED
	HPR Connections	KN3HPR
	UDP Connections	KN3UDP
Enterprise EE Connections Overview	EE Connections Details	KN3EED
Enterprise HPR Connections Overview	HPR Connections	KN3HPR
EE Connections	EE Connections	KN3EEC
	EE Connections Details	KN3EED
HPR Connection Details	HPR Connections	KN3HPR
HPR Connections	HPR Connections	KN3HPR

Usage

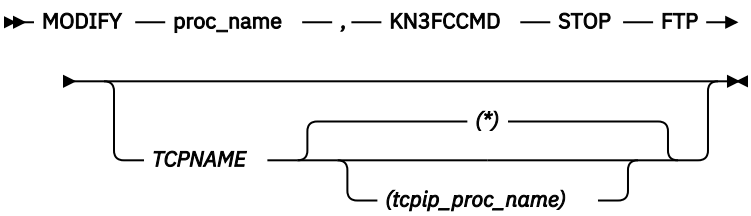
Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP EEHPR'
KN3C116I STOP FOR COMPONENT EEHPR ACCEPTED.
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP FTP

The KN3FCCMD STOP FTP command stops the monitoring of FTP sessions and transfers.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this command applies to.

*****
Indicates that this applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Stops the monitoring of FTP sessions and transfers.

The following attribute groups and workspaces are affected by this command:

Table 31. Attribute groups and workspaces affected by the KN3FCCMD STOP FTP command

Workspace name	Attribute group name	Attribute group name prefix
Active FTP Sessions	FTP Sessions Attributes	KN3FSE
Enterprise FTP Sessions Find		
FTP Sessions		
FTP Sessions for Selected File transfer		
Active FTP Transfers	TCPIP FTP Attributes	KN3FTP
Enterprise FTP Transfers Find		
FTP Transfers		
FTP Transfers for Session		
FTP Transfers for Selected FTP Session	TCPIP FTP	KN3FTP
Enterprise FTP Sessions Overview	FTP Sessions Attributes	KN3FSE
	TCPIP FTP Attributes	KN3FTP
FTP Session Details	FTP Sessions Attributes	KN3FSE
	TCPIP Details	KN3TCP
FTP Transfer Details	FTP Sessions Attributes	KN3FSE
	TCPIP Details	KN3TCP

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP FTP'
KN3C115I STOP FOR COMPONENT FTP ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

Sample output 2:

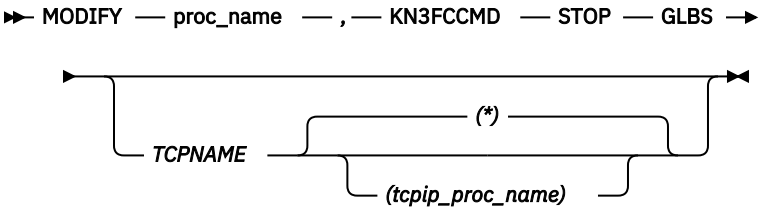
```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP FTP TCPNAME(TCPIP)'
```

```
KN3C115I STOP FOR COMPONENT FTP ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP GLBS

The KN3FCCMD STOP GLBS command stops TCP/IP stack layer statistics data collection.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this command applies to.

*****
Indicates that this applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Stops TCP/IP stack layer statistics data collection. The following attribute groups and workspaces are affected by this command:

Table 32. Attribute groups and workspaces affected by the KN3FCCMD STOP GLBS command

Workspace name	Attribute group name	Attribute group name prefix
Address Space	TCPIP Address Space	KN3TAS
ICMP Statistics	KN3 ICMP Global Counters	KN3GCG
	KN3 ICMP Type Counters	KN3GCT
IP Statistics	KN3 IP Counter Statistics	KN3GIC
	KN3 IP General Statistics	KN3GIG
TCP Statistics	KN3 TCP Counter Statistics	KN3GTC
TCP/IP Stack Layers	KN3 TCPIP Stack Layer	KN3TSL
TCP/IP Stack Layers History	KN3 TCPIP Stack Layer	KN3TSL
TCP/IP Summary	KN3 TCPIP Address Space	KN3TAS
TCP/IP Summary History	KN3 TCPIP Address Space	KN3TAS
UDP Statistics	KN3 UDP Counter Statistics	KN3GUC

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP GLBS'
```

```
KN3C115I STOP FOR COMPONENT GLBS ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

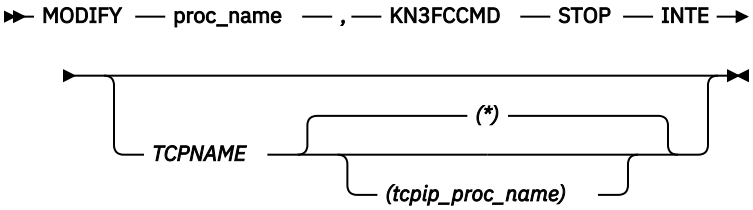
Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP  GLBS TCPNAME(TCPIP)'
KN3C115I STOP FOR COMPONENT GLBS ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP INTE

The KN3FCCMD STOP INTE command stops interface data link control (DLC) data collection.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this command applies to.

*****
Indicates that this applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Stops interface data link control (DLC) data collection.

The following attribute groups and workspaces are affected by this command:

Table 33. Attribute groups and workspaces affected by the KN3FCCMD STOP INTE command

Workspace name	Attribute group name	Attribute group name prefix
Data Link Control (DLC) Read and Write Queue Statistics	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
Enterprise HiperSockets Interfaces Overview	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise Interfaces Overview	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise OSA Interfaces Overview	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP INTE
KN3C115I STOP FOR COMPONENT INTE ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

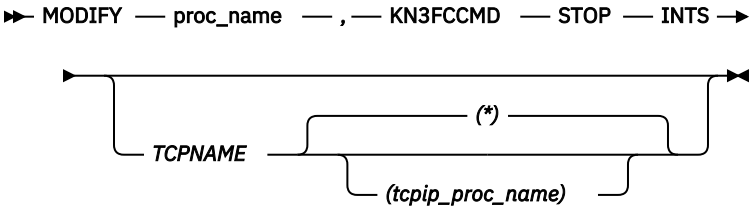
Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP  INTE TCPNAME(TCPIP)'
KN3C115I STOP FOR COMPONENT INTE ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP INTS

The KN3FCCMD STOP INTS command stops interface statistics data collection.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this command applies to.

*****
Indicates that this applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Stops interface statistics data collection. The following attribute groups and workspaces are affected by this command:

Table 34. Attribute groups and workspaces affected by the KN3FCCMD STOP INTS command

Workspace name	Attribute group name	Attribute group name prefix
Enterprise HiperSockets Interfaces Overview	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise Interfaces Overview	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise OSA Interfaces Overview	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS

Table 34. Attribute groups and workspaces affected by the KN3FCCMD STOP INTS command (continued)		
Workspace name	**Attribute group name**	**Attribute group name prefix**
Gateways and Devices	TCPIP Devices	KN3TDV
Interface Statistics	KN3 Interface Statistics	KN3IFS
Interface Statistics History	KN3 Interface Statistics	KN3IFS
Interface Status	KN3 Interfaces	KN3IFE
Interfaces	Interfaces	KN3TIF
Interfaces History	Interfaces	KN3TIF

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP INTS
KN3C115I STOP FOR COMPONENT INTS ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

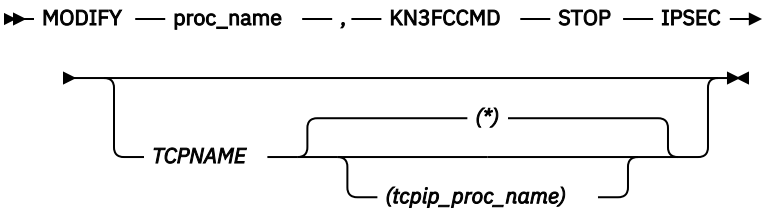
Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP  INTS TCPNAME(TCPIP)'
KN3C115I STOP FOR COMPONENT INTS ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP IPSEC

The KN3FCCMD STOP IPSEC command stops collection of IPSEC data.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this command applies to.

*****
Indicates that this applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Stops collection of IPSec data.

The following attribute groups and workspaces are affected by this command:

Table 35. Attribute groups and workspaces affected by the KN3FCCMD STOP IPSEC command		
Workspace name	**Attribute group name**	**Attribute group name prefix**
Current IP Filters	Current IP Filters	KN3IFC
Current IP Filters by Destination Address		
Current IP Filters by Filter Rule Definition Name		
Current IP Filters in Scan Order		
Dynamic IP Tunnels	Dynamic IP Tunnels	KN3ITD
Dynamic IP Tunnels by Destination Address		
Dynamic IP Tunnels by Filter Rule Definition Name		
Dynamic IP Tunnels by Tunnel ID		
Dynamic IP Tunnels with Byte Rate < 2048		
Dynamic IP Tunnel Statistics	IPSec Status	KN3ISS
IKE Tunnels	IKE Tunnels	KN3ITI
IKE Tunnels by Security Endpoint		
IKE Tunnels by Tunnel ID		
IKE Tunnels with Byte Rate < 1024		
Manual IP Tunnels	Manual IP Tunnels	KN3ITM
Manual IP Tunnels by Tunnel ID		

Usage

Sample output of this command using the default value of all TCP/IP address spaces is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP IPSEC'
KN3C110I STOP FOR COMPONENT IPSEC ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

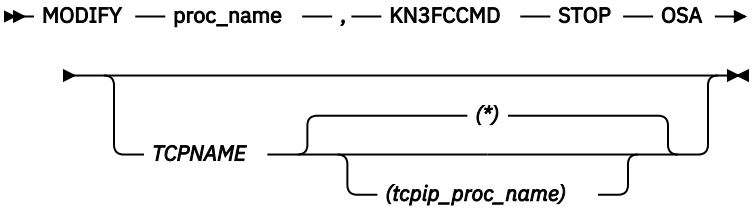
Sample output of this command using a specific TCP/IP address space is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP IPSEC  TCPNAME(TCPIP)'
KN3C110I STOP FOR COMPONENT IPSEC ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP OSA

The KN3FCCMD STOP OSA command stops data collection for OSA.

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this command applies to.

*****
Indicates that this applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Stops data collection for OSA. The following attribute groups and workspaces are affected by this command:

Table 36. Attribute groups and workspaces affected by the KN3FCCMD STOP OSA command

Workspace name	Attribute group name	Attribute group name prefix
Enterprise OSA-Express Channels Overview	OSA-Express Channels	KN3TCH
Enterprise OSA-Express Ports Overview	OSA-Express3 Ports Errors	KN3THE
	OSA-Express Ports	KN3TPO
	OSA 10 Gigabit Ports Errors	KN3TTE
	OSA 10 Gigabit Ports Summary	KN3TTS
OSA Channels	OSA-Express Channels	KN3TCH
OSA Ports	OSA-Express Ports	KN3TPO
OSA LPARs	OSA-Express LPARs	KN3TLP
OSA-Express2 10 Gigabit Port Errors	OSA-Express Channels	KN3TCH
OSA-Express2 10 Gigabit Port Control	OSA 10 Gigabit Ports Control	KN3TTC
OSA-Express2 10 Gigabit Ports Summary	OSA 10 Gigabit Ports Summary	KN3TTS
OSA-Express2 10 Gigabit Port Throughput Detail	OSA 10 Gigabit Ports Throughput	KN3TTT
OSA-Express3 Port Control	OSA-Express3 Ports Control	KN3THC
OSA-Express3 Port Errors	OSA-Express3 Ports Errors	KN3THE

Table 36. Attribute groups and workspaces affected by the KN3FCCMD STOP OSA command (continued)		
Workspace name	**Attribute group name**	**Attribute group name prefix**
OSA-Express3 Ports Summary	OSA-Express3 Ports Summary	KN3THS
OSA-Express3 Port Throughput Detail	OSA-Express3 Ports Throughput	KN3THT

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP OSA
KN3C115I STOP FOR COMPONENT OSA ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

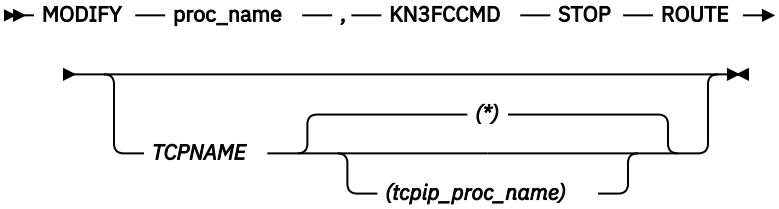
Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP  OSA TCPNAME(TCPIP)'
KN3C115I STOP FOR COMPONENT OSA ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP ROUTE

The KN3FCCMD STOP ROUTE command stops the monitoring of routing information, which is displayed in Tivoli Enterprise Portal in the Gateway workspace.

Format



Where:

TCPNAME

Identifies which TCP/IP address spaces this applies to.

*****

Indicates that this command applies to all TCP/IP address spaces.

tcpip_proc_name

Is the name of a TCP/IP address space in your environment.

Purpose

Stops the monitoring of routing information, which is displayed in Tivoli Enterprise Portal in the Gateway workspace. The TCPNAME option identifies which TCP/IP address spaces this command applies to.

The following attribute groups and workspaces are affected by this command:

Table 37. Attribute groups and workspaces affected by the KN3FCCMD STOP ROUTE command		
Workspace name	**Attribute group name**	**Attribute group name prefix**
Gateways and Devices	TCPIP Gateways	KN3TGA

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP ROUTE'
KN3C115I STOP FOR COMPONENT ROUTE ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

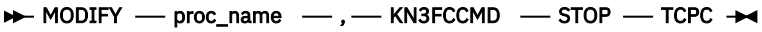
Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP ROUTE TCPNAME(TCPIP)'
KN3C115I STOP FOR COMPONENT ROUTE ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP TCPC

The KN3FCCMD STOP TCPC command stops the monitoring of TCP/IP and VTAM statistics.

Format



Purpose

Stops the monitoring of TCP/IP and VTAM statistics.

After you stop collection of TCP/IP and VTAM statistics, you must issue the following command to have collection started again:

```
MODIFY proc_name,KN3FCCMD START TCPC
```

If you want to change the value for either TCPCVIOU or TCPCINTV when you start TCPC collection, you must issue these commands:

```
MODIFY proc_name,KN3FCCMD INSTALL TCPC TCPCVIOU(vio_unit) TCPCINTV(collection_interval)
MODIFY proc_name,KN3FCCMD START TCPC
```

The following attribute groups and workspaces are affected by this command:

Table 38. Attribute groups and workspaces affected by the KN3FCCMD STOP TCPC command

Workspace name	Attribute group name	Attribute group name prefix
Active FTP Sessions	FTP Sessions	KN3FSE
Active TN3270 Server Connections for Selected Port	TN3270 Server Sess Avail	KN3TNA
Active FTP Transfers	TCPIP FTP	KN3FTP
Address Space	TCPIP Address Space	KN3TAS
Application Connections	TCPIP Connections	KN3TCN
Application Details	TCPIP Applications	KN3TAP
Application TCP Connections	TCPIP Details	KN3TCP
Application TCP Listeners	TCP Listener	KN3TCL
Application UDP Endpoints	UDP Connections	KN3UDP
Applications	TCPIP Applications	KN3TAP

Table 38. Attribute groups and workspaces affected by the KN3FCCMD STOP TCPC command (continued)		
Workspace name	**Attribute group name**	**Attribute group name prefix**
Command Log	KN3 Take Action Command Attributes	KN3CTA
	KN3 Take Action Command Response Attributes	KN3RTA
Connections	TCPIP Connections	KN3TCN
CSM Buffer Pools	CSM Storage	KN3CSM
Current IP Filters	Current IP Filters	KN3IFC
Current IP Filters by Destination Address		
Current IP Filters by Filter Rule Definition Name		
Current IP Filters in Scan Order		
Data Link Control (DLC) Read and Write Queue Statistics	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
Dynamic IP Tunnel Statistics	IPSec Status	KN3ISS
Dynamic IP Tunnels	Dynamic IP Tunnels	KN3ITD
Dynamic IP Tunnels by Destination Address		
Dynamic IP Tunnels by Filter Rule Definition Name		
Dynamic IP Tunnels by Tunnel ID		
Dynamic IP Tunnels with Byte Rate < 2048		
EE Connection Summary	EE Connection Details	KN3EED
	HPR Connections	KN3HPR
	UDP Connections	KN3UDP
EE Connection Details	EE Connection Details	KN3EED
EE Connections	EE Connection	KN3EEC
Enterprise Applications Health	TCPIP Applications	KN3TAP
Enterprise Connections Find	TCPIP Details	KN3TCP
Enterprise Connections Health	TCPIP Details	KN3TCP
Enterprise FTP Sessions Find	FTP Sessions	KN3FSE

Table 38. Attribute groups and workspaces affected by the KN3FCCMD STOP TCPC command (continued)		
Workspace name	**Attribute group name**	**Attribute group name prefix**
Enterprise FTP Sessions Overview	FTP Sessions	KN3FSE
	TCPIP FTP	KN3FTP
Enterprise FTP Transfers Find	TCPIP FTP	KN3FTP
Enterprise HiperSockets Interfaces Overview	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise Interfaces Overview	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise OSA-Express Channels Overview	OSA-Express Channels	KN3TCH
Enterprise OSA-Express Ports Overview	OSA-Express3 Ports Errors	KN3THE
	OSA-Express Ports	KN3TPO
	OSA 10 Gigabit Ports Errors	KN3TTE
	OSA 10 Gigabit Ports Summary	KN3TTS
Enterprise OSA Interfaces Overview	KN3 Interface Read Queue	KN3IFR
	KN3 Interface Write Queue	KN3IFW
	KN3 Interface Status	KN3IFE
	KN3 Interface Statistics	KN3IFS
Enterprise TN3270 Find	TN3270 Server Sess Avail	KN3TNA
FTP Session Details	FTP Sessions	KN3FSE
	TCPIP Details	KN3TCP
FTP Sessions	FTP Sessions	KN3FSE
FTP Sessions for selected file transfer	FTP Sessions	KN3FSE
FTP Transfer Details	TCPIP FTP	KN3FTP
	TCPIP Details	KN3TCP
FTP Transfers	TCPIP FTP	KN3FTP
FTP Transfers for link selected	TCPIP FTP	KN3FTP
FTP Transfers for Session	TCPIP FTP	KN3FTP
Gateways and Devices	TCPIP Devices	KN3TDV
	TCPIP Gateways	KN3TGA
HPR Connections	HPR Connections	KN3HPR

Table 38. Attribute groups and workspaces affected by the KN3FCCMD STOP TCPC command (continued)		
Workspace name	**Attribute group name**	**Attribute group name prefix**
ICMP Statistics	KN3 ICMP Global Counters	KN3GCG
	KN3 ICMP Type Counters	KN3GCT
Interface Statistics	KN3 Interface Statistics	KN3IFS
Interface Statistics History	KN3 Interface Statistics	KN3IFS
Interface Status	KN3 Interface Status	KN3IFE
Interfaces	Interfaces	KN3TIF
Interfaces History		
IP Statistics	KN3 IP Counter Statistics	KN3GIC
	KN3 IP General Statistics	KN3GIG
IKE Tunnels	IKE Tunnels	KN3ITI
IKE Tunnels by Security Endpoint		
IKE Tunnels by Tunnel ID		
IKE Tunnels with Byte Rate < 1024		
IKE Tunnels Statistics	IPSec Status	KN3ISS
IPSec Status		
Manual IP Tunnels	Manual IP Tunnels	KN3ITM
Manual IP Tunnels by Tunnel ID		
NetView for z/OS: Packet Trace – Start	KN3 DWL to 3270	KN3DWL3270
NetView for z/OS: Packet Trace – Stop	KN3 DWL to 3270	KN3DWL3270
OSA Channels	OSA-Express Channels	KN3TCH
OSA-Express2 10 Gigabit Port Errors	OSA 10 Gigabit Ports Errors	KN3TTE
OSA-Express2 10 Gigabit Port Control	OSA 10 Gigabit Ports Control	KN3TTC
OSA-Express2 10 Gigabit Ports Summary	OSA 10 Gigabit Ports Summary	KN3TTS
OSA-Express2 10 Gigabit Port Throughput Detail	OSA 10 Gigabit Ports Throughput	KN3TTT
OSA-Express3 Port Control	OSA-Express3 Ports Control	KN3THC
OSA-Express3 Port Errors	OSA-Express3 Ports Errors	KN3THE
OSA-Express3 Ports Summary	OSA-Express3 Ports Summary	KN3THS

Table 38. Attribute groups and workspaces affected by the KN3FCCMD STOP TCPC command (continued)		
Workspace name	**Attribute group name**	**Attribute group name prefix**
OSA-Express3 Port Throughput Detail	OSA-Express3 Ports Throughput	KN3THT
OSA LPARs	OSA-Express LPARs	KN3TLP
OSA Port Interfaces	OSA Port Interfaces	KN3TIF
OSA Ports	OSA-Express Ports	KN3TPO
TCP Connection Details	TCPIP Details	KN3TCP
TCP Connections	TCPIP Details	KN3TCP
TCP Connections Link	TCPIP Details	KN3TCP
TCP Listeners	TCP Listener	KN3TCL
TCP Statistics	KN3 TCP Counter Statistics	KN3GTC
TCP/IP Memory Statistics	TCPIP Memory Statistics	KN3TPV
TCP/IP Stack Layers	TCPIP Stack Layer	KN3TSL
TCP/IP Stack Layers History	TCPIP Stack Layer	KN3TSL
TCP/IP Summary	TCPIP Address Space	KN3TAS
TCP/IP Summary History	TCPIP Address Space	KN3TAS
TN3270 Active Server Session Summary for Remote IP	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Availability	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Pair	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Summary for Remote IP		
TN3270 Server Session Summary for SNA Name		
TN3270 Server Sessions for Remote IP		
TN3270 Server Sessions for SNA Name		
TN3270 Server Session Details	TN3270 Server Sess Avail	KN3TNA
	TN3270 Response Time Buckets	KN3TNB
TN3270 Server Sessions	TN3270 Server Sess Avail	KN3TNA
UDP Endpoints	UDP Connections	KN3UDP
UDP Statistics	KN3 UDP Counter Statistics	KN3GUC

Usage

Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP TCPC'
KN3CT004 TCP/IP STATISTICS COLLECTOR IS TERMINATING
KN3CT104 TCP/IP SERVICE THREAD IS TERMINATING
KN3CT107 TCP/IP SERVICE THREAD COMPLETED TERMINATION
KN3CT007 TCP/IP STATISTICS COLLECTOR COMPLETED TERMINATION.
KN3FC000 KN3FCCMD PROCESSING COMPLETE
KN3IR005 TCP SUBNODE DEREGISTERED FOR ORIGINNODE TCPIP:0239
KN3IR006 TCP SUBNODE MONITOR STOPPED FOR ORIGINNODE TCPIP:0239
KN3IR005 VTAM SUBNODE DEREGISTERED FOR ORIGINNODE VTAM:0239
KN3IR006 VTAM SUBNODE MONITOR STOPPED FOR ORIGINNODE VTAM:0239
```

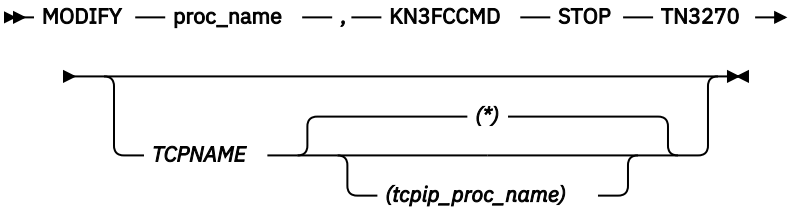
Note: Buffer Pool And VTAM Environment Data Collection continues to be collected by the SNAC collector, but the following data collection is stopped with the STOP TCPC command:

- Enterprise Extender and High Performance Routing Statistics Collection
- ALL High Performance Routing Connections Collection
- CSM Buffer Reporting Collection
- TCP/IP Connection and Application Performance Statistics Collection
- IP Security Statistics
- Collection Routing Table Statistics Collection
- TN3270 Server Statistics Collection
- FTP Data Collection

KN3FCCMD STOP TN3270

The KN3FCCMD STOP TCPC command stops the monitoring of TN3270 server sessions

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this applies to.

*****
Indicates that this command applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Stops the monitoring of TN3270 server sessions. The TCPNAME option identifies which TCP/IP address spaces this applies to.

The following attribute groups and workspaces are affected by this command:

Table 39. Attribute groups and workspaces affected by the KN3FCCMD STOP TN3270 command		
Workspace name	**Attribute group name**	**Attribute group name prefix**
Active TN3270 Server Connections for Selected Port workspace	TN3270 Server Sess Avail	KN3TNA
Enterprise TN3270 Find workspace	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Availability	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Sessions	TN3270 Server Sess Avail	KN3TNA
TN3270 Active Server Session Summary for Remote IP	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Details	TN3270 Server Sess Avail	KN3TNA
	TN3270 Response Time Buckets	KN3TNB
TN3270 Server Session Pair	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Summary for Remote IP	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Session Summary for SNA Name	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Sessions for Remote IP	TN3270 Server Sess Avail	KN3TNA
TN3270 Server Sessions for SNA Name	TN3270 Server Sess Avail	KN3TNA

Usage

Sample output 1:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP TN3270'
KN3C115I STOP FOR COMPONENT TN3270 ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

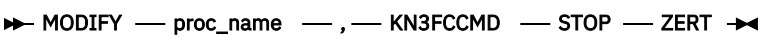
Sample output 2:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP  TN3270 TCPNAME(TCPIP)'
KN3C115I STOP FOR COMPONENT TN3270 ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP ZERT

The KN3FCCMD STOP ZERT command stops the monitoring of zERT summary data.

Format



Purpose

Stops the monitoring of zERT summary data.

The following attribute groups and workspaces are affected by this command:

Table 40. Attribute groups and workspaces affected by the KN3FCCMD STOP ZERT command		
Workspace name	**Attribute group name**	**Attribute group name prefix**
zERT ALL Sessions	zERT Common Session Data	KN3ZCM
zERT SSH Sessions	zERT SSH Session Data	KN3ZSH
zERT TLS Sessions	zERT TLS Session Data	KN3ZTL
zERT IPSec Sessions	zERT IPSec Session Data	KN3ZIP
zERT Session Distinguished Names	zERT DNs Session Data	KN3ZDN

Usage

Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP ZERT'
KN3C116I STOP FOR COMPONENT ZERT ACCEPTED.
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

Attributes

Use the IBM Z OMEGAMON Network Monitor attributes to build table views, charts, and situations that monitor the performance of your network.

Associating attributes with table views: There is a direct relationship between the IBM Z OMEGAMON Network Monitor attributes and table views. An attribute group corresponds to a table view. For each attribute group, there are one or more attribute items. The attribute items correspond to columns in a table view. To find general information about an attribute group, select it from the Help Table of Contents.

The table views provide real-time information for many of the attributes. These views are available to you at any time, independent of whether you are using IBM Z OMEGAMON Network Monitor to monitor situations.

IBM Z OMEGAMON Network Monitor provides Tivoli Enterprise Portal workspaces that are accessed from the Navigator and 3270 workspaces access from the Enhanced 3270 user interface. Each of these workspaces displays views that can be altered or replaced, to meet your needs. Each workspace is associated with one or more attribute tables.

Unsigned integers: When an attribute is described as "an unsigned integer" or "an unsigned two-byte integer", the value will be displayed as a positive value in the Tivoli Enterprise Portal and the IBM Z OMEGAMON Network Monitor. However, the IBM Tivoli Data Warehouse stores all integers as signed values. In addition, the TEMS will evaluate situations with all integer attributes as signed integers. A signed integer may have a maximum value of 2,147,483,647 (x'7FFFFFFF'). A signed two-byte integer may have a maximum value of 32,767 (x'7FFF'). To test for an unsigned value over 2,147,483,647 in a situation, you must instead test for a value less than zero (<0).

CSM Storage Attributes

Use the CSM storage attributes to create situations that monitor buffer pools that are shared between SNA and TCP/IP for each z/OS system image. CSM buffer pool data are displayed if the network systems programmer chose to collect CSM Buffer Data when configuring the IBM Z OMEGAMON Network Monitor monitoring agent.

Collection Time The time and date of the data sampling. This time is displayed in the following format

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Current Page Fixed Storage In Use The amount of page fixed-storage currently in use, stored in kilobytes. Page fixed-storage includes ECSA storage and 31-bit and 64-bit backed data space. The format is 64-bit signed integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Maximum ECSA Storage Allowed The maximum number of Extended Common System Area (ECSA) storage, stored in kilobytes, allowed. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Maximum Page Fixed Storage Allowed The maximum page fixed-storage allowed, stored in kilobytes. Page fixed-storage includes ECSA storage and 31-bit and 64-bit backed data space. This value is stored as a 64-bit signed integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Maximum Page Fixed Storage Since IPL The maximum page fixed storage allocated since IPL, stored in kilobytes. Page fixed-storage includes ECSA storage and 31-bit and 64-bit backed data space. This value is stored as a 64-bit signed integer. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Percent ECSA Allocated Storage The percentage of Extended Common System Area (ECSA) storage currently allocated compared to the maximum ECSA storage allowed. The format is an integer between 0 and 100 inclusive.

Percent ECSA In Use Storage The percentage of ECSA storage currently in use compared to the maximum ECSA storage allowed. The format is an integer between 0 and 100 inclusive.

Percent Page Fixed Storage Allocated The percentage of page fixed storage currently allocated, as compared to the maximum page fixed storage allowed. The format is an integer between 0 and 100 inclusive.

Percent Page Fixed Storage In Use The percentage of page fixed storage currently in use, as compared to the maximum page fixed storage allowed. The format is an integer between 0 and 100 inclusive.

Storage Allocated Across DSP Pools The cumulative storage, stored in kilobytes, allocated across all Data Space Pool (DSP) pools. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated Across ECSA Pools The cumulative storage, stored in kilobytes, allocated across all Extended Common System Area (ECSA) pools. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated Across Pools The cumulative storage, stored in kilobytes, allocated across all pools. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated To DSP16K Pool The amount of CSM storage, stored in kilobytes, allocated to the DSP16K pool. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated To DSP180K Pool The amount of CSM storage, stored in kilobytes, allocated to the DSP180K pool. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated To DSP32K Pool The amount of CSM storage, stored in kilobytes, allocated to the DSP32K pool. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated To DSP4K Pool The amount of CSM storage, stored in kilobytes, allocated to the DSP4K pool. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated To DSP60K Pool The amount of CSM storage, stored in kilobytes, allocated to the DSP60K pool. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated To ECSA16K Pool The amount of CSM storage, stored in kilobytes, allocated to the ECSA16K pool. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated To ECSA180K Pool The amount of CSM storage, stored in kilobytes, allocated to the ECSA180K pool. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated To ECSA32K Pool The amount of CSM storage, stored in kilobytes, allocated to the ECSA32K pool. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated To ECSA4K Pool The amount of CSM storage, stored in kilobytes, allocated to the ECSA4K pool. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated To ECSA60K Pool The amount of CSM storage, stored in kilobytes, allocated to the ECSA60K pool. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Free Across DSP Pools The cumulative storage free, stored in kilobytes, across all DSP pools. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Free Across ECSA Pools The cumulative storage free, stored in kilobytes, across all ECSA pools. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Free Across Pools The cumulative storage free, stored in kilobytes, across all pools. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage In Use Across DSP Pools The cumulative storage in use, stored in kilobytes, across all DSP pools. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage In Use Across ECSA Pools The cumulative storage in use, stored in kilobytes, across all ECSA pools. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage In Use Across Pools The cumulative storage in use, stored in kilobytes, across all pools. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

Current IP Filters Attributes

Use the Current IP Filters attributes to display IP filter information for the filters currently in use by the TCP/IP stack.

Action The action to be applied to the packet when filter condition is met. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = PERMIT
- 2 = DENY
- 3 = IPSEC

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Create Time The time when the filter was created, based on how the filter was created.

- For a statically defined filter originating from the Policy Agent configuration, this field represents the time that the filter was first defined to the current instance of the Policy Agent. Filters of this type have the value of **1** meaning Policy for the Filter Set attribute.
- For a filter originating from the TCP/IP profile, this field represents the time that the profile filter configuration was last replaced. Filters of this type have the value of **0** meaning Default for the Filter Set attribute.
- For dynamically defined filters, this field is blank. Dynamically defined filters have a value of **DYNAMIC**, **NATTDYN**, or **NRF**.

This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Destination Address Destination IP address or addresses affected by the current filter. This address may be in IPv4 or IPv6 format. Filters apply to either IPv4 addresses or IPv6 addresses, but not both. If the filter applies to all destination IP addresses, the field will be displayed as blank and a value of "0" is stored in the table. If the filter is for a range of destination IP addresses, this is the lower address in the range. The format is a UTF-8 encoded character string of up to 45 characters.

Destination Address Granularity Indicates the origin of the destination address used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter.
- 1 = FILTER: Destination address for the tunnel is from the filter definition.
- 2 = PACKET: Destination address for the tunnel is from the packet requiring the tunnel activation.

Destination Port Granularity Indicates the origin of the destination port used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter.
- 1 = FILTER: The destination address for the tunnel is from the filter definition.
- 2 = PACKET: The destination address for the tunnel is from the packet requiring the tunnel activation.

A value of FILTER indicates the destination port comes from the filter definition. A value of PACKET indicates the destination port comes from the packet. This field is significant if the filter type indicates this is a dynamic anchor filter. If the filter is not a dynamic anchor filter, a value of zero (0) is stored and blank is displayed in the field.

Direction Indicates the direction of the IP traffic. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = INBOUND
- 2 = OUTBOUND

Filter Rule Definition Name The name specified for an IP filter rule definition. This column is stored as a 48-character string.

Filter Set Identifies which filter set is currently in use by the TCP/IP stack. One of two filter sets may be in use at any time.

- The default filter set, which is made up of filters defined in the TCP/IP profile.
- The policy filter set, which is made up of filters defined in the Policy Agent configuration files.

This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Default
- 1 = Policy

Filter Use Indicator The value in this column is used to identify the filters that are matching the most packets. Values 1 to 4 are used to identify the 5 filters with the most matches, the most denies by DENY and the most denies by mismatch. Value 5 is used to identify filters 6 to 100 with the most matches. A query can return the 5 filters with the most matches by using a where clause like:

```
(Filter Use Indicator = 1) OR (Filter Use Indicator = 3)
```

A query can return the 100 filters with the most matches by adding another OR clause to the previous condition:

```
(Filter Use Indicator = 5)
```

This value is stored as a one character string and is displayed as a string. Valid values are:

- 1 = MostMatched: The filter is one of the 5 most-matched filters.
- 2 = MostDENY: The filter is one of the 5 filters with a DENY action that has the most matched packets. This also means that the filter has denied the most packets due to DENY.
- 3 = MostMatchedAndMostDeny: The filter is both one of the five most matched filters and one of the five filters that has denied the most packets by DENY.
- 4 = MostMismatched: The filter is one of the 5 filters that has the most mismatched packets.
- 5 = MostMatchedAndMostMismatched: The filter is both one of the five most matched filters and one of the five most mismatched filters.
- 6 = MostMatched6to100: The filter is one of the 6 to 100 filters that has the most matches.

Group Name The name of the filter group that the filter rule is associated with. This field is stored as blanks if the filter rule is not associated with a filter group. The format is an alphanumeric string of up to 48 characters.

ICMP Code The Internet Control Message Protocol (ICMP) code that qualifies the ICMP Type Code attribute. This field is displayed as blank if the filter applies to all ICMP codes. This field is defined as an integer of up to 3 digits. 0 is a defined ICMP code. The value in this field is not meaningful unless a non-blank value appears in the ICMP Type Code field.

ICMP Type Code The Internet Control Message Protocol (ICMP) code that identifies the ICMP traffic to be filtered. This field is displayed as blank if the filter applies to all ICMP types. This field is defined as an integer of up to 3 digits. 0 is a defined ICMP Type Code.

IP Address Version The version of the IP addresses being used for the traffic descriptor and the security endpoints. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4: The traffic descriptor and the security endpoints are using IPv4 addresses.
- 1 = IPv6: The traffic descriptor and the security endpoints are using IPv6 addresses.

Last Page The value in this column saves the page number of the last page of filters. It is used in queries to determine whether more pages of filters are available to retrieve. This value is stored as a 4-character string, with 0000 representing the first page.

Local Start Action Name The name specified for an IpLocalStartAction statement that is referenced by this filter. The IpLocalStartAction statement specifies how to determine the local IP, remote IP, local port, remote port, and protocol specification for the local activation of a dynamic virtual private network (VPN). This field is stored as blanks if no local start action name is associated with this filter. This field is stored as a 48-character string.

Log Indicator Indicates which packets to log. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE: Do not log any packets.
- 1 = PERMIT: Log packets permitted by the filter.
- 2 = DENY: Log packets denied by the filter.
- 3 = ALL: Log all packets that match this filter.

Lower Destination Address The lower address in a range of IP addresses being filtered. If the filter is for a range of destination IP addresses, this is the lower address in the range. Otherwise, this field is stored as blanks. The format is a string of up to 45 characters.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Lower Destination Port If the filter is for a range of destination IP port addresses, this is the low value for the range. This field is stored as blanks if the filter is not for a range of IP port addresses and applies to all ports. This value is represented as a 5-character string.

Lower Source Port If the filter is for a range of IP ports, this is the low value for the range. This field is stored as blanks if the filter is not for a range of IP port addresses and applies to all ports. This value is represented as a 5-character string.

NAPT Indicator Indicates whether a network address port translation (NAPT) has been detected in front of the IPSec peer. This field is significant for filters with a type of dynamic. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

NAT Indicator Indicates whether network address translation (NAT) has been detected in front of the IPSEC peer. This field is significant for filters with a type of dynamic. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

NAT Traversal Gateway Indicates that the peer is acting as an IPSec gateway and the tunnel uses UDP encapsulation. This field is significant for dynamic filters. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

NATT Client ID If the peer is behind a NAT and a gateway and the peer supplied a client ID, indicates the NAT traversal gateway (NATT) client ID. This field contains an IPv4 dotted decimal address if the NATT Client ID Type is IPv4_ADDR. This field contains an IPv4 dotted decimal address if the NATT Client ID Type is IPv4_ADDR_RANGE. The address in the field is the lower address for the range. This field will have an MD5 hash of the client ID if the NATT Client ID Type is OTHER. If the NATT Client ID Type is 0, this field is stored as blanks. The format is a string of up to 32 characters.

NATT Client ID Type If the peer is behind a NAT and a gateway and the peer supplied a client ID, indicates what type of client ID was supplied. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 1 = IPv4_ADDR

- 2 = IPv4_ADDR_RANGE
- 3 = IPv4_ADDR_RANGE
- 4 = OTHER

NATT Peer UDP Port If this is a dynamic filter for UDP-encapsulated NAT Traversal (NATT) traffic, this is the UDP port for the IKE peer. Otherwise, this field is stored as blanks. This field is represented as a character string of up to 5 characters.

NRF Original Port If this is a NAT Traversal Resolution Filter (NRF), this field contains the original remote port for the TCP or UDP traffic. Otherwise this field is stored as blanks. This field is represented as a character string of up to 5 characters.

On Demand Indicator Indicates whether on-demand activations are allowed for the traffic described for this filter. On demand activations are activations of tunnels initiated automatically when traffic requiring the use of the tunnel is sent. This field is meaningful if the filter type is one of the following:

- Dynamic anchor filter
- Dynamic filter
- Network Address Translation (NAT) Traversal anchor filter
- NAT Traversal dynamic filter

This value is stored as an integer and displayed as a string. The field contains a zero (0) when the filter type is not one of these. Valid values are:

- 0 = <blank>
- 1 = NOT_PERMITTED
- 2 = PERMITTED

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

OSPF Type Identifies Open Shortest Path First (OSPF) protocol traffic to be filtered. This field is displayed as blanks if the filter applies to all OSPF traffic. The format is an integer.

Packets Denied by Mismatch The number of packets denied due to a mismatch with this filter action during the most recent collection interval. The format is an integer.

Packets Matched The total number of packets that matched this filter condition and action during the most recent collection interval. The format is an integer.

Page The value in this column is used to group the filters into logical pages. Each page contains 500 filters. Links are implemented so that you can request all the filters on a particular page. This value is stored as a 4-character string, with 0000 representing the first page.

Percent Total Packets Denied by Mismatch The percentage of total packets denied due to an action mismatch by this filter compared to the total packets denied due to an action mismatch by all filters on the TCP/IP stack since the stack was started. The format is a number between 0 and 100 inclusive.

Percent Total Packets Matched The percentage of total packets matched by this filter compared to the total packets matched by all filters on the TCP/IP stack since the stack was started. The format is a number between 0 and 100 inclusive.

Protocol Granularity Indicates the origin of the protocol used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter.
- 1 = FILTER: The protocol for the tunnel is from the filter definition.
- 2 = PACKET: The protocol for the tunnel is from the packet requiring the tunnel activation.

Protocol Number IP protocol number to match in the IPv4 or IPv6 header of packets. If the filter applies to all IP protocols, this field is stored as blanks. This value is expressed as a string of up to 3 characters. 0 is a valid IP protocol number.

Rule ID This column concatenates the Filter Rule Definition Name, Rule Tag and Tunnel ID into a single string that can be used to uniquely identify filter rules. The Rule ID is used to identify rules on graph views so that the values displayed on the graphs can be correlated with the rows in the table view. The three components of the Rule ID are separated by a colon (:) character. If the rule is not associated with a Tunnel ID, that component of the ID is omitted. This column is represented as a character string of 106 characters.

Rule Tag The filter rule definition name extension. The extension is assigned by the stack to identify related rules derived from the same definition. The column is stored as an 8-character string.

Scope The type of traffic that this filter applies to. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = LOCAL
- 2 = ROUTED
- 3 = SCOPEALL.

Security Class The IP filter security class. This filter is applied to all packets traversing the IP interfaces, and these interfaces are associated with security classes. This value is expressed as an integer between 0 and 255 inclusive. A value of zero (0) means that all security classes are filtered. If a non-zero value is specified for the security class, then the filter applies to data traversing all interfaces associated with the specified security class.

Sequence Number The value in this column is used to ensure that filters are displayed in the order that the network management interface (NMI) returns them. This value is represented as an integer.

Source Address Source IP address or addresses that the filter applies to. Filters apply to either IPv4 addresses or IPv6 address, but not both. If the filter applies to all destination IP addresses, the field will be displayed as blank and a value of "0" is stored in the table. If the filter is for a range of source IP addresses, this field displays the lower address in the range. The format is a UTF-8 encoded character string of up to 45 characters.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Source Address Granularity Indicates the origin of the source address used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter.
- 1 = FILTER: The source address for the tunnel is from filter definition.
- 2 = PACKET: The source address for the tunnel is from the packet requiring the tunnel activation.

Source Port Granularity Indicates the origin of the source port used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter.
- 1 = FILTER: The source port for tunnel is from the filter definition.
- 2 = PACKET: The source port for tunnel is from the packet requiring the tunnel activation

State Current filter state. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = ACTIVE
- 1 = INACTIVE

SWSA Shadow Indicator Indicates whether the filter originated from a distributing stack (SHADOW) or the local stack (NOT_SHADOW). This value is only meaningful for dynamic filters. If the filter type is not dynamic, the value is saved as 0 and displayed as blank (Tivoli Enterprise Portal) or 0 (3270). This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>

- 1 = NOT_SHADOW
- 2 = SHADOW

A value of SHADOW indicates that the filter originated from a distributing stack.

Sysplex Name The name of the sysplex that the monitored system is part of.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCP Connect Indicates what types of TCP connect attempts are to be filtered. TCP connect attempts (SYN packets) in the direction opposite that specified in this field do not match this filter. This field is meaningful for generic or anchor filters only. It is zero (0) when the filter is not one of these types. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 1 = INBOUND
- 2 = OUTBOUND

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Packets Denied by Mismatch The total number of packets denied due to a mismatch with this filter action since the start of the TCP/IP stack. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Packets Denied by Mismatch (in G)** column to calculate the cumulative number of packets denied by mismatch. The format is an integer.

Total Packets Denied by Mismatch (in G) The total number of packets denied due to a mismatch with this filter action since the start of the TCP/IP stack, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the **Total Packets Denied By Mismatch** column to calculate the cumulative number of packets denied by mismatch. The format is an integer.

Total Packets Matched The total number of packets that matched this filter condition and action since the start of the TCP/IP stack. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Packets Matched (in G)** column to calculate the cumulative number of packets matched. The format is an integer.

Total Packets Matched (in G) The total number of packets that matched this filter condition and action since the start of the TCP/IP stack, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the **Total Packets Matched** column to calculate the cumulative number of packets matched. The format is an integer.

Tunnel ID Identifier for the associated tunnel. The tunnel ID is generated by the stack. It is not unique. Several related tunnels may have the same tunnel ID. The related tunnels are different instances of the same security association. Usually the related instances exist due to the expiration and refresh of tunnels. This field will be blank if filter is not associated with a tunnel. The ID is a character string of up to 48 characters.

Type Indicates the filter type. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = GENERIC
- 2 = MANUAL
- 3 = DYNANCHOR
- 4 = DYNAMIC
- 5 = NATTANCHOR
- 6 = NATTDYN
- 7 = NRF
- 8 = DEFENSIVE

Update Time The time when the filter was updated, based on how the filter was created.

- For a statically defined filter originating from the Policy Agent configuration, this field represents the time that the filter's attributes were last updated in the current instance of the Policy Agent. Filters of this type have the value of **1** meaning Policy for the Filter Set attribute.
- For a filter originating from the TCP/IP profile, this field represents the time that the profile filter configuration was last replaced. Filters of this type have the value of **0** meaning Default for the Filter Set attribute.
- For dynamically defined filters, this field is blank. Dynamically defined filters have a filter Type of **DYNAMIC**, **NATTDYN**, or **NRF**.

This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Upper Destination Address The higher address in a range of IP addresses being filtered. If the filter is for a range of destination IP addresses, this is the higher address in the range. Otherwise, this field is stored as blanks. The format is a string of up to 45 characters.

Upper Destination Port If the filter is for a range of destination IP port addresses, this is the high value for the range. This field is stored as blanks if the filter is not for a range of IP port addresses and applies to all ports. This value is represented as a 5-character string.

Upper NATT Client ID If the peer is behind a NAT and a gateway and the peer supplied a client ID, indicates the upper address range of the NAT traversal gateway (NATT) client ID. This field contains an IPv4 dotted decimal address if the **NATT Client ID Type** is IPv4_ADDR_RANGE. If the **NATT Client ID Type** is 0, 1, or 4, this field is stored as blanks. This field is a character string of up to 15 characters.

Upper Source Address If the filter is for a range of source IP addresses, this is the high value for the range. If the filter does not apply to a range of destination IP addresses, the field is displayed as blank and a value of zero "0" is stored in the table. The format is a UTF-8 encoded character string of up to 45 characters.

Upper Source Port If the filter is for a range of source IP port addresses, this is the high value for the range. This field is stored as blanks if filter is not for a range of IP port addresses and applies to all ports. This value is represented as a 5-character string.

VPN Action Name The name specified on a virtual private network (VPN) action definition statement. The VPN action describes how to protect the traffic that flows on the tunnel. It specifies attributes of the tunnel, such as what type of encryption to use. The name is a character string of up to 48 characters.

Dynamic IP Tunnels Attributes

Use the Dynamic IP Tunnels attributes to display the availability and performance statistics for dynamic IP tunnels known to the Internet Key Exchange (IKE) daemon and the TCP/IP stack.

Activation Method Indicates how the tunnel was activated. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = USER: User activation from the command line.
- 2 = REMOTE: Remote activation from the IPSec peer.
- 3 = ONDEMAND: On-demand activation caused by IP traffic.
- 5 = TAKEOVER: Sysplex-Wide Security Associations (SWSA) activation as a result of a Dynamic Virtual IP Addressing (DVIPA) takeover.
- 6 = AUTOACT: Auto-activation.

Authentication Algorithm Identifies the authentication algorithm used for this tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 38 = MD5
- 39 = SHA1

Authentication Protocol Identifies the authentication protocol to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 51 = AH
- 50 = ESP

Bytes The number of inbound and outbound bytes for this tunnel during the most recent time interval. The format is an integer.

Byte Rate The number of inbound or outbound bytes, per minute, for this tunnel during the most recent time interval. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day

- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Current Life Size The number of bytes of data that have traversed the tunnel since the tunnel was activated. This value is zero (0) if no life size was negotiated for the tunnel. The format is an integer.

Dest NAT-OA Payload The destination network address translation original address (NAT-OA) payload. NAT-OA payloads are exchanged only for certain UDP-encapsulated tunnels. During NAT traversal negotiations, the Internet Key Exchange (IKE) peer sends the known destination IPv4 address. If NAT traversal negotiation does not occur, or if peer does not send a source NAT-OA payload, this column is blank. This column is stored as a 15-character string.

Destination Address Destination IP address for data protected by the tunnel. This value may be an IPv4 or IPv6 address. If the traffic protected by the tunnel may have any destination IP address, this field is displayed as blanks and stored as "0". If the traffic protected by the tunnel is a range of destination IP addresses, the value displayed is the lower address in the range. The format is a UTF-8 encoded character string of up to 45 characters

Destination Port Destination port for traffic protected by the tunnel. If the tunnel protects data for all destination ports, this value is 0. This field is represented by a 5-character string.

Diffie-Hellman Group Diffie-Hellman group used to generate keying material for the tunnel. Each group identifies the number of bits to be used in a prime number that is used to generate keying material. This column is blank if PFS (perfect forward security) was not negotiated for the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 99 = <blank>
- 0 = NONE
- 1 = GROUP1
- 2 = GROUP2
- 5 = GROUP5
- 14 = GROUP14

Encapsulation Mode Encapsulation mode to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = TUNNEL
- 2 = TRANSPORT

Encryption Algorithm Tunnel encryption algorithm. This field is undefined if the tunnel state is PENDING or INCOMPLETE. A value of 99 is assigned to the field in this case and blanks are displayed. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 3 = 3DES
- 11 = NULL
- 12 = AES
- 18 = DES
- 99 = <blank>

Extended State Indicates progress of tunnel negotiation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = INIT: No key exchange messages have been initiated.
- 1 = KEP: Key exchange messages have been initiated.

- 2 = DONE: All key exchange messages have been completed, and the tunnel is usable for traffic.
- 3 = PENDING_NOTIFY: Key exchange messages have been completed, waiting to receive connection notification.
- 4 = PENDING_START: Waiting for the activation of an Internet Key Exchange (IKE) tunnel.

Filter Rule Definition Name The name specified for the filter rule definition that this tunnel is associated with. This column is stored as a 48-character string.

Inbound Authentication SPI Tunnel inbound authentication security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This field is an unsigned 4-byte integer and is displayed in hexadecimal. This field is undefined and displayed as blanks if the state of the tunnel is PENDING or INCOMPLETE.

Inbound Bytes The number of inbound bytes for this tunnel during the most recent time interval. The format is an integer.

Inbound Encryption SPI Tunnel inbound encryption security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and is displayed in hexadecimal. This field is undefined and displayed as blanks if the state of the tunnel is PENDING or INCOMPLETE.

Inbound Packets The number of inbound packets for this tunnel during the most recent time interval. The format is an integer.

Initiation Indicator Indicates if the local security endpoint may initiate dynamic tunnel negotiations with the remote security endpoint. Either security endpoint may initiate refreshes regardless of the value of this indicator. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

IP Address Version The version of the IP addresses being used for the traffic descriptor and the security endpoints. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4: The traffic descriptor and the security endpoints are using IPv4 addresses.
- 1 = IPv6: The traffic descriptor and the security endpoints are using IPv6 addresses.

Life Expiration Time The time at which the tunnel will expire. This column is blank if no life time was negotiated. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute

- S = Second
- m = Millisecond

Life Refresh Time The time at which the tunnel is refreshed. This column is blank if no life time was negotiated. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Life Size The number of bytes of data that may traverse the tunnel over the life of the tunnel. This value is zero (0) if no life size was negotiated for the tunnel. The format is an integer.

Local Client ID The Internet Security Associations Key Management Protocol (ISAKMP) identity of local client. A string containing an identifier as described by Local Client ID Type. Some of the ID strings can get as long as 2048 characters. The ID is always truncated at 100 characters. If no IDs are exchanged, this fields contains blanks. The format is a string of up to 100 characters.

Local Client ID Type Internet Security Associations Key Management Protocol (ISAKMP) identity type for the local client ID as defined in RFC 2407. If client IDs were not exchanged during negotiation, this column is blank. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = IPv4_ADDR
- 2 = FQDN
- 3 = USER_FQDN
- 4 = IPv4_ADDR_SUBNET
- 5 = IPv6_ADDR
- 6 = IPv6_ADDR_SUBNET
- 7 = IPv4_ADDR_RANGE
- 8 = IPv6_ADDR_RANGE
- 9 = DER_ASN1_DN
- 10 = DER_ASN1_GN
- 11 = KEY_ID

Local Dynamic VPN Rule Name The name specified on a z/OS Communications Server Policy Agent LocalDynVpnRule configuration statement. The statement describes traffic that is to be protected by a tunnel that is activated on demand using the ipsec command or when the Internet Key Exchange (IKE) daemon or the TCP/IP stack is started or both. This field is stored as blanks if the tunnel is not associated with a local rule. The name is a character string of up to 48 characters.

Local NAT Indicator Indicates if a NAT has been detected in front of the local security endpoint. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Local Security Endpoint The IP address of the local security endpoint responsible for negotiating the tunnel. The format is a UTF-8 encoded character string of up to 45 characters.

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Outbound Authentication SPI Tunnel outbound authentication security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and is displayed in hexadecimal. This field is undefined and displayed as blanks if the state of the tunnel is PENDING or INCOMPLETE.

Outbound Bytes The number of outbound bytes for this tunnel during the most recent time interval. The format is an integer.

Outbound Encryption SPI Tunnel outbound encryption security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and is displayed in hexadecimal. This field is undefined and displayed as blanks if the state of the tunnel is PENDING or INCOMPLETE.

Outbound Packets The number of outbound packets for this tunnel during the most recent time interval. The format is an integer.

Packet Rate The number of inbound or outbound packets, per minute, for this tunnel during the most recent time interval. The format is an integer.

Packets The number of inbound and outbound packets for this tunnel during the most recent time interval. The format is an integer.

Parent IKE Tunnel ID Tunnel ID for this parent IKE (Phase 1) tunnel. The Internet Key Exchange (IKE) tunnel is used to negotiate the IP tunnel. This field is represented as a 48-character string.

Pending New Indicator Pending new activation indicator. If set, this field indicates that dynamic IP tunnel is in the pending state and it represents a new activation rather than a refresh. If it is not set, the tunnel is either not in pending state or is not a new activation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Protocol The IP protocol number for the data to be carried in the tunnel. A value of zero (0) indicates that tunnel protects data for any protocol. The format is an integer representing an Internet Engineering Task Force (IETF)-defined protocol number.

Refresh Life Size The number of bytes that may traverse the tunnel before a refresh is needed. This value is zero (0) if no life size was negotiated. The format is an integer.

Remote Client ID Internet Security Associations Key Management Protocol (ISAKMP) identity of remote client. A string containing an identifier as described by Remote Client ID Type. Some of the ID strings can get as long as 2048 characters. The ID is always truncated at 100 characters. If no IDs are exchanged, this field contains blanks. The format is a string of up to 100 characters.

Remote Client ID Type Internet Security Associations Key Management Protocol (ISAKMP) identity type for the remote client ID as defined in RFC 2407. If the client IDs were not exchanged during negotiation, this column is blank. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = IPv4_ADDR
- 2 = FQDN
- 3 = USER_FQDN
- 4 = IPv4_ADDR_SUBNET
- 5 = IPv6_ADDR
- 6 = IPv6_ADDR_SUBNET
- 7 = IPv4_ADDR_RANGE
- 8 = IPv6_ADDR_RANGE
- 9 = DER_ASN1_DN
- 10 = DER_ASN1_GN
- 11 = KEY_ID

Remote IKE UDP Port The IKE UDP port of the remote security endpoint. This column is blank when UDP encapsulation is not being used by the tunnel. This column is stored as a 5-character string.

Remote NAPT Indicator Indicates if a network address port translation (NAPT) has been detected in front of the remote security endpoint. It is possible that an NAPT may exist but is detected only as a NAT. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote NAT Indicator Indicates if a NAT has been detected in front of the remote security endpoint. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote NAT Traversal Gateway Indicator Indicates if the remote security endpoint is acting as a NAT traversal gateway. If the remote security endpoint is acting as a NAT traversal gateway, the tunnel uses UDP encapsulation and the remote security endpoint is acting as an IPSec gateway. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote Security Endpoint The IP address of the remote security endpoint responsible for negotiating the tunnel. The format is a UTF-8 encoded character string of up to 45 characters.

Remote zOS Indicator Indicates if the remote peer is a z/OS system. This can be detected only if NAT traversal is enabled. Even if NAT traversal is enabled, it is possible for the remote peer to be a z/OS system and this indicator not to be set. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Source Address Source IP address for data protected by this tunnel. This value may be an IPv4 or IPv6 address. If the traffic protected by the tunnel may have any destination IP address, this field is displayed as blanks and stored as "0". If the traffic protected by the tunnel is a range of destination IP addresses, the value displayed is the lower address in the range. The format is a UTF-8 encoded character string of up to 45 characters.

Source NAT-OA Payload The source network address translation original address (NAT-OA) payload. NAT-OA payloads are exchanged only for certain UDP-encapsulated tunnels. During NAT traversal negotiations, the Internet Key Exchange (IKE) peer sends the source IPv4 address that it is aware of. If NAT traversal negotiation did not occur, or if peer did not send a source NAT-OA payload, this column is blank. This column is stored as a 15-character string.

Source Port Source port for traffic protected by tunnel. If the tunnel protects data for all source ports, this value is 0. This field is represented by a 5-character string.

State Current state of tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 2 = PENDING: Waiting for negotiation to start.
- 3 = INCOMPLETE: Negotiation in progress.
- 4 = ACTIVE: Tunnel is active and ready for use.
- 5 = EXPIRED: Expired and cannot be used.

SWSA Shadow Indicator Sysplex-Wide Security Associations shadow indicator. If this value is set, the tunnel is a SWSA shadow tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Sysplex Name The name of the sysplex that the monitored system is part of.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Bytes The total number of inbound and outbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Bytes (in G)** column to calculate the total bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Bytes (in G) The total number of inbound and outbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the **Total Bytes** column to calculate the total bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Inbound Bytes The total number of inbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Inbound Bytes (in G)** column to calculate the total inbound bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Inbound Bytes (in G) The total number of inbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the **Total Inbound Bytes** column to calculate the total inbound bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Inbound Packets The total number of inbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Inbound Packets (in G)** column to calculate the total inbound packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Inbound Packets (in G) The total number of inbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the **Total Inbound Packets** column to calculate the total inbound packets for the

tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Outbound Bytes The total number of outbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Outbound Bytes (in G)** column to calculate the total outbound bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Outbound Bytes (in G) The total number of outbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Outbound Bytes column to calculate the total outbound bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Outbound Packets The total number of outbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Outbound Packets (in G)** column to calculate the total outbound packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Outbound Packets (in G) The total number of outbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the **Total Outbound Packets** column to calculate the total outbound packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Packets The total number of inbound and outbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Packets (in G)** column to calculate the total packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Packets (in G) The total number of inbound and outbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the **Total Packets** column to calculate the total packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Tunnel ID Tunnel identifier. This identifier is generated by TCP/IP and is not unique. Multiple related tunnels may have the same tunnel ID. The format is an alphanumeric string of up to 48 characters.

Upper Destination Address If the traffic protected by the tunnel is a range of destination IP addresses, this is the upper address in the range. This value may be an IPv4 or IPv6 address. If the traffic protected by the tunnel is not a range of addresses, this field is displayed as blanks and stored as "0". The format is a UTF-8 encoded character string of up to 45 characters.

Upper Source Address If the traffic protected by the tunnel is a range of source IP addresses, this is the upper address in the range. This may be an IPv4 or IPv6 address. If the traffic protected by the tunnel is not a range of addresses or is all addresses, this field is stored as blanks. The format is a UTF-8 encoded character string of up to 45 characters.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

VPN Action Name The name specified on a virtual private network (VPN) action definition statement. The VPN action describes how to protect the traffic that flows through the tunnel. It specifies attributes of the tunnel, such as what type of encryption to use. The format of the name is a character string of up to 48 characters.

VPN Life Expiration Time The time at which the tunnel should no longer be refreshed. This column is blank (Tivoli Enterprise Portal) or zeros (3270) if no life time was negotiated for the VPN (security attributes implemented by the tunnel). This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

EE Connections Attributes

Use the Enterprise Extender (EE) Connections attributes to create situations that monitor performance data for EE links. This attribute group applies to an EE link where the local IP address for that EE link resides on a monitored z/OS system image.

Bytes Received The number of SNA bytes received during the most recent time interval. The format is a long long integer.

Bytes Received (deprecated) The number of SNA bytes received during the most recent time interval as an integer. When the value in the **Bytes Received** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Received (in GB)** field and the remainder is stored in the **Bytes Received** field. The format is an integer.

Bytes Received (in GB) (deprecated) The number of SNA bytes received during the most recent time interval, divided by 1,073,741,824. When the value in the **Bytes Received** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Received (in GB)** field and the remainder is stored in the **Bytes Received** field. The format is an integer.

Bytes Sent The number of SNA bytes sent during the most recent time interval. The format is a long long integer.

Bytes Sent (deprecated) The number of SNA bytes sent during the most recent time interval as an integer. When the value in the Bytes Sent field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Sent (in GB)** field and the remainder is stored in the **Bytes Sent** field. The format is an integer.

Bytes Sent (in GB) (deprecated) The number of SNA bytes sent during the most recent time interval, divided by 1,073,741,824. When the value in the **Bytes Sent** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Sent (in GB)** field and the remainder is stored in the **Bytes Sent** field. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

EE Connection ID The unique identifier of this Enterprise Extender connection. The format is a hexadecimal string up to 16 characters in length.

Local IP Address The local IP address for this EE connection. The format is an alphanumeric string no longer than 45 characters.

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Packet Retransmission Rate The number of HPR network-layer packets that was retransmitted over this EE connection, per minute, during the most recent time interval. The format is an integer.

Packets Received The number of HPR network-layer packets that was received during the most recent time interval. The format is an integer.

Packets Retransmitted The number of HPR network-layer packets that was retransmitted during the current time interval. The format is an integer.

Packets Sent The number of HPR network-layer packets that was sent during the most recent time interval. The format is an integer.

Percent Packets Retransmitted The percentage of HPR network-layer packets that was retransmitted during the most recent time interval. The format is an integer.

PU Name The name of the local physical unit (PU). The format is an alphanumeric string no longer than 8 characters.

Receive Byte Rate The number of bytes received, per minute, during the most recent time interval. The format is an integer.

Receive Packet Rate The number of HPR network-layer packets that was received, per minute, during the most recent time interval. The format is an integer.

Remote IP Address The remote IP address for this EE connection. The format is an alphanumeric string no longer than 45 characters.

RTP Pipes The number of RTP pipes flowing over this EE connection. The format is an integer.

Sessions The number of LU-to-LU sessions flowing over this EE connection. The format is an integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

Transmit Byte Rate The number of bytes sent, per minute, during the most recent time interval. The format is an integer.

Transmit Packet Rate The number of HPR network-layer packets that was sent, per minute, during the most recent time interval. The format is an integer.

VTAM STC Name The VTAM started task name. The format is an eight-character string.

EE Connections Details Attributes

Use the Enterprise Extender (EE) Connections Details attributes to create situations that monitor performance data for EE links. This attribute group applies to an EE link where the local IP address for that EE link resides on a monitored z/OS system image.

Bytes Received The number of SNA bytes received during the most recent time interval. The format is a long long integer.

Bytes Received (deprecated) The number of SNA bytes received during the most recent time interval as an integer. When the value in the Bytes Received field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Received (in GB**) field and the remainder is stored in the **Bytes Received** field. The format is an integer.

Bytes Received (in GB) (deprecated) The number of SNA bytes received during the most recent time interval, divided by 1,073,741,824. When the value in the **Bytes Received** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Received (in GB)** field and the remainder is stored in the **Bytes Received** field. The format is an integer.

Bytes Sent The number of SNA bytes sent during the most recent time interval. The format is a long long integer.

Bytes Sent (deprecated) The number of SNA bytes sent during the most recent time interval as an integer. When the value in the Bytes Sent field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Sent (in GB)** field and the remainder is stored in the **Bytes Sent** field. The format is an integer.

Bytes Sent (in GB) (deprecated) The number of SNA bytes sent during the most recent time interval, divided by 1,073,741,824. When the value in the **Bytes Sent** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Sent (in GB)** field and the remainder is stored in the **Bytes Sent** field. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month

- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

EE Connection ID The unique identifier of this Enterprise Extender connection. The format is an alphanumeric string no longer than 16 characters.

Local IP Address The local IP address for this EE connection. The format is an alphanumeric string no longer than 45 characters.

Local/Remote port The local and remote port. The local port is always the same as the remote port. The format is an integer.

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Packets Received The number of HPR network-layer packets that was received during the most recent time interval. The format is an integer.

Packets Sent The number of HPR network-layer packets that was sent during the most recent time interval. The format is an integer.

PU Name The name of the local physical unit (PU). The format is an alphanumeric string no longer than 8 characters.

Receive Byte Rate The number of SNA bytes received, per minute, for the Type Of Service (TOS) value during the most recent time interval. The format is an integer.

Receive Packet Rate The number of HPR network-layer packets that was received, per minute, for the Type Of Service (TOS) value during the most recent time interval. The format is an integer.

Remote IP Address The remote IP address for this EE connection. The format is an alphanumeric string no longer than 45 characters.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

Transmit Byte Rate The number of SNA bytes sent, per minute, for the Type Of Service (TOS) value during the most recent time interval. The format is an integer.

Transmit Packet Rate The number of HPR network-layer packets that was sent, per minute, for the Type Of Service (TOS) value during the most recent time interval. The format is an integer.

Type Of Service The type of service that is used for TCP/IP communication. These are the possible Type Of Service values:

- Low
- Medium
- High
- Network
- Signal

FTP Sessions Attributes

Use the FTP Sessions attributes to create situations that monitor the sessions from either a remote client to a z/OS FTP server or from a z/OS client to a remote FTP server.

Application Name The name of the FTP application. The format is an alphanumeric string no longer than 8 characters.

ASID The z/OS address space ID of the address space that opened the socket. This value is displayed as a 4-digit hexadecimal number.

Cipher Specification The current cipher specification for this connection when the security mechanism is TLS or AT-TLS. This value is used for the data encryption or decryption. See the description of the TTLSCipherParms statement in the "Policy Agent and Policy Applications" chapter of the *IBM z/OS Communications Server: IP Configuration Reference* v1.12 or later book for a list of possible cipher values. This value is stored as a long integer and displayed as a string. Valid values for this integer are:

- blank = 0X00000000
- SSL_RC4_US = 0X0000F0F1
- SSL_RC4_EXPORT = 0X0000F0F2
- SSL_RC2_US = 0X0000F0F3
- SSL_RC2_EXPORT = 0X0000F0F4
- SSL_DES_US = 0X0000F0F6
- SSL_3DES_US = 0X0000F0F7
- SSL_NULL_MD5 = 0X0001F0F1
- SSL_NULL_SHA = 0X0001F0F2
- SSL_RC4_MD5_EX = 0X0001F0F3
- SSL_RC4_MD5 = 0X0001F0F4
- SSL_RC4_SHA = 0X0001F0F5
- SSL_RC2_MD5_EX = 0X0001F0F6
- SSL_DES_SHA = 0X0001F0F9
- SSL_3DES_SHA = 0X0001F0FA
- SSL_AES_128_SHA = 0X0001F2C6
- SSL_AES_256_SHA = 0X0001F3F5
- TLS_RC4_128_WITH_MD5 = 0X0002F0F1
- TLS_RC4_128_EXPORT40_WITH_MD5 = 0X0002F0F2
- TLS_RC2_CBC_128_CBC_WITH_MD5 = 0X0002F0F3
- TLS_RC2_CBC_128_CBC_EXPORT40_WITH_MD5 = 0X0002F0F4
- TLS_DES_64_CBC_WITH_MD5 = 0X0002F0F6
- TLS_DES_192_EDE3_CBC_WITH_MD5 = 0X0002F0F7
- TLS_NULL_WITH_NULL_NULL = 0X0003F0F0
- TLS_RSA_WITH_NULL_MD5 = 0X0003F0F1
- TLS_RSA_WITH_NULL_SHA = 0X0003F0F2
- TLS_RSA_EXPORT_WITH_RC4_40_MD5 = 0X0003F0F3
- TLS_RSA_WITH_RC4_128_MD5 = 0X0003F0F4
- TLS_RSA_WITH_RC4_128_SHA = 0X0003F0F5
- TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 = 0X0003F0F6
- TLS_RSA_WITH_DES_CBC_SHA = 0X0003F0F9
- TLS_RSA_WITH_3DES_EDE_CBC_SHA = 0X0003F0C1
- TLS_DH_DSS_WITH_DES_CBC_SHA = 0X0003F0C3
- TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA = 0X0003F0C4
- TLS_DH_RSA_WITH_DES_CBC_SHA = 0X0003F0C6
- TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA = 0X0003F1F0
- TLS_DHE_DSS_WITH_DES_CBC_SHA = 0X0003F1F2
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA = 0X0003F1F3
- TLS_DHE_RSA_WITH_DES_CBC_SHA = 0X0003F1F5

- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA = 0X0003F1F6
- TLS_RSA_WITH_AES_128_CBC_SHA = 0X0003F2C6
- TLS_DH_DSS_WITH_AES_128_CBC_SHA = 0X0003F3F0
- TLS_DH_RSA_WITH_AES_128_CBC_SHA = 0X0003F3F1
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA = 0X0003F3F2
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA = 0X0003F3F3
- TLS_RSA_WITH_AES_256_CBC_SHA = 0X0003F3F5
- TLS_DH_DSS_WITH_AES_256_CBC_SHA = 0X0003F3F6
- TLS_DH_RSA_WITH_AES_256_CBC_SHA = 0X0003F3F7
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA = 0X0003F3F8
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA = 0X0003F3F9

Client User ID The local user name (login name) of the client. This column applies to client transfers only. The format is an alphanumeric string no longer than 8 characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

FTP Session ID The unique identifier for this FTP session. The format is an alphanumeric string no longer than 16 characters.

FTP Type Identifies whether this FTP session is using the FTP client or the FTP server on the local system. This value is stored as an integer and displayed as a string. This field displays the string. Valid values are:

- Client = 0
- Server = 1

FTP Type Int Identifies whether this FTP session is using the FTP client or the FTP server on the local system. This value is stored as an integer. This field displays the integer. Valid values are:

- 0 = Client
- 1 = Server

Local IP Address The local IP address for this FTP control connection. The format is an alphanumeric string no longer than 45 characters.

Local Port The local port for the FTP control connection. The format is a four-byte integer.

Local Port (deprecated) The local port for the FTP control connection, as a two-byte integer.

Local Port String The local port for the FTP control connection as a string. The format is a string up to five characters in length.

Login Failure Reason Code The reason returned when a login fails. This value is stored and displayed as a number.

When the **FTP Type** value is Server, the following reason codes are possible:

- 01: Password not valid
- 02: Password has expired
- 03: User ID has been revoked
- 04: User does not have access to server
- 05: FTCHKPWD exit routine rejected login
- 06: Too many incorrect passwords specified
- 07: Group ID process failed
- 08: User ID is unknown
- 09: Certificate not valid
- 10: Client name does not match user name

When the **FTP Type** value is Client, the following reason codes are possible. These client values are documented in the *z/OS Communications Server: IP User's Guide and Commands*. Additional information about the failure might be available in that book.

- 01: Internal error
- 02: Server error
- 04: Invalid parameter
- 05: Input stream open failed
- 06: Already connected
- 07: Usage error
- 08: Connect failed
- 09: Connection timeout
- 10: Session error
- 11: Invalid ID or password or account
- 12: Input error
- 13: Input EOF
- 14: Not found
- 15: Invalid FTP environment
- 16: FTP not enabled
- 17: Security authentication or negotiation failure
- 18: File access
- 19: Cannot read file
- 20: Cannot write file
- 21: Conversion error
- 22: Proxy error
- 23: SQL error

- 24: Unspecified client error

Login Failure Reason Description The reason that the login failed. This value is stored as a number and displayed as a string.

When the **FTP Type** value is Server, the following reason codes are possible:

- Password not valid = 1
- Password expired = 2
- User ID has been revoked = 3
- User does not have access to server = 4
- FTCHKPWD exit routine rejected login = 5
- Too many incorrect passwords specified = 6
- Group ID process failed = 7
- User ID is unknown = 8
- Certificate not valid = 9
- Client name does not match user name = 10

When the **FTP Type** value is Client, the following reason codes are possible. The FTP client error codes, found in parentheses below, are documented in the *z/OS Communications Server: IP User's Guide and Commands*. Additional information about the failure might be available in that book.

- Internal error = 101 (01)
- Server error = 102 (02)
- Invalid parameter = 104 (04)
- Input stream open failed = 105 (05)
- Already connected = 106 (06)
- Usage error = 107 (07)
- Connect failed = 108 (08)
- Connection timeout = 109 (09)
- Session error = 110 (10)
- Invalid ID or password or account = 111 (11)
- Input error = 112 (12)
- Input EOF = 113 (13)
- Not found = 114 (14)
- Invalid FTP environment = 115 (15)
- FTP not enabled = 116 (16)
- Security authentication or negotiation failure = 117 (17)
- File access = 118 (18)
- Cannot read file = 119 (19)
- Cannot write file = 120 (20)
- Conversion error = 121 (21)
- Proxy error = 122 (22)
- SQL error = 123 (23)
- Unspecified client error = 124 (24)

Login Method The current login method for this connection. This value is stored as a single character and displayed as a string. The following are valid:

- C= Certificate

- P = Password
- T= Kerberos_Ticket
- U= Undefined

NMI FTP Enhancements IBM internal use only.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Remote IP Address The remote IP address for the FTP control connection. The format is an alphanumeric string no longer than 45 characters.

Remote Port The remote port for the FTP control connection. The format is a four-byte integer.

Remote Port (Deprecated) The remote port for the FTP control connection, as a two-byte integer.

Remote Port String The remote port for the FTP control connection as a string. The format is a string up to five characters in length.

Security Mechanism The current security mechanism for this connection. This value is stored as a single character and displayed as a string. The following are valid:

- A = AT_TLS
- G = GSSAPI
- N = None
- T = TLS

Security Protocol Level The current security protocol level for this connection when the security mechanism is TLS or AT-TLS. The format is a character string.

Server Logging Session ID The ID that uniquely identifies sessions between z/OS FTP servers and FTP clients. The format is a 15-character string. The identifier is generated from FTP daemon job name, followed by a 5-digit number in range 00000-99999. The value is displayed in the SYSLOGD file log entries when FTP activity logging is enabled.

Session Duration The duration of the session. This value is stored in seconds and displayed as a time value (for example, 4.00000s or 4m 20s).

Session End The date and time when the control session ended. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour

- M = Minute
- S = Second
- m = Millisecond

When the session has not ended, this value is stored as a character string of zeros and displayed as blank.

Session End Reason Code A code indicating the reason that the control connection ended. This value is stored and displayed as a number.

When the **FTP Type** value is Server, the following reason codes are possible:

- 0: Normal session end
- 1: Security authentication or negotiation failure
- 2: Socket or network error
- 3: Client closed control connection unexpectedly
- 4: Invalid sequence read from control connection

When the **FTP Type** value is Client, the following reason codes are possible. The FTP client error codes are documented in the *z/OS Communications Server: IP User's Guide and Commands*. Additional information about the failure might be available in that book.

- 0: Normal session end
- 1: Internal error
- 2: Server error
- 4: Invalid parameter
- 5: Input stream open failed
- 6: Already connected
- 7: Usage error
- 8: Connect failed
- 9: Connection timeout
- 10: Session error
- 11: Invalid ID or password or account
- 12: Input error
- 13: Input EOF
- 14: Not found
- 15: Invalid FTP environment
- 16: FTP not enabled
- 17: Security authentication or negotiation failure
- 18: File access
- 19: Cannot read file
- 20: Cannot write file
- 21: Conversion error
- 22: Proxy error
- 23: SQL error
- 24: Unspecified client error

Session End Reason Description The description of the session end reason code. This value is stored as an integer and displayed as a string.

When the **FTP Type** value is Server and Client, the following reason codes are possible:

- Normal session end = 0

When the **FTP Type** value is Server, the following reason codes are possible:

- Password not valid = 1
- Password expired = 2
- User ID has been revoked = 3
- User does not have access to server = 4
- FTCHKPWD exit routine rejected login = 5
- Too many incorrect passwords specified = 6
- Group ID process failed = 7
- User ID is unknown = 8

When the **FTP Type** value is Client, the following reason codes are possible. These FTP client error codes are documented in the *z/OS Communications Server: IP User's Guide and Commands* Additional information about the failure might be available in that manual.

- Internal error = 101
- Server error = 102
- Invalid parameter = 104
- Input stream open failed = 105
- Already connected = 106
- Usage error = 107
- Connect failed = 108
- Connection timeout = 109
- Session error = 110
- Invalid ID or password or account = 111
- Input error = 112
- Input EOF = 113
- Not found = 114
- Invalid FTP environment = 115
- FTP not enabled = 116
- Security authentication or negotiation failure = 117
- File access = 118
- Cannot read file = 119
- Cannot write file = 120
- Conversion error = 121
- Proxy error = 122
- SQL error = 123
- Unspecified client error = 124

Session Protection Level The current session protection level for this connection. This value is stored as a character and displayed as a string. Valid values are:

- **C** = Clear
- **N** = None
- **P** = Private
- **S** = Safe
- **U** = Unknown

Session Start The date and time at which the control session was established. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

State The status of this FTP session. This value is stored as an integer and displayed as a number. The following are valid values:

- **0** Unknown - In the history file, the value was Active during historical collection.
- **1** Inactive - A close record was received for this open record.
- **2** Active - No close record was received.
- **4** Complete - The record was closed.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCP Control Connection ID The TCP connection ID for the connection being used for the control connection. This value is displayed as an 8-digit hexadecimal number.

This value is displayed as a hexadecimal number that uniquely identifies the TCP connection being used for the FTP control connection. The TCP connection ID (or resource ID) is displayed under the Local Socket column adjacent to the IP address in the output of a NETSTAT command.

TCPIP STC Name The TCP/IP job name. The format is an alphanumeric string no longer than 8 characters.

Total Bytes Transferred The number of bytes in all files sent and received since the FTP connection started. The format is a long long integer.

Total Files Transferred The number of files sent and received since the FTP connection started. The format is an integer.

Transfer Protection Level The current transfer protection level for this connection. This value is stored as a single character and displayed as a string. The following are valid:

- C = Clear
- N = None
- P = Private

- S = Safe
- U = Unknown

User ID on Server The user name that was used to log in to the server. The format is an alphanumeric string no longer than 8 characters. When the actual user ID is longer then 8 characters, it is truncated. See User ID on Server Extended for longer user IDs.

User ID on Server Extended The user name that was used to log in to the server. The format is an alphanumeric string no longer than 63 characters.

HPR Connections Attributes

Use the HPR Connections attributes to create situations that monitor the performance data of High Performance Routing (HPR) connections. This attribute group applies to connections where one end point resides on a monitored z/OS system image.

Activation Time The date and time when the RTP pipe was activated. This time is displayed on the interface in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Actual Throughput Rate The actual throughput rate, specified in kilobits per second, for this RTP pipe. The rate is calculated as a sliding-window throughput rate. The format is an integer.

Alive Timer The value, in seconds, of the liveness timer. The format is an integer.

Allowed Throughput Rate The allowed throughput rate, in kilobits per second, for this RTP pipe. The rate is calculated as a sliding-window throughput rate. The format is an integer.

ARB Mode The current status of this RTP pipe. This value is stored as an integer and displayed as a string. The current status of this RTP pipe is expressed as:

- **0 - Green** - Data transmission is occurring without significant network congestion.
- **1 - Yellow** - Data transmission is being slowed because network congestion has been detected.
- **2 - Red** - Data transmission is being affected by severe network congestion that might result in packet loss.

Bytes Received The number of SNA bytes received during the most recent time interval. The format is a long long integer.

Bytes Received (deprecated) The number of SNA bytes received during the most recent time interval, as an integer. When the value in the **Bytes Received** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Received (in GB)** field and the remainder is stored in the **Bytes Received** field. The format is an integer.

Bytes Received (in GB) (deprecated) The number of SNA bytes received during the most recent time interval, divided by 1,073,741,824. When the value in the **Bytes Received** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Received (in GB)** field and the remainder is stored in the **Bytes Received** field. The format is an integer.

Bytes Sent The number of SNA bytes sent during the most recent time interval. The format is a long long integer.

Bytes Sent (deprecated) The number of SNA bytes sent during the most recent time interval, as in integer. When the value in the Bytes Sent field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Sent (in GB**) field and the remainder is stored in the **Bytes Sent** field. The format is an integer.

Bytes Sent (in GB) (deprecated) The number of SNA bytes sent during the most recent time interval, divided by 1,073,741,824. When the value in the **Bytes Sent** field exceeds 1,073,741,823 (1GB), the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Sent (in GB)** field and the remainder is stored in the **Bytes Sent** field. The format is an integer.

Class of Service Name The name of the original class of service for this RTP pipe. The format is an alphanumeric string no longer than 12 characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Compare Throughput Rate A comparison of the initial and actual throughput rates. The following are valid values:

- **1** - The actual throughput rate is less than initial throughput rate.
- **0** - The actual throughput rate is not less than the initial throughput rate.

Current ARB Threshold The current receiver threshold in microseconds. This threshold is not applicable for the original ARB algorithm. The format is an integer.

EE Connection ID The unique identifier of the Enterprise Extender connection that this HPR connection is associated with. The format is a hexadecimal string up to 16 characters in length. A value of 0000000000000000 indicates that this HPR connection is not associated with an EE connection.

Initial Throughput Rate The initial throughput rate, specified in kilobits per second, for this RTP pipe. The format is an integer.

Local CP Name The fully qualified (with network ID) name of the local control point (CP). The format is an alphanumeric string no longer than 17 characters.

Local RTP PU Name The name of the local RTP physical unit (PU). The format is an alphanumeric string no longer than 8 characters.

Local TCID The transport connection identifier (TCID) for the local RTP connection. The format is an alphanumeric string no longer than 32 characters.

Maximum ARB Threshold The maximum receiver threshold in microseconds. This threshold is not applicable for the original ARB algorithm. The format is an integer.

Minimum ARB Threshold The minimum receiver threshold in microseconds. This threshold is not applicable for the original ARB algorithm. The format is an integer.

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Out of Sequence Buffers The number of buffers that are in the out-of-sequence queue. The format is an integer.

Packet Retransmission Rate The number of HPR network-layer packets that was retransmitted, per minute, during the most recent time interval. The format is an integer.

Packets Queued The number of HPR network-layer packets that are in the waiting-to-send queue. The format is an integer.

Packets Received The number of HPR network-layer packets that was received during the most recent time interval. The format is an integer.

Packets Retransmitted The number of HPR network-layer packets that was retransmitted during the current time interval. The format is an integer.

Packets Sent The number of HPR network-layer packets that was sent during the most recent time interval. The format is an integer.

Path Switch Timestamp The date and time when the most recent path switch occurred. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year

- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

When no path switch has occurred, this value is stored as a character string of zeros and displayed as blank.

Path Switch Trigger The reason for the most recent path switch. This value is stored as an integer and displayed as a string. Valid values for Path Switch Trigger are:

- 1 = XMIT stall switch
- 2 = TGINOP
- 4 = SRT retries
- 6 = No NCB
- 8 = Modify RTP command
- 10 = Auto path switch
- 12 = Partner initiated
- 14 = MNPS initiated

Path Switches The number of path switches that was initiated by the remote or local nodes. The format is an integer.

Percent Packets Retransmitted The percentage of HPR network-layer packets that was retransmitted during the most recent time interval. The format is an integer.

Receive Byte Rate The number of bytes received, per minute, during the most recent time interval. The format is an integer.

Receive Packet Rate The number of HPR network-layer packets that was received, per minute, during the most recent time interval. The format is an integer.

Remote CP Name The fully qualified (with network ID) name of the remote control point (CP). The format is an alphanumeric string no longer than 17 characters.

Remote TCID The transport connection identifier (TCID) for the remote RTP connection. The format is an alphanumeric string no longer than 32 characters.

Response Time Variance The average round-trip time variance, in milliseconds, or the smooth deviation for this RTP pipe. The format is an integer.

Sessions The number of LU to LU sessions using this RTP pipe. The format is an integer.

Smoothed Round Trip Time The round-trip delay for this RTP connection, in units of 1/1000th of a second (ms). The format is an unsigned integer.

SNA Links The network ID and control point (CP) names of APPN nodes traversed by the RTP pipe. The format is a string up to 175 characters in length.

SNA Links Count The number of SNA links that are traversed by this RTP pipe. The format is an integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

Transmit Byte Rate The number of bytes sent, per minute, during the most recent time interval. The format is an integer.

Transmit Packet Rate The number of HPR network-layer packets that was sent, per minute, during the most recent time interval. The format is an integer.

Unacknowledged Buffers The number of buffers that are in the unacknowledged queue. The format is an integer.

Unacknowledged Buffers High Water Mark The high-water mark for the Unacknowledged Buffers column. The format is an integer.

Unacknowledged Buffers High Water Mark Time Stamp The date and time when the value for the high-water mark was collected.This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

VTAM STC Name The VTAM started task name. The format is an eight-character string.

Interfaces Attributes

Use the Interfaces attributes to display performance and identifying information for a specific interface.

Notes®:

1. If the address space being monitored is running z/OS v1.11 or earlier, the values for this attribute group are retrieved using SNMP. If the address space being monitored is running z/OS v1.12 or later, the values for this attribute group are retrieved using the z/OS Communications Server callable network management interface (NMI).
2. If you are viewing this workspace on z/OS v1.12, non-strategic interfaces report only status information. Performance-related attributes show a value of zero (0). The strategic interfaces have one of the following Interface Types:
   - Loopback
   - OSA-Express Queued Direct I/O (QDIO) Ethernet
   - HiperSockets
   - Multipath Channel Point-To-Point (MPCPTP)

   Only these attributes will show data for non-strategic interfaces:
   - Interface Name
   - Interface Associated Name

- Interface Status
- Device and Datapath Status
- Interface Index
- Interface Type
- Last Status Change timestamp

3. It is possible for the value of the Percent Inbound Packets in Error attribute to actually exceed 100%. This occurrence is due to the way inbound packets and errors are counted in the Communications Server TCP/IP stack. Many errors are encountered and recorded before the stack can determine how many packets were received, or whether the packets are unicast, multicast, or broadcast. In this case, the TCP/IP stack records the error, but not the inbound packet. In unusual circumstances, the number of errors recorded might exceed the number of inbound packets recorded.

Bandwidth Utilization The total percentage of bandwidth being used during the most recent sample. This value is the total of the **Transmit Bandwidth Utilization** and the **Receive Bandwidth Utilization** values. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Current State The current operational state of the interface. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = Up
- 2 = Down
- 3 = Testing
- 4 = Unknown
- 5 = Dormant
- 6 = NotPresent
- 7 = LowerLayerDown
- 8 = DAD_Pending

Description A textual string containing information about the interface. This string includes the name of the manufacturer, the product name, and the version of the interface hardware or software or both. The format is a string up to 255 characters in length.

Inbound Packet Discard Rate The number of packets received that have been discarded, per minute, during the most recent sample. This rate applies to packets that were chosen to be discarded, though no errors had been detected to prevent them from being delivered to a higher-layer protocol. One reason for discarding packets might be to free up buffer space. The format is an integer.

Inbound Packets Discarded The number of packets received that have been discarded during the most recent sample. This number includes packets that were chosen to be discarded, though no errors had been detected to prevent them from being delivered to a higher-layer protocol. One reason for discarding packets might be to free up buffer space. The format is an integer.

Inbound Packets in Error The number of inbound packets that was not received during the most recent time interval because of errors. The format is an integer.

Interface Capacity An estimate, in bits per second (z/OS v1r11 or earlier) or million bits per second (z/OS v1r12 or later), of the current data rate capacity for the interface. The format is an integer.

Interface Index The interface index associated with this interface. The format is an unsigned integer.

Interface Name The textual name of the interface. The value of this object is the name of the interface that is assigned by the local device. The format is a string up to 16 characters in length.

Interface Type The type of interface. This value is stored as an integer and displayed as a string. Valid values are:

- other=1
- regular1822=2
- hdh1822=3
- ddnX25=4
- rfc877x25=5
- ethernetCsmacd=6
- iso88023Csmacd=7
- iso88024TokenBus=8
- iso88025TokenRing=9
- iso88026Man=10
- starLan=11
- proteon10Mbit=12
- proteon80Mbit=13
- hyperchannel=14
- fddi=15
- lapb=16
- sdlc=17
- ds1=18
- e1=19
- basicISDN=20
- primaryISDN=21
- propPointToPointSerial=22
- ppp=23
- softwareLoopback=24
- eon=25

- ethernet3Mbit=26
- nsip=27
- slip=28
- ultra=29
- ds3=30
- sip=31
- frameRelay=32
- rs232=33
- para=34
- arcnet=35
- arcnetPlus=36
- atm=37
- miox25=38
- sonet=39
- x25ple=40
- iso88022llc=41
- localTalk=42
- smdsDxi=43
- frameRelayService=44
- v35=45
- hssi=46
- hippi=47
- modem=48
- aal5=49
- sonetPath=50
- sonetVT=51
- smdsIcip=52
- propVirtual=53
- propMultiplexor=54
- ieee80212=55
- fibreChannel=56
- hippiInterface=57
- frameRelayInterconnect=58
- aflane8023=59
- aflane8025=60
- cctEmul=61
- fastEther=62
- isdn=63
- v11=64
- v36=65
- g703at64k=66
- g703at2mb=67
- qllc=68

- fastEtherFX=69
- channel=70
- ieee80211=71
- ibm370parChan=72
- escon=73
- dlsw=74
- isdns=75
- isdnu=76
- lapd=77
- ipSwitch=78
- rsrb=79
- atmLogical=80
- ds0=81
- ds0Bundle=82
- bsc=83
- async=84
- cnr=85
- iso88025Dtr=86
- eplrs=87
- arap=88
- propCnls=89
- hostPad=90
- termPad=91
- frameRelayMPI=92
- x213=93
- adsl=94
- radsl=95
- sdsl=96
- vdsl=97
- iso88025CRFPInt=98
- myrinet=99
- voiceEM=100
- voiceFXO=101
- voiceFXS=102
- voiceEncap=103
- voiceOverIp=104
- atmDxi=105
- atmFuni=106
- atmIma=107
- pppMultilinkBundle=108
- ipOverCdlc=109
- ipOverClaw=110
- stackToStack=111

- virtualIpAddress=112
- mpc=113
- ipOverAtm=114
- iso88025Fiber=115
- tdlc=116
- gigabitEthernet=117
- hdlc=118
- lapf=119
- v37=120
- x25mlp=121
- x25huntGroup=122
- trasnpHdlc=123
- interleave=124
- fast=125 ip=126
- docsCableMaclayer=127
- docsCableDownstream=128
- docsCableUpstream=129
- a12MppSwitch=130
- tunnel=131 coffee=132
- ces=133
- atmSubInterface=134
- l2vlan=135
- l3ipvlan=136
- l3ipxvlan=137
- digitalPowerline=138
- mediaMailOverIp=139
- dtm=140
- dcn=141
- ipForward=142
- msdsl=143
- ieee1394=144
- if-gsn=145
- dvbRccMacLayer=146
- dvbRccDownstream=147
- dvbRccUpstream=148
- atmVirtual=149
- mplsTunnel=150
- srp=151
- voiceOverAtm=152
- voiceOverFrameRelay=153
- idsl=154 compositeLink=155
- ss7SigLink=156
- propWirelessP2P=157

- frForward=158
- rfc1483=159
- usb=160
- ieee8023adLag=161
- bgppolicyaccounting=162
- frf16MfrBundle=163
- h323Gatekeeper=164
- h323Proxy=165
- mpls=166
- mfSigLink=167
- hdsl2=168
- shdsl=169
- ds1FDL=170
- pos=171
- dvbAsiIn=172
- dvbAsiOut=173
- plc=174
- nfas=175
- tr008=176
- gr303RDT=177
- gr303IDT=178
- isup=179
- propDocsWirelessMaclayer=180
- propDocsWirelessDownstream=181
- propDocsWirelessUpstream=182
- hiperlan2=183
- propBWAp2Mp=184
- sonetOverheadChannel=185
- digitalWrapperOverheadChannel=186
- aal2=187
- radioMAC=188
- atmRadio=189
- imt=190
- mvl=191
- reachDSL=192
- frDlciEndPt=193
- atmVciEndPt=194
- opticalChannel=195
- opticalTransport=196
- propAtm=197
- voiceOverCable=198
- infiniband=199
- teLink=200

- q2931=201
- virtualTg=202
- sipTg=203
- sipSig=204
- docsCableUpstreamChannel=205
- econet=206
- pon155=207
- pon622=208
- bridge=209
- linegroup=210
- voiceEMFGD=211
- voiceFGDEANA=212
- voiceDID=213
- mpegTransport=214
- sixToFour=215
- gtp=216
- pdnEtherLoop1=217
- pdnEtherLoop2=218
- opticalChannelGroup=219
- homepna=220
- gfp=221
- ciscoISLvlan=222
- actelisMetaLOOP=223
- fcipLink=224
- rpr=225
- qam=226
- lmp=227
- Unknown=228
- Loopback=229
- OSA_QDIO_ethernet_OSD=230
- OSA_QDIO_ethernet_OSM=231
- OSA_QDIO_ethernet_OSX=232
- Hipersocket=233
- MPC_ptp=234
- MPC_ptp_samehost=235
- MPC_ptp_xcf=236
- Static_virtual=237
- ATM=238
- CLAW=239
- CTC=240
- HCH=241
- LCS_ethernet_V2=242
- LCS_ethernet_8023=243

- LCS_ethernet_V2OR8023=244
- LCS_tokenring=245
- LCS_FDDI=246
- OSA_QDIO_tokenring=247
- MPCOSA_ethernet=248
- MPCOSA_FDDI=249
- SNA_LU0=250
- SNA_LU62=251
- X25_NPSI=252
- CDLC=253

Note: For systems or LPARs running z/OS v1.12 or later, any of these Interface Type values can be displayed in this workspace. However, performance data is available in this workspace for strategic interfaces (types 229 through 236) only. Status data is available for all Interface Types.

MTU Size The size of the largest packet that can be sent or received on the interface. This value is specified in octets. For interfaces that transmit network packets, this MTU size is the size of the largest network packet that can be sent on the interface. The format is an integer.

Note: The value for this attribute in the Interfaces workspace reflects the capacity of the interface to handle DVIPA data, not the capacity of the DVIPA to route data. Traffic is limited by the MTU size of the route, not the size of the interface. Therefore, for a defined DVIPA. it is more likely that the **MTU Value** attribute in the Gateways and Devices workspace controls the size of the packets flowing over DVIPA, so the **MTU Value** attribute in the Gateways attribute group is more pertinent for debugging.

Multi/Broadcast Receive Packet rate The number of received broadcast or multicast packets, per minute, delivered to a higher layer protocol during the most recent time interval. The format is an integer.

Multi/Broadcast Transmit Packet rate The number of packets transmitted to a broadcast or multicast address, per minute, during the most recent time interval. The format is an integer.

Octets Received The number of octets, including framing characters, received since TCP/IP initialization. When the value in the **Octets Received** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Octets Received (in GB)** field and the remainder is stored in the **Octets Received** field. This value is an integer.

Octets Received (in GB) The number of octets, including framing characters, received since TCP/IP initialization, divided by 1,073,741,824. When the value in the **Octets Received** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Octets Received (in GB)** field and the remainder is stored in the Octets Received field. This value is an integer.

Octets Transmitted The number of octets, including framing characters, transmitted out of the interface since TCP/IP initialization. When the value in the Octets Transmitted field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Octets Transmitted (in GB)** field and the remainder is stored in the **Octets Transmitted** field. This value is an integer.

Octets Transmitted (in GB) The number of octets, including framing characters, transmitted out of the interface since TCP/IP initialization, divided by 1,073,741,824. When the value in the **Octets Transmitted** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Octets Transmitted (in GB**) field and the remainder is stored in the **Octets Transmitted** field. This value is an integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is a string up to 32 characters in length.

Outbound Packet Discard Rate The number of packets sent that was discarded, per minute, during the most recent sample. This rate applies to packets chosen to be discarded though no errors had been detected to prevent them being delivered to a higher-layer protocol. One reason for discarding packets might be to free up buffer space. The format is an integer.

Outbound Packets Discarded The number of packets sent that was discarded during the most recent sample. This number includes packets chosen to be discarded though no errors had been detected to prevent them being transmitted. One possible reason for discarding such packets might be to free up buffer space. The format is an integer.

Outbound Packets in Error The number of packets sent that was not transmitted, because of errors, during the most recent time interval. The format is an integer.

Percent Inbound Packets in Error The percentage of inbound packets that was not received, during the most recent time interval, because of errors. The format for this value is in the range of 1 to 100%.

Percent Outbound Packets in Error The percentage of packets sent that was not transmitted, because of errors, during the most recent time interval. The format for this value is in the range of 1 to 100%.

Percent Packets Discarded The percentage of total interface packets (both sent and received) that were discarded during the most recent sample. The format for this value is in the range of 1 to 100%.

Percent Packets in Error The percentage of total interface packets (both sent and received) that was in error during the most recent time interval. The format for this value is in the range of 1 to 100%.

Physical Address The address of the interface at the protocol sublayer. The format is a string up to 12 characters in length. This field is blank when the interface is not active or is not one of the following types:

- ATM
- HYPERchannel
- LCS Ethernet
- MPCIPA OSA-Express QDIO

Physical Address (deprecated) The address of the interface at the protocol sublayer. The format is a string up to 4 characters in length.

Receive Bandwidth Utilization The percentage of bandwidth being used to receive data during the most recent sample. The format is an integer.

Receive Error Rate The number of inbound packets or transmission units, per minute, that was not received during the most recent time interval because of errors. The format is an integer.

Receive Packet Rate The number of packets received, per minute, during the most recent sample. This rate applies to packets delivered by this sublayer to a higher sublayer that were not addressed to a multicast or broadcast address at this sublayer. The format is an integer.

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Time Entered Current State The time when the interface entered its current operational state. If the current state was entered before the most recent reinitialization of the local network management subsystem, then the value of this field is 0 (zero). This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)

- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Transmit Bandwidth Utilization The percentage of bandwidth being used to transmit data during the most recent sample. The format is an integer.

Transmit Error Rate The number of packets or transmission units sent, per minute, that was not transmitted, because of errors, during the most recent time interval. The format is an integer.

Transmit Packet Rate The number of packets sent, per minute during the most recent sample. This rate applies to packets that higher-level protocols requested to be transmitted, but which were not addressed to a multicast or broadcast address at this sublayer. This rate includes packets that were discarded or not sent. The format is an integer.

Internet Key Exchange (IKE) Tunnels Attributes

Use the IKE tunnels attribute to display availability and performance statistics for IKE tunnels known to the IKE daemon for a specific stack. IKE tunnels are used by a security endpoint (IKE daemon) to negotiate dynamic IP tunnels.

Active Dynamic Tunnels Current count of active dynamic tunnels associated with this Internet Key Exchange (IKE) tunnel. The format is an integer.

Authentication Algorithm The authentication algorithm used for this tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 38 = MD5
- 39 = SHA1

Byte Rate The number of bytes protected, per minute, for this tunnel during the most recent time interval. The format is an integer.

Bytes The number of bytes protected by this tunnel during the most recent time interval. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month

- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Diffie-Hellman Group Diffie-Hellman group used to generate keying material for the tunnel. Each group identifies the number of bits to be used in a prime number that is used to generate keying material. This column is blank if PFS (perfect forward security) was not negotiated for the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 1 = GROUP1
- 2 = GROUP2
- 5 = GROUP5
- 14 = GROUP14

Encryption Algorithm Encryption algorithm used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 3 = 3DES
- 12 = AES
- 18 = DES

Exchange Mode Exchange mode used by a tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 2 = MAIN
- 4 = AGGRESSIVE

Extended State Indicates the progress of the tunnel negotiation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = INIT: No key exchange messages have been initiated.
- 1 = WAIT_SA: The first key exchange message has been sent and the endpoint is waiting for a response.
- 2 = IN_KE: A key exchange response has been sent.
- 3 = WAIT_KE: A key exchange message has been sent and the endpoint is waiting on a response.
- 4 = DONE: All key exchange messages have been completed and the tunnel is ready for data traffiic.
- 5 = EXPIRED: Tunnel has exceeded its life time or life size and is not available for data traffic.

In Progress Dynamic Tunnels Current count of in-progress dynamic tunnels associated with this Internet Key Exchange (IKE) tunnel. The format is an integer.

Initiation Indicator Indicates if the local security endpoint may initiate Internet Key Exchange (IKE) tunnel negotiations with the remote security endpoint. Either security endpoint may initiate refreshes regardless of the value of this indicator. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Initiator Cookie A string of hexadecimal digits that, when combined with the Responder Cookie, uniquely identifies the SA for the tunnel. This value is stored as a 16-character string.

IP Address Version The version of the IP addresses being used for the security endpoints. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4: The traffic descriptor and the security endpoints are using IPv4 addresses.
- 1 = IPv6: The traffic descriptor and the security endpoints are using IPv6 addresses.

Key Exchange Action Name The name specified on a z/OS Communications Server Policy Agent KeyExchangeAction configuration statement. This name identifies the action being used to activate this Internet Key Exchange (IKE) tunnel. Key exchange actions describe how key exchanges between security endpoints should be protected. This field is stored as a 48-character string.

Key Exchange Rule Name The name specified on a z/OS Communications Server Policy Agent KeyExchangeRule configuration statement. This name identifies the rule being used to activate this Internet Key Exchange (IKE) tunnel. Key exchange rules identify the security endpoints for an IKE tunnel and the policy to be used for the tunnel by referencing a key exchange action. This field is stored as a 48-character string.

Life Expiration Time The time at which the tunnel will expire. This column is blank if no life time was negotiated. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Life Refresh Time The time at which the tunnel is refreshed. This column is blank if no life time was negotiated. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year

- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Life Size The number of bytes of data that may traverse the tunnel over the life of the tunnel. This value is 0 if no life size was negotiated for the tunnel. The format is an integer.

Life Time The amount of time, in seconds, that the tunnel is to remain active. The format is an integer.

Local NAT Indicator Indicates if network address translation (NAT) has been detected in front of the local security endpoint. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Local Security Endpoint The IP address of the local security endpoint (IKE) responsible for negotiating the tunnel. The format is a UTF-8 encoded character string of up to 45 characters.

Local Security Endpoint ID Internet Security Associations Key Management Protocol (ISAKMP) identity of local security endpoint. This field is a string containing an identifier, as described by local security endpoint ID type. Some ID strings can be as long as 2048 characters. The ID is always truncated at 100 characters. If no IDs are exchanged, this field is stored as blanks.

Local Security Endpoint ID Type Internet Security Associations Key Management Protocol (ISAKMP) identity type for the local security endpoint as defined in RFC 2407. If client IDs were not exchanged during negotiation, this column is blank. ISAKMP peers exchange and verify each other's identities as part of the Internet Key Exchange (IKE) tunnel (Phase 1) negotiation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = IPv4_ADDR
- 2 = FQDN
- 3 = USER_FQDN
- 4 = IPv4_ADDR_SUBNET
- 5 = IPv6_ADDR
- 6 = IPv6_ADDR_SUBNET
- 7 = IPv4_ADDR_RANGE
- 8 = IPv6_ADDR_RANGE
- 9 = DER_ASN1_DN
- 10 = DER_ASN1_GN
- 11 = KEY_ID

NAT Traversal Indicator Indicates if the network address translation (NAT) traversal function is enabled for the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

NAT Traversal Support Level Indicates the type of network address translation (NAT) traversal support being used. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE: No NAT traversal support. Support is either not configured or not negotiated.
- 1 = RFCD2: RFC 3947 draft 2 support.
- 3 = RFCD3: RFC 3947 draft 3 support.

- 4 = RFC: RFC 3947 support with non-z/OS peer.
- 5 = ZOS: RFC 3947 support with z/OS peer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Peer Authentication Method Peer authentication method. This value is stored as an integer and displayed as a string. Valid values are:

- 3 = PRESHAREDKEY
- 2 = RSASIGNATURE

Percent Failed Activations The percent of dynamic tunnel activations that have failed for this Internet Key Exchange (IKE) tunnel. The format is a number between 0 and 100 inclusive.

Percent In Progress Dynamic Tunnels The percentage of dynamic tunnels in progress compared to active dynamic tunnels. The format is a number between 0 and 100 inclusive.

Remote IKE UDP Port Remote UDP port used for Internet Key Exchange (IKE) negotiations. This column is stored as a 5-character string.

Remote NAT Indicator Indicates if a NAT has been detected in front of the remote security endpoint. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote NAPT Indicator Indicates if a network address port translation (NAPT) has been detected in front of the remote security endpoint. It is possible that a NAPT may exist but is detected only as a NAT. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote Security Endpoint The IP address of the remote security endpoint (IKE) responsible for negotiating the tunnel. The format is a UTF-8 encoded character string of up to 45 characters.

Remote Security Endpoint ID Internet Security Associations Key Management Protocol (ISAKMP) identity of remote security endpoint. This field is a string containing an identifier, as described by remote security endpoint ID type. Some ID strings can be as long as 2048 characters. The ID is always truncated at 100 characters. If no IDs are exchanged, this field is stored as blanks.

Remote Security Endpoint ID Type Internet Security Associations Key Management Protocol (ISAKMP) identity type for the remote security endpoint as defined in RFC 2407. If client IDs were not exchanged during negotiation, this column is blank (Tivoli Enterprise Portal) or 0 (3270). ISAKMP peers exchange and verify each other's identities as part of the Internet Key Exchange (IKE) tunnel (Phase 1) negotiation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = IPv4_ADDR
- 2 = FQDN
- 3 = USER_FQDN
- 4 = IPv4_ADDR_SUBNET
- 5 = IPv6_ADDR
- 6 = IPv6_ADDR_SUBNET
- 7 = IPv4_ADDR_RANGE
- 8 = IPv6_ADDR_RANGE
- 9 = DER_ASN1_DN
- 10 = DER_ASN1_GN
- 11 = KEY_ID

Responder Cookie A string of hexadecimal digits that, when combined with the Initiator Cookie, uniquely identifies the SA for the tunnel. This value is stored as a 16-character string.

Role Role of the local security endpoint in the activation of the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = INITIATOR
- 2 = RESPONDER

State Current state of the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 3 = INCOMPLETE: Tunnel negotiation is in progress.
- 4 = ACTIVE: Tunnel is active and ready for use.
- 5 = EXPIRED: Tunnel has expired and cannot be used.

Sysplex Name The name of the sysplex that the monitored system is part of.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Bytes The cumulative number of bytes protected by this tunnel since the tunnel was activated. The value in this column can be added to the product of 1,073,741,823 and the value in the **Total Bytes (in G)** column to calculate the total bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Bytes (in G) The cumulative number of bytes protected by this tunnel since the tunnel was activated, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the **Total Bytes** column to calculate the total bytes for the tunnel. The format is an integer.

Total Failed Local Activations Cumulative count of failed locally initiated dynamic tunnel activations for this Internet Key Exchange (IKE) tunnel. The format is an integer.

Total Failed Remote Activations Cumulative count of failed remotely initiated dynamic tunnel activations for this Internet Key Exchange (IKE) tunnel. The format is an integer.

Total Successful Local Activations Cumulative count of successful locally initiated dynamic tunnel activations for this Internet Key Exchange (IKE) tunnel. The format is an integer.

Total Successful Remote Activations Cumulative count of successful remotely initiated dynamic tunnel activations for this Internet Key Exchange (IKE) tunnel. The format is an integer.

Tunnel ID Tunnel identifier. This identifier is generated by the Internet Key Exchange (IKE) daemon and is not unique. Multiple related tunnels may have the same tunnel ID. This value is a character string of up to 48 characters.

IPSec Status Attributes

Use the IPSec Status attributes to display IP stack security configuration information and IP stack security statistics.

Active Dynamic SWSA Shadow Tunnels The current number of active dynamic Sysplex-Wide Security Associations shadow tunnels known to the TCP/IP stack. The format is an integer.

Active Dynamic Tunnels The current number of active dynamic tunnels known to the TCP/IP stack. This number does not include Sysplex-Wide Security Associations (SWSA) shadow tunnels or manual tunnels. The format is an integer.

Active IKE Tunnels The number of Internet Key Exchange (IKE) tunnels that are currently active. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Dynamic Tunnels in Progress The number of dynamic tunnels in progress. The state of the tunnel is either PENDING or IN NEGOTIATION. The format is an integer where:

- 0 means PENDING
- 1 means IN NEGOTIATION

Expired Dynamic Tunnels The number of dynamic tunnels that are currently expired. This value includes shadow and non-shadow tunnels. The format is an integer.

Expired IKE Tunnels The number of Internet Key Exchange (IKE) tunnels that are currently expired. The format is an integer.

Filter Logging Indicates whether filter logging is enabled for the TCP/IP stack. Filter logging was enabled by coding the LOGENABLE parameter of the IPSEC statement in the TCP/IP profile. For more information about the IPSEC statement, see the most recent edition of the *IBM z/OS Communication Server: IP Configuration Guide* or *IBM z/OS Communication Server: IP Configuration Reference.* This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Disabled
- 1 = Enabled

Filter Set In Use Identifies which filter set is currently in use by the TCP/IP stack. One of two filter sets may be in use at any time:

- The default filter set that is made up of filters defined in the TCP/IP profile.
- The policy filter set that is made up of filters defined in Policy Agent configuration files.

This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Default
- 1 = Policy

IKE Bytes Protected The number of bytes protected by Internet Key Exchange (IKE) tunnels in the last interval. The format is an integer.

IKE Inbound Bytes Protected The number of inbound bytes protected by IKE tunnels in the last interval. The format is an integer.

IKE Inbound Protected Byte Rate The number of inbound bytes flowing through Internet Key Exchange (IKE) tunnels every minute. The format is an integer.

IKE Outbound Bytes Protected The number of outbound bytes protected by Internet Key Exchange (IKE) tunnels in the last interval. The format is an integer.

IKE Outbound Protected Byte Rate The number of outbound bytes flowing through Internet Key Exchange (IKE) tunnels every minute. The format is an integer.

IKE Protected Byte Rate The number of bytes flowing through Internet Key Exchange (IKE) tunnels every minute. The format is an integer.

IKE Total Bytes Protected The cumulative number of inbound and outbound bytes of Internet Key Exchange (IKE) traffic protected by IKE tunnels since the IKE daemon was started. The value in this column can be added to the product of 1,073,741,824 and the value in the IKE Total Bytes Protected (in G) column to calculate the cumulative total bytes of IKE traffic protected by IKE tunnels. The format is an integer.

IKE Total Bytes Protected (in G) The cumulative number of inbound and outbound bytes of Internet Key Exchange (IKE) traffic protected by IKE tunnels since the IKE daemon was started, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the IKE Total Bytes Protected column to calculate the cumulative total bytes of IKE traffic protected by IKE tunnels. The format is an integer.

IKE Total Inbound Bytes Protected The cumulative number of inbound bytes of IKE traffic protected by IKE tunnels since the IKE daemon was started. The value in this column can be added to the product of 1,073,741,824 and the value in the IKE Inbound Bytes Protected (in G) column to calculate the cumulative number of IKE Inbound Bytes Protected. The format is an integer.

IKE Total Inbound Bytes Protected (in G) The cumulative number of inbound bytes of IKE traffic protected by dynamic tunnels since the start of the IKE daemon, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the IKE Inbound Bytes Protected column to calculate the cumulative number of IKE inbound bytes protected. The format is an integer.

IKE Total Invalid Key Messages Cumulative number of invalid key exchange (phase 1) messages received since the Internet Key Exchange (IKE) daemon was started. This does not include message authentication failures. The format is an integer.

IKE Total Key Message Authentication Failures The cumulative number of key exchange (phase 1) message authentication failures since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

IKE Total Outbound Bytes Protected The cumulative number of outbound bytes of IKE traffic protected by IKE tunnels since the IKE daemon was started. The value in this column can be added to the product of 1,073,741,824 and the value in the IKE Outbound Bytes Protected (in G) column to calculate the cumulative number of IKE Outbound Bytes Protected. The format is an integer.

IKE Total Outbound Bytes Protected (in G) The cumulative number of outbound bytes of IKE traffic protected by dynamic tunnels since the start of the IKE daemon, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the IKE Outbound Bytes Protected column to calculate the cumulative number of IKE outbound bytes protected. The format is an integer.

IKE Total Replayed Key Messages The cumulative number of replayed key exchange (phase 1) messages received since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

IKE Total Retransmitted Key Messages The cumulative number of retransmitted key exchange (phase 1) messages that was sent since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

IKE Tunnels in Progress The number of Internet Key Exchange (IKE) tunnels currently in progress. The format is an integer where:

- 0 means PENDING
- 1 means IN NEGOTIATION

IP Bytes Protected The number of bytes of IP traffic protected by dynamic IP tunnels in the last interval. The format is an integer.

IP Inbound Bytes Protected The number of inbound bytes protected by IP tunnels in the last interval. The format is an integer.

IP Inbound Protected Byte Rate The number of inbound bytes flowing through IP tunnels every minute. The format is an integer.

IP Outbound Bytes Protected The number of outbound bytes protected by IP tunnels in the last interval. The format is an integer.

IP Outbound Protected Byte Rate The number of outbound bytes flowing through IP tunnels every minute. The format is an integer.

IP Protected Byte Rate The number of bytes of IP traffic flowing through dynamic IP tunnels every minute. The format is an integer.

IP Security Indicates whether IP security functions are enabled for IPv4 interfaces. IP security was enabled by coding IPCONFIG IPSECURITY in the TCP/IP profile. For more information about the IPSEC statement, see the most recent edition of the *IBM z/OS Communication Server: IP Configuration Guide* or *IBM z/OS Communication Server: IP Configuration Reference.* This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Disabled
- 1 = Enabled

IP Total Bytes Protected The cumulative number of inbound and outbound bytes of IP traffic protected by dynamic tunnels since the TCP/IP stack was started. The value in this column can be added to the product of 1,073,741,824 and the value in the IP Total Bytes Protected (in G) column to calculate the cumulative total bytes of IP traffic protected by dynamic tunnels. The format is an integer.

IP Total Bytes Protected (in G) The cumulative number of inbound and outbound bytes of IP traffic protected by dynamic tunnels since the TCP/IP stack was started, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the IP Total Bytes Protected column to calculate the cumulative total bytes of IP traffic protected by dynamic tunnels. The format is an integer.

IP Total Inbound Bytes Protected The cumulative number of inbound bytes of IP traffic protected by dynamic tunnels since the start of the TCP/IP stack. The value in this column can be added to the product of 1,073,741,823 and the value in the IP Inbound Bytes Protected (in G) column to calculate the cumulative number of IP Inbound Bytes Protected. The format is an integer.

IP Total Inbound Bytes Protected (in G) The cumulative number of inbound bytes of IP traffic protected by dynamic tunnels since the start of the TCP/IP stack, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the IP Inbound Bytes Protected column to calculate the cumulative number of IP inbound bytes protected. The format is an integer.

IP Total Outbound Bytes Protected The cumulative number of outbound bytes of IP traffic protected by dynamic tunnels since the start of the TCP/IP stack. The value in this column can be added to the product of 1,073,741,823 and the value in the IP Outbound Bytes Protected (in G) column to calculate the cumulative number of IP Outbound Bytes Protected. The format is an integer.

IP Total Outbound Bytes Protected (in G) The cumulative number of outbound bytes of IP traffic protected by dynamic tunnels since the start of the TCP/IP stack, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the IP Outbound Bytes Protected column to calculate the cumulative number of IP outbound bytes protected. The format is an integer.

IPv6 Security Indicates whether IP security functions are enabled for IPv6 interfaces. IPv6 security was enabled by coding IPCONFIG IPSECURITY and IPCONFIG6 IPSECURITY in the TCP/IP profile. For more information about the IPSEC statement, see the most recent edition of the *IBM z/OS Communication Server: IP Configuration Guide* or *IBM z/OS Communication Server: IP Configuration Reference*. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Disabled
- 1 = Enabled

NAT Keep Alive Interval The NAT keep-alive interval, in seconds. The interval is used to regulate the sending of NAT keep-alive messages for a NAT traversal tunnel when a NAT is detected in front of the local host. The format is an integer expressed in seconds.

Number of Configured Filters The number of configured IP Filters for this stack. The format is an integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Packets Denied by DENY The number of packets denied by a DENY action on any filter during the most recent collection interval. The format is an integer.

Packets Denied by Mismatch The number of packets denied by a mismatched action on any filter during the most recent interval. The format is an integer.

Packets Filtered The number of packets filtered by the filter rule set during the most recent collection interval. The format is an integer.

Packets Matched The number of packets that matched the condition and action for any filter during the most recent interval. The format is an integer.

Packets Permitted The number of packets permitted by any filter during the most recent interval. The format is an integer.

Percent Packets Denied by DENY The percentage of packets denied by a DENY action on any filter during the most recent interval. The format is a number between 0 and 100 inclusive.

Percent Packets Denied by Mismatch The percentage of packets denied by a mismatched action on any filter during the most recent interval. The format is a number between 0 and 100 inclusive.

Percent Packets Permitted The percentage of packets permitted by any filter during the most recent interval. The format is a number between 0 and 100 inclusive.

Percent Total Packets Denied by DENY The percentage of total packets denied by a DENY action on any filter since the TCP/IP stack was started. The format is a number between 0 and 100 inclusive.

Percent Total Packets Denied by Mismatch The percentage of total packets denied due to a mismatch with any filter action since the stack was started. The format is a number between 0 and 100 inclusive.

Percent Total Packets Permitted The percentage of total packets that was permitted by any filter since the TCP/IP stack was started. The format is a number between 0 and 100 inclusive.

Pre-Decapsulation Filtering Indicates whether pre-decapsulation filtering is enabled. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Disabled
- 1 = Enabled

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

Sysplex Name The name of the sysplex that the monitored system is part of.

Sysplex-Wide Security Associations (SWSA) Indicates whether sysplex-wide security associations (SWSA) are enabled. SWSA was enabled by coding the DVIPSEC parameter on the IPSEC statement in the TCP/IP profile. For more information about the IPSEC statement, see the most recent edition of the *IBM z/OS Communication Server: IP Configuration Guide* or *IBM z/OS Communication Server: IP Configuration Reference*. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Disabled
- 1 = Enabled

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Active Dynamic Tunnels The total number of currently active dynamic tunnels. This includes active dynamic System-Wide Security Association (SWSA) shadow tunnels and dynamic IP tunnels. The format is an integer.

Total Failed Dynamic Tunnel Activations The cumulative number of failed dynamic tunnel activations since the TCP/IP stack was started. The format is an integer.

Total Failed IKE Tunnel Activations The cumulative number of failed Internet Key Exchange (IKE) tunnel activations that was initiated locally or remotely since the IKE daemon was started. The format is an integer.

Total Failed Local IKE Tunnel Activations The cumulative number of failed Internet Key Exchange (IKE) tunnel activations that was initiated locally since the IKE daemon was started. The format is an integer.

Total Failed Remote IKE Tunnel Activations The cumulative number of failed remote Internet Key Exchange (IKE) tunnel activations since the IKE daemon was started. The format is an integer.

Total Invalid QUICKMODE Messages The cumulative number of invalid QUICKMODE (phase 2) messages received since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

Total Packets Denied by DENY The total number of packets denied by a DENY action on any filter since the TCP/IP stack was started. If the value in the **Total Packets Denied By DENY (in G)** column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in the **Total Packets Denied by DENY (in G)** column to calculate the packets denied by DENY for any filter. The format is an integer.

Total Packets Denied by DENY (in G) The total number of packets denied by a DENY action on any filter since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the **Total Packets Denied by DENY** column to calculate the P**ackets Denied by DENY** for any filter. The format is an integer.

Total Packets Denied by Mismatch The total number of packets denied due to a mismatch with any filter action since the TCP/IP stack was started. If the value in the **Total Packets Denied By Mismatch (in G)** column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in the **Packets Denied by Mismatch (in G)** column to calculate the packets permitted. The format is an integer.

Total Packets Denied by Mismatch (in G) The total number of packets denied due to a mismatch with any filter action since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the **Total Packets Denied by Mismatch** column to calculate the packets denied by an action mismatch. The format is an integer.

Total Packets Filtered The total number of packets processed by the filter rule set since the TCP/IP stack was started. If the value in the **Total Packets Filtered (in G)** column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in the T**otal Packets Filtered (in G)** column to calculate the total packets processed. The format is an integer.

Total Packets Filtered (in G) The total number of packets processed by the filter rule set since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the **Total Packets Filtered** column to calculate the total packets processed. The format is an integer.

Total Packets Matched The total number of packets that matched both the condition and action for any filter since the TCP/IP stack was started. If the value in the **Total Packets Matched (in G)** column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in **Total Packets Matched (in G)** column to calculate the total packets matched. The format is an integer.

Total Packets Matched (in G) The total number of packets that matched both the condition and action for any filter since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not

0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Matched column to calculate the total packets matched. The format is an integer.

Total Packets Permitted The total number of packets that was permitted by any filter since the TCP/IP stack was started. If the value in the **Total Packets Permitted (in G)** column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in **Total Packets Permitted (in G)** column to calculate the packets permitted. The format is an integer.

Total Packets Permitted (in G) The total number of packets that was permitted by any filter, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the **Total Packets Permitted** column to calculate the packets permitted. The format is an integer.

Total Replayed QUICKMODE Messages The cumulative number of replayed QUICKMODE (phase 2) messages received since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

Total Retransmitted QUICKMODE Messages The cumulative number of retransmitted QUICKMODE (phase 2) messages sent since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

Total Successful Dynamic Tunnel Activations The cumulative number of successful dynamic tunnel activations since the TCP/IP stack was started. The format is an integer.

Total Successful IKE Tunnel Activations The cumulative number of successful Internet Key Exchange (IKE) tunnel activations that was initiated locally or remotely since the IKE daemon was started. The format is an integer.

Total Successful Local IKE Tunnel Activations The cumulative number of successful locally initiated Internet Key Exchange (IKE) tunnel activations since the IKE daemon was started. The format is an integer.

Total Successful Remote IKE Tunnel Activations The cumulative number of successful Internet Key Exchange (IKE) tunnel activations that was initiated locally or remotely since the IKE daemon was started. The format is an integer.

KN3 Agent Status Attributes

Use the KN3 Agent Status attributes to view configuration and status information about the IBM Z OMEGAMON Network Monitor monitoring agent.

Agent Group ID The numeric group ID value of the OMVS security group to which the IBM Z OMEGAMON Network Monitor monitoring agent user ID belongs. Job KN3UAUTH generated during configuration adds user name KN3USER to the OMVS security group. The format is a 4-byte integer.

Agent Group Name The OMVS security group name to which the IBM Z OMEGAMON Network Monitor monitoring agent user belongs. Job KN3UAUTH generated by during configuration adds user name KN3USER to the OMVS security group. The format is an 8-character string.

Agent Procedure Name The name specified on the PROC or JOB statement of the JCL used to start the IBM Z OMEGAMON Network Monitor monitoring agent. The format is an 8-character string.

Agent Start Time The time and date at which this instance of the monitoring agent was started. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute

- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Agent User ID The numeric user ID value associated with the IBM Z OMEGAMON Network Monitor monitoring agent OMVS security group user name. Job KN3UAUTH is generated during configuration. This job adds user name KN3USER to the OMVS security group and defines a numeric value for the user name. The format is a 4-byte integer.

Agent User Name The OMVS security group user name for the IBM Z OMEGAMON Network Monitor monitoring agent started task. Job KN3UAUTH is generated during configuration. This job adds user name KN3USER to the OMVS security group. Job KN3UAUTH also defines a profile named MfNProcName.* in the STARTED class and sets the user name to KN3USER. This action causes user name KN3USER to be used for the IBM Z OMEGAMON Network Monitor monitoring agent task. The system administrator can choose to edit the KN3UAUTH sample. The format is an 8-character string.

If the KN3UAUTH job has defined UID(0) for the Agent User ID, then the Agent User Name attribute will show a value of ROOT. If the UID is not UID(0), the Agent User Name is displayed as KN3USER (the default user name in the sample file) or the user name that the system administrator coded on the RACF ADDUSER statement.

Collection Time The time and date at which status information was collected. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

IKE Daemon Started Indicates whether the Internet Key Exchange (IKE) daemon has been started on the monitored system. The IKE daemon must be started for IPSec data to be available for collection. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes
- 2 = Unknown

A value of **Unknown** means the status could not be determined due to an internal error in the agent. If you see this value, contact IBM Software Support.

The default jobname, identifier, and step name for the IKE Daemon procedure are all **IKED**. The value of this attribute might not be correct if the substring **IKED** is not part of the jobname, identifier, or step name for the IKE Daemon procedure. Also, if you use the substring **IKED** as part of another procedure's or job's jobname, or identifier, or step name, the value for this attribute might not be correct. For more information about jobname and identifier, see the "Starting a System Task from a Console" topic in the *IBM z/OS: MVS System Commands* book.

Origin Node The unique identifier for the IBM Z OMEGAMON Network Monitor agent node on the navigation tree. The format is an alphanumeric string no longer than 32 characters.

PAGENT Daemon Started Indicates whether the Policy Agent (PAGENT) daemon is started on the monitored system. The PAGENT daemon must be started in order for IPSec data to be available for collection. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes
- 2 = Unknown

A value of **Unknown** means the status could not be determined due to an internal error in the agent. If you see this value, contact IBM Software Support.

The default jobname, identifier, and step name for the PAGENT Daemon procedure are all **PAGENT**. The value of this attribute might not be correct if the substring **PAGENT** is not part of the jobname, or the identifier, or the step name for the PAGENT Daemon procedure. Also, if you use the substring **PAGENT** as part of another procedure's or job's jobname, or identifier, or step name, the value for this attribute might not be correct. For more information about jobname and identifier, see the "Starting a System Task from a Console" topic in the *IBM z/OS: MVS System Commands* book.

SNA Collection Interval The interval in minutes between data collection samples for the VTAM buffer pool and VTAM address space performance data. A value of 1 means that SNA data is collected every minute. This value is expressed as a whole number from 1 to 60, indicating the collection interval in minutes. The default is 5 minutes.

This interval is defined by the SNA Data Collection Interval value that was set in the Configuration Tool on the "Specify VTAM APPLID Values (Page 4)" panel or the KN3_SNA_VTAM_SNAC_SNACINTV PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the SNACINTV parameter on the KN3FCCMD START SNAC command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

SNA Collection Start Time The time and date when SNA data collection for this monitoring agent instance was last started. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour

- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

SNA Collection Started Indicates whether the agent SNA data collection is started on the monitored system. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

If you indicated in the Configuration Tool or during PARMGEN configuration that VTAM environment and buffer pool data are to be collected, then the SNA collector is started when the agent is started.

These are possible reasons that the value of this attribute might be **No**:

- You did not respond **Y** to the Buffer Pool/VTAM Environment Data Collection parameter in the Configuration Tool or the KN3_SNA_VTAM_COLLECT_DATA PARMGEN parameter.
- The agent's PMI exit and its aliases are not available to VTAM. To confirm that this issue is what is preventing SNA data collection, check the RKLVLOG for message KN3PN023. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for information on making the PMI exit and its aliases available to VTAM.
- The VTAM application needed by the agent to collect VTAM environment and buffer pool data is either not defined to VTAM or is not in the correct state. To confirm that this issue is preventing SNA data collection, check the RKLVLOG for message KN3PN011 or KN3PN022. See the "Troubleshooting SNA collector problems" topic in the *IBM Z OMEGAMON Network Monitor: Troubleshooting Guide* for more information about this problem.

Sysplex Name The name of the sysplex that the monitored system is part of. The format is a string of up to 8 characters.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCP Collection Interval The interval in minutes between data collection samples by the TCP/IP data collector. This collection interval is used by the network monitoring interface (NMI) collector and the SNMP collector. SNA data such as Communications Storage Manager (CSM) and High Performance Route (HPR) and Enterprise Extender (EE) data are collected by the NMI collector and use this interval also. A value of 1 means that TCP data is collected every minute. This value is expressed as a whole number from 1 to 60, indicating the collection interval in minutes. The default is 5 minutes.

This interval is defined by the TCP/IP Sample Interval value that was set in the Configuration Tool on the "Specify Component Configuration" panel or the KN3_TCP_SAMPLE_INTERVAL PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the TCPCINTV parameter on the KN3FCCMD INSTALL TCPC command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

TCP Collection Start Time The time and date at which TCP Collection was last started. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

TCP Collection Started Indicates whether TCP data collection has been started. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

TCP Collector SNMP Parameter Dataset Name The name of the data set that contains parameters used by the TCP/IP data collector to communicate with the SNMP agents for each of the TCP/IP stacks on the system. The format is an alphanumeric string of up to 54 characters.

This data set is identified on the KN3SNMP DD statement of the IBM Z OMEGAMON Network Monitor started task procedure. A sample of what should be in this dataset is provided in member KN3SNMP of the RKANSAMU data set. For each TCP/IP stack being monitored, this data set needs to provide the following information:

- IP address
- SNMP agent port number
- SNMP protocol version
- Community name

If this information cannot be located or the data set is unreadable, no data will be available for any of the workspaces whose data source is SNMP. If no data set name is provided or someone has the data set open in write mode, this attribute will be set to a value of **UNKNOWN**.

If the TCP Collector SNMP parameter data set name attribute has a value of **UNKNOWN**, verify that the KN3SNMP DD statement is not commented out in the IBM Z OMEGAMON Network Monitor started task procedure and that it refers to a data set that exists on the system where the monitoring agent will run. If access to the data set is being controlled by a SAF product, also make sure that the agent user ID has permission to read the data set.

If any of the SNMP parameters defined in the TCP Collector SNMP parameter data set are incorrect for a stack, check the KN3ACTCS log for the monitoring agent for error messages that may have been generated when processing the data set. If no error messages are found there, examine the parameters in the data set and verify that the information is correct for the TCP/IP stack or stacks. Also verify that no one has the data set open in write mode.

This data set name is defined by the SNMP Configuration file value that was set in the Configuration Tool on the "Specify Component Configuration (Page 2)" panel or with the KN3_SNMP_CONFIG_FILE PARMGEN parameter. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

Virtual IO Unit Name The TCP/IP virtual I/O unit name to be used for temporary data sets. The default is **VIO**. The format is an alphanumeric string no longer than 8 characters.

This value is defined by the "Specify your site's VIO unit name" question that was set in the Configuration Tool on the "Specify Agent Configuration" panel or using the KN3_TCP_VIO_UNIT PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the TCPCVIOU parameter on the KN3FCCMD INSTALL TCPC command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

KN3 DWL Attributes

Use the KN3 DWL attributes to describe the fields required for the IBM(R) Tivoli(R) NetView(R) for z/OS(R) Packet Trace operation.

Note: These attributes are not viewable in any workspace, but appear in the Query Editor.

KFW EMU Host The IP address or URL for the LPAR to which the TN3270 sessions will connect. The format is a string of up to 256 characters.

KFW EMU Port The port address of a TN3270 listener on the KFW EMU host. The format is an integer.

KFW EMU Term Type Terminal type. Although the Tivoli Enterprise Portal terminal emulator supports all 3270 terminal types, only the 3270 (24x80) terminal type is supported for this implementation. The format is a string of up to 16 characters.

KFW LU Group The name of a Logical Unit Group to which the TN3270 session will be joined. The LU group is needed only if the Telnet UNIX System Services (USS) is not being used as the default 3270 connection on z/OS. The "Dynamic XE to 3270 linking" feature requires that USS accept a LOGON APPLID(xxxxxxxx) command. The format is a string of up to 8 characters.

Origin Node The unique identifier for the IBM Z OMEGAMON Network Monitor agent node on the navigation tree. The format is an alphanumeric string no longer than 32 characters.

ZOS EMU Agent Applid The VTAM APPLID of the NetView for z/OS application to which the terminal emulator will connect. The format is a string of up to 8 characters.

ZOS User Data The UNIX System Services (USS) user data that is passed to the NetView for z/OS application during logon processing. The format is a string of up to 109 characters.

KN3 ICMP Global Counters Attributes

Use the KN3 Internet Control Message Protocol (ICMP) Global Counters attributes to view statistics for the Internet Control Message Protocol (ICMP) and ICMPv6 on z/OS v1r12 or later systems.

Note: This attribute group is available only on systems running z/OS(R) v1.12 or later.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

ICMP Version The Internet Control Message Protocol (ICMP) version to which the statistics in this table row apply. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = ICMP
- 1 = ICMPv6

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Percent Inbound In Error For this Internet Control Message Protocol (ICMP) type, the percentage of inbound messages in error compared to Total Messages Received during the most recent sampling interval. The format is an integer between 0 and 100 inclusive.

Percent Outbound In Error For this Internet Control Message Protocol (ICMP) type, the percentage of outbound messages in error compared to Total Messages Sent during the most recent sampling interval. The format is an integer between 0 and 100 inclusive.

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Total Inbound Messages In Error The number of messages of the Internet Control Message Protocol (ICMP) Version received that have errors since TCP/IP initialization. The format is an unsigned integer.

Total Messages Received For this version of Internet Control Message Protocol (ICMP), the total number of messages that this TCP/IP stack received, including messages that contained errors since TCP/IP initialization. The format is an unsigned integer.

Total Messages Sent For this version of Internet Control Message Protocol (ICMP), the total number of messages that this TCP/IP stack attempted to send, including messages sent in error since TCP/IP initialization. The format is an unsigned integer.

Total Messages Sent Received The total number of messages sent and received for the specified Internet Control Message Protocol (ICMP) Type since TCP/IP initialization. The format is an unsigned integer.

Total Outbound Messages In Error The number of messages of the Internet Control Message Protocol (ICMP) Version that were not sent due to errors since TCP/IP initialization. The format is an unsigned integer.

Total Percent Inbound In Error The percentage of Inbound Messages In Error compared to Messages Received for the specified Internet Control Message Protocol (ICMP) Type since TCP/IP initialization. The format is an integer between 0 and 100 inclusive.

Total Percent Outbound In Error The percentage of Outbound Messages In Error compared to Messages Sent for the specified Internet Control Message Protocol (ICMP) Type since TCP/IP initialization. The format is an integer between 0 and 100 inclusive.

KN3 ICMP Type Counters Attributes

Use the KN3 ICMP Type Counters attributes to statistics for the Internet Control Message Protocol (ICMP) and ICMPv6 on z/OS v1r12 or later systems. For more information about ICMP message types, see the ICMP types and codes appendix of the *IBM z/OS Communications Server: IP System Administrator's Commands* book.

Note: This attribute group is available only on systems running z/OS(R) v1.12 or later.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

ICMP Type The type of Internet Control Message Protocol (ICMP) message used to report the processing of datagrams. This value is stored as an integer and displayed as a string. Valid values for ICMP are:

- 0 = Echo_Reply
- 3 = Destination_Unreachable
- 4 = Source_Quench
- 5 = Redirect
- 8 = Echo_Request
- 9 = Router_Advertisement
- 10 = Router_Solicitation
- 11 = Time_Exceeded
- 12 = Parameter_Problem
- 13 = Timestamp_Request
- 14 = Timestamp_Reply
- 15 = Information_Request
- 16 = Information_Reply
- 17 = Address_Mask_Request
- 18 = Address_Mask_Reply

Valid values for ICMPv6 are:

- 2 = Packet_Too_Big
- 3 = Destination_Unreachable
- 11 = Time_Exceeded
- 12 = Parameter_Problem
- 128 = Echo_Request
- 129 = Echo_Reply
- 130 = Group_Membership_Query
- 131 = Group_Membership_Reply
- 132 = Group_Membership_Reduction
- 133 = Router_Solicitation
- 134 = Router_Advertisement
- 135 = Neighbor_Solicitation
- 136 = Neighbor_Advertisement
- 137 = Redirect

Not all ICMP types are supported for both inbound and outbound ICMP messages. The Inbound Messages Supported and Outbound Messages Supported attributes identify where specific counters are valid.

ICMP Version The Internet Control Message Protocol (ICMP) version to which the statistics in this table row apply. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = ICMP
- 1 = ICMPv6

Inbound Messages Supported The indicator of whether the inbound message counter is supported by the TCP/IP stack for the Internet Control Message Protocol (ICMP) Type. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.h

Outbound Messages Supported The indicator of whether the outbound message counter is supported by the TCP/IP stack for the Internet Control Message Protocol (ICMP) Type. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Total Messages Received The total number of messages received for the specified Internet Control Message Protocol (ICMP) Type since TCP/IP initialization. The format is an unsigned integer.

Total Messages Sent The number of messages sent for the specified Internet Control Message Protocol (ICMP) Type since TCP/IP initialization. The format is an unsigned integer.

Total Messages Sent Received The total number of messages sent and received for the specified Internet Control Message Protocol (ICMP) Type since TCP/IP initialization. The format is an unsigned integer.

Total Percent Inbound In Error The percentage of Total Inbound Messages In Error compared to Total Messages Received for the specified Internet Control Message Protocol (ICMP) Type since TCP/IP initialization. The format is an integer between 0 and 100 inclusive.

Total Percent Outbound In Error The percentage of Total Outbound Messages In Error compared to Total Messages Sent for the specified Internet Control Message Protocol (ICMP) Type since TCP/IP initialization. The format is an integer between 0 and 100 inclusive.

KN3 Interface Address Attributes

Use the KN3 Interface Address attributes to display interface address information for a specific interface defined to a z/OS(R) v1r12 or later system.

Note: This attribute group is available only on systems running z/OS v1.12 or later.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Interface Index The interface Index. The format is a 4-byte unsigned integer.

IP Address The IP address of the interface. The format is a 45-character string.

IP Address Type The IPv6 address type. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = Global
- 2 = Loopback
- 3 = Link_local

IP Address Version The version of the IP address used by this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4
- 1 = IPv6

IPv4 Primary Address Indicates whether this is an IPv4 primary address. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

IPv6 Address Unavailable Indicates whether IPv6 addresses are available to this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

IPv6 Address Unavailable Reason Indicates the reason why an IPv6 addresses is unavailable. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = DAD
- 2 = Duplicate
- 3 = DAD_Pending
- 4 = DAD_Prevented
- 5 = Interface_ID_Unavailable

IPv6 Autoconfigured Address Indicates whether this is an IPv6 autoconfigured address. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

IPv6 Deprecated Address Indicates whether this is an IPv6 deprecated address. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

IPv6 Manual Prefix Indicates whether the prefix of the IPv6 address was manually configured. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

IPv6 Temporary Address Indicates whether the IPv6 address is temporary. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

KN3 Interface Read Queue Attributes

Use the KN3 Interface Read Queue attributes to analyze input at the Data Link Control (DLC) layer level. This layer provides z/OS(R) Communications Server tuning statistics for the following types of interfaces on a z/OS v1r12 or later system:

- HiperSockets
- Queued direct I/O (QDIO) OSA features

Some OSA-Express features support up to eight read queues while HiperSockets supports only a single read queue. Data is provided for each read queue associated with the supported datapath device (subchannel address). When interfaces share a datapath device number (data subchannel address), the statistics for each interface sharing the datapath device are identical.

Note: This attribute group is available only on systems running z/OS v1.12 or later.

Accelerated Bytes The number of received bytes subsequently routed outbound using queued direct I/O (QDIO) routing or the QDIO Accelerator since the statistics were last reset. The format is an unsigned long long integer.

This attribute applies to IPv4 interfaces only.

Accelerated Packets The number of received packets subsequently routed outbound using queued direct I/O (QDIO) routing or the QDIO Accelerator since the statistics were last reset. The format is an unsigned long long integer.

This attribute applies to IPv4 interfaces only.

Average Bytes Per SBAL The average number bytes per used storage block address list (SBAL) since the statistics were last reset. The format is an unsigned long long integer.

Average Packets Per SBAL The average number packets per used storage block address list (SBAL) since the statistics were last reset. The format is an unsigned long long integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Datapath Device Number The datapath device number. The format is an unsigned 2-byte integer displayed in hexadecimal.

Frame Invalidation Packets The number of frame invalidation packets identified by this interface. The format is an unsigned long long integer.

Frame validation packets are an innovation in OSA-Express3 transparent error handling for the inbound data stream. OSA-Express3 individually marks packets with errors as invalid and z/OS Communications Server later discards packets marked as invalid, reducing the number of unnecessary retransmissions and improving I/O efficiency.

Frame Invalidation Support Indicates whether the Frame Invalidation Packets counter is supported for this interface. If this attribute value is **No**, the value of the Frame Invalidation Packets attribute is zero. If this attribute value is **Yes**, the value of the **Frame Invalidation Packets** attribute may be greater than zero. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

Frame invalidation packets are packets that were received but were marked not valid by the OSA-Express feature. This marking of packets applies to OSA-Express3 and subsequent OSA features only.

Interface Index The interface index for this interface. The format is an unsigned integer.

Interface Name The interface name sharing the read queue. The format is an alphanumeric string no longer than 16 characters.

This value is specified with the *intf_name* parameter on the INTERFACE statement or the *link_name* parameter on the LINK statement in the TCPIP.PROFILE dataset. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Interface Status The status of this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = Active
- 2 = Not_Active
- 3 = DAD_Pending

Interface Type The type of interface. This value is stored as an integer and displayed as a string. Valid values are:

- 2 = OSA_QDIO_ethernet_OSD
- 3 = OSA_QDIO_ethernet_OSM. This is the intranode management network (INMN), a private 1000BASE-T Ethernet network operating at 1 Gbps that is required for the Unified Resource Manager to manage the resources within a single zEnterprise(TM) node. The INMN connects the Support Element (SE) to the z196 and to any attached zBX. This interface is associated with thezEnterprise(TM) mainframe server.
- 4 = OSA_QDIO_ethernet_OSX. This is the private 10 Gigabit Ethernet network for application data communications within an ensemble. Data communications for workloads can flow over the IEDN within and between nodes of an ensemble. All of the physical and logical resources of the IEDN are configured, provisioned, and managed by the Unified Resource Manager. This interface is associated with the zEnterprise(TM) mainframe server.
- 5 = Hipersocket

IP Address Version The version of the IP address for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4
- 1 = IPv6

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Percent Accelerated Bytes The percentage of Accelerated QDIO (queued direct I/O) Bytes in comparison to the number of Received Bytes since the statistics were last reset. The format is an integer between 0 and 100 inclusive.

Notes: This attribute applies to IPv4 interfaces only. The value is zero (0) for IPv6 interfaces.

Percent Accelerated Packets The percentage of Accelerated QDIO (queued direct I/O) Packets in comparison to the number of Received Packets since the statistics were last reset. The format is an integer between 0 and 100 inclusive.

Notes: This attribute applies to IPv4 interfaces only. The value is zero (0) for IPv6 interfaces.

Percent Frame Invalidation Packets The percentage of Frame Invalidation Packets in comparison to the number of Received Packets since the statistics were last reset. The format is an integer between 0 and 100 inclusive.

Percent Real PCI Interrupts The percentage of Real PCI Interrupts in comparison to the number of Total PCI Interrupts since the statistics were last reset. The format is an integer between 0 and 100 inclusive.

Percent Threshold PCI Interrupts The percentage of Threshold Peripheral Component Interconnect (PCI) Interrupts in comparison to the number of Real PCI Interrupts since the statistics were last reset. The format is an integer between 0 and 100 inclusive.

Percent Unproductive PCI Interrupts The percentage of Unproductive Peripheral Component Interconnect (PCI) interrupts in comparison to the number of Real PCI Interrupts since the statistics were last reset. The format is an integer between 0 and 100 inclusive.

Percent Virtual PCI Interrupts The percentage of Virtual Peripheral Component Interconnect (PCI) interrupts in comparison to the number of Total PCI Interrupts since the statistics were last reset. The format is an integer between 0 and 100 inclusive.

QDIO Accelerator Whether or not internal queued direct I/O (QDIO) routing or the QDIO Accelerator is in effect. When this attributed displays as **Yes**, the following counters are being incremented:

- Accelerated Packets
- Accelerated Bytes

If this attribute displays as **No**, the counters might be non-zero but are not being incremented. This attribute applies to IPv4 interfaces only. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

Queue ID The read queue identifier. The format is an unsigned integer.

Queue Workload Name The name that identifies the type of workload with packets that are directed to this queue. The OSA-Express features includes one primary queue and possibly several ancillary queues. The primary queue is used for packets that do not belong on an ancillary queue. For the primary queue, the workload name is always PRIMARY. The format is a string of up to 8 characters.

Read Control Device Number The read control device number. The format is an unsigned integer in hexadecimal format.

Read Processing Deferral Rate The number of read processing deferrals per minute for the PRIMARY read queue during the most recent sampling interval. The format is an integer.

Read Processing Deferrals The number of read processing deferrals for the PRIMARY read queue during the most recent sampling interval. The format is a long long integer.

Read Replenishment Deferral Rate The number of Read Replenishment Deferrals per minute for the PRIMARY read queue during the most recent sampling interval. The format is an integer.

Read Replenishment Deferrals The number of read replenishment deferrals for the PRIMARY read queue during the most recent sampling interval. The format is a long long integer.

Reads Exhausted The number of reads exhausted due to full read buffers during the most recent sampling interval. The format is a long long integer.

Reads Exhausted Rate The number of reads exhausted due to full read buffers per minute during the most recent sampling interval. The format is an integer.

Real PCI Interrupts The number of real Peripheral Component Interconnect (PCI) interrupts since the statistics were last reset. The format is an unsigned long long integer.

A real PCI is an execution of the queued direct I/O (QDIO) Program-Controlled Interrupt Exit as a result of a call from the system interrupt handler. Real PCIs can be viewed as the QDIO datapath device "pushing" read completions to the datapath device driver. The higher the ratio of real PCIs to virtual PCIs, the less successful the QDIO facility is at avoiding the overhead of the system interrupt handler.

Read PCI interrupts are provided for the primary read queue only. The value of this attribute is the sum of the interrupts for all read queues (primary and ancillary).

Received Bytes The number of bytes received by this read queue since the statistics were last reset. The format is an unsigned long long integer.

Received Packets The number of packets received by this read queue since the statistics were last reset. The format is an unsigned long long integer.

Reset Time Stamp The z/OS time stamp when the interface counter values were last reset. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

System ID The SMF system ID. The format is a string up to 4 characters in length.

Threshold PCI Interrupts The number of threshold Peripheral Component Interconnect (PCI) interrupts for the PRIMARY read queue since the statistics were last reset. The value is the sum of the interrupts for all read queues (primary and ancillary). The format is an unsigned long long integer.

A threshold PCI is a real PCI generated by the queued direct I/O (QDIO) datapath device because one of the threshold conditions which controls the PCI processing was met. A count of zero indicates the QDIO datapath device driver is providing sufficient resources to keep pace with the inbound data stream from the interface.

A Threshold PCI Interrupt value is provided for the primary Read queue only.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Total PCI Interrupts The total number of Peripheral Component Interconnect (PCI) interrupts, including virtual and real interrupts since the statistics were last reset. The format is an unsigned long long integer.

Total Read Processing Deferrals The total number of read processing deferrals for the PRIMARY read queue since the statistics were last reset. The value is the sum of the deferrals for all read queues (primary and ancillary). The format is an unsigned long long integer.

A read processing deferral occurs when the queued direct I/O (QDIO) program-controlled interrupt (PCI) Exit must defer processing a read completion, because a control block cannot be obtained to present the inbound data. Read processing deferrals (along with read replenishment deferrals) can cause the value of the NWMIfStExtRNoReads field to be incremented.

Read processing deferrals are provided only for the primary read queue.

Total Read Replenishment Deferrals The total number of read replenishment deferrals for the PRIMARY read queue since the statistics were last reset. The value is the sum of the deferrals for all read queues (primary and ancillary). The format is an unsigned long long integer.

A read processing deferral occurs when the queued direct I/O (QDIO) program-controlled interrupt (PCI) Exit must defer processing a read completion, because a control block cannot be obtained to present the inbound data. Read processing deferrals (along with read replenishment deferrals) can cause the value of the Total Reads Exhausted attribute to be incremented.

Read Replenishment Deferrals are provided for the primary read queue only.

Total Reads Exhausted The total number of read operations exhausted due to full read buffers since the statistics were last reset. The format is an unsigned long long integer.

If this value is not zero, a lack of read buffers might be indicated for the queued direct I/O (QDIO) datapath device. A lack of read buffers can result in dropped packets, possibly leading to packet retransmission.

TRLE Name The transport resource list (TRL) name for this interface. The format is a string of up to 8 characters.

Unproductive PCI Interrupts The number of unproductive Peripheral Component Interconnect (PCI) interrupts for the PRIMARY read queue since the statistics were last reset. The value is the sum of the interrupts for all read queues (primary and ancillary). The format is an unsigned long long integer.

An unproductive PCI is a real PCI where the datapath device driver found no reads have completed. Unproductive PCIs primarily occur when the interval between two PCIs is minimal and the first PCI thread has already processed the read completion for which the second PCI was generated.

Unproductive PCI interrupts are provided for the primary read queue only.

Used SBALs The number of storage block address list control blocks (SBALs) used since the statistics were last reset. The format is an unsigned long long integer.

For OSA-Express interfaces, an SBAL represents 16 4K read buffers (a single 64K read). For HiperSockets interfaces, the SBAL size is variable. For a specific read operation, not all of the buffers may be used (some might contain inbound packets, for example).

Virtual PCI Interrupts The number of virtual Peripheral Component Interconnect (PCI) interrupts for the PRIMARY read queue since the statistics were last reset. The value is the sum of the interrupts for all read queues (primary and ancillary). The format is an unsigned long long integer.

A virtual PCI is an execution of the queued direct I/O (QDIO) Program-Controlled Interrupt Exit as a result of a call from the datapath device driver. Virtual PCIs can be viewed as the datapath device driver "pulling" read completions from the QDIO datapath device. The higher the ratio of virtual PCI to real PCI, the more successful the QDIO facility is at avoiding the overhead of the system interrupt handler.

Virtual PCI Interrupts are provided for the primary read queue only.

KN3 Interface Statistics Attributes

Use the KN3 Interface Statistics attributes to display information about status and data flow through the interface on a z/OS(R) v1r12 or later system. The statistics that are returned by the request are similar to those in the output of the `Netstat DEVLINKS/-d` report. Statistics are provided for all strategic interface types except for VIPA interfaces; the stack does not maintain counters for VIPA interfaces.

Notes: This attribute group is available only on systems running z/OS v1.12 or later.

Bandwidth Utilization The total percentage of bandwidth being used during the most recent sampling interval. This value is the sum of Transmit Bandwidth Utilization and Receive Bandwidth Utilization. The format is an integer between 0 and 100 inclusive.

Bytes Received The number of input bytes during the most recent sampling interval. The format is an unsigned long long integer.

Bytes Received or Transmitted The number of bytes sent and received during the most recent sampling interval. The format is an unsigned long long integer.

Bytes Transmitted The number of output bytes during the most recent sampling interval. The format is an unsigned long long integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Device or Datapath Status The device or datapath status. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = Starting
- 2 = Sent_Setup
- 3 = Enabling
- 4 = Connecting
- 5 = Connecting2
- 6 = Negotiating
- 7 = Active
- 8 = Deactivating
- 9 = Not_Active

Inbound Packet Discard Rate The number of inbound packets that have been discarded per minute during the most recent sampling interval. This rate applies to packets that were chosen to be discarded even though no errors had been detected to prevent them from being delivered to a higher-layer protocol as well as packets discarded due to error. One possible reason for discarding such packets can be to free up buffer space. The format is a four-byte unsigned integer.

Inbound Packets Discarded The number of inbound packets that have been discarded during the most recent sample. This number includes packets that were chosen to be discarded even though no errors had been detected to prevent them from being delivered to a higher-layer protocol. One possible reason for discarding such packets can be to free up buffer space. The format is a four-byte unsigned integer.

Interface Index The interface index. The format is a 4-byte unsigned integer.

Interface Index Specified Indicates whether the workspace is invoked with an Interface Index specified. This value is stored as an integer and displayed as a string. Valid values are

- 0 = No
- 1 = Yes

Interface Name The interface Name. The format is an alphanumeric string no longer than 16 characters.

This value is specified with the *intf_name* parameter on the INTERFACE statement or the *link_name* parameter on the LINK statement in the TCPIP.PROFILE dataset. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Interface Status The status of this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = Active
- 2 = Not_Active
- 3 = DAD_Pending

Interface Type The interface type. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = Loopback
- 2 = OSA_QDIO_ethernet_OSD
- 3 = OSA_QDIO_ethernet_OSM. This is the intranode management network (INMN), a private 1000BASE-T Ethernet network operating at 1 Gbps that is required for the Unified Resource Manager to manage the resources within a single zEnterprise(TM) node. The INMN connects the Support Element (SE) to the z196 and to any attached zBX. This interface is associated with the zEnterprise(TM) mainframe server.
- 4 = OSA_QDIO_ethernet_OSX. This is the private 10 Gigabit Ethernet network for application data communications within an ensemble. Data communications for workloads can flow over the IEDN within and between nodes of an ensemble. All of the physical and logical resources of the IEDN are configured, provisioned, and managed by the Unified Resource Manager. This interface is associated with the zEnterprise(TM) mainframe server.
- 5 = Hipersocket
- 6 = MPC_ptp
- 7 = MPC_ptp_samehost
- 8 = MPC_ptp_xcf

IP Address Version The version of the IP address for the interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4
- 1 = IPv6

Multi/Broadcast Receive Packet Rate The number of received broadcast or multicast packet per minute delivered to a higher-layer protocol during the most recent sampling interval. The format is a 4-byte unsigned integer.

Multi/Broadcast Transmit Packet Rate The number of packets transmitted to a broadcast or multicast address per minute during the most recent sampling interval. The format is a 4-byte unsigned integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Outbound Packet Discard Rate The number of outbound packets that has been discarded per minute during the most recent sampling interval. This rate applies to packets that were chosen to be discarded even though no errors had been detected to prevent them from being delivered to a lower-layer protocol as well as packets discarded due to errors. One possible reason for discarding such packets could be to free up buffer space. The format is a four-byte unsigned integer.

Outbound Packets Discarded The number of outbound packets that have been discarded during the most recent sample. This number includes packets that were chosen to be discarded even though no errors had been detected to prevent them from being delivered to a higher-layer protocol. One possible reason for discarding such packets could be to free up buffer space. The format is a four-byte unsigned integer.

Outbound Packets Discarded in Error The number of output packets discarded due to errors other than an out-of-storage condition during the last sampling interval. The format is an unsigned integer.

Percent Inbound Packets in Error The percentage of inbound packets that could not be received during the most recent sampling interval because of errors. The format is an integer between 0 and 100 inclusive.

Percent Outbound Packets in Error The percentage of outbound packets that could not be transmitted during the most recent sampling interval because of errors. The format is an integer between 0 and 100 inclusive.

Percent Packets Discarded The percentage of total interface packets (both transmitted and received) that were discarded during the most recent sampling interval. The format is an integer between 0 and 100 inclusive.

Percent Packets in Error The percentage of total interface packets (both transmitted and received) that were in error during the most recent sampling interval. The format is an integer between 0 and 100 inclusive.

Receive Bandwidth Utilization The percentage of bandwidth being used to receive data during the most recent sampling interval. The format is an integer between 0 and 100 inclusive.

Receive Error Rate The number of inbound packets or transmission units per minute that could not be received during the most recent sampling interval because of errors. The format is a four-byte unsigned integer.

Receive Packet Rate The number of packets received per minute during the most recent sampling interval. This rate applies to packets that were delivered by this sublayer to a higher sublayer and were not addressed to a multicast or broadcast address at this sublayer. The format is an unsigned integer.

Received Packets Discarded in Error The number of input packets discarded due to an error validating the packet during the last collection interval. The format is an unsigned integer.

Reset Time Stamp The time and date when the counters were last reset to zero. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour

- M = Minute
- S = Second
- m = Millisecond

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Total Broadcast Packets Received The number of input packets addressed to a broadcast address since the statistics were last reset. The format is an unsigned long long integer.

Total Broadcast Packets Transmitted The number of output packets addressed to a broadcast address since the statistics were last reset. The format is an unsigned long long integer.

Total Bytes Received The number of input bytes since the statistics were last reset. The format is an unsigned long long integer.

Total Bytes Received or Transmitted The number of bytes sent and received since the statistics were last reset. The format is an unsigned long long integer.

Total Bytes Transmitted The number of output bytes since the statistics were last reset. The format is an unsigned long long integer.

Total Inbound Packets Discarded in Error The number of input packets discarded due to an error validating the packet since the statistics were last reset. The format is an unsigned integer.

Total Multicast Packets Received The number of input packets addressed to a multicast address since the statistics were last reset. The format is an unsigned long long integer.

Total Multicast Packets Transmitted The number of output packets addressed to a multicast address since the statistics were last reset. The format is an unsigned long long integer.

Total Outbound Packets Discarded in Error The number of outbound packets discarded due to errors other than an out-of-storage condition since the statistics were last reset. The format is an unsigned integer.

Total Outbound Packets Discarded for No Storage The number of output packets discarded due to an out-of-storage condition since the statistics were last reset. The format is an unsigned integer.

Total Outbound Packets Queued The number of output packets that are queued and waiting for neighbor resolution since the statistics were last reset. The format is an unsigned integer.

Total Packets Discarded for Unknown Protocol The number of input packets discarded due to an unknown protocol type since the statistics were last reset. The format is an four-byte unsigned integer.

Total Received Packets Discarded for No Storage The number of input packets discarded due to an out-of-storage condition since the statistics were last reset. The format is an four-byte unsigned integer.

Total Unicast Packets Received The number of input unicast packets not addressed to a multicast or broadcast address since the statistics were last reset. The format is an unsigned long long integer.

Total Unicast Packets Transmitted The number of output packets not addressed to a multicast or broadcast address since the statistics were last reset. The format is an unsigned long long integer.

Transmit Bandwidth Utilization The percentage of bandwidth being used to transmit data during the most recent sampling interval. The format is an integer between 0 and 100 inclusive.

Transmit Error Rate The number of outbound packets or transmission units, per minute, that could not be transmitted during the most recent sampling interval because of errors. The format is a four-byte unsigned integer.

Transmit Packet Rate The number of packets sent, per minute, during the most recent sampling interval. This rate applies to packets that higher-level protocols requested be transmitted and were not addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent. The format is an unsigned integer.

KN3 Interface Status Attributes

Use the KN3 Interface Status attributes to display status information for all interfaces defined to a z/OS(R) v1r12 or later system.

Notes:

1. This attribute group is available only on systems running z/OS v1.12 or later.
2. A blank in any of these fields means that this attribute does not apply to this interface either at all or at this time.

Actual Dynamic Type The actual dynamic inbound performance type. This value is stored as an integer and displayed as a string. Valid values are:

- 128 = WORKLOADQ_in_effect

The value for this attribute will be non-zero only when the Actual Inbound Performance Type has a value of DYNAMIC.

This value is specified with the INBPERF optional parameter on the LINK statement in the TCPIP.PROFILE dataset. The DYNAMIC setting causes the host to dynamically signal the OSA-Express feature to change the timer-interrupt value, based on current inbound workload conditions. The DYNAMIC setting is effective only for OSA-Express2 features on an IBM System z9® EC or z9® BC with the corresponding Dynamic LAN Idle functional support. See the *IBM z/OS Communications Server IP Configuration Reference* for more information.

Actual Inbound Performance Type The actual inbound performance type. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = BALANCED
- 2 = DYNAMIC
- 3 = MINCPU
- 4 = MINLATENCY

This value is specified with the INBPERF optional parameter on the LINK statement in the TCPIP.PROFILE dataset and indicates how frequently the OSA adapter should interrupt the host for inbound traffic. See the *IBM z/OS Communications Server IP Configuration Reference* for more information.

Actual MTU Value The actual maximum transmission unit (MTU) value. The format is a 2-byte unsigned integer.

Maximum transmission unit (MTU), or maximum packet size in TCP/IP terms is the maximum size for the data field. For a static route, the MTU size for a route is configured using the on either a ROUTE statement in a BEGINROUTES block or on a GATEWAY statement in the TCP/IP profile. For each IPv4 dynamic route added by OMPROUTE over an interface, the configured route MTU comes from the value of the MTU keyword specified on the RIP_INTERFACE, OSPF_INTERFACE or INTERFACE statement in the TCPIP.PROFILE dataset for that interface in the OMPROUTE configuration file. If you do not specify an MTU for an interface, OMPROUTE uses 576. For IPv6, OMPROUTE learns the interface MTU value from TCP/IP, and you cannot specify a configured route MTU in the OMPROUTE configuration file.

See the *IBM z/OS Communications Server IP Configuration Guide* for more information about this parameter.

Actual Router Type The actual router type. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = NONROUTER
- 2 = PRIROUTER
- 3 = SECROUTER

These router type values are optional parameters on the z/OS Communications Server DEVICE statement in the TCPIP.PROFILE dataset that control the behavior of a datagram that is received at the subject

device from an unknown IP address. See the *IBM z/OS Communications Server IP Configuration Reference* for more information.

ARP Offload Active Indicates whether the Address Resolution Protocol (ARP) offload function is active for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

The ARP Offload function can be configured to cause all ARP processing to the offloaded to the OSA adapter. See the *z/OS Communications Server IP Configuration Guide* for more information about this function.

ARP Offload Reported Indicates whether the Address Resolution Protocol (ARP) offload function is being reported to the TCP/IP stack for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

The ARP Offload function can be configured to cause all ARP processing to the offloaded to the OSA adapter. See the *IBM z/OS Communications Server IP Configuration Guide* for more information about this function.

ARP or ND/VIPA Owner Indicates whether this interface is the owner of the Address Resolution Protocol or the Neighbor Discovery/ Virtual IP Address(ND/VIPA) process for this virtual LAN (VLAN) group. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

See the *IBM z/OS Communications Server IPv6 Network and Application Design Guide* for more information about this function.

Autorestart Active Indicates whether the autorestart function is active for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

AUTORESTART is a parameter on the z/OS Communications Server DEVICE statement in the TCPIP.PROFILE dataset that controls device failure reactivation behavior. NOAUTORESTART is the default parameter. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Checksum Offload Active Indicates whether the checksum offload function is active for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

CHECKSUM is a parameter on the LINK statement in the TCPIP.PROFILE dataset. With checksum offloading active, TCP/IP offloads most IPv4 (outbound and inbound) checksum processing (IP header, TCP, and UDP checksums) to the OSA. See *IBM z/OS Communications Server IP Configuration Guide* for more information about this parameter.

CHPID The Channel Path Identifier (CHPID) value for this interface. This value is set for Hipersockets, active OSA, and inactive OSA OSX interfaces. The format is an unsigned integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Configured Dynamic Type The configured dynamic type. This value is stored as an integer and displayed as a string. Valid values are:

- 128 = WORKLOADQ_specified

The value for this attribute will be non-zero only when the Actual Inbound Performance Type has a value of DYNAMIC.

This value is specified with the INBPERF optional parameter on the LINK statement in the TCPIP.PROFILE dataset. The DYNAMIC setting causes the host to dynamically signal the OSA-Express feature to change the timer-interrupt value, based on current inbound workload conditions. The DYNAMIC setting is effective only for OSA-Express2 features on an IBM System z9 EC or z9 BC with the corresponding Dynamic LAN Idle functional support. See the *IBM z/OS Communications Server IP Configuration Reference* for more information.

Configured Inbound Performance Type The configured inbound performance type. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = BALANCED
- 2 = DYNAMIC
- 3 = MINCPU
- 4 = MINLATENCY

This value is specified with the INBPERF optional parameter on the LINK statement in the TCPIP.PROFILE dataset and indicates how frequently the OSA adapter should interrupt the host for inbound traffic. See the *IBM z/OS Communications Server IP Configuration Reference* for more information.

Configured MTU Value The configured maximum transmission unit (MTU) value. The format is a 2-byte unsigned integer.

Maximum transmission unit (MTU), or maximum packet size in TCP/IP terms, is the maximum size for the data field. For a static route, the MTU size for a route is configured using either a ROUTE statement in a BEGINROUTES block or on a GATEWAY statement in the TCP/IP profile. For each IPv4 dynamic route added by OMPROUTE over an interface, the configured route MTU comes from the value of the MTU keyword specified on the RIP_INTERFACE, OSPF_INTERFACE or INTERFACE statement in the TCPIP.PROFILE dataset for that interface in the OMPROUTE configuration file. If you do not specify an MTU for an interface, OMPROUTE uses 576. For IPv6, OMPROUTE learns the interface MTU value from TCP/IP, and you cannot specify a configured route MTU in the OMPROUTE configuration file.

See the *IBM z/OS Communications Server IP Configuration Guide* for more information about this parameter.

Configured Router Type The configured router type. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = NONROUTER
- 2 = PRIROUTER
- 3 = SECROUTER

These router type values are optional parameters on the z/OS Communications Server DEVICE statement in the TCPIP.PROFILE dataset that controls the behavior of a datagram that is received at the subject device for an unknown IP address. The default is NONROUTER (do not route the datagram). See the *IBM z/OS Communications Server IP Configuration Reference* for more information.

Datapath Device Number The datapath device number. This field is valid only for IPAQENET and IPAQENET6 interfaces. The format is an unsigned integer.

Destination Address The routing destination address. The format is an alphanumeric string no longer than 45 characters.

This address only applies to IPv4 multipath channel (MPC) point-to-point device (PTP) interface defined by DEVICE/LINK profile statements. The value is set by the following parameters:

- BSDROUTINGPARMS profile statement
- OMPROUTE configuration statement
- Stack sets default of gateway address or destination addr of a route over the interface.

Device or Datapath Status The device or datapath status. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = Starting
- 2 = Sent_Setup
- 3 = Enabling
- 4 = Connecting
- 5 = Connecting2
- 6 = Negotiating
- 7 = Active
- 8 = Deactivating
- 9 = Not_Active

Duplicate Address Count The number of times to attempt duplicate address detection for this interface. The format is a 2-byte unsigned integer.

This value is specified with the optional DUPADDRDET *count* parameter on the INTERFACE statement in the TCPIP.PROFILE dataset. This parameter is used to specify the number of times to attempt duplicate address detection. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Dynamic VLAN Registration Capable Indicates whether this interface is capable of handling dynamic virtual LAN (VLAN) registration. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

Dynamic VLAN registration is a parameter on the z/OS Communications Server LINK statement in the TCPIP.PROFILE dataset that controls VLAN ID configuration behavior for this link. Dynamic registration of VLAN IDs is handled by the OSA-Express feature and the physical switch on your LAN. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Dynamic VLAN Registration Configured Indicates whether this interface is configured for dynamic virtual LAN (VLAN) registration. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

Dynamic VLAN registration is a parameter on the z/OS Communications Server LINK statement in the TCPIP.PROFILE dataset that controls VLAN ID configuration behavior for this link. Dynamic registration of VLAN IDs is handled by the OSA-Express feature and the physical switch on your LAN. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Dynamic XCF Interface Indicates whether this interface was created by the dynamic cross-system coupling facility (Dynamic XCF). This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

The dynamic cross-system coupling facility (Dynamic XCF) creates a single IP address by which all other stacks in a sysplex can reach a stack. Dynamic XCF support is available for both IPv4 and IPv6, and is enabled with the DYNAMICXCF parameter on the IPCONFIG or IPCONFIG6 statement, respectively. See the *IBM z/OS Communications Server IP Configuration Guide* for more information about this parameter.

Interface Associated Name The interface Associated Name, when available, is the name of the DEVICE, PORT or TRLE associated with the interface. The format is an alphanumeric string no longer than 16 characters.

Interface Definition The indicator of how this interface is defined. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Device_Link
- 1 = Interface

IPv4 interfaces may be defined with either the DEVICE/LINK or INTERFACE statements. IPv6 interface are defined with the INTERFACE statements in the TCPIP.PROFILE dataset.

Interface Description More information about the values shown by the Interface Type attribute. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = Loopback
- 2 = OSA-Express_QDIO_Ethernet_OSD
- 3 = OSA-Express_QDIO_Ethernet_OSM
- 4 = OSA-Express_QDIO_Ethernet_OSX
- 5= HiperSockets
- 6= Multipath_Channel_Point-to-Point
- 7= Multipath_Channel_Point-to-Point_Samehost
- 8= Multipath_Channel_Point-to-Point_XCF
- 9= Virtual_IP_Address
- 10 = ATM
- 11 = IBM_CLAW
- 12 = Channel_to_Channel_(3088)
- 13 = Network_Systems_Hyperchannel
- 14 = LAN_Channel_Station_Ethernet_V2
- 15 = LAN_Channel_Station_Ethernet_802.3
- 16 = LAN_Channel_Station_Ethernet_(V2_or_802.3)
- 17 = LAN_Channel_Station_Token Ring

- 18 = LAN_Channel_Station_FDDI
- 19 = OSA-Express_QDIO_Token_RIng
- 20 = MPC_OSA_Fast_Ethernet
- 21 = MPC_OSA_FDDI
- 22 = SNA_LU0
- 23 = SNA_LU6.2
- 24 = X.25_NPSI
- 25 = IP-over-Channel_(CDLC)

Interface ID The IPv6 interface identifier. The format is an alphanumeric string no longer than 19 characters.

The Interface ID is a number that uniquely identifies the interface among the collection of all OSPF interfaces on this TCP/IP stack It is specified with the option INTFID *interface_id* parameter on the INTERFACE statement in the TCPIP.PROFILE datase. It is a 64-bit interface identifier in colon-hexadecimal format. If INTFID is not coded, TCP/IP generates a random value to be used to form the link-local address. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Interface ID Specified Indicates whether the interface ID for this interface is active. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

The Interface ID is a number that uniquely identifies the interface among the collection of all OSPF interfaces on this TCP/IP stack It is specified with the option INTFID *interface_id* parameter on the INTERFACE statement in the TCPIP.PROFILE datase. It is a 64-bit interface identifier in colon-hexadecimal format. If INTFID is not coded, TCP/IP generates a random value to be used to form the link-local address. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Interface Index (not displayed) The interface index. For interfaces defined by DEVICE and LINK, this is the LINK interface index. The format is a 4-byte unsigned integer.

Interface Index Specified The interface index. For interfaces defined by DEVICE and LINK, this is the LINK interface index. The format is a 4-byte unsigned integer.

Interface Name The interface Name. The format is an alphanumeric string no longer than 16 characters.

This value is specified with the *intf_name* parameter on the INTERFACE statement or the *link_name* parameter on the LINK statement in the TCPIP.PROFILE dataset. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Interface Speed The interface speed, expressed as million bits per second. The format is a 4-byte unsigned integer.

This field applies to the following interface types only:

- OSA-Express_QDIO_Ethernet_OSD
- OSA-Express_QDIO_Ethernet_OSM
- OSA-Express_QDIO_Ethernet_OSX

The value is specified with the optional IFHSPEED *ifhspeed* parameter on the LINK statement in the TCPIP.PROFILE dataset and is defined as an estimate of the interface's current bandwidth in one million bits per second units. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Interface Status The status of this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = Active

- 2 = Not_Active
- 3 = DAD_Pending

Interface Type The type of interface. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = Loopback
- 2 = OSA_QDIO_ethernet_OSD
- 3 = OSA_QDIO_ethernet_OSM. This is the intranode management network (INMN), a private 1000BASE-T Ethernet network operating at 1 Gbps that is required for the Unified Resource Manager to manage the resources within a single zEnterprise(TM) node. The INMN connects the Support Element (SE) to the z196 and to any attached zBX. This interface is associated with the zEnterprise(TM) mainframe server.
- 4 = OSA_QDIO_ethernet_OSX. This is the private 10 Gigabit Ethernet network for application data communications within an ensemble. Data communications for workloads can flow over the IEDN within and between nodes of an ensemble. All of the physical and logical resources of the IEDN are configured, provisioned, and managed by the Unified Resource Manager. This interface is associated with the zEnterprise(TM) mainframe server.
- 5 = Hipersocket
- 6 = MPC_ptp
- 7 = MPC_ptp_samehost
- 8 = MPC_ptp_xcf
- 9 = Static_virtual
- 10 = ATM
- 11 = CLAW
- 12 = CTC
- 13 = HCH
- 14 = LCS_ethernet_V2
- 15 = LCS_ethernet_8023
- 16 = LCS_ethernet_V2OR8023
- 17 = LCS_tokenring
- 18 = LCS_FDDI
- 19 = OSA_QDIO_tokenring
- 20 = MPCOSA_ethernet
- 21 = MPCOSA_FDDI
- 22 = SNA_LU0
- 23 = SNA_LU62
- 24 = X25_NPSI
- 25 = CDLC

IP Address Version The version of the IP address used by this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4
- 1 = IPv6

ISOLATE Specified Indicates whether the ISOLATE parameter is being specified on the INTERFACE statement in the TCPIP PROFILE dataset for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

The NOISOLATE and ISOLATE are parameters for the IPAQENET and IPAQENET6 OSA-Express queued direct input/output (QDIO) interfaces on the INTERFACE statement in the TCPIP.PROFILE dataset. They are used to disable and enable connection isolation. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

LAN ARP or ND Owner The name of the interface that owns Address Resolution Protocol (ARP) or Neighbor Discovery (ND) responsibility for this interface. The format is an alphanumeric string no longer than 16 characters.

The IPv4 networking layer uses the Address Resolution Protocol (ARP) to map an IP address into a hardware address. In the IPv6 networking layer, this mapping is performed by the Neighbor Discovery (ND function). On local area networks (LANs), such an address is called a media access control (MAC) address. See the *IBM z/OS Communications Server IPv6 Network and Application Design Guide* for more information about this function.

LAN Group Number The number of the LAN group to which this interface belongs. The format is a 2-byte unsigned integer.

Last Status Change The z/OS time and date of the last time that the interface status values changed. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

MONSYSPLEX Active Indicates whether MONSYSPLEX is ACTIVE for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

MONSYSPLEX is a parameter on the INTERFACE statement in the TCPIP.PROFILE dataset. It specifies that sysplex autonomics should monitor the interface's status. This parameter can be modified dynamically using the VARY TCPIP,,OBEYFILE command. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

MONSYSPLEX Configured Indicates whether the indicator for MONSYSPLEX has been configured for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No

- 1 = Yes

MONSYSPLEX is a parameter on the INTERFACE statement in the TCPIP.PROFILE dataset. It specifies that sysplex autonomics should monitor the interface's status. This parameter can be modified dynamically using the VARY TCPIP,,OBEYFILE command. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

MPCPTP Checksum An indicator of whether the CHECKSUM parameter was specified on the LINK statement in the TCPIP PROFILE dataset for this multipath channel (MPC) point-to-point device (PTP) interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Multicast Capable An indicator of whether this interface is capable of handling multicast packets. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

Multicast capability is a characteristic of a number of IP commands. Use the NETSTAT command to determine if the interface is multicast capable. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about commands with multicast dependencies.

Multiwrite Status The hipersockets multiwrite status when the interface is in the ACTIVE state. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = Enabled
- 2 = Enabled_ZIIP
- 3 = Disabled
- 4 = Unsupported

Multiwrite status is determined with the IQDMULTIWRITE and NOIQDMULTIWRITE parameters on the GLOBALCONFIG command. HiperSockets multiple write might reduce CPU usage and might provide a performance improvement for large outbound messages that are typically generated by traditional streaming workloads such as file transfer, and interactive web-based services workloads such as XML or SOAP. This parameter applies to all HiperSockets interfaces See the *IBM z/OS Communications Server IP Configuration Guide* for more information about HiperSockets multiple write support.

OLM Active Indicates whether optimized latency mode (OLM) function is ACTIVE for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

To configure an OSA-Express3 feature to operate in optimized latency mode, use the INTERFACE statement in the TCPIP.PROFILE dataset with the OLM parameter. Because optimized latency mode affects both inbound and outbound interrupts, it supersedes other inbound performance settings set by the INBPERF parameter. For more information about optimized latency mode and the OLM and INBPERF parameters on the INTERFACE statement for IPAQENET and IPAQENET6, see the *IBM z/OS Communications Server IP Configuration Reference* .

OLM Configured Indicates whether optimized latency mode (OLM) parameter was configured for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

To configure an OSA-Express3 feature to operate in optimized latency mode, use the INTERFACE statement in the TCPIP.PROFILE dataset with the OLM parameter. Because optimized latency mode

affects both inbound and outbound interrupts, it supersedes other inbound performance settings set by the INBPERF parameter. For more information about optimized latency mode and the OLM and INBPERF parameters on the INTERFACE statement for IPAQENET and IPAQENET6, see the *IBM z/OS Communications Server IP Configuration Reference*.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

OSA Code Level The OSA code level. The format is a 2-byte unsigned integer that is displayed in hexadecimal format.

To determine the OSA-Express microcode level, use the DISPLAY TRL command. If a specific OSA-Express function is documented with a minimum microcode level, you can use this command to determine whether that function is supported. IBM service might request the microcode level for problem diagnosis. For more information about the DISPLAY TRL command, see *IBM z/OS Communications Server SNA Operation*.

Outbound Hop Limit The outbound hop limit for IPAQENET6 interface type. The value is either provided by a router advertisement or, if IGNOREROUTERHOPLIMIT was specified on IPCONFIG6, it is the global HOPLIMIT value from IPCONFIG6. The format is a 2-byte unsigned integer.

The IPv6 header contains a hop limit field that controls the number of hops over which a datagram can be sent before being discarded. This field is similar to the TTL field in the IPv4 header. The IPAQENET6 interface specifies IPv6 OSA-Express queued direct input/output (QDIO) interfaces. See the *IBM z/OS Communications Server IP Network and Application Design Guide* for more information about this parameter.

Physical MAC Address The physical MAC address. The format is an alphanumeric string no longer than 17 characters in colon-hexadecimal format.

Port Interface Index The OSA-Express QDIO port interface index. For interfaces defined by DEVICE and LINK, this index is the DEVICE interface index. For interfaces defined by INTERFACE, this interface is the dynamically generated interface index for the port. This field only applies to the following interface types:

- OSA-Express_QDIO_Ethernet_OSD (external data network type, which is the default value)
- OSA-Express_QDIO_Ethernet_OSM (intra-node management network, which requires IPv6)
- OSA-Express_QDIO_Ethernet_OSX (intra-ensemble data network)

The format is an unsigned integer. For more information about these interface types, see *IBM z/OS Communications Server: IP Configuration Guide*.

Read Storage Size The actual amount of storage currently allocated to READSTORAGE, expressed as 64K blocks. The format is a 2-byte unsigned integer.

This value is specified with the READSTORAGE optional parameter on the LINK statement in the TCPIP.PROFILE dataset. It indicates the amount of fixed storage that z/OS Communications Server should keep available for read processing for this OSA adapter. The READSTORAGE parameter is also available on INTERFACE statements for certain types of interfaces. See the *IBM z/OS Communications Server IP Configuration Guide* for more information about this parameter.

Read Storage Type The read storage type. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = GLOBAL
- 2 = MAX
- 3 = AVG
- 4 = MIN

This value is specified with the READSTORAGE optional parameter on the LINK statement in the TCPIP.PROFILE dataset. It indicates the amount of fixed storage that z/OS Communications Server should keep available for read processing for this OSA adapter. See the *IBM z/OS Communications Server IP Configuration Guide* for more information about this parameter.

Routing Mask Bits The routing subnet number of mask bits for IPv4 interfaces. The format is a 2-byte unsigned integer.

The number of mask bits (*num_mask_bits* parameter on a number of IP commands) is an integer in the range 1 - 32 that represents the number of bits, counting from left to right, of the network and subnet portion of the IPv4 address mask. The value may be set using any of the following methods:

- INTERFACE profile statement
- BSDROUTINGPARMS profile statement
- DYNAMICXCF parm on the IPCONFIG profile statement
- OMPROUTE configuration statement
- IP address class mask

See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Routing Metric The routing metric or hop count for this interface. The format is a 2-byte unsigned integer.

This attribute applies only to IPv4 interfaces defined by DEVICE/LINK profile statements or by the DYNAMICXCF parm on IPCONFIG profile statement. This value may be set using one of the following methods:

- BSDROUTINGPARMS profile statement
- DYNAMICXCF parm on IPCONFIG profile statement
- OMPROUTE configuration statement

See the *IBM z/OS Communications Server IP Configuration Guide* for more information about defining this parameter.

Routing MTU Size The routing maximum transmission unit (MTU) size. The format is a 2-byte unsigned integer.

Maximum transmission unit (MTU), or maximum packet size in TCP/IP terms is the maximum size for the data field. For a static route, the MTU size for a route is configured using the on either a ROUTE statement in a BEGINROUTES block or on a GATEWAY statement in the TCP/IP profile. For each IPv4 dynamic route added by OMPROUTE over an interface, the configured route MTU comes from the value of the MTU keyword specified on the RIP_INTERFACE, OSPF_INTERFACE or INTERFACE statement in the TCPIP.PROFILE datasetfor that interface in the OMPROUTE configuration file. If you do not specify an MTU for an interface, OMPROUTE uses 576. For IPv6, OMPROUTE learns the interface MTU value from TCP/IP, and you cannot specify a configured route MTU in the OMPROUTE configuration file.

See the *IBM z/OS Communications Server IP Configuration Guide* for more information about this parameter.

SECCLASS Value The SECCLASS (security class) value for this interface. The format is a 2-byte unsigned integer.

The SECCLASS value is a parameter on the LINK or INTERFACE statements used to associate a security class for IP filtering with this interface. See the *IBM z/OS Communications Server IP Configuration Guide* for more information about this parameter.

Send Receive Broadcast Packets Indicates whether this interface is capable of sending and receiving broadcast packets. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

The ability to send and receive broadcast packets is specified on many IP commands with the IPBCAST parameter, which specifies that the interface both sends and receives IP broadcast packets. If this parameter is not specified, no IP broadcast packets are sent or received on this interface. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Source VIPA Name The name of the source virtual IP address (VIPA) interface. The format is an alphanumeric string no longer than 16 characters.

This value is specified with the optional SOURCEVIPAINTERFACE *vipa_name* parameter on the INTERFACE command. It specifies which previously defined static VIPA interface is to be used for SOURCEVIPA (when IPCONFIG6 SOURCEVIPA is specified). For more information, see the default source address selection algorithm information in the *IBM z/OS Communications Server in z/OS IPv6 Network and Application Design Guide* or the *z/OS Communications Server IP Configuration Reference*.

Source VIPA Specified Indicates whether the source virtual IP address (VIPA) interface name is specified for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

This value is specified with the optional SOURCEVIPAINTERFACE *vipa_name* parameter on the INTERFACE command. It specifies which previously defined static VIPA interface is to be used for SOURCEVIPA (when IPCONFIG6 SOURCEVIPA is specified). For more information, see the default source address selection algorithm information in the *IBM z/OS Communications Server in z/OS IPv6 Network and Application Design Guide* or the *IBM z/OS Communications Server IP Configuration Reference*.

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCP Segmentation Offload Active Indicates whether the TCP segmentation offload function is active for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

The TCP/IP stack can offload most IPv4 outbound TCP segmentation processing to an OSA-Express feature in queued direct input/output (QDIO) mode using TCP segmentation offload support. You can configure this function by specifying the SEGMENTATIONOFFLOAD parameter on the GLOBALCONFIG profile statement. See the *IBM z/OS Communications Server IP Configuration Guide* for more information about this parameter.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Temporary IP Address Prefix Indicates whether the temporary IP address prefix is being specified for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

This value is specified with the ADDTEMPPREFIX parameter of the IPAQENET6 interface statement. This prefix represents the number of unmasked leading bits in the ipaddress value. The prefix length value can be in the range 0 - 127 for IPv6 addresses. An IP packet matches this condition if its unmasked bits are identical to the unmasked bits defined. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Temporary Prefix Type The temporary prefix type. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = ALL
- 2 = Prefix_specified
- 3 = NONE
- 4 = Disabled_DAD_failures

This value is specified with the ADDTEMPPREFIX parameter of the IPAQENET6 interface statement. This prefix represents the number of unmasked leading bits in the ipaddress value. The prefix length value can be in the range 0 - 127 for IPv6 addresses. An IP packet matches this condition if its unmasked bits are identical to the unmasked bits defined. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

VLAN ID The virtual LAN (VLAN) identifier. The format is a 2-byte unsigned integer.

The VLAN ID is an optional parameter followed by a decimal number indicating the Virtual LAN identifier to be assigned to the OSA-Express INTERFACE. See the *IBM z/OS Communications Server IP Configuration Reference* for more information.

VLAN ID Specified Indicates whether a virtual LAN (VLAN) identifier is specified for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

The VLAN ID is an optional parameter followed by a decimal number indicating the Virtual LAN identifier to be assigned to the OSA-Express INTERFACE. See the *IBM z/OS Communications Server IP Configuration Reference* for more information.

VLAN Priority Tagging Active Indicates whether the virtual LAN (VLAN) priority tagging function is active for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

VLAN priority tagging extends the capabilities of priority queuing beyond the server to include LAN bridges and switches, providing a way to manage consistent QoS traffic prioritization and service differentiation end-to-end, across switched LAN and WAN networks. See the *IBM z/OS Communications Server IP Configuration Guide* and the *IBM System z9 and zSeries Open Systems Adapter-Express Customer's Guide and Reference* for more information about this attribute.

VMAC Active Indicates whether the Virtual MAC (VMAC) address function is ACTIVE for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

VMAC is a parameter on the INTERFACE statement. VMAC specifies the virtual MAC address, which can be represented by 12 hexadecimal characters. The OSA-Express device uses this address rather than the physical MAC address of the device for all IPv4 packets sent to and received from this TCP/IP stack. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

VMAC Address Specified Indicates whether the Virtual MAC (VMAC) address is specified for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

VMAC is a parameter on the INTERFACE statement. VMAC specifies the virtual MAC address, which can be represented by 12 hexadecimal characters. The OSA-Express device uses this address rather than the physical MAC address of the device for all IPv4 packets sent to and received from this TCP/IP stack. See the *IBM z/OS Communications Server IP Configuration Reference* for more information about this parameter.

VMAC ROUTELCL Active Indicates whether the ROUTELCL parameter (meaning route only packets that come from registered IP addresses to the VMAC) is active in the Virtual MAC (VMAC) address definition for this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

ROUTELCL is a parameter on the INTERFACE statement. It specifies that only traffic destined for the virtual MAC and whose destination IP address is registered with the OSA-Express device by this TCP/IP stack is forwarded by the OSA-Express. See the router information in the *IBM z/OS Communications Server IP Configuration Guide* for more information about this parameter.

KN3 Interface Write Queue Attributes

Use the KN3 Interface Write Queue attributes to display data link control (DLC) tuning statistics for each write queue supported for an active datapath device used by an OSA-Express QDIO ethernet or HiperSockets interface.

Note: This workspace returns data only on systems running z/OS v1.12 or later

Accelerated Bytes The number of transmitted bytes that were routed outbound using internal queued direct I/O (iQDIO) routing or QDIO Accelerator since the statistics were last reset. This attribute applies to IPv4 interfaces only. The format is an unsigned long long integer.

Accelerated Packets The number of transmitted packets that were routed outbound using internal queued direct I/O (iQDIO) routing or QDIO Accelerator since the statistics were last reset. This attribute applies to IPv4 interfaces only. The format is an unsigned long long integer.

Average Active SBALs The average number of active storage block address lists (SBALs) since the statistics were last reset. The format is an unsigned integer between 0 - 128 inclusive.

This counter represents the smoothed average number of SBALs waiting to be written. The average is calculated when the device driver write initiator has built as many writes as possible (due either to no remaining SBALs or no more data to be written) and is about to exit.

Average SBALs Per SIGA The average number of storage block address lists (SBALs) written per signal adapter (SIGA) since the statistics were last reset. The format is an unsigned integer.

For OSA-Express interfaces, an SBAL represents 16 4K write buffers (a single 64K write). For HiperSockets interfaces, the SBAL size is variable. For a specific write operation, all buffers might not be used (for example, those containing outbound packets).

Average Staging Queue Depth The average number of work elements that remained on the outbound work queue since the statistics were last reset. This format is one of the following:

- A number in the range of 0-254 inclusive
- 255, meaning that more than 254 elements remained

A nonzero value indicates that the interface is not accepting outbound data as fast as the device driver is presenting it. The maximum number is calculated each time the device driver write initiator has built as many writes as possible (due either to no remaining storage block address lists (SBALs) or no more data to be written) and is about to exit.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour

- M = Minute
- S = Second
- m = Millisecond

Datapath Device Number The datapath device number. The format is an unsigned 2-byte integer displayed in hexadecimal.

Frame Invalidation Support Indicates whether the Frame Invalidation Packets counter is supported for this interface. If this attribute value is **No**, the value of the Frame Invalidation Packets attribute is zero. If this attribute value is **Yes**, the value of the Frame Invalidation Packets attribute may be greater than zero. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

Interface Index The interface index associated with this interface. The format is an unsigned integer.

Interface Name The interface name sharing the write queue. The format is an alphanumeric string no longer than 16 characters.

This value is specified with the *intf_name* parameter on the INTERFACE statement or the *link_name* parameter on the LINK statement in the TCPIP.PROFILE dataset. See the *z/OS Communications Server IP Configuration Reference* for more information about this parameter.

Interface Status The status of this interface. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = Active
- 2 = Not_Active
- 3 = DAD_Pending

Interface Type The type of interface. This value is stored as an integer and displayed as a string. Valid values are:

- 2 = OSA_QDIO_ethernet_OSD
- 3 = OSA_QDIO_ethernet_OSM. This is the intranode management network (INMN), a private 1000BASE-T Ethernet network operating at 1 Gbps that is required for the Unified Resource Manager to manage the resources within a single zEnterprise(TM) node. The INMN connects the Support Element (SE) to the z196 and to any attached zBX. This interface is associated with the zEnterprise(TM) mainframe server.
- 4 = OSA_QDIO_ethernet_OSX. This is the private 10 Gigabit Ethernet network for application data communications within an ensemble. Data communications for workloads can flow over the IEDN within and between nodes of an ensemble. All of the physical and logical resources of the IEDN are configured, provisioned, and managed by the Unified Resource Manager. This interface is associated with the zEnterprise(TM) mainframe server.
- 5 = Hipersocket

IP Address Version The version of the IP address for the associated write queue. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4
- 1 = IPv6

iQDIO Multiple Write SIGA Count The number of internal queued direct I/O (iQDIO) multiple write signal adapter (SIGA) instructions issued since the statistics were last reset. This attribute applies to HiperSocket interfaces only when the IQDMULTIWRITE parameter is specified on the GLOBALCONFIG profile statement. The format is an unsigned long long integer.

Maximum Active SBALs The maximum number of active storage block address lists (SBALs) since the statistics were last reset. The format is an unsigned integer between 0 - 128 inclusive.

This counter represents the maximum number of SBALs waiting to be written. The maximum number is calculated each time the device driver write initiator has built as many writes as possible (due either to no remaining SBALs or no more data to be written) and is about to exit.

Maximum Staging Queue Depth The maximum number of work elements that remain on the outbound work queue since the statistics were last reset. The following formats are valid:

- A number in the range of 0-254 inclusive
- 255, meaning that more than 254 elements remain

A nonzero value indicates that the interface is not accepting outbound data as fast as the device driver is presenting it. The maximum number is calculated each time the device driver write initiator has built as many writes as possible (due either to no remaining storage block address lists (SBALs) or no more data to be written) and is about to exit.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Percent Accelerated Bytes The percentage of outbound bytes that were routed using internal queued direct I/O (iQDIO) routing or QDIO Accelerator since the statistics were last reset. The format is an integer between 0 and 100 inclusive.

Notes: This attribute applies to IPv4 interfaces only. The value is zero (0) for IPv6 interfaces.

Percent Accelerated Packets The percentage of outbound packets that were routed using internal queued direct I/O (iQDIO) routing or QDIO Accelerator since the statistics were last reset. The format is an integer between 0 and 100 inclusive.

Notes: This attribute applies to IPv4 interfaces only. The value is zero (0) for IPv6 interfaces.

QDIO Accelerator Whether or not internal queued direct I/O (QDIO) routing or the QDIO Accelerator is in effect. When this attributed displays as **Yes**, the following counters are being incremented:

- Accelerated Packets
- Accelerated Bytes

If this attribute displays as **No**, the counters might be non-zero but are not being incremented. This attribute applies to IPv4 interfaces only. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

QDIO SIGA Count The number of queued direct I/O (QDIO) signal adapter (SIGA) instructions issued since the statistics were last reset. The format is an unsigned long long integer.

A SIGA instruction tells the QDIO interface that data is ready to be written. QDIO interfaces support adding additional writes to a write already in progress, removing the need for a new SIGA instruction. A low value for this counter indicates that write processing is benefitting from this additional QDIO write function.

Queue Priority The queue priority to which the attributes in a row of data pertain. The format is an unsigned integer.

Reset Time Stamp The z/OS time stamp when the counter values were last reset to zero. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year

- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

SBALs Per SIGA The number of storage block address lists (SBALs) written per signal adapter (SIGA) during the most recent sampling interval. The format is an unsigned integer.

For OSA-Express interfaces, an SBAL represents 16 4K write buffers (a single 64K write). For HiperSockets interfaces, the SBAL size is variable. For a specific write operation, all buffers might not be used (for example, those containing outbound packets).

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Transmitted Bytes The number of transmitted bytes since the statistics were last reset. The format is an unsigned long long integer.

Transmitted Packets The number of transmitted packets since the statistics were last reset. The format is an unsigned long long integer.

TRLE Name The transport resource list (TRL) name for this interface. The format is a string of up to 8 characters.

Used SBALs The number of storage block address list (SBAL) control blocks used since the statistics were last reset. The format is an unsigned long long integer.

For OSA-Express interfaces, an SBAL represents 16 4K write buffers (a single 64K write). For HiperSockets interfaces, the SBAL size is variable. For a specific write operation, all buffers might not be used (for example, those containing outbound packets).

Write Control Device Number The write control device number. The format is an unsigned 2-byte integer displayed in hexadecimal.

KN3 IP Counter Statistics Attributes

Use the KN3 IP Counter Statistics attributes to display statistics for IPv4 and IPv6 on z/OS v1r12 or later systems.

Note: This attribute group is available only on systems running z/OS v1.12 or later.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year

- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Input Datagram Delivery Rate The rate at which input datagrams were delivered during the most recent sampling interval. The format is an integer.

Input Datagram Forward Rate The rate at which datagrams were forwarded during the most recent sampling interval. The format is an integer.

Input Datagrams Discarded The number of input datagrams that were discarded and are not accounted for in another input discard counter during the most recent sampling interval. The format is an unsigned integer.

Input Discard Percentage The percentage of IP segments that this TCP/IP address space received from the network that were undeliverable and discarded during the most recent sampling interval. The format is a number between 0 and 100 inclusive.

IP Version The version of IP used by this TCP/IP address space. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4
- 1 = IPv6

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Output Datagrams Discarded The number of output datagrams generated by this stack that could not be transmitted during the most recent sampling interval. The format is an unsigned integer.

Output Discard Percentage The percentage of IP segments that this TCP/IP address space sent to the network that were undeliverable and discarded during the most recent sampling interval. The format is a number between 0 and 100 inclusive.

Receive Datagram Rate The number of datagrams received per minute during the most recent sampling interval. The format is an integer.

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Total Fragmentation Creates The number of datagram fragments that have been generated as a result of fragmentation since TCP/IP initialization. The format is an unsigned integer.

Total Fragmentation Failure Percentage The percentage of IP segments requiring fragmentation that were not successfully fragmented since TCP/IP initialization. The format is a number between 0 and 100 inclusive.

Total Fragmentation Failures The number of datagrams discarded because they could not be fragmented since TCP/IP initialization. The format is an unsigned integer.

Total Fragmentation Percentage The percentage of IP segments successfully fragmented since TCP/IP initialization. The format is a number between 0 and 100 inclusive.

Total Fragmentations The number of datagrams successfully fragmented since TCP/IP initialization. The format is an unsigned integer.

Total Fragmentations Required The number of datagrams that required fragmentation in order to be transmitted since TCP/IP initialization. The format is an unsigned integer.

Total Header Errors The number of input datagrams discarded due to errors in their IP headers since TCP/IP initialization. The format is an unsigned integer.

Total Input Datagrams Delivered The number of input datagrams successfully delivered to IP user protocols since TCP/IP initialization. The format is an unsigned long long integer.

Total Input Datagrams Discarded The number of input datagrams that was discarded that are not accounted for in another input discard counter since TCP/IP initialization. The format is an unsigned integer.

Total Input Datagrams Forwarded The number of input datagrams forwarded to their final destination since TCP/IP initialization. The format is an unsigned long long integer.

Total Input Datagrams Received The number of input datagrams received from interfaces since TCP/IP initialization. The format is an unsigned long long integer.

Total Input Discard Percentage The percentage of IP segments this TCP/IP address space received from the network that were undeliverable and discarded since TCP/IP initialization. The format is a number between 0 and 100 inclusive.

Total Input zIIP Packets The number of input packets that were processed by System z® Integrated Information Processors (zIIP) since TCP/IP initialization. This counter applies only to IPSec workloads, whose CPU cycles are being displaced to a zIIP. The format is an unsigned integer.

Total Invalid Address Errors The number of input datagrams discarded because the IP address in the IP header destination field was invalid since TCP/IP initialization. The format is an unsigned integer.

Total No Route Errors The number of input datagrams discarded because no route could be found to transmit them to their destination since TCP/IP initialization. The format is an unsigned integer.

Total Output Datagram Requests The number of datagrams that local IP user protocols supplied to IP in requests for transmission since TCP/IP initialization. The format is an unsigned long long integer.

Total Output Datagrams Discarded The number of output datagrams generated by this stack that could not be transmitted since TCP/IP initialization. The format is an unsigned integer.

Total Output Datagrams Forwarded The number of datagrams for which this stack was not their final IP destination and for which the stack was successful in finding a path to their final destination since TCP/IP initialization. The format is an unsigned long long integer.

Total Output Discard Percentage The percentage of IP segments that this TCP/IP address space sent to the network that were undeliverable and discarded since TCP/IP initialization. The format is a number between 0 and 100 inclusive.

Total Output No Routes The number of output datagrams discarded because no routes could be found to transmit them to their final destinations since TCP/IP initialization. The format is an unsigned integer.

Total Output zIIP Packets The number of output packets that were processed by System z Integrated Information Processors (zIIP) since TCP/IP initialization. This counter applies only to IPSec workloads with CPU cycles that are displaced to a zIIP. The format is an unsigned integer.

Total Reassemblies The number of datagrams successfully reassembled since TCP/IP initialization. The format is an unsigned integer.

Total Reassemblies Required The number of fragments received that needed to be reassembled since TCP/IP initialization. The format is an unsigned integer.

Total Reassembly Failure Percentage The percentage of IP segments requiring reassembly that could not be reassembled since TCP/IP initialization. The format is a number between 0 and 100 inclusive.

Total Reassembly Failures The number of failures detected by the IP reassembly algorithm since TCP/IP initialization. The format is an unsigned integer.

Total Reassembly Percentage The percentage of IP segments reassembled successfully since TCP/IP initialization. The format is a number between 0 and 100 inclusive.

Total Reassembly Timeouts The number of datagrams that were being held for reassembly but were discarded because the remaining fragments were not received within the reassembly timeout period since TCP/IP initialization. The format is an unsigned integer.

Total Truncation Errors The number of input datagrams discarded because the datagram frame did not carry enough data since TCP/IP initialization. The format is an unsigned integer.

Total Unknown Protocol Errors The number of input datagrams discarded because of an unknown or unsupported protocol since TCP/IP initialization. The format is an unsigned integer.

Transmit Datagram Rate The number of datagrams submitted to be transmitted per minute during the most recent sampling interval. The format is an integer.

KN3 IP General Statistics Attributes

Use the KN3 IP General Statistics attributes to displays statistics for IPv4 and IPv6 on z/OS v1r12 or later systems.

Note: This attribute group is available only on systems running z/OS v1.12 or later.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Total Device Layer Calls The number of times that the inbound TCP/IP Data Path has received control from the Device Layer of TCP/IP since TCP/IP initialization. The format is an unsigned integer.

Total Frame Unpack Errors The number of times that a received frame could not be unpacked into its constituent datagrams since TCP/IP initialization. The format is an unsigned integer.

Total Input Datagrams Discarded for Memory Shortage The number of input datagrams that were discarded due to a Communications Storage Manager (CSM) storage shortage condition since TCP/IP initialization. The format is an unsigned integer.

Total Output Datagrams Discarded for Asynchronous Error The number of output datagrams that were discarded due to an asynchronous error in the Data Link Control since TCP/IP initialization. The format is an unsigned integer.

Total Output Datagrams Discarded for Memory Shortage The number of output datagrams that were discarded due to a Communications Storage Manager (CSM) storage shortage condition since TCP/IP initialization. The format is an unsigned integer.

Total Output Datagrams Discarded for Synchronous Error The number of output datagrams that were discarded due to a synchronous error in the Data Link Control since TCP/IP initialization. The format is an unsigned integer.

KN3 OSA-Express5S Ports Control Attributes

Use the KN3 OSA-Express5S Ports Control attributes to monitor individual ports on a OSA-Express5S feature.

There can be two physical ports on each OSA channel path identifier, each with different data. When two ports are present, each one is assigned a separate ifIndex by the operating system. Each ifIndex contains the data for the corresponding port.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of two hexadecimal characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Pause Frames Received The number of pause frames received during the most recent time interval. The format is a long, long integer.

Pause Frames Transmitted The number of pause frames transmitted during the most recent time interval. The format is a long, long integer.

Port Name The name of the port as specified by the VTAM Transport Resource List Entry (TRLE). The format is a 32-character alphanumeric string.

Port Number The physical port number for this port. The format is an integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Pause Frames Received The total number of pause frames received since the OSA port was reset. The format is a long, long integer.

Total Pause Frames Transmitted The total number of pause frames transmitted since the OSA port was reset. The format is a long, long integer.

Trap Control Flags The value of this object determines which traps will be generated by the OSA. The value of this object is initially all zeros, indicating that all traps will be sent to the OSA subagent. Setting the appropriate bit prevents a particular trap from being sent to the subagent. When the bit value of the disableEthLANChange bit is set to zero (0), then the trap ibmOsaExp5SLanStateChange is sent. The format is a 4-digit hexadecimal number. Valid values are:

- x'0000' meaning the trap is enabled.
- x'8000' meaning the trap is disabled.

KN3 OSA-Express5S Ports Errors Attributes

Use the KN3 OSA-Express5S Ports Errors attributes to monitor error and control data for individual ports on an OSA-Express5S feature.

There can be two physical ports on each OSA channel path identifier, each with different data. When two ports are present, each one is assigned a separate ifIndex by the operating system. Each ifIndex contains the data for the corresponding port.

Alignment Errors The number of packets received during the most recent time interval with alignment errors (the packet is not an integer number of bytes in length). This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of two hexadecimal characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)

- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Frame Check Sequence Errors The number of frame check sequence errors during the latest collection interval. Frame check sequence (FCS) errors indicate that frames of data are being corrupted during transmission. FCS error count is the number of frames that were transmitted or received with a bad checksum (CRC value) in the Ethernet frame. These frames are dropped and not propagated onto other ports. Software flow control issues and partner point-to-point protocol (PPP) issues can contribute to function control sequence (FCS) errors. The format is a long, long integer.

Interface Index The interface index associated with this port. The format is a four-byte integer.

Jabber Frames Received The number of frames received by the OSA during the most recent time interval that passed address filtering, were greater than maximum size in length, and had a bad cyclic redundancy check (CRC). The format is a long, long integer.

The maximum transmission unit (MTU) is the maximum packet size, in bytes, that can be sent on an interface. You can set the MTU size (as long as you stay within the limits and maximum values of the OSA) using TCP/IP profile statements. You can also set the parameters of the neighboring network interface card (NIC) and port (usually a port on a switch, but could be another OSA). For information about setting maximum size for OSA devices, see the *IBM z/OS Communications Server: IP Configuration Reference.*

Length Error Packets Received The number of length-error packets received by the OSA during the most recent time interval. A length error occurs if an incoming packet passes filter criteria, but is undersized or oversized. The format is a long, long integer.

No Free Buffer Space on NIC The number of times during the latest collection interval that a received packet came into the network interface controller (NIC), but the NIC had no free (available) buffer space to load the packet into. The format is a long, long integer.

No Free Descriptors on LAN The number of times during the latest collection interval that a received packet came into the network interface controller (NIC), but the OSA driver had no free (available) descriptors to load the packet into. The format is a long, long integer.

No Free Descriptors on NIC The number of times during the latest collection interval that a received packet came into the network interface controller (NIC), but the NIC had no free (available) descriptors to load the packet into. The format is a long, long integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Oversized Frames Received The number of frames received by the OSA during the most recent time interval that passed address filtering and had a valid cyclic redundancy check (CRC), but were longer than the maximum size of 1522 bytes for operating-system embedded (OSE) non-queued direct I/O (non-QDIO) features or 16384 bytes for OSD queued direct I/O (QDIO) features. The format is a long, long integer.

Port Name The name of the port as specified by the TCP/IP. The format is a 32-character alphanumeric string.

Port Number The physical port number for this port. The format is an integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Alignment Errors The total number of packets received by the OSA since the last time the OSA port was reset with alignment errors (the packet is not an integer number of bytes in length). This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is a long, long integer.

Total Frame Check Sequence Errors The total number of frame check sequence errors on the OSA port. Frame check sequence (FCS) errors indicate that frames of data are being corrupted during transmission. FCS error count is the number of frames that were transmitted or received with a bad checksum (CRC value) in the Ethernet frame. These frames are dropped and not propagated onto other ports. Software flow control issues and partner point-to-point protocol (PPP) issues can contribute to function control sequence (FCS) errors. The format is a long, long integer.

Total Jabber Frames Received The number of frames received by the OSA since the last time the OSA port was reset that passed address filtering, were greater than maximum size in length, and had a bad cyclic redundancy check (CRC). The format is a long, long integer.

The maximum transmission unit (MTU) is the maximum packet size, in bytes, that can be sent on an interface. You can set the MTU size (as long as you stay within the limits and maximum values of the OSA) using TCP/IP profile statements. You can also set the parameters of the neighboring network interface card (NIC) and port (usually a port on a switch, but could be another OSA). For information about setting maximum size for OSA devices, see the *IBM z/OS Communications Server: IP Configuration Reference.*

Total Length Error Packets Received The number of packet length-error events received by the OSA since the last time the OSA port was reset. A length error occurs if an incoming packet passes filter criteria, but is undersized or oversized. The format is a long, long integer.

Total No Free Buffer Space on NIC The total number of times that a received packet came into the network interface controller (NIC), but the NIC had no free (available) buffer space to load the packet into. The format is a long, long integer.

Total No Free Descriptors on LAN The total number of times that a received packet came into the network interface controller (NIC), but the OSA driver had no free (available) descriptors to load the packet into. The format is a long, long integer.

Total No Free Descriptors on NIC The total number of times that a received packet came into the network interface controller (NIC), but the NIC had no free (available) descriptors to load the packet into. The format is a long, long integer.

Total Oversized Frames Received The number of frames received by the OSA since the last time the OSA port was reset that passed address filtering and had a valid cyclic redundancy check (CRC), but were longer than the maximum size of 1522 bytes for operating-system embedded (OSE) non-queued direct I/O (non-QDIO) features or 16384 bytes for OSD queued direct I/O (QDIO) features. The format is a long, long integer.

Total Undersized Frames Received The number of frames received by the OSA during the most recent time interval that passed address filtering, were smaller than the minimum size of 64 bytes, and had a valid cyclic redundancy check (CRC). Packets shorter than 64 bytes must be padded and may indicate that the LAN is incorrectly configured and not performing up to capacity. The format is a long, long integer.

Undersized Frames Received The total number of frames received by the OSA that passed address filtering, were smaller than the minimum size of 64 bytes, and had a valid cyclic redundancy check (CRC). Packets shorter than 64 bytes must be padded and may indicate that the LAN is incorrectly configured and not performing up to capacity. The format is a long, long integer.

KN3 OSA-Express5S Ports Summary Attributes

Use the KN3 OSA-Express5S Ports Summary attributes to monitor individual ports on an OSA-Express5S feature.

There can be two physical ports on each OSA channel path identifier, each with different data. When two ports are present, each one is assigned a separate ifIndex by the operating system. Each ifIndex contains the data for the corresponding port.

Active MAC Address A 6-byte octet string that contains the current MAC address in use on the adapter. The values are in canonical format. The format is a 12-digit hexadecimal string.

Active Speed Mode The actual speed and mode in which the OSA is running. This value is stored as an integer but displayed as a string. The possible values are:

- 0 = unknown
- 1 = tenMegabits
- 2 = tenMbFullDuplex
- 3 = oneHundredMbHalfDuplex
- 4 = oneHundredMbFullDuplex
- 6 = oneThousandMbFullDuplex
- 8 = tenGigabitFullDuplex

Burned In MAC Address A 6-byte octet string that contains the burned-in MAC address on the OSA. The values are in canonical format. The format is a 12-digit hexadecimal string.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of two hexadecimal characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Configuration Name The name of the configuration that is on the OSA. This value is set using the Open Systems Adapter/Support Facility (OSA/SF). It is not used by the OSA. The format is a string of up to 34 characters.

Configuration Speed Mode The configured port speed. This field shows the speed that was configured by the user for the OSA-Express Fast Ethernet feature. It is not used by OSA-Express Gigabit or 10 Gigabit Ethernet feature and returns notValidGigabit for these devices. This value is stored as an integer and displayed as a string with the following possible values:

- -1 = notValidGigabit
- 0 = autoNegotiate
- 1 = tenMbHalfDuplex

- 2 = tenMbFullDuplex
- 3 = oneHundredMbHalfDuplex
- 4 = oneHundredMbFullDuplex
- 6 = oneThousandMbFullDuplex
- 8 = tenGigabitFullDuplex

Disabled Status Reasons for the disabled state. When the value of the LAN Traffic State attribute is disabled (5), this attribute explains the reasons for the disabled state. The value for this object may be a combination of the bits shown in the list which follows. This value is stored as a hexadecimal integer and displayed as a 4-digit hexadecimal number mapped by the bit settings below:

- 0 = reserved
- 1 = internalPortFailure
- 2 = reserved
- 3 = reserved
- 4 = reserved
- 5 = reserved
- 6 = portTemporarilyDisabled
- 7 = reserved
- 8 = reserved
- 9 = serviceProcessorRequest
- 10 = networkRequest
- 11 = osasfRequest
- 12 = configurationChange
- 13 = linkFailureThresholdExceeded
- 14 = reserved
- 15 = reserved

Exclusive Usage ID Specifies the exclusive usage ID that, when paired with the corresponding Exclusive Usage Media Access Control (MAC), defines one of multiple Ethernet ports that can be used in parallel to increase the link speed beyond the limits of any single port. The format is an 8-character text string

Exclusive Usage MAC Specifies the exclusive usage Media Access Control (MAC) that, when paired with the corresponding Exclusive Usage ID, defines one of multiple Ethernet ports that can be used in parallel to increase the link speed beyond the limits of any single port. The format is a 12-digit hexadecimal string.

Interface Index The interface index associated with this port. The format is an unsigned integer.

IPv4 Layer 3 VMAC Specifies the Media Access Control (MAC) address being used if a Layer 3 Virtual MAC is being used for IPv4 on this stack. If the Layer 3 VMAC for IPv4 is not assigned, this field will contain all zeros. The format is a 12-digit hexadecimal string.

IPv6 Layer 3 VMAC Specifies the Media Access Control (MAC) address being used if a Layer 3 Virtual MAC is being used for IPv6 on this stack. If the Layer 3 VMAC for IPv6 is not assigned, this field will contain all zeros. The format is a 12-digit hexadecimal string.

LAN Traffic State The LAN state, expressed in value ranges from 0 to 8. A value of 5 (disabled) is further explained by the Disabled Status attribute. This value is stored as an integer and displayed as a string. The possible values are:

- 0 = undefined
- 1 = unavailable
- 2 = enabling
- 3 = disabling

- 4 = enabled
- 5 = disabled
- 6 = linkMonitor
- 7 = definitionError
- 8 = configuredOffline

For more information about these values, see the *zSeries Open Systems Adapter-Express Customer's Guide and Reference*.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Octet Rate The average number of octets received or transmitted by the OSA, per minute, during the most recent time interval. The format is a long, long integer.

Octets Received The number of octets received by the OSA during the most recent time interval. This count includes octets of all lengths, octets containing errors, and flow-control octets. The format is a long, long integer.

Octets Received or Transmitted The number of octets received or transmitted by the OSA during the most recent time interval. The format is a long, long integer.

Octets Transmitted The number of octets transmitted by the OSA during the most recent time interval. The format is a long, long integer.

Packet Rate The average number of packets received or transmitted by the OSA, per minute, during the most recent time interval. The format is a long, long integer.

Packets Received The number of packets received by the OSA during the most recent time interval. All packets are counted, including packets of all lengths and flow-control packets. The format is a long, long integer.

Packets Received or Transmitted The number of packets received or transmitted by the OSA during the most recent time interval. All packets are counted, including packets of all lengths, packets containing errors, and flow-control packets. The format is a long, long integer.

Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval. All packets are counted, including packets of all lengths, packets containing errors, and flow-control packets. The format is a long, long integer.

Port Interface Index The OSA-Express QDIO port interface index. For interfaces defined by DEVICE and LINK, this is the DEVICE interface index. For interfaces defined by INTERFACE, this is the dynamically generated interface index for the port. This field only applies to the following interface types:

- OSA-Express_QDIO_Ethernet_OSD (external data network type, which is the default value)
- OSA-Express_QDIO_Ethernet_OSM (intra-node management network, which requires IPv6)
- OSA-Express_QDIO_Ethernet_OSX (intra-ensemble data network)

The format is an unsigned integer. For more information about these interface types, see *IBM z/OS Communications Server: IP Configuration Guide*.

Port Name The name of the port as specified by the VTAM Transport Resource List Entry (TRLE). The format is a 32-character alphanumeric string.

Port Number The physical port number for this port. The format is an integer.

Port Type The physical port type. This value is stored as an integer but displayed as a string. Valid values are:

- 195 = osaexp5SgigabitEthernet
- 196 = osaexp5SoneThousandBaseTEthernet
- 197 = osaexp5StenGigabitEthernet

Service Mode An indicator of whether the processor is in service mode. This value is stored as an integer but displayed as a string. The possible values are:

- 0 = NotInServiceMode
- 1 = InServiceMode

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Octets The number of octets received or transmitted by the OSA since the last time the OSA port was reset. This count includes octets of all lengths, octets containing errors, and flow-control octets. The format is a long, long integer.

Total Octets Received The number of octets received by the OSA since the last time the OSA port was reset. This count includes octets of all lengths, octets containing errors, and flow-control octets. The format is a long, long integer.

Total Octets Transmitted The number of octets transmitted by the OSA since the last time the OSA port was reset. This count includes octets of all lengths, octets containing errors, and flow-control octets. The format is a long, long integer.

Total Packets The number of packets received or transmitted by the OSA since the last time the OSA port was reset. All packets are counted, including packets of all lengths and flow-control packets. The format is a long, long integer.

Total Packets Received The number of packets received by the OSA since the last time the OSA port was reset. All packets are counted, including packets of all lengths, packets containing errors, and flow-control packets. The format is a long, long integer.

Total Packets Transmitted The number of packets transmitted by the OSA since the last time the OSA port was reset. All packets are counted, including packets of all lengths and flow-control packets. The format is a long, long integer.

KN3 OSA-Express5S Ports Throughput Attributes

Use the KN3 OSA-Express5S Ports Throughput attributes to monitor individual ports on an OSA-Express5S feature.

There can be two physical ports on each OSA Channel Path Identifier (CHPID), and each contains different data. When two ports are present, each one is assigned a separate ifIndex by the operating system. Each ifIndex contains the data for the corresponding port.

63 Byte Packets Received The number of packets received by the OSA during the most recent time interval that are up to 63 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

Note: 64 bytes is the minimum length for an Ethernet packet. Packets shorter than 64 bytes have to be padded. This value is of interest because it indicates whether the LAN is configured incorrectly and not performing up to capacity.

63 Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that are up to 63 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

Note: 64 bytes is the minimum length for an Ethernet packet. Packets shorter than 64 bytes have to be padded. This value is of interest because it indicates whether the LAN is configured incorrectly and not performing up to capacity.

64 to 126 Byte Packets Received The number of packets received by the OSA during the most recent time interval that are 64 to 126 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

64 to 126 Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that are 64 to 126 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

127 to 254 Byte Packets Received The number of packets received by the OSA during the most recent time interval that are 127 to 254 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

127 to 254 Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that are 127 to 254 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

255 to 510 Byte Packets Received The number of packets received by the OSA during the most recent time interval that are 255 to 510 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

255 to 510 Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that are 255 to 510 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

511 to 1022 Byte Packets Received The number of packets received by the OSA during the most recent time interval that are 511 to 1022 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

511 to 1022 Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that are 511 to 1022 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

1023 to 1517 Byte Packets Received The number of packets received by the OSA during the most recent time interval that are 1023 to 1517 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

1023 to 1517 Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that are 1023 to 1517 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

1518 to Max Byte Packets Received The number of packets received by the OSA during the most recent time interval that were 1518 bytes or longer in length. This count does not include flow-control packets. The format is an unsigned integer.

1518 to Max Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that were 1518 bytes or longer in length. This count does not include flow-control packets. The format is an unsigned integer.

Broadcast Packets Received The number of good (without error) broadcast packets received by the OSA during the most recent time interval. The format is a long, long integer.

Broadcast Packets Transmitted The number of broadcast packets transmitted by the OSA during the most recent time interval. The format is a long, long integer.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a 2-byte hexadecimal string.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute

- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Multicast Packets Received The number of good (without error) multicast packets received by the OSA during the most recent time interval. The format is a long, long integer.

Multicast Packets Transmitted The number of multicast packets transmitted by the OSA during the most recent time interval. The format is a long, long integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Port Name The name of the port as specified by the VTAM Transport Resource List Entry (TRLE). The format is a 32-character alphanumeric string.

Port Number The physical port number for this port. The format is an integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total 63 Byte Packets Received The number of packets received by the OSA that are up to 63 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Note: 64 bytes is the minimum length for an Ethernet packet. Packets shorter than 64 bytes have to be padded. This value is of interest because it indicates whether the LAN is configured incorrectly and not performing up to capacity.

Total 63 Byte Packets Transmitted The number of packets transmitted by the OSA that are up to 63 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Note: 64 bytes is the minimum length for an Ethernet packet. Packets shorter than 64 bytes have to be padded. This value is of interest because it indicates whether the LAN is configured incorrectly and not performing up to capacity.

Total 64 to 126 Byte Packets Received The number of packets received by the OSA that are 64 to 126 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Total 64 to 126 Byte Packets Transmitted The number of packets transmitted by the OSA that are 64 to 126 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Total 127 to 254 Byte Packets Received The number of packets received by the OSA that are 127 to 254 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Total 127 to 254 Byte Packets Transmitted The number of packets transmitted by the OSA that are 127 to 254 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Total 255 to 510 Byte Packets Received The number of packets received by the OSA that are 255 to 510 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Total 255 to 510 Byte Packets Transmitted The number of packets transmitted by the OSA that are 255 to 510 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Total 511 to 1022 Byte Packets Received The number of packets received by the OSA that are 511 to 1022 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Total 511 to 1022 Byte Packets Transmitted The number of packets transmitted by the OSA that are 511 to 1022 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Total 1023 to 1517 Packets Received The number of packets received by the OSA that are 1023 to 1517 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Total 1023 to 1517 Byte Packets Transmitted The number of packets transmitted by the OSA that are 1023 to 1517 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Total 1518 to Max Byte Packets Received The number of packets received by the OSA that are 1518 bytes or longer in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Total 1518 to Max Byte Packets Transmitted The number of packets transmitted by the OSA that are 1518 bytes or longer in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is a long, long integer.

Total Broadcast Packets Received The number of good (without error) broadcast packets received by the OSA since the last time the OSA port was reset. The format is a long, long integer.

Total Broadcast Packets Transmitted The number of broadcast packets transmitted by the OSA since the last time the OSA port was reset. The format is a long, long integer.

Total Multicast Packets Received The number of good (without error) multicast packets received by the OSA since the last time the OSA port was reset. The format is a long, long integer.

Total Multicast Packets Transmitted The count of the number of multicast packets transmitted by the OSA since the last time the OSA port was reset. The format is a long, long integer.

KN3 SNA Collector Status Attributes

Use the KN3 SNA Collector Status attributes to view configuration and status information about the IBM Z OMEGAMON Network Monitor SNA collector.

Agent VTAM Application Name The name of the agent VTAM application that acts as a secondary program operator. The default value is CTDN3SP, which is the application name in the CTDN3N member of the RKANSAMU data set. The format is an 8-character string.

This VTAM application must be defined to VTAM and have a status of **ACTIVE** before the VTAM environment and buffer pool data can be collected successfully. If the SNA Collection Started attribute in the Agent Status Attribute table has a value of **No**, indicating that the SNA collector is not started, this field will be blank.

Agent VTAM Application Status Indicates the current status of the VTAM application used by the agent to collect VTAM buffer pool and environment data. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = Unknown
- 1 = CONCT (Connectable)
- 2 = ACTIV (Active)

- 3 = INACT (Inactive)

The status strings displayed for this attribute match the status strings displayed by the DISPLAY NET command. CONCT, ACTIV, and INACT are the values expected most of the time. Less common, transient states are represented by displaying a value of **Unknown**. If a value of Unknown is displayed, issue a DISPLAY NET command to verify the actual status of the resource.

If the SNA Collector Status column of the Agent Status table has a value of **Yes**, then a value other than ACTIV for this attribute means that you need to take one of the following actions, depending on the value of this attribute:

- Unknown: Activate the agent VTAM major node
- INACT: Activate the agent VTAM application
- CONCT: Check the RKLVLOG for error messages indicating why the VTAM application access control block (ACB) cannot be opened.

If the SNA Collector Status column of the Agent Status table has a value of **No**, then the value in this column will be **Unknown**. If you want to collect VTAM buffer pool and environment data, start SNA data collection. Refer to the description of the SNA Collection Started attribute in the Agent Status table for information about why SNA data collection is not started.

Note: A value of **Unknown** might be the result of an internal error. If you think this is the case, contact IBM Software Support.

Agent VTAM Major Node Name The name of a dataset member that contains the definition of a VTAM major node that defines the application used by the agent to collect VTAM buffer pool and environment data. The member must be on the VTAMLST concatenation list. By default the name of the member is **CTDN3N**. A sample that can be copied to VTAMLST is available in the RKANSAMU dataset. The format is an 8-character string.

This major node must be active for VTAM buffer pool and environment data to be successfully collected. If the value of the Agent VTAM Application Name is blanks, the value of this attribute will also be blanks.

Agent VTAM Major Node Status Indicates the current status of the agent VTAM major node. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = Unknown
- 1 = ACTIV (Active)

The status string ACTIV displayed for this attribute matches the status string displayed by the DISPLAY NET command. Less common, transient states are represented by displaying a value of **Unknown**. If a value of Unknown is displayed, issue a DISPLAY NET command to verify the actual status of the resource.

If a value of **Unknown** is displayed because the VTAM major node is inactive, and you would like to collect VTAM buffer pool and environment data, activate the VTAM major node that defines the application identified by the Agent VTAM Application Name attribute. For more information on how to activate the VTAM major node using the sample provided, see the *IBM Z OMEGAMON Network Monitor: Configuration Guide*.

Note: A value of **Unknown** might be the result of an internal error. If you think this is the case, contact IBM Software Support.

ALL HPR Collection Indicates whether statistics are being collected for all high performance routing (HPR) connections. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = No
- 1 = Yes

If the value for this attribute is **No**, then data is only collected for only those HPR connections that flow data over Enterprise Extender (EE) connections.

This parameter is defined by the All High Performance Routing Connections value that was set in the Configuration Tool on the "Specify Component Configuration (Page 3)" panel or the KN3_TCP_ALLHPR PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the ALLHPR parameter on the KN3FCCMD START EEHPR command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute will have a value of **No** when the TCP collector is not started, regardless of what value was specified during configuration. Once the TCP collector is started, this attribute displays the value that what was configured for the stack.

Buffer Pool And VTAM Environment Collection Indicates whether VTAM buffer pool and environment statistics are being collected. The SNA collector assembles this data once every SNA collection interval. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = No
- 1 = Yes

If the value for this attribute is **Yes**, then data for VTAM buffer pools, applications, extents, and address spaces is being collected. This parameter is defined by the Buffer Pool/VTAM Environment Data Collection value that was set in the Configuration Tool on the "Specify Component Configuration (Page 3)" panel or by the KN3_SNA_VTAM_COLLECT_DATA PARMGEN parameter.

These are possible reasons that the value of this attribute might be **No**:

- You did not respond **Y** to the Buffer Pool/VTAM Environment Data Collection parameter in the Configuration Tool or select **Y** as the value for the KN3_SNA_VTAM_COLLECT_DATA PARMGEN parameter.
- The agent's PMI exit and its aliases are not available to VTAM. To confirm that this issue is what is preventing SNA data collection, check the RKLVLOG for message KN3PN023. See the *IBM Tivoli Monitoring for Mainframe Networks: Planning and Configuration Guide* for information on making the PMI exit and its aliases available to VTAM.
- The VTAM application needed by the agent to collect VTAM environment and buffer pool data is either not defined to VTAM or is not in the correct state. To confirm that this issue is preventing SNA data collection, check the RKLVLOG for message KN3PN011 or KN3PN022. See the "Troubleshooting SNA collector problems" topic in the *IBM Z OMEGAMON Network Monitor: Troubleshooting Guide* for more information about this problem.

Collection Time The time and date at which status information was collected. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day

- H = Hour
- M = Minute
- S = Second
- m = Millisecond

CSM Buffer Reporting Collection Indicates whether VTAM communications storage manager (CSM) buffer reporting statistics are being collected. The SNA network monitoring interface (NMI) collects this data once every TCP collection interval. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = No
- 1 = Yes

This parameter is defined by the CSM Buffer Reporting value that was set in the Configuration Tool on the "Specify Component Configuration (Page 3)" panel or the KN3_TCP_CSM PARMGEN parameter. CSM Buffer Reporting Collection can be started while the monitoring agent is running with the KN3FCCMD START CSM command. The interval that you specified for this value during configuration can be modified while the monitoring agent is running using the TCPCINTV parameter on the KN3FCCMD INSTALL TCPC command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute will have a value of **No** when the TCP collector is not started, regardless of what value was specified during configuration. Once the TCP collector is started, this attribute displays the value that what was configured for the stack.

EE And HPR Collection Indicates whether Enterprise Extender (EE) and High Performance Routing (HPR) connection statistics are to be collected. The SNA network monitoring interface (NMI) collects this data once every TCP collection interval. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = No
- 1 = Yes

This parameter is defined by the Enterprise Extender and High Performance Routing Statistics Collection value that was set in the Configuration Tool on the "Specify Component Configuration (Page 3)" panel or the KN3_TCP_EEHPR PARMGEN parameter. EE and HPR Collection can be started while the monitoring agent is running with the KN3FCCMD START EEHPR command. The interval that you specified for this value during configuration can be modified while the monitoring agent is running using the TCPCINTV parameter on the KN3FCCMD INSTALL TCPC command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute will have a value of **No** when the TCP collector is not started, regardless of what value was specified during configuration. Once the TCP collector is started, this attribute displays the value that what was configured for the stack.

Origin Node The unique identifier for the IBM Z OMEGAMON Network Monitor agent node on the navigation tree. The format is an alphanumeric string no longer than 32 characters.

PMI Exit Name The alias name of the agent VTAM performance monitor interface (PMI) exit being used by this monitoring agent instance. The format is an 8-character string.

The agent PMI exit and its aliases must be made accessible to VTAM before VTAM environment and buffer pool data can be collected successfully. If the SNA Collection Started attribute in the Agent Status Attribute table has a value of **No**, indicating that the SNA collector is not started, this field will be blank.

PMI Exit Status Indicates the current status of the agent VTAM performance monitor interface (PMI) exit. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = Unknown
- 2 = ACTIVE

The ACTIVE value shown is the same value that is seen in the output of the `DISPLAY NET` command.

If the SNA Collector Status column of the Agent Status table has a value of **Yes**, then a value of Unknown for this attribute means that an operator or a program operator application (POA) has temporarily deactivated the PMI exit. The agent may reactivate it automatically. If, after waiting two or three data collection cycles, this attribute does not show a value of ACTIVE, you might need to stop and restart the agent.

If the SNA Collector Status column of the Agent Status table has a value of **No**, then the value of this attribute will be **Unknown**. If you would like to collect VTAM buffer pool and environment data, start SNA data collection. See the description of the SNA Collection Started attribute in the Agent Status table for information about why SNA data collection is not started.

Note: A value of **Unknown** might be the result of an internal error. If you think this is the case, contact IBM Software Support.

SNA NMI Enabled Indicates whether the SNA network monitoring interface (NMI) is enabled. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = No
- 1 = Yes
- 2 = Unknown

A value of **Unknown** means that the status could not be determined due to an internal error in the agent. If you see this value, contact IBM Software Support.

If you want to collect high performance routing (HPR) or enterprise extended (EE) data or communications storage manager (CSM) data and the SNA NMI is not enabled, you must enable it. See the *IBM z/OS Communications Server: IP Programmer's Guide* for information about enabling the SNA NMI. See the "Enabling the z/OS Communications Server network management interface" section of the "Preparing your z/OS Environment" chapter of the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

Sysplex Name The name of the sysplex that the monitored system is part of. The format is a string of up to 8 characters.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

KN3 Take Action Command Attributes

Use the KN3 Take Action Command attributes to display the Take Action commands processed by the IBM Z OMEGAMON Network Monitor command handler.

Command The Take Action command issued. The format is an alphanumeric string of up to 256 characters.

Command ID The Take Action command identifier. The format is an alphanumeric string of up to 8 characters.

Command Timestamp The time and date when the Take Action command was issued. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Command Type The type of Take Action command being issued. This value is stored as an integer and displayed as a string. The following are valid values:

- 1 = N3 XMCS console command

Jobname The target address space against which the Take Action command was issued. The format is an alphanumeric string no longer than 8 characters.

Origin Node The unique identifier for the IBM Z OMEGAMON Network Monitor agent node on the navigation tree. The format is an alphanumeric string no longer than 32 characters.

Response Message The response message, indicating that the Take Action command was issued or the reason why the Take Action command was not issued. The format is an alphanumeric string of up to 256 characters.

Return Code The return code of the Take Action command. The format is an integer.

System ID The SMF system ID. The format is a string up to 4 characters in length.

User ID The User ID of the Tivoli Enterprise Portal user or the TSO user (3270) issuing the Take Action command. The format is an alphanumeric string of up to 10 characters.

KN3 Take Action Command Response Attributes

Use the KN3 Take Action Command Response attributes to display the Take Action command output processed by the IBM Z OMEGAMON Network Monitor command handler.

Command Output The Take Action command response. The format is an alphanumeric string of up to 256 characters.

Command ID The Take Action command identifier. The format is an alphanumeric string of up to 8 characters.

Command Timestamp The time and date when the Take Action command was issued. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Origin Node The unique identifier for the IBM Z OMEGAMON Network Monitor agent node on the navigation tree. The format is an alphanumeric string no longer than 32 characters.

KN3 TCP Collector Status Attributes

Use the KN3 TCP Collector Status attributes to view configuration and status information about the IBM Z OMEGAMON Network Monitor TCP collector.

Collection Status The completion status of the most recent collection cycle for this TCP/IP stack. This value is stored as an integer and displayed as a string. Valid values for this integer are:

- 0 = OK
- 1 = TCP_AS_NotFound
- 2 = TCP_AS_SwappedOut
- 3 = Proc_Not_TCP
- 4 = Collector_ABENDED
- 5 = User_Stopped_Monitoring

If the stack was not designated for monitoring during configuration, then this attribute value is blank, and the Monitor attribute in this table has a value of **No**.

Collection Time The time and date at which status information was collected. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second

- m = Millisecond

Connections and Applications Collection Indicates whether TCP/IP connection and application performance statistics are being collected for this stack. This value is stored as an integer and displayed as a string. Valid values for this integer are:

- 0 = No
- 1 = Yes

This parameter is defined by the TCP/IP Connection and Application Performance Statistics Collection value that was set in the Configuration Tool on the "Specify Component Configuration (Page 2)" panel or the KN3_TCP_CONN PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the KN3FCCMD START CONN command or the KN3FCCMD STOP CONN command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute will have a value of **No** when the TCP collector is not started, regardless of what value was specified during configuration. Once the TCP collector is started, this attribute displays the value that what was configured for the stack.

Data Link Control Statistics Collection Indicates whether interface Data Link Control (DLC) statistics are to be collected for this stack. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

This parameter is defined by the Interface Data Link Control Statistics Collection value that was set in the Configuration Tool on the "Specify Component Configuration" panel or the KN3_TCP_INTE PARMGEN parameter. This configured value can be modified while the monitoring agent is running using the KN3FCCMD START INTE command or the KN3FCCMD STOP INTE command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute displays a value of **No** if TCP collection is not started. If TCP collection is stopped and restarted using the KN3FCCMD z/OS MODIFY commands, three collection cycles must pass before the value for this attribute reflects what is actually configured.

FTP Collection Indicates whether FTP statistics are being collected for this stack. This value is stored as an integer and displayed as a string. Valid values for this integer are:

- 0 = No
- 1 = Yes

This parameter is defined by the FTP Data Collection value that was set in the Configuration Tool on the "Specify Component Configuration (Page 2)" panel or the KN3_TCP_FTP PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the KN3FCCMD START FTP command or the KN3FCCMD STOP FTP command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute will have a value of **No** when the TCP collector is not started, regardless of what value was specified during configuration. Once the TCP collector is started, this attribute displays the value that what was configured for the stack.

FTP Data Display Interval Determines how long FTP data will be displayed on the Tivoli Enterprise Portal for this address space. A value of 1 means that FTP data is displayed for one hour. This value is expressed as a whole number in hours from 1 to 24. The default is 2 hours.

This interval is defined by the FTP Data Display Interval value that was set in the Configuration Tool on the "Specify Component Configuration (Page 2)" panel or the KN3_TCP_FTP_DSPINTV PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the DSPINTV parameter on the KN3FCCMD START FTP command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute will have a value of **0** (zero) when the TCP collector is not started, regardless of what value was specified during configurationl.

Host Name The TCP host name of the monitored stack as specified in the HOSTNAME statement of the TCPIP DATA configuration file for the stack. The format is an alphanumeric character string of up to 255 characters. See the *IBM z/OS Communications Server: IP Configuration Reference* for more about the format of this name and what name can be substituted if the HOSTNAME statement is not specified in the TCPIP.DATA file.

Interface Statistics Collection Indicates whether interface statistics are to be collected for this stack. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

This parameter is defined by the Interface Statistics Collection value that was set in the Configuration Tool on the "Specify Component Configuration" panel or the KN3_TCP_INTS PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the KN3FCCMD START INTS command or the KN3FCCMD STOP INTS command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute displays a value of **No** if TCP collection is not started. If TCP collection is stopped and restarted using the KN3FCCMD z/OS MODIFY commands, three collection cycles must pass before the value for this attribute reflects what is actually configured.

IP Address The IP address used to locate SNMP configuration information for this stack, as defined by the TCP Collector SNMP Parameter Dataset Name attribute in the Agent Status attribute group. This IP address is the default local IP address of the host where the monitored TCP/IP stack is running. This address is specified using the PRIMARYINTERFACE statement or the first address in the HOME list of the TCP/IP profile (PROFILE.TCPIP). See the *IBM z/OS Communications Server: IP Configuration Reference* for more information about these statements.

IP Security Collection Indicates whether IP security statistics are being collected for this stack. This value is stored as an integer and displayed as a string. Valid values for this integer are:

- 0 = No
- 1 = Yes

This parameter is defined by the IP Filters and IPSec Tunnels Statistics Collection value that was set in the Configuration Tool on the Specify Component Configuration (Page 2) panel or the KN3_TCP_IPSEC PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the KN3FCCMD START IPSEC command or the KN3FCCMD STOP IPSEC command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute will have a value of **No** when the TCP collector is not started, regardless of what value was specified during configuration. Once the TCP collector is started, this attribute displays the value that what was configured for the stack.

IPv4 Security Enabled Indicates whether IP security is enabled for IPv4 interfaces. This value is stored as an integer and displayed as a string. Valid values for this integer are:

- 0 = No
- 1 = Yes
- 2 = Unknown

A value of **Unknown** means that the status could not be determined due to an internal error in the agent. If you see this value, contact IBM Software Support.

IPv6 Security Enabled Indicates whether IP security is enabled for IPv6 interfaces. This value is stored as an integer and displayed as a string. Valid values for this integer are:

- 0 = No
- 1 = Yes
- 2 = Unknown

A value of **Unknown** means that the status could not be determined due to an internal error in the agent. If you see this value, contact IBM Software Support.

Monitor Indicates whether monitoring is enabled for this stack. This value is stored as an integer and displayed as a string. Valid values for this integer are:

- 0 = No
- 1 = Yes

This parameter is defined by the "Do you want to monitor this stack?" value that was set in the Configuration Tool on the Add/Copy/Update TCP/IP Monitored Systems Info panels or the KN3_TCP_COLLECT_STACK PARMGEN parameter.

Origin Node The unique identifier for the IBM Z OMEGAMON Network Monitor agent node on the navigation tree. The format is an alphanumeric string no longer than 32 characters.

OSA Statistics Collection Indicates whether OSA statistics are to be collected for this stack. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

This parameter is defined by the OSA Statistics Collection value that was set in the Configuration Tool on the "Specify Component Configuration" panel or the KN3_TCP_OSA PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the KN3FCCMD START OSA command or the KN3FCCMD STOP OSA command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute displays a value of **No** if TCP collection is not started. If TCP collection is stopped and restarted using the KN3FCCMD z/OS MODIFY commands, three collection cycles must pass before the value for this attribute reflects what is actually configured.

Routing Table Collection Indicates whether routing table statistics are being collected for this stack. This value is stored as an integer and displayed as a string. Valid values for this integer are:

- 0 = No
- 1 = Yes

This parameter is defined by the Routing Table Statistics Collection value that was set in the Configuration Tool on the "Specify Component Configuration" panel or the KN3_TCP_ROUTE_TBL PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the KN3FCCMD START ROUTE command or the KN3FCCMD STOP ROUTE command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute will have a value of **No** when the TCP collector is not started, regardless of what value was specified during configuration. Once the TCP collector is started, this attribute displays the value that what was configured for the stack.

Routing Table Collection Frequency The number of TCP collection intervals to wait between routing table statistics collections. A value of 1 means that routing information is collected every collection interval. A value of "2" means that routing information is collected every other collection interval. This format is a whole number from 1 to 99 inclusive. The default value is 10.

This interval is defined by the Routing Table Collection Frequency value that was set in the Configuration Tool on the "Specify Component Configuration (Page 2)" panel or the KN3_TCP_ROUTE_TBL_FREQ PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the FREQ parameter on the KN3FCCMD START ROUTE command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute will have a value of **0** (zero) when the TCP collector is not started, regardless of what value was specified during configuration.

SMF Service Enabled Indicates whether the real-time SMF record information service is enabled. This value is stored as an integer and displayed as a string. Valid values for this integer are:

- 0 = No
- 1 = Yes
- 2 = Unknown

A value of **Unknown** means that the status could not be determined due to an internal error in the agent. If you see this value, contact IBM Software Support.

If the value of this attribute is **No**, verify that the real-time SMF record information service function is enabled for this stack. The real-time SMF record information service provides an interface for the monitoring agent to obtain information about FTP and Telnet connections on this stack. To correct this problem, enable the real-time SMF record information service. See the "Enabling FTP and TN3270 monitoring" topic in the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* chapter on "Preparing your z/OS Environment."

SNMP Agent Jobname The job name for the application that is bound to the SNMP agent port for this TCP/IP stack. The SNMP agent port is specified in the IBM Z OMEGAMON Network Monitor SNMP configuration file. If no application is bound to the port or no SNMP agent port definition was found in the SNMP configuration file for this TCP/IP stack, then a value of UNKNOWN is displayed. A status of UNKNOWN can also mean that the monitoring agent encountered an error in retrieving data. The format is an 8-character string.

SNMP Agent Port The port used to connect to the SNMP agent. The format is a string of up to 5 characters. This parameter is obtained from the TCP Collector SNMP Parameter Dataset. For more information, see the "Format of the SNMP configuration file" appendix in the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide*.

This attribute is blank for all monitored stacks if one of these conditions is true:

- There is a syntax error in the SNMP Configuration file.
- The agent procedure JCL does not have a KN3SNMP DD statement specifying the name of the SNMP Configuration file or it does have a KN3SNMP DD but the file cannot be found or opened.

This attribute is blank for a specific stack if the IP Address displayed for the stack cannot be found in the SNMP Configuration file. For more information, see the "Format of the SNMP configuration file" appendix in the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide*.

SNMP Version The version of the SNMP protocol that is used to send SNMP requests to the SNMP agent. The format is a string of up to 8 characters. The only value supported is **snmpv2**.

This parameter is obtained from the TCP Collector SNMP Parameter Dataset. For more information, see the "Format of the SNMP configuration file" appendix in the *IBM Z OMEGAMON Network Monitor Configuration Guide*.

This attribute is blank for all monitored stacks if one of these conditions is true:

- There is a syntax error in the SNMP Configuration file.
- The agent procedure JCL does not have a KN3SNMP DD statement specifying the name of the SNMP Configuration file or it does have a KN3SNMP DD but the file cannot be found or opened.

This attribute is blank for a specific stack if the IP Address displayed for the stack cannot be found in the SNMP Configuration file.

Stack Layer Statistics Collection Indicates whether stack layer statistics are to be collected for this stack. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes

This parameter is defined by the TCP/IP Stack Layer Statistics Collection value that was set in the Configuration Tool on the "Specify Component Configuration" panel or the KN3_TCP_GLBS PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the KN3FCCMD START GLBS command or the KN3FCCMD STOP GLBS command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute displays a value of **No** if TCP collection is not started. If TCP collection is stopped and restarted using the KN3FCCMD z/OS MODIFY commands, three collection cycles must pass before the value for this attribute reflects what is actually configured.

Sysplex Name The name of the sysplex that the monitored system is part of. The format is a string of up to 8 characters.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP Address Space Status The status of the TCP/IP address space the last time that TCP data was collected for this TCP/IP stack. This value is stored as integer and displayed as a string. Valid values for this integer are:

- 0 = NOT_FOUND
- 1 = ACTIVE
- 2 = TERMINATING
- 3 = DOWN
- 4 = STOPPED OR STOPPING
- 5 = ABENDED
- 99 = <blank>

The attribute is blank if data is not being collected for the stack. If the stack was not designated for monitoring during configuration, the Monitor attribute in this table has a value of **No** .

TCPIP Procedure Name The name specified on the PROC or JOB statement of the JCL used to start the TCP/IP procedure. The IBM Z OMEGAMON Network Monitor monitoring agent has been configured to monitor this TCP/IP address space. The format is a string of up to 8 characters.

TCPIP Profile Dataset Name The name of the data set that contains the TCP/IP profile. This data set can be either a partitioned data set or a sequential data set. The format is a string of up to 54 characters. Sequential data set names are expressed as a sequence of period-separated qualifiers. Partitioned data sets are expressed as a sequence of period-separated qualifiers ending with a member name enclosed in parentheses.

This parameter is defined by the "TCP/IP profile dataset name" and "Member name" values that were set in the Configuration Tool on the Add/Copy/Update TCP/IP Monitored Systems Info panels, or the KN3_TCPXnn_TCPIP_PROFILES_DSN and KN3_TCPXnn_TCPIP_PROFILES_MBR PARMGEN parameters.

TCPIP Version The version and release of the stack. The format is an 8-character string with a value of CS V*x*R*yy*. The characters in this string are defined as follows:

- CS means Communications Server
- V means version.
- *x* identifies the version.
- R means release.
- *yy* identifies the release.

Leading zeros are not displayed in the release identifier. For example, if the version for the a selected stack is 1 and the release is 9, then the string "CS V1R9" is displayed. However, if the version is 1 and the release is 10, then "CS V1R10" is displayed.

TN3270 Data Display Interval Determines how long TN3270 server statistics are displayed on the Tivoli Enterprise Portal. This value is expressed as a whole number in hours from 1 to 24. The default is 2 hours.

This interval is defined by the TN3270 Data Display Interval value that was set in the Configuration Tool on the "Specify Component Configuration (Page 2)" panel or the KN3_TCP_TN3270_DSPINTV PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the DSPINTV parameter on the KN3FCCMD START TN3270 command or the KN3FCCMD STOP TN3270 command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute will have a value of **0** (zero) when the TCP collector is not started, regardless of what value was specified during configuration.

TN3270 Server Collection Indicates whether TN3270 server statistics are being collected for this stack. This value is stored as integer and displayed as a string. Valid values for this integer are:

- 0 = No
- 1 = Yes

This parameter is defined by the TN3270 Server Statistics Collection value that was set in the Configuration Tool on the "Specify Component Configuration (Page 2)" panel or the KN3_TCP_TN3270 PARMGEN parameter. The configured value can be modified while the monitoring agent is running using the KN3FCCMD START TN3270 command. See the *IBM Z OMEGAMON Network Monitor: Planning and Configuration Guide* for more information.

This attribute will have a value of **No** when the TCP collector is not started, regardless of what value was specified during configuration. Once the TCP collector is started, this attribute displays the value that what was configured for the stack.

KN3 TCP Counter Statistics Attributes

Use the KN3 TCP Counter Statistics attributes to view TCP protocol statistics for the selected the TCP/IP stack on a z/OS v1r12 or later system.

Collection Time The time and date at which status information was collected. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Connections Established The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT since TCP/IP initialization. The format is an unsigned integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Out-of-Order Segments Percentage The percentage of segments received that was out-of order over during the most recent sampling interval compared to the total number of segments transmitted. The format is an integer between 1 and 100 inclusive.

Receive Segment Rate The number of segments received per minute during the most recent sampling interval. The format is an unsigned integer.

Received Segment Error Rate The rate at which segments in error were received during the most recent sampling interval. The format is an unsigned integer.

Segment Retransmission Rate The rate at which TCP segments were retransmitted during the most recent sampling interval. The format is an unsigned integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters. This field is not displayed.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Accepted Connections The number of binary TCP connections accepted by all listening applications since TCP/IP initialization. The format is an unsigned long long integer.

Total ACKs with Header Prediction The number of binary input TCP acknowledgements with successful header prediction since TCP/IP initialization. The format is an unsigned integer.

Total Active Socket OPENs The number of TCP connections that have made a direct transition to the SYN-SENT state from the CLOSED state since TCP/IP initialization. The format is an unsigned integer.

An Active OPEN means that during TCP connection setup, the client process that is using TCP takes the active role and initiates the connection by sending a TCP SYN message to start the connection. The opposite is a Passive OPEN where a TCP application listens for clients.

Total All Data After Window The number of binary input TCP segments with all data after the current window since TCP/IP initialization. The format is an unsigned integer.

Total All Data Before Window The number of binary input TCP segments with all data before the current window, indicating that the segment contains duplicate data since TCP/IP initialization. The format is an unsigned integer.

Total Attempt Failures The number of TCP connections that have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus those that have made a direct transition to the LISTEN state from the SYN-RCVD state since TCP/IP initialization. The format is an unsigned integer.

Total BulkData AIQ Segments The number of binary input TCP segments that are received over the BulkData Ancillary Input Queue (AIQ) when using the queued direct I/O (QDIO) inbound workload queueing function since TCP/IP initialization. The format is an unsigned long long integer.

Total Connections Closed The number of TCP connections with a socket that has been closed since TCP/IP initialization. The format is an unsigned integer.

Total Data Segments Predicted The number of binary input TCP data segments with successful header prediction since TCP/IP initialization. The format is an unsigned integer.

Total Delayed Output ACKs The number of binary delayed output TCP acknowledgements since TCP/IP initialization. The format is an unsigned integer.

Total Discards for Bad Checksum The number of binary input TCP segments discarded due to a bad checksum since TCP/IP initialization. The format is an unsigned integer.

Total Discards for Bad Length The number of binary input TCP segments discarded due to a bad header length since TCP/IP initialization. The format is an unsigned integer.

Total Discards for Length Too Short The number of input TCP segments discarded due to the data length being shorter than the segment length since TCP/IP initialization. The format is an unsigned integer.

Total Discards for Old Time Stamp The number of input TCP segments discarded due to old time stamps since TCP/IP initialization. The format is an unsigned integer.

Total Duplicate ACKs The number of binary input duplicate TCP acknowledgements (ACKs) since TCP/IP initialization. The format is an unsigned integer.

Total Established Resets The number of TCP connections that have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state since TCP/IP initialization. The format is an unsigned integer.

Total FINWAIT2 Drops The number of binary TCP connections dropped due to the FINWAIT2 timer expiring before receiving FIN segments since TCP/IP initialization. The format is an unsigned integer.

When a socket is closed abnormally (for example, no longer needed) it is not made available immediately. Instead it is placed into a state called FINWAIT2 (which is what shows up in the netstat -s command). It waits there for a period of time before it is made available in the free pool. The default for this is 600 seconds.

Total Flow Controls The sum of Input Window Probes, Input Window Updates, Output Window Probes, and Output Window Updates since TCP/IP initialization. The format is an unsigned long long integer.

Total Input After Closed The number of binary input TCP segments received after the corresponding sockets have been closed since TCP/IP initialization. The format is an unsigned integer.

Total Input Segments Received The number of input TCP segments received, including those received in error, since TCP/IP initialization. The format is an unsigned long long integer.

Total Input Window Probes The number of binary input TCP segments processed while the current receive window size is zero since TCP/IP initialization. The format is an unsigned integer.

Total Input Window Updates The number of binary input TCP segments that change only the receive window size since TCP/IP initialization. The format is an unsigned integer.

Total Keepalive Drops The number of binary TCP connections dropped due to no response while sending keepalive probe requests since TCP/IP initialization. The format is an unsigned integer.

Total Keepalive Probes The number of binary output TCP keepalive probe requests since TCP/IP initialization. The format is an unsigned integer.

Total Out-of-Order Segments The number of binary input TCP segments that did not contain the next expected sequence number since TCP/IP initialization. The format is an unsigned integer.

Total Output RSTs The number of binary TCP segments sent containing the TCP/IP reset (RST) flag since TCP/IP initialization. The format is an unsigned integer.

Total Output Segments Sent The number of binary output TCP segments sent since TCP/IP initialization. The format is an unsigned long long integer.

Total Output Window Probes The number of binary output window probe requests since TCP/IP initialization. The format is an unsigned integer.

Total Output Window Updates The number of binary output TCP segments that change only the receive window size since TCP/IP initialization. The format is an unsigned integer.

Total Passive Drops The number of passive TCP connection requests discarded since TCP/IP initialization. The format is an unsigned integer.

Total Passive Socket OPENs The number of TCP connections that have made a direct transition to the SYN-RCVD state from the LISTEN state since TCP/IP initialization. The format is an unsigned integer.

A Passive OPEN is where a TCP application listens for clients. The opposite is an Active OPEN, which means that during TCP connection setup, the client process that is using TCP takes the active role and initiates the connection by actually sending a TCP message to start the connection, a SYN message.

Total PMTU Errors The number of TCP connections that exceeded the path maximum transmission unit (MTU) discovery retransmit threshold since TCP/IP initialization. When TCP/IP has to lower the path MTU and retransmit segments three or more times for a TCP connection, this counter is incremented. The format is an unsigned integer.

Total PMTU Retransmits The number of TCP segments retransmitted due to path maximum transmission unit (MTU) discovery since TCP/IP initialization. When TCP/IP receives notification that an IP packet was too large, TCP will retransmit with a smaller packet and increment this counter. The format is an unsigned integer.

Total Retransmission Percentage The percentage of TCP segments that required retransmission compared to the total number of segments transmitted since TCP/IP initialization. The format is an integer between 1 and 100 inclusive.

Total Retransmit Drops The number of binary TCP connections dropped due to the retransmit threshold being exceeded since TCP/IP initialization. The format is an unsigned integer.

Total Retransmit Timeouts The number of binary TCP retransmit timer pops since TCP/IP initialization. The format is an unsigned integer.

Total Segments Discarded The number of input TCP segments discarded since TCP/IP initialization. This attribute provides the count of all discarded segments. Other attributes provide more granular counters for some of the reasons that segments were discarded. The format is an unsigned long long integer.

Total Segments Retransmitted The number of binary TCP segments retransmitted since TCP/IP initialization. The format is an unsigned integer.

Total Some Data After Window The number of binary input TCP segments with some data after the current window since TCP/IP initialization. The format is an unsigned integer.

Total Some Data Before Window The number of binary input TCP segments with some data before the current window, indicating that the segment contains some duplicate data since TCP/IP initialization. The format is an unsigned integer.

Total Timewait Reused The number of TCP connections in the TIMEWAIT state that have been reused for connections in the SYN-RCVD state since TCP/IP initialization. The format is an unsigned integer.

Total Window Probe Drops The number of binary TCP connections dropped due to no response while sending window probe requests since TCP/IP initialization. The format is an unsigned integer.

Transmit Segment Rate The number of segments transmitted per minute during the most recent sampling interval since TCP/IP initialization. The format is an unsigned integer.

KN3 UDP Counter Statistics Attributes

Use the KN3 UDP Counter Statistics attributes to view UDP protocol statistics for the selected the TCP/IP stack on z/OS v1r12 or later systems.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second

- m = Millisecond

Datagram Error Percentage The percentage of UDP errors compared to Datagram Received during the most recent sampling interval. The format is an integer between 1 and 100 inclusive.

Discard Percentage The percentage of UDP datagrams discarded as undeliverable because they were received in error (including "No Port Found" errors) compared to Datagrams Received during the most recent sampling interval. The format is an integer between 1 and 100 inclusive.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Receive Datagram Rate The number of UDP datagrams received per minute during the most recent sampling interval. The format is an unsigned integer.

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Total Datagram Error Percentage The percentage of UDP datagrams in error compared to Datagrams Received since TCP/IP initialization. The format is an integer between 1 and 100 inclusive.

Total Datagrams Discarded The number of datagrams discarded since TCP/IP initialization. The format is an unsigned long long integer.

Total Datagrams in Error The number of input datagrams that could not be delivered for reasons other than the lack of an application at the destination port since TCP/IP initialization. The format is an unsigned integer.

Total Datagrams Received The number of input datagrams received since TCP/IP initialization. The format is an unsigned long long integer.

Total Datagrams Sent The number of output datagrams sent since TCP/IP initialization. The format is an unsigned long long integer.

Total Datagrams Sent Received The total number of UDP datagrams sent and received since TCP/IP initialization. The format is an unsigned long long integer.

Total Discard Percentage The percentage of UDP datagrams discarded as undeliverable because they were received in error (including "No Port Found" errors) compared to Datagrams Received since TCP/IP initialization. The format is an integer between 1 and 100 inclusive.

Total No Ports The number of input datagrams for which no appropriate application could be found at the destination port since TCP/IP initialization. The format is an unsigned integer.

Transmit Datagram Rate The number of UDP datagrams transmitted per minute during the most recent sampling interval. The format is an unsigned integer.

Manual IP Tunnels Attributes

Use the Manual IP Tunnels attributes to display information about manually defined IP tunnels known to the TCP/IP stack.

Authentication Algorithm Identifies the authentication algorithm used for this tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 38 = MD5
- 39 = SHA1

Authentication Protocol Identifies the authentication protocol to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 51 = AH
- 50 = ESP

Byte Rate The number of inbound or outbound bytes, per minute, for this tunnel during the most recent collection interval. The format is an integer.

Bytes The number of inbound and outbound bytes for this tunnel during the most recent collection interval. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Encapsulation Mode Tunnel encapsulation mode to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = TUNNEL
- 2 = TRANSPORT

Encryption Algorithm Encryption algorithm to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 3 = 3DES
- 11 = NULL
- 12 = AES
- 18 = DES
- 99 = <blank>

Inbound Authentication SPI Tunnel inbound authentication security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and displayed in hexadecimal.

Inbound Bytes The number of inbound bytes for this tunnel during the most recent collection interval. The format is an integer.

Inbound Encryption SPI Tunnel inbound encryption security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and displayed in hexadecimal.

Inbound Packets The number of inbound packets for this tunnel during the most recent collection interval. The format is an integer.

IP Address Version The version of the IP addresses being used for the security endpoints. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4: The traffic descriptor and the security endpoints are using IPv4 addresses.
- 1 = IPv6: The traffic descriptor and the security endpoints are using IPv6 addresses.

Local Security Endpoint The IP address of the local security endpoint responsible for negotiating the tunnel. The format is a UTF-8 encoded character string of up to 45 characters.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Outbound Authentication SPI Tunnel outbound authentication security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This field is an unsigned 4-byte integer and displayed in hexadecimal.

Outbound Bytes The number of outbound bytes for this tunnel during the most recent collection interval. The format is an integer.

Outbound Encryption SPI Tunnel outbound encryption security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This field is an unsigned 4-byte integer and displayed in hexadecimal.

Outbound Packets The number of outbound packets for this tunnel during the most recent time interval. The format is an integer.

Packet Rate The number of inbound or outbound packets, per minute, for this tunnel during the most recent collection interval. The format is an integer.

Packets The number of inbound and outbound packets for this tunnel during the most recent collection interval. The format is an integer.

Remote Security Endpoint The IP address of the remote security endpoint responsible for negotiating the tunnel. The format is a UTF-8 encoded character string of up to 45 characters.

State Current tunnel state. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = INACTIVE
- 4 = ACTIVE

Sysplex Name The name of the sysplex that the monitored system is part of.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Bytes The total number of inbound and outbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Bytes (in G)** column to calculate the total bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Bytes (in G) The total number of inbound and outbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the **Total Bytes** column to calculate the total bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Inbound Bytes The total number of inbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Inbound Bytes (in G)** column to calculate the total inbound bytes for the tunnel. The format is an integer.

Total Inbound Bytes (in G) The total number of inbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the **Total Inbound Bytes** column to calculate the total inbound bytes for the tunnel. The format is an integer.

Total Inbound Packets The total number of inbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Inbound Packets (in G)** column to calculate the total inbound packets for the tunnel. The format is an integer.

Total Inbound Packets (in G) The total number of inbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the **Total Inbound Packets** column to calculate the total inbound packets for the tunnel. The format is an integer.

Total Outbound Bytes The total number of outbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Outbound Bytes (in G)** column to calculate the total outbound bytes for the tunnel. The format is an integer.

Total Outbound Bytes (in G) The total number of outbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the **Total Outbound Bytes** column to calculate the total outbound bytes for the tunnel. The format is an integer.

Total Outbound Packets The total number of outbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Outbound Packets (in G)** column to calculate the total outbound packets for the tunnel. The format is an integer.

Total Outbound Packets (in G) The total number of outbound packets for this tunnel since the tunnel was established, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the **Total Outbound Packets** column to calculate the total outbound packets for the tunnel. The format is an integer.

Total Packets The total number of inbound and outbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the **Total Packets (in G)** column to calculate the total packets for the tunnel. The format is an integer.

Total Packets (in G) The total number of inbound and outbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the **Total Packets** column to calculate the total packets for the tunnel. The format is an integer.

Tunnel ID Tunnel identifier. This identifier is generated by TCP/IP and is not unique. Multiple related tunnels may have the same tunnel ID. The format is an alphanumeric string of up to 48 characters.

VPN Action Name The virtual private network (VPN) Action Name is the name associated with the definition of a security association. The security association describes the attributes of the tunnel. An example is the encryption algorithm to be used. The name is a character string of up to 48 characters.

OSA-Express Channels Attributes

Use the OSA-Express Channels attributes to create situations that monitor OSA-Express channels usage.

Channel Hardware Level The hardware model of the channel. This value is stored as an integer but displayed as a string. The possible values are:

```
unavailable=0
unknown=1
osaExp150=2
```

```
osaExp175=3
osaExp300=4
osaExp400=5
osaExp500=6
osaExp600=7
osaExp6=8
osaExp7=9
```

The value osaExp6(8) indicates a hardware level of 6, which also defines this feature as OSA-Express6. The value osaExp7(9) indicates a hardware level of 7, which also defines this feature as OSA-Express7.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of two hexadecimal characters.

Channel Type The type of channel for this interface. This value is stored as an integer but displayed as a string. The possible values are:

- 16 = OSAExpress
- 17 = OSADirectExpress
- 48 = osaIntraensembleData
- 49 = osaIntraensembleManage

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Control Unit Number The logical control unit number associated with the OSA-Express Channel. The format is an integer, displayed as 2-digit hexadecimal string in the range of 0x0000 to 0xFFFF.

Note: This field is not available for the OSA direct SNMP interface.

Current LPAR Name The name of the LPAR from which this data was retrieved. The format is an alphanumeric string, with a maximum of 8 characters.

Note: This field is not available for the OSA direct SNMP interface.

Current LPAR Number The number of the LPAR from which this data was retrieved. The format is an integer.

Note: This field is not available for the OSA direct SNMP interface.

Device or Port Name The name of the TCP/IP device or port associated with this channel. The format is an alphanumeric string, with a maximum of 16 characters.

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Managing LPAR Name The LPAR name of the OSA Support Facility managing this channel. Only one OSA/SF can manage an OSA-Express Channel within an z/OS Sysplex, though multiple OSA/SFs can retrieve information from the same OSA-Express Channel. The format is an alphanumeric string, with a maximum of 8 characters.

Note: This field is not available for the OSA direct SNMP interface.

Managing LPAR Number The LPAR number of the OSA Support Facility managing this channel (set to 0xFFFF if not being managed by an OSA/SF). The format is an integer and 0xFFFF is displayed as spaces.

Note: This field is not available for the OSA direct SNMP interface.

Micro Code Level The firmware (or micro code level) of the OSA feature. The format is an integer 2 bytes in length that is represented as 4-digit hexadecimal number in the range of 0x0000 to 0x0FFF.

Mode The configured mode of the OSA-Express adapter. The mode is set to **nothingConfigured** for channels that are not configured for LAN Emulation. This value is stored as an integer but displayed as a string. The possible values are:

- ' ' = 0 blank
- 1 = nothingConfigured
- 2 = passThruMode
- 3 = snaMode
- 4 = passThruAndSna
- 5 = atmLePassThru
- 6 = atmLeSna
- 7= atmLePassThruAndSna
- 8 = atmNative
- 9 = atmLe

Note: This field is not available for the OSA direct SNMP interface.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

PCI Utilization Per Five Minutes The average, over a 5-minute interval, of the percentage of time that the PCI bus was utilized to transfer data. This count does not include idle time or time used by routine maintenance tasks. The range for this value is from 0% to 100%.

PCI Utilization Per Minute The average, over a 1-minute interval, of the percentage of time that the PCI bus was utilized to transfer data. This count does not include idle time or time used by routine maintenance tasks. The range for this value is from 0% to 100%.

PCI Utilization Per One Hour The average, over a 1-hour interval, of the percentage of time that the PCI bus was utilized to transfer data. This count does not include idle time or time used by routine maintenance tasks. The range for this value is from 0% to 100%.

Port Count The number of ports on the OSA-Express adapter. For ATM155 QDIO LAN Emulation mode adapters, the value can be 1 or 2, depending on the number of logical ports configured. The format is an unsigned integer.

Processor Utilization Per Five Minutes The average, over a 5 minute interval, of the percentage of time that the channel path identifier (CHPID) processor was utilized to transfer data. This count does not include idle time or time used by routine maintenance tasks. The range for this value is from 0% to 100%.

Processor Utilization Per Minute The average, over a 1 minute interval, of the percentage of time that the channel path identifier (CHPID) processor was utilized to transfer data. This count does not include idle time or time used by routine maintenance tasks. The range for this value is from 0% to 100%.

Processor Utilization Per One Hour The average, over a 1 hour interval, of the percentage of time that the channel path identifier (CHPID) processor was utilized to transfer data. This count does not include idle time or time used by routine maintenance tasks. The range for this value is from 0% to 100%.

Share Indicator Indicates whether the OSA-Express feature can be shared across multiple LPARs. This value is stored as an integer but displayed as a string. The possible values are:

- 0 = notShared
- 1 = shared

State The state of the hardware channel. This value is stored as an integer but displayed as a string. The possible values are:

- 0= null
- 1 = online
- 3 = notInstalled
- 5 = offline

Note: This field is not available for the OSA direct SNMP interface.

Subtype The type of OSA feature present. This value is stored as an integer but displayed as a string. The possible values are:

```
unknown=1
gigabit=2
fastEthernet=3
atmNative=4
atmLanEmulation=5
noPortsDefined=6
oneLogicalEthPort=7
oneLogicalTokenRingPort=8
twoLogicalEthPorts=9
twoLogicalTokenRingPorts=10
logicalEthernetAndTokenRingPorts=11
logicalTokenRingAndEthPorts=12
gigabitEthernet=65
fastEthernet=81
tokenRing=82
oneThousandBaseTEthernet=97
tenGigabitEthernet=145
osaexp3gigabitEthernet=161
osaexp3oneThousandBaseTEthernet=177
osaexp3tenGigabitEthernet=193
osaexp5gigabitEthernet=195
osaexp5oneThousandBaseTEthernet=196
osaexp5tenGigabitEthernet=197
osaexp71000BaseTE=198
osaexp71GbE=199
osaexp710GbE=200
osaexp725GbE=201
atmEmulatedEthernet=2304
```

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

OSA-Express LPARS Attributes

Use the OSA-Express LPARS attributes to create situations that monitor OSA-Express LPAR usage.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of two hexadecimal characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Kilobyte Rate In Per Minute The average, over a 1 minute interval, of the number of kilobytes received that were processed for the specific LPAR. When the **Processor Utilization Per Minute** attribute for a specific LPAR has a value of -1, then the interval data was not retrieved from the adapter and this attribute has a value of 0. The format is an unsigned integer.

Kilobyte Rate In Per Five Minutes The average, over a 5 minute interval, of the number of kilobytes received that were processed for the specific LPAR. When the **Processor Utilization Per Five Minutes** attribute for a specific LPAR has a value of -1, then the interval data was not retrieved from the adapter and this attribute has a value of 0. The format is an unsigned integer.

Kilobyte Rate In Per Hour The average, over a 1 hour interval, of the number of kilobytes received that were processed for the specific LPAR. When the **Processor Utilization Per Hour** attribute for a specific LPAR has a value of -1, then the interval data was not retrieved from the adapter and this attribute has a value of 0. The format an unsigned integer.

Kilobyte Rate Out Per Minute The average, over a 1 minute interval, of the number of kilobytes sent that were processed for the specific LPAR. The format is an unsigned integer.

Kilobyte Rate Out Per Five Minutes The average, over a 5 minute interval, of the number of kilobytes sent that were processed for the specific LPAR. When the **Processor Utilization Per Five Minutes** attribute for a specific LPAR has a value of -1, then the interval data was not retrieved from the adapter and this attribute has a value of 0. The format is an unsigned integer.

Kilobyte Rate Out Per Hour The average, over a 1 hour interval, of the number of kilobytes sent that were processed for the specific LPAR. When the **Processor Utilization Per Hour** attribute for a specific LPAR has a value of -1, then the interval data was not retrieved from the adapter and this attribute has a value of 0. The format is an unsigned integer.

LPAR Logical Channel Subsystem The logical channel subsystem to which the performance data refers. For an IBM eServer zSeries 800 or 900 system, there is only one logical channel subsystem that is indicated by a value of **0** (zero). For a IBM eServer zSeries 990 system, there can be multiple logical channels. They are numbered starting with zero (for example, five subsystems would be number 0 to 4). The format is an unsigned integer.

LPAR Name The name of the logical partition from which this data was retrieved. This is not necessarily the z/OS system ID. The format is an alphanumeric string, with a maximum of 8 characters.

LPAR Number The number of the logical partition from which this data was retrieved. The format is an unsigned integer.

LPAR Status The status of the LPAR. This attribute is valid for IBM eServer zSeries 990 or greater hardware only and indicates whether the LPAR is unknown, online, or offline. This value is stored as an unsigned integer and displayed as a string. The possible values are:

- 0 = unknown
- 1 = offline
- 2 = online

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Processor Utilization Per Five Minutes The average, over a 5 minute interval, of the percentage of time that the channel path identifier (CHPID) processor was used to transfer data for the specific LPAR. This count does not include idle time or time used by routine maintenance tasks. The range for this value is from 0% to 100%. The format is an unsigned integer.

Processor Utilization Per Minute The average, over a 1 minute interval, of the percentage of time that the channel path identifier (CHPID) processor was used to transfer data for the specific LPAR. This count does not include idle time or time used by routine maintenance tasks. The range for this value is from 0% to 100%. The format is an unsigned integer.

Processor Utilization Per Hour The average, over a 1 hour interval, of the percentage of time that the channel path identifier (CHPID) processor was used to transfer data for the specific LPAR. This count does not include idle time or time used by routine maintenance tasks. The range for this value is from 0% to 100%. A value of -1 indicates that the value was not retrieved from the adapter. The format is an unsigned integer.

OSA-Express Ports Attributes

Use the OSA-Express Ports attributes to create situations that monitor OSA-Express ports usage.

Active MAC Address The current MAC address in use on the adapter. The format is a 12-digit hexadecimal string.

Active Speed The actual speed and mode in which the OSA is running. The format is an integer with the following possible values:

- 0 = unknown
- 1 = tenMbHalfDuplex
- 2 = tenMbFullDuplex
- 3 = oneHundredMbHalfDuplex
- 4 = oneHundredMbFullDuplex
- 6 = oneThousandMbFullDuplex

Burned In MAC Address The burned-in MAC address on the OSA. The format is a 12-digit hexadecimal string.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of 2 hexadecimal characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month

- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Configuration Name The name of the configuration that is on the OSA. It is set using OSA/SF. It is not used by OSA. The format is an alphanumeric string, with a maximum of 34 characters.

Configuration Speed The configured port speed in megabits per second. This field shows the speed that was configured for the OSA-Express Fast Ethernet feature. It is not used by OSA. Express gigabit features are displayed as n/a. The format is an integer with the following possible values:

- 0 = autoNegotiate
- - 1 = notValidGigabit
- 1 = tenMbHalfDuplex
- 2 = tenMbFullDuplex
- 3 = oneHundredMbHalfDuplex
- 4 = oneHundredMbFullDuplex
- 6 = oneThousandMbFullDuplex

Current Broadcast Frames The count of the number of broadcast frames received by this port during the most recent time interval. A channel path identifier (CHPID) reset causes this value to be reset to zero. The format is an unsigned integer, stored in units of K (1024). The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Current Group Frames In The count of the number of group frames received by this port during the most recent time interval. A channel path identifier (CHPID) reset causes this value to be reset to zero. The format is an unsigned integer.

Current Packets In The count of the number of packets received by this port during the most recent time interval. A channel path identifier (CHPID) reset causes this value to be reset to zero. The format is an unsigned integer.

Current Packets Out The count of the number of packets transmitted from this port during the most recent time interval. A channel path identifier (CHPID) reset causes this value to be reset to zero. The format is an unsigned integer.

Current Unknown IP Frames The count of the number of packets that were discarded during the most recent time interval because they did not have a matching IP address. There was neither a primary nor a secondary router default defined. This object is not supported for Fast Ethernet adapters so the value is zero. The format is an unsigned integer.

Disabled Status When the value of the Hardware State attribute is disabled, this attribute explains the reasons for the disabled state. The format is a string of up to 180 characters. This field can contain any combination of the following reasons:

- Internal port failure
- Service processor request
- Network request
- OSA/SF request
- Configuration change
- Link failure threshold exceeded
- Port temporarily disabled
- Unknown

Disabled Status When the value of the Hardware State attribute is disabled, this attribute explains the reasons for the disabled state. This value is stored as a hexadecimal integer and displayed as a 4-digit hexadecimal number mapped by the bit settings below:

- 0 = reserved
- 1 = internalPortFailure
- 2 = reserved
- 3 = reserved
- 4 = reserved
- 5 = reserved
- 6 = portTemporarilyDisabled
- 7 = reserved
- 8 = reserved
- 9 = serviceProcessorRequest
- 10 = networkRequest
- 11 = osasfRequest
- 12 = configurationChange
- 13 = linkFailureThresholdExceeded
- 14 = reserved
- 15 = reserved

Hardware State The state of the port. If the port is disabled, see Disabled Status for details. This value is stored as an integer but displayed as a string. These are the possible values:

- 0 = undefined
- 1 = unavailable
- 2 = enabling
- 3 = disabling
- 4 = enabled
- 5 = disabled
- 6 = linkMonitor
- 7 = definitionError
- 8 = configuredOffline
- 17 = unknown
- 18 = linkFailure
- 19 = disabled

- 20 = enabled

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Interface Index The interface index associated with this port. The format is an unsigned integer.

Link Name The name of the TCP/IP link associated with this port. The format is an alphanumeric string no longer than 16 characters.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Port Interface Index The OSA-Express QDIO port interface index. For interfaces defined by DEVICE and LINK, this index is the DEVICE interface index. For interfaces defined by INTERFACE, this index is the dynamically generated interface index for the port. This field only applies to the following interface types:

- OSA-Express_QDIO_Ethernet_OSD (external data network type, which is the default value)
- OSA-Express_QDIO_Ethernet_OSM (intra-node management network, which requires IPv6)
- OSA-Express_QDIO_Ethernet_OSX (intra-ensemble data network)

The format is an unsigned integer. For more information about these interface types, see the *IBM z/OS Communications Server: IP Configuration Guide*.

Note: This attribute is available only when the monitoring agent is running on z/OS v1.12 or later.

Port Name Specifies the port name that must also be entered at the connection manager on the host and the application. The format is an alphanumeric string no longer than 16 characters.

Port Number The physical port number for this port. The format is an integer.

Port Type The physical port type. This value is stored as an integer and displayed as a string. Possible port types are:

- 65 = gigabitEthernet
- 81 = fastEthernet
- 97 = oneThousandBaseTEthernet
- 145 = tenGigabitEthernet

Service Mode Indicates whether the processor is in service mode. The format is an integer. The possible values are:

- 0 = NotInServiceMode
- 1 = InServiceMode

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Broadcast Frames (K) The total number of broadcast frames received by this port. A channel path identifier (CHPID) reset causes this value to be reset to zero. The format is an unsigned integer.

Total Group Frames In (K) The count of the number of group frames received by this port. A channel path identifier (CHPID) reset causes this value to be reset to zero. The format is an unsigned integer, stored in units of K (1024). The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Total Packets In (K) The total number of packets received by this port. A channel path identifier (CHPID) reset causes this value to be reset to zero. The format is an unsigned integer, stored in units of K (1024). The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Total Packets Out (K) The total number of packets transmitted from this port. A channel path identifier (CHPID) reset causes this value to be reset to zero. The format is an unsigned integer, stored in units of K

(1024). The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Total Unknown IP Frames (K) The total number of packets that were discarded because they did not have a matching IP address. There was neither a primary nor a secondary router default defined. This object is not supported for Fast Ethernet adapters so the value is zero. The format is an unsigned integer, stored in units of K (1024). The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

User Data The data set by the user, expressed as a string. It is ignored by the OSA. The format is an alphanumeric string no longer than 32 characters.

zOS Release IBM internal use only.

OSA-Express3 Ports Control Attributes

Use the OSA-Express3 Ports Control attributes to monitor individual ports on a OSA-Express3 feature.

There can be two physical ports on each OSA channel path identifier, each with different data. When two ports are present, each one is assigned a separate ifIndex by the operating system. Each ifIndex contains the data for the corresponding port.

Transmitter on (XON) and transmitter off (XOFF) packets are flow-control packets between the OSA and the switch to which it is connected. They are used to provide flow control between the two ports, and are of particular interest if the port is at 100% utilization.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of two hexadecimal characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Port Name The name of the port as specified by the VTAM Transport Resource List Entry (TRLE). The format is a 32-character alphanumeric string.

Port Number The physical port number for this port. The format is an integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total XOFF Packets Received The number of valid XOFF (Transmitter OFF) packets received by the OSA since the last time the OSA port was reset. XOFF packets can use the global address or the station address. Receiving XOFF packets indicates that the sender experienced a problem with a queue filling up or some other software-initiated action. The format is an unsigned integer.

Total XOFF Packets Transmitted The number of XOFF (Transmitter OFF) packets transmitted by the OSA since the last time the OSA port was reset. Sending XOFF packets indicates that the queue is filling up or some software-initiated action has occurred. The format is an unsigned integer.

Total XON Packets Received The number of XON (Transmitter ON) packets received by the OSA since the last time the OSA port was reset. XON packets can use the global address or the station address. Receiving XON packets indicates that the sender experienced a problem with a queue filling up or some other software-initiated action. The format is an unsigned integer.

Total XON Packets Transmitted The number of XON (Transmitter ON) packets transmitted by the OSA since the last time the OSA port was reset. Sending XON packets indicates that the queue is filling up or some software-initiated action has occurred. The format is an unsigned integer.

Trap Control Flags The value of this object determines which traps will be generated by the OSA. The value of this object is initially all zeros, indicating that all traps will be sent to the OSA subagent. Setting the appropriate bit prevents a particular trap from being sent to the subagent. When the bit value of the disableEthLANChange bit is set to zero (0), then the trap ibmOSAExp10GigEthLANStateChange is sent. The format is a 4-digit hexadecimal number. Valid values are:

- x'0000' meaning the trap is enabled.
- x'8000' meaning the trap is disabled.

XOFF Packets Received The number of XOFF (Transmitter OFF) packets received by the OSA during the most recent time interval. XOFF packets can use the global address or the station address. Receiving XOFF packets indicates that the sender experienced a problem with a queue filling up or some other software-initiated action. The format is an unsigned integer.

XOFF Packets Transmitted The number of XOFF (Transmitter OFF) packets transmitted by the OSA during the most recent time interval. Sending XOFF packets indicates that the queue is filling up or some software-initiated action has occurred. The format is an unsigned integer.

XON Packets Received The number of XON (Transmitter ON) packets received by the OSA during the most recent time interval. XON packets can use the global address or the station address. Receiving XON packets indicates that the sender experienced a problem with a queue filling up or some other software-initiated action. The format is an unsigned integer.

XON Packets Transmitted The number of XON (Transmitter ON) packets transmitted by the OSA during the most recent time interval. Sending XON packets indicates that the queue is filling up or some software-initiated action has occurred. The format is an unsigned integer.

OSA-Express3 Ports Errors Attributes

Use the OSA-Express3 Ports Errors attributes to monitor error and control data for individual ports on a OSA-Express3 feature.

There can be two physical ports on each OSA channel path identifier, each with different data. On z/OS verion 1.10 or later, when two ports are present, each one is assigned a separate ifIndex by the operating system. Each ifIndex contains the data for the corresponding port.

Alignment Errors The number of packets received during the most recent time interval with alignment errors (the packet is not an integer number of bytes in length). This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of two hexadecimal characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

CRC Errors The number of packets received with cyclic redundancy check (CRC) errors during the most recent time interval. The format is an unsigned integer.

Deferred Events The number of events that were deferred by the OSA during the most recent time interval. A deferred event occurs when the transmitter cannot immediately send a packet because the medium is busy for one of these reasons:

- A device other than the OSA is transmitting.
- The inter-packet gap (IPG) timer has not expired.
- Problems occurred when receiving transmitter off (XOFF) frames.
- The link is down.

This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Excessive Collisions The number of times that a packet successfully transmitted by the OSA encountered more than 16 collisions during the most recent time interval. This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Fragmented Frames Received The number of frames received by the OSA during the most recent time interval that passed address filtering, were smaller than the minimum size of 64 bytes, and had a bad cyclic redundancy check (CRC). The format is an unsigned integer.

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Interface Index The interface index associated with this port. The format is a four-byte integer.

Jabber Frames Received The number of frames received by the OSA during the most recent time interval that passed address filtering, were greater than maximum size in length, and had a bad cyclic redundancy check (CRC). The format is an unsigned integer.

The maximum transmission unit (MTU) is the maximum packet size, in bytes, that can be sent on an interface. You can set the MTU size (as long as you stay within the limits and maximum values of the OSA) using TCP/IP profile statements. You can also set the parameters of the neighboring network interface card (NIC) and port (usually a port on a switch, but could be another OSA). For information about setting maximum size for OSA devices, see the *IBM z/OS Communications Server: IP Configuration Reference*.

Late Collisions The number of late collisions encountered by the OSA during the most recent time interval. Late collisions occur under the following circumstances:

- After the 64-byte time into the transmissions of the packet while working in 10-100 Mb/sec data rate.
- After the 512-byte time into the transmission of the packet while working in the 1000 Mb/sec data rate.

This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Length Error Packets Received The number of length-error packets received by the OSA during the most recent time interval. A length error occurs if an incoming packet passes filter criteria, but is undersized or oversized. The format is an unsigned integer.

Missed Packets The number of packets that were missed by the OSA during the most recent time interval because not enough space was available to store the incoming packet. The format is an unsigned integer.

Multiple Collisions The number of times that a packet successfully transmitted by the OSA encountered more than 1 collision, but fewer than 16, during the most recent time interval. This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Not Stored Frames Received The number of times that frames were received by the OSA during the most recent time interval when no buffers were available in host memory to store those frames. The format is an unsigned integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Oversized Frames Received The number of frames received by the OSA during the most recent time interval that passed address filtering and had a valid cyclic redundancy check (CRC), but were longer than the maximum size of 1522 bytes for operating-system embedded (OSE) non-queued direct I/O (non-QDIO) features or 16384 bytes for OSD queued direct I/O (QDIO) features. The format is an unsigned integer.

Port Name The name of the port as specified by the VTAM Transport Resource List Entry (TRLE). The format is a 32-character alphanumeric string.

Port Number The physical port number for this port. The format is an integer.

Sequence Errors The number of sequence error events transmitted over the OSA interface during the most recent time interval. The proper sequence of 8b/10b symbols is as follows:

- Idle
- Start-of-frame
- Data
- Pad
- End-of-frame
- Fill

This count increments for any illegal sequence of delimiters. This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Single Collisions The number of times that a packet successfully transmitted by the OSA encountered a single collision during the most recent time interval. This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Alignment Errors The number of packets received by the OSA since the last time the OSA port was reset with alignment errors (the packet is not an integer number of bytes in length). This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Total CRC Errors The number of packets received by the OSA with cyclic redundancy check (CRC) errors since the last time the OSA port was reset. The format is an unsigned integer.

Total Deferred Events The number of events deferred by the OSA since the last time the OSA port was reset. A deferred event occurs when the transmitter cannot immediately send a packet because the medium is busy for one of these reasons:

- A device other than the OSA is transmitting.
- The inter-packet gap (IPG) timer has not expired.
- Problems occurred when receiving transmitter off (XOFF) frames.
- The link is down.

This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Total Excessive Collisions The number of times since the OSA port was reset that a packet that was successfully transmitted by the OSA encountered more than 16 collisions during transmission. This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Total Fragmented Frames Received The number of frames received by the OSA since the last time the OSA port was reset that passed address filtering, were smaller than the minimum size of 64 bytes, and had a bad cyclic redundancy check (CRC). The format is an unsigned integer.

Total Jabber Frames Received The number of frames received by the OSA since the last time the OSA port was reset that passed address filtering, were greater than maximum size in length, and had a bad cyclic redundancy check (CRC). The format is an unsigned integer.

The maximum transmission unit (MTU) is the maximum packet size, in bytes, that can be sent on an interface. You can set the MTU size (as long as you stay within the limits and maximum values of the OSA) using TCP/IP profile statements. You can also set the parameters of the neighboring network interface card (NIC) and port (usually a port on a switch, but could be another OSA). For information about setting maximum size for OSA devices, see the *IBM z/OS Communications Server: IP Configuration Reference.*

Total Length Error Packets Received The number of packet length-error events received by the OSA since the last time the OSA port was reset. A length error occurs if an incoming packet passes filter criteria, but is undersized or oversized. The format is an unsigned integer.

Total Late Collisions The number of late collisions encountered by the OSA since the last time the OSA port was reset. Late collisions occur under the following circumstances:

- After the 64-byte time into the transmissions of the packet while working in 10-100 Mb/sec data rate.
- After the 512-byte time into the transmission of the packet while working in the 1000 Mb/sec data rate.

This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Total Missed Packets The number of packets that were missed by the OSA since the last time the OSA port was reset because too little space was available to store the incoming packet. The format is an unsigned integer.

Total Multiple Collisions The number of times that a packet successfully transmitted by the OSA encountered more than 1 collision, but fewer than 16, since the last time the OSA port was reset. This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Total Not Stored Frames Received The number of times that frames were received by the OSA since the last time the OSA port was reset when no buffers were available in host memory to store those frames. The format is an unsigned integer.

Total Oversized Frames Received The number of frames received by the OSA since the last time the OSA port was reset that passed address filtering and had a valid cyclic redundancy check (CRC), but were longer than the maximum size of 1522 bytes for operating-system embedded (OSE) non-queued direct I/O (non-QDIO) features or 16384 bytes for OSD queued direct I/O (QDIO) features. The format is an unsigned integer.

Total Sequence Errors The number of sequence error events transmitted over the OSA interface since the last time the OSA port was reset. The proper sequence of 8b/10b symbols is as follows:

- Idle
- Start-of-frame
- Data
- Pad
- End-of-frame
- Fill

This count increments for any illegal sequence of delimiters. This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Total Single Collisions The number of times that a packet successfully transmitted by the OSA encountered a single collision by the OSA since the last time the OSA port was reset. This field is not valid for 10 gigabit features and will be zero (0) for these devices. The format is an unsigned integer.

Total Undersized Frames Received The number of frames received by the OSA since the last time the OSA port was reset that passed address filtering, were smaller than the minimum size of 64 bytes, and had a valid cyclic redundancy check (CRC). Packets shorter than 64 bytes must be padded and may indicate that the LAN is incorrectly configured and not performing up to capacity. The format is an unsigned integer.

Undersized Frames Received The number of frames received by the OSA during the most recent time interval that passed address filtering, were smaller than the minimum size of 64 bytes, and had a valid cyclic redundancy check (CRC). Packets shorter than 64 bytes must be padded and may indicate that the LAN is incorrectly configured and not performing up to capacity. The format is an unsigned integer.

OSA-Express3 Ports Summary Attributes

Use the OSA-Express3 Ports Summary attributes to monitor individual ports on a OSA-Express3 feature.

There can be two physical ports on each OSA channel path identifier, each with different data. When two ports are present, each one is assigned a separate ifIndex by the operating system. Each ifIndex contains the data for the corresponding port.

Active Speed Mode The actual speed at which the OSA is running. This value is stored as an integer but displayed as a string. The possible values are:

- 0 = unknown
- 1 = tenMegabits
- 2 = tenMbFullDuplex
- 3 = oneHundredMbHalfDuplex
- 4 = oneHundredMbFullDuplex
- 6 = oneThousandMbFullDuplex
- 8 = tenGigabitFullDuplex

Active MAC Address A 6-byte octet string that contains the current MAC address in use on the adapter. The values are in canonical format. The format is a 12-digit hexadecimal string.

Burned In MAC Address A 6-byte octet string that contains the burned-in MAC address on the OSA. The values are in canonical format. The format is a 12-digit hexadecimal string.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of two hexadecimal characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Configuration Name The name of the configuration on the OSA. This value is set using the Open Systems Adapter/Support Facility (OSA/SF). It is not used by the OSA. The format is a string of up to 34 characters.

Configuration Speed Mode The configured port speed. This field shows the speed that was configured by the user for the OSA-Express Fast Ethernet feature. It is not used by OSA-Express Gigabit or 10 Gigabit Ethernet feature. This value is stored as an integer and displayed as a string with the following possible values:

- -1 = notValidGigabit
- 0 = autoNegotiate
- 1 = tenMbHalfDuplex
- 2 = tenMbFullDuplex
- 3 = oneHundredMbHalfDuplex
- 4 = oneHundredMbFullDuplex
- 6 = oneThousandMbFullDuplex
- 8 = tenGigabitFullDuplex

Disabled Status Reasons for the disabled state. When the value of the LAN Traffic State attribute is disabled (5), this attribute explains the reasons for the disabled state. The value for this object may be a combination of the bits shown in the list which follows. This value is stored as a hexadecimal integer and displayed as a 4-digit hexadecimal number mapped by the bit settings below:

- 0 = reserved
- 1 = internalPortFailure
- 2 = reserved

- 3 = reserved
- 4 = reserved
- 5 = reserved
- 6 = portTemporarilyDisabled
- 7 = reserved
- 8 = reserved
- 9 = serviceProcessorRequest
- 10 = networkRequest
- 11 = osasfRequest
- 12 = configurationChange
- 13 = linkFailureThresholdExceeded
- 14 = reserved
- 15 = reserved

Exclusive Usage ID Specifies the exclusive usage ID that, when paired with the corresponding Exclusive Usage Media Access Control (MAC), defines one of multiple Ethernet ports that can be used in parallel to increase the link speed beyond the limits of any single port. The format is an 8-character text string

Exclusive Usage MAC Specifies the exclusive usage Media Access Control (MAC) that, when paired with the corresponding Exclusive Usage ID, defines one of multiple Ethernet ports that can be used in parallel to increase the link speed beyond the limits of any single port. The format is a 12-digit hexadecimal string.

Good Octets Received The number of good (without error) octets received by the OSA during the most recent time interval. This count does not include flow-control octets. When the measured value exceeds 2,147,483,647 (the maximum value), the attribute will be set to 2,147,483,647. The format is an unsigned integer.

Good Octets Transmitted The number of good (without error) octets transmitted by the OSA during the most recent time interval. This count does not include flow-control octets. When the measured value exceeds 2,147,483,647 (the maximum value), the attribute will be set to 2,147,483,647. The format is an unsigned integer.

Good Packets Received The number of good packets of any length received by the OSA during the most recent time interval. This count does not include received flow-control packets and packets that fail filtering. The format is an unsigned integer.

Good Packets Transmitted The number of good packets of any length transmitted by the OSA during the most recent time interval. A good packet is defined as one that is 64 or more bytes in length. This count does not include flow-control packets The format is an unsigned integer.

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Interface Index The interface index associated with this port. The format is an unsigned integer.

IPv4 Layer 3 VMAC Specifies the Media Access Control (MAC) address being used if a Layer 3 Virtual MAC is being used for IPv4 on this stack. If the Layer 3 VMAC for IPv4 is not assigned, this field will contain all zeros. The format is a 12-digit hexadecimal string.

IPv6 Layer 3 VMAC Specifies the Media Access Control (MAC) address being used if a Layer 3 Virtual MAC is being used for IPv6 on this stack. If the Layer 3 VMAC for IPv6 is not assigned, this field will contain all zeros. The format is a 12-digit hexadecimal string.

LAN Traffic State The LAN state, expressed in value ranges from 0 to 8. A value of 5 (disabled) is further explained by the Disabled Status attribute. This value is stored as an integer and displayed as a string. The possible values are:

- 0 = undefined

- 1 = unavailable
- 2 = enabling
- 3 = disabling
- 4 = enabled
- 5 = disabled
- 6 = linkMonitor
- 7 = definitionError
- 8 = configuredOffline

For more information about these values, see the *zSeries Open Systems Adapter-Express Customer's Guide and Reference*.

Octet Rate The average number of octets received or transmitted by the OSA, per minute, during the most recent time interval. When the measured value exceeds 2,147,483,647 (the maximum value), the attribute will be set to 2,147,483,647. The format is an unsigned integer.

Octets Received The number of octets received by the OSA during the most recent time interval. This count includes octets of all lengths, octets containing errors, and flow-control octets. When the measured value exceeds 2,147,483,647 (the maximum value), the attribute will be set to 2,147,483,647. The format is an unsigned integer.

Octets Received or Transmitted The number of octets received or transmitted by the OSA during the most recent time interval. When the measured value exceeds 2,147,483,647 (the maximum value), the attribute will be set to 2,147,483,647. The format is an unsigned integer.

Octets Transmitted The number of octets transmitted by the OSA during the most recent time interval. This count includes octets of all lengths and flow-control octets. When the measured value exceeds 2,147,483,647 (the maximum value), the attribute will be set to 2,147,483,647. The format is an unsigned integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Packet Rate The average number of packets received or transmitted by the OSA, per minute, during the most recent time interval. The format is an unsigned integer.

Packets Received The number of packets received by the OSA during the most recent time interval. All packets are counted, including packets of all lengths and flow-control packets. The format is an unsigned integer.

Packets Received or Transmitted The number of packets received or transmitted by the OSA during the most recent time interval. All packets are counted, including packets of all lengths, packets containing errors, and flow-control packets. The format is an unsigned integer.

Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval. All packets are counted, including packets of all lengths, packets containing errors, and flow-control packets. The format is an unsigned integer.

Port Interface Index The OSA-Express QDIO port interface index. For interfaces defined by DEVICE and LINK, this is the DEVICE interface index. For interfaces defined by INTERFACE, this is the dynamically generated interface index for the port. This field only applies to the following interface types:

- OSA-Express_QDIO_Ethernet_OSD (external data network type, which is the default value)
- OSA-Express_QDIO_Ethernet_OSM (intra-node management network, which requires IPv6)
- OSA-Express_QDIO_Ethernet_OSX (intra-ensemble data network)

The format is an unsigned integer. For more information about these interface types, see *IBM z/OS Communications Server: IP Configuration Guide*.

Note: This attribute is available only when the monitoring agent is running on z/OS v1.12 or later.

Port Name The name of the port as specified by the VTAM Transport Resource List Entry (TRLE). The format is a 32-character alphanumeric string.

Port Number The physical port number for this port. The format is an integer.

Port Type The physical port type. This value is stored as an integer but displayed as a string. Valid values are:

- 161 = osaexp3gigabitEthernet
- 177 = osaexp3oneThousandBaseTEthernet
- 193 = osaexp3tenGigabitEthernet

Service Mode An indicator of whether the processor is in service mode. This value is stored as an integer but displayed as a string. The possible values are:

- 0 = No
- 1 = Yes

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Good Octets Received The number of good (without error) octets received by the OSA since the last time the OSA port was reset. This count does not include flow-control octets. The format is a long long integer.

Total Good Octets Received The number of good (without error) octets received by the OSA since the last time the OSA port was reset. This count does not include flow-control octets. When the value in the **Total Good Octets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Good Octets Received (in G)** field, and the remainder is stored in the **Total Good Octets Received** field. The format is an unsigned integer.

Total Good Octets Received (in G) The number of good (without error) octets received by the OSA since the last time the OSA port was reset, expressed in G. This count does not include flow-control octets. When the value in the **Total Good Octets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Good Octets Received (in G)** field, and the remainder is stored in the **Total Good Octets Received** field. The format is an unsigned integer.

Total Good Octets Transmitted The number of good (without error) octets transmitted by the OSA since the last time the OSA port was reset. This count does not include flow-control octets. The format is a long long integer.

Total Good Octets Transmitted The number of good (without error) octets transmitted by the OSA since the last time the OSA port was reset. This count does not include flow-control octets. When the value in the T**otal Good Octets Transmitted** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Good Octets Transmitted (in G**) field, and the remainder is stored in the **Total Good Octets Transmitted** field. The format is an unsigned integer.

Total Good Octets Transmitted (in G) The number of good (without error) octets transmitted by the OSA since the last time the OSA port was reset, expressed in G. This count does not include flow-control octets. When the value in the **Total Good Octets Transmitted** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Good Octets Transmitted (in G)** field, and the remainder is stored in the **Total Good Octets Transmitted** field. The format is an unsigned integer.

Total Good Packets Received The number of good packets of any length received by the OSA since the last time the OSA port was reset. This count does not include received flow-control packets and packets that fail filtering. The format is a long long integer.

Total Good Packets Received The number of good packets of any length received by the OSA since the last time the OSA port was reset. This count does not include received flow-control packets and packets that fail filtering. When the value in the **Total Good Packets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Good Packets Received (in**

G) field and the remainder is stored in the **Total Good Packets Received** field. The format is an unsigned integer.

Total Good Packets Received (in G) The number of good packets of any length received by the OSA since the last time the OSA port was reset, expressed in G. This count does not include received flow-control packets and packets that fail filtering. When the value in the **Total Good Packets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Good Packets Received (in G)** field, and the remainder is stored in the **Total Good Packets Received** field. The format is an unsigned integer.

Total Good Packets Transmitted The number of good packets of any length transmitted by the OSA since the last time the OSA port was reset. A good packet is defined as one that is 64 or more bytes in length. This count does not include flow-control packets. The format is a long long integer.

Total Good Packets Transmitted The number of good packets of any length transmitted by the OSA since the last time the OSA port was reset. A good packet is defined as one that is 64 or more bytes in length. This count does not include flow-control packets. When the value in the **Total Good Packets Transmitted** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Good Packets Transmitted (in G)** field, and the remainder is stored in the **Total Good Packets Transmitted** field. The format is an unsigned integer.

Total Good Packets Transmitted (in G) The number of good packets of any length transmitted by the OSA since the last time the OSA port was reset, expressed in G. A good packet is defined as one that is 64 or more bytes in length. This count does not include flow-control packets. When the value in the **Total Good Packets Transmitted** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Good Packets Transmitted (in G)** field, and the remainder is stored in the **Total Good Packets Transmitted** field. The format is an unsigned integer.

Total Octets The number of octets received or transmitted by the OSA since the last time the OSA port was reset. The format is a long long integer.

Total Octets The number of octets received or transmitted by the OSA since the last time the OSA port was reset. When the value in the **Total Octets** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Octets (in G)** field, and the remainder is stored in the **Total Octets** field. The format is an unsigned integer.

Total Octets (in G) The number of octets received or transmitted by the OSA since the last time the OSA port was reset, expressed in G. When the value in the **Total Octets** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Octets (in G)** field, and the remainder is stored in the **Total Octets** field. The format is an unsigned integer.

Total Octets Received The number of octets received by the OSA since the last time the OSA port was reset. This count includes octets of all lengths, octets containing errors, and flow-control octets. The format is a long long integer.

Total Octets Received The number of octets received by the OSA since the last time the OSA port was reset. This count includes octets of all lengths, octets containing errors, and flow-control octets. When the value in the **Total Octets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Octets Received (in G)** field, and the remainder is stored in the **Total Octets Received** field. The format is an unsigned integer.

Total Octets Received (in G) The number of octets received by the OSA since the last time the OSA port was reset, expressed in G. This count includes octets of all lengths, octets containing errors, and flow-control octets. When the value in the **Total Octets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Octets Received (in G)** field, and the remainder is stored in the **Total Octets Received** field. The format is an unsigned integer.

Total Octets Transmitted The number of octets transmitted by the OSA since the last time the OSA port was reset. This count includes octets of all lengths, octets containing errors, and flow-control octets. The format is a long long integer.

Total Octets Transmitted The number of octets transmitted by the OSA since the last time the OSA port was reset. This count includes octets of all lengths, octets containing errors, and flow-control octets. When the value in the **Total Octets Transmitted** field exceeds 1,073,741,823 (1 G), the number is

divided by 1,073,741,824. The quotient is stored in the **Total Octets Transmitted (in G)** field, and the remainder is stored in the **Total Octets Transmitted** field. The format is an unsigned integer.

Total Octets Transmitted (in G) The number of octets transmitted by the OSA since the last time the OSA port was reset, expressed in G. This count includes octets of all lengths, octets containing errors, and flow-control octets. When the value in the T**otal Octets Transmitted** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Octets Transmitted (in G)** field, and the remainder is stored in the **Total Octets Transmitted** field. The format is an unsigned integer.

Total Packets The number of packets received or transmitted by the OSA since the last time the OSA port was reset. All packets are counted, including packets of all lengths and flow-control packets. The format is a long long integer.

Total Packets The number of packets received or transmitted by the OSA since the last time the OSA port was reset. All packets are counted, including packets of all lengths and flow-control packets. When the value in the **Total Packets** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Packets (in G)** field, and the remainder is stored in the **Total Packets** field. The format is an unsigned integer.

Total Packets (in G) The number of packets received or transmitted by the OSA since the last time the OSA port was reset, expressed in G. All packets are counted, including packets of all lengths and flow-control packets. When the value in the **Total Packets** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Packets (in G)** field, and the remainder is stored in the **Total Packets** field. The format is an unsigned integer.

Total Packets Received The number of packets received by the OSA since the last time the OSA port was reset. All packets are counted, including packets of all lengths, packets containing errors, and flow-control packets. The format is a long long integer.

Total Packets Received The number of packets received by the OSA since the last time the OSA port was reset. All packets are counted, including packets of all lengths, packets containing errors, and flow-control packets. When the value in the **Total Packets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Packets Received (in G)** field, and the remainder is stored in the **Total Packets Received** field. The format is an unsigned integer.

Total Packets Received (in G) The number of packets received by the OSA since the last time the OSA port was reset, expressed in G. All packets are counted, including packets of all lengths, packets containing errors, and flow-control packets. When the value in the **Total Packets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Packets Received (in G)** field, and the remainder is stored in the **Total Packets Received** field. The format is an unsigned integer.

Total Packets Transmitted The number of packets transmitted by the OSA since the last time the OSA port was reset. All packets are counted, including packets of all lengths and flow-control packets. The format is a long long integer.

Total Packets Transmitted The number of packets transmitted by the OSA since the last time the OSA port was reset. All packets are counted, including packets of all lengths and flow-control packets. When the value in the **Total Packets Transmitted** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Packets Transmitted (in G)** field, and the remainder is stored in the **Total Packets Transmitted** field. The format is an unsigned integer.

Total Packets Transmitted (in G) The number of packets transmitted by the OSA since the last time the OSA port was reset, expressed in G. All packets are counted, including packets of all lengths and flow-control packets. When the value in the **Total Packets Transmitted** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Packets Transmitted (in G)** field, and the remainder is stored in the **Total Packets Transmitted** field. The format is an unsigned integer.

zOS Release IBM internal use only.

OSA-Express3 Ports Throughput Attributes

Use the OSA-Express3 Ports Throughput attributes to monitor individual ports on an OSA-Express3 feature.

There can be two physical ports on each OSA Channel Path Identifier (CHPID), and each contains different data. On z/OS version 1.10 or later, when two ports are present, each one is assigned a separate ifIndex by the operating system. Each ifIndex contains the data for the corresponding port.

64 Byte Packets Received The number of packets received by the OSA during the most recent time interval that are exactly 64 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

Note: 64 bytes is the minimum length for an Ethernet packet. Packets shorter than 64 bytes have to be padded. This value is of interest because it indicates whether the LAN is configured incorrectly and not performing up to capacity.

64 Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that are exactly 64 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

Note: 64 bytes is the minimum length for an Ethernet packet. Packets shorter than 64 bytes have to be padded. This value is of interest because it indicates whether the LAN is configured incorrectly and not performing up to capacity.

65 to 127 Byte Packets Received The number of packets received by the OSA during the most recent time interval that are 65 to 127 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

65 to 127 Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that are 65 to 127 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

128 to 255 Byte Packets Received The number of packets received by the OSA during the most recent time interval that are 128 to 255 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

128 to 255 Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that are 128 to 255 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

256 to 511 Byte Packets Received The number of packets received by the OSA during the most recent time interval that are 256 to 511 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

256 to 511 Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that are 256 to 511 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

512 to 1023 Byte Packets Received The number of packets received by the OSA during the most recent time interval that are 512 to 1023 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

512 to 1023 Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that are 512 to 1023 bytes in length. This count does not include flow-control packets. The format is an unsigned integer.

1024 to Max Byte Packets Received The number of packets received by the OSA during the most recent time interval that are 1024 bytes or longer in length. This count does not include flow-control packets. The format is an unsigned integer.

1024 to Max Byte Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval that are 1024 bytes or longer in length. This count does not include flow-control packets. The format is an unsigned integer.

Broadcast Packets Received The number of good (without error) broadcast packets received by the OSA during the most recent time interval. The format is an unsigned integer.

Broadcast Packets Transmitted The number of broadcast packets transmitted by the OSA during the most recent time interval. The format is an unsigned integer.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a 2-byte hexadecimal string.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Multicast Packets Received The number of good (without error) multicast packets received by the OSA during the most recent time interval. The format is an unsigned integer.

Multicast Packets Transmitted The number of multicast packets transmitted by the OSA during the most recent time interval. The format is an unsigned integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Port Name The name of the port as specified by the VTAM Transport Resource List Entry (TRLE). The format is a 32-character alphanumeric string.

Port Number The physical port number for this port. The format is an integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total 64 Byte Packets Received The number of packets received by the OSA that are exactly 64 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is an unsigned integer.

Note: 64 bytes is the minimum length for an Ethernet packet. Packets shorter than 64 bytes have to be padded. This value is of interest because it indicates whether the LAN is configured incorrectly and not performing up to capacity.

Total 64 Byte Packets Transmitted The number of packets transmitted by the OSA that are exactly 64 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is an unsigned integer.

Note: 64 bytes is the minimum length for an Ethernet packet. Packets shorter than 64 bytes have to be padded. This value is of interest because it indicates whether the LAN is configured incorrectly and not performing up to capacity.

Total 65 to 127 Byte Packets Received The number of packets received by the OSA that are 65 to 127 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is an unsigned integer.

Total 65 to 127 Byte Packets Transmitted The number of packets transmitted by the OSA that are 65 to 127 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is an unsigned integer.

Total 128 to 255 Byte Packets Received The number of packets received by the OSA that are 128 to 255 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is an unsigned integer.

Total 128 to 255 Byte Packets Transmitted The number of packets transmitted by the OSA that are 128 to 255 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is an unsigned integer.

Total 256 to 511 Byte Packets Received The number of packets received by the OSA that are 256 to 511 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is an unsigned integer.

Total 256 to 511 Byte Packets Transmitted The number of packets transmitted by the OSA that are 256 to 511 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is an unsigned integer.

Total 512 to 1023 Byte Packets Received The number of packets received by the OSA that are 512 to 1023 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is an unsigned integer.

Total 512 to 1023 Byte Packets Transmitted The number of packets transmitted by the OSA that are 512 to 1023 bytes in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is an unsigned integer.

Total 1024 to Max Byte Packets Received The number of packets received by the OSA that are 1024 bytes or longer in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is an unsigned integer.

Total 1024 to Max Byte Packets Transmitted The number of packets transmitted by the OSA that are 1024 bytes or longer in length since the last time the OSA port was reset. This count does not include flow-control packets. The format is an unsigned integer.

Total Broadcast Packets Received The number of good (without error) broadcast packets received by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

Total Broadcast Packets Transmitted The number of broadcast packets transmitted by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

Total Multicast Packets Received The number of good (without error) multicast packets received by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

Total Multicast Packets Transmitted The count of the number of multicast packets transmitted by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

OSA 10 Gigabit Ports Control Attributes

Use the OSA 10 Gigabit Ports Control attributes to monitor the data associated with a port on an OSA-Express2 10 Gigabit Ethernet feature.

Transmitter on (XON) and transmitter off (XOFF) packets are flow-control packets between the OSA and the switch to which it is connected. They are used to provide flow control between the two ports, and are of particular interest if the port is at 100% utilization.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of two hexadecimal characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Pause MAC Packets Received The number of valid Pause MAC control packets received by the OSA during the most recent time interval. The format is an unsigned integer.

Pause MAC Packets Transmitted The number of valid Pause MAC control packets transmitted by the OSA during the most recent time interval. The format is an unsigned integer.

Port Name The name of the port as specified by the VTAM Transport Resource List Entry (TRLE). The format is a 16-character alphanumeric string.

Port Number The physical port number for this port. Currently, this value can be only zero (0). The format is an integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Pause MAC Packets Received The number of valid Pause MAC control packets received by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

Total Pause MAC Packets Transmitted The number of valid Pause MAC control packets transmitted by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

Total XOFF Packets Received The number of XOFF (Transmitter OFF) packets received by the OSA since the last time the OSA port was reset. XOFF packets can use the global address or the station address. Receiving XOFF packets indicates that the sender experienced a problem with a queue filling up or some other software-initiated action. The format is an unsigned integer.

Total XOFF Packets Transmitted The number of XOFF (Transmitter OFF) packets transmitted by the OSA since the last time the OSA port was reset. Sending XOFF packets indicates that the queue is filling up or some software-initiated action has occurred. The format is an unsigned integer.

Total XON Packets Received The number of XON (Transmitter ON) packets received by the OSA since the last time the OSA port was reset. XON packets can use the global address or the station address. Receiving XON packets indicates that the sender experienced a problem with a queue filling up or some other software-initiated action. The format is an unsigned integer.

Total XON Packets Transmitted The number of XON (Transmitter ON) packets transmitted by the OSA since the last time the OSA port was reset. Sending XON packets indicates that the queue is filling up or some software-initiated action has occurred. The format is an unsigned integer.

Trap Control Flags The value of this object determines which traps will be generated by the OSA. The value of this object is initially all zeros, indicating that all traps will be sent to the OSA subagent. Setting the appropriate bit prevents a particular trap from being sent to the subagent. When the bit value of the disableEthLANChange bit is set to zero (0), then the trap ibmOSAExp10GigEthLANStateChange is sent. The format is a 4-digit hexadecimal number. Valid values are:

- x'0000' meaning the trap is enabled.
- x'8000' meaning the trap is disabled.

XOFF Packets Received The number of XOFF (Transmitter OFF) packets received by the OSA during the most recent time interval. XOFF packets can use the global address or the station address. Sending XOFF packets indicates that the sender experienced a problem with a queue filling up or some other software-initiated action. The format is an unsigned integer.

XOFF Packets Transmitted The number of XOFF (Transmitter OFF) packets transmitted by the OSA during the most recent time interval. Sending XOFF packets indicates that the queue is filling up or some software-initiated action has occurred. The format is an unsigned integer.

XON Packets Received The number of XON (Transmitter ON) packets received by the OSA during the most recent time interval. XON packets can use the global address or the station address. Receiving XON packets indicates that the sender experienced a problem with a queue filling up or some other software-initiated action. The format is an unsigned integer.

XON Packets Transmitted The number of XON (Transmitter ON) packets transmitted by the OSA during the most recent time interval. Sending XON packets indicates that the queue is filling up or some software-initiated action has occurred. The format is an unsigned integer.

OSA 10 Gigabit Ports Errors Attributes

Use the OSA 10 Gigabit Ports Errors attributes to monitor the data associated with a port on an OSA-Express2 10 Gigabit Ethernet feature.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of two hexadecimal characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month

- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

CRC Errors The number of cyclic redundancy check (CRC) errors on packets received on the LAN during the most recent time interval. The format is an unsigned integer.

Deferred Events The number of events deferred during the most recent time interval. A deferred event occurs when the transmitter cannot immediately send a packet because the medium is busy, XOFF (Transmitter OFF) frames are being sent, or the link is not up. The format is an unsigned integer.

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Interface Index The interface index associated with this port. The format is a four-byte integer.

Jabber Frames Received The number of frames received by the OSA during the most recent time interval that passed address filtering, were longer than maximum size, and had a bad cyclic redundancy check (CRC). The format is an unsigned integer.

The maximum transmission unit (MTU) is the maximum packet size, in bytes, that can be sent on an interface. In queued direct I/O (QDIO) mode, the MTU size used by the OSA feature is 8992 bytes. In non-QDIO mode, the MTU size used by the OSA is 1492 bytes. You can set the MTU size (as long as you stay within the limits and maximum values of the OSA) using TCP/IP profile statements. You can also set the parameters of the neighboring network interface card (NIC) and port (usually a port on a switch, but could be another OSA). For information about setting maximum size for OSA devices, see the *IBM z/OS Communications Server: IP Configuration Reference.*

Length Error Packets Received The number of length-error packets received by the OSA during the most recent time interval. A length error occurs if an incoming packet passes the filter criteria but the Length field does not match the number of bytes counted in the Data field. In the case of MAC control frames (including Pause), this attribute determines if the Data field is correctly padded to 46 bytes. The format is an unsigned integer.

Local Faults The number of times that local faults were detected during the most recent time interval. Local faults are errors on the local side of the link (that is, at the OSA card). The format is an unsigned integer.

Missed Packets The number of packets missed by the OSA during the most recent time interval. Packets are missed when the receiving FIFO (first in, first out) buffer has insufficient space to store the incoming packet. This could be due to too few buffers being allocated, or because there is insufficient bandwidth on the I/O bus. The format is an unsigned integer.

Not Stored Frames Received The number of times that frames were received by the OSA during the most recent time interval when no descriptor buffers were available to store frames. The format is an unsigned integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Oversized Frames Received The number of frames received by the OSA during the most recent time interval that passed address filtering and were longer than the maximum size, regardless of whether the cyclic redundancy check (CRC) was valid. The format is an unsigned integer.

The maximum transmission unit (MTU) is the maximum packet size, in bytes, that can be sent on an interface. In queued direct I/O (QDIO) mode, the MTU size used by the OSA feature is 8992 bytes. In non-QDIO mode, the MTU size used by the OSA is 1492 bytes. You can set the MTU size (as long as you stay within the limits and maximum values of the OSA) using TCP/IP profile statements. You can also set the parameters of the neighboring network interface card (NIC) and port (usually a port on a switch, but could be another OSA). For information about setting maximum size for OSA devices, see the *IBM z/OS Communications Server: IP Configuration Reference.*

Port Name The name of the port as specified by the VTAM Transport Resource List Entry (TRLE). The format is a 16-character alphanumeric string.

Port Number The physical port number for this port. Currently, this value can be only zero (0). The format is an integer.

Remote Faults The number of times that remote faults were detected during the most recent time interval. Remote faults are errors on the remote side of the link (for example, a client or switch endpoint). The format is an unsigned integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total CRC Errors The number of cyclic redundancy check (CRC) errors on packets received on the LAN by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

Total Deferred Events The number of events deferred by the OSA since the last time the OSA port was reset. A deferred event occurs when the transmitter cannot immediately send a packet because the medium is busy, XOFF (Transmitter OFF) frames are being sent, or the link is not up. The format is an unsigned integer.

Total Jabber Frames Received The number of frames received by the OSA since the last time the OSA port was reset that passed address filtering, were longer than maximum size, and had a bad cyclic redundancy check (CRC). The format is an unsigned integer.

The maximum transmission unit (MTU) is the maximum packet size, in bytes, that can be sent on an interface. In queued direct I/O (QDIO) mode, the MTU size used by the OSA feature is 8992 bytes. In non-QDIO mode, the MTU size used by the OSA is 1492 bytes. You can set the MTU size (as long as you stay within the limits and maximum values of the OSA) using TCP/IP profile statements. You can also set the parameters of the neighboring network interface card (NIC) and port (usually a port on a switch, but could be another OSA). For information about setting maximum size for OSA devices, see the *IBM z/OS Communications Server: IP Configuration Reference.*

Total Length Error Packets Received The number of length-error packets received by the OSA since the last time the OSA port was reset. A length error occurs if an incoming packet passes the filter criteria but the Length field does not match the number of bytes counted in the Data field. In the case of MAC control frames (including Pause), this attribute determines if the Data field is correctly padded to 46 bytes. The format is an unsigned integer.

Total Local Faults The number of times that local faults were detected by the OSA since the last time the OSA port was reset. Local faults are errors on the local side of the link (that is, at the OSA card). The format is an unsigned integer.

Total Missed Packets The number of packets missed by the OSA since the last time the OSA port was reset. Packets are missed when the receiving FIFO (first in, first out) buffer has insufficient space to store the incoming packet. This could be due to too few buffers being allocated, or because there is insufficient bandwidth on the I/O bus. The format is an unsigned integer.

Total Not Stored Frames Received The number of times that frames were received by the OSA since the last time the OSA port was reset when no descriptor buffers were available to store frames. The format is an unsigned integer.

Total Oversized Frames Received The number of frames received by the OSA since the last time the OSA port was reset that passed address filtering and were longer than the maximum size, regardless of whether the cyclic redundancy check (CRC) was valid. The format is an unsigned integer.

The maximum transmission unit (MTU) is the maximum packet size, in bytes, that can be sent on an interface. In queued direct I/O (QDIO) mode, the MTU size used by the OSA feature is 8992 bytes. In non-QDIO mode, the MTU size used by the OSA is 1492 bytes. You can set the MTU size (as long as you stay within the limits and maximum values of the OSA) using TCP/IP profile statements. You can also set the parameters of the neighboring network interface card (NIC) and port (usually a port on a switch, but could be another OSA). For information about setting maximum size for OSA devices, see the *IBM z/OS Communications Server: IP Configuration Reference.*

Total Remote Faults The number of times that remote faults were detected by the OSA since the last time the OSA port was reset. Remote faults are errors on the remote side of the link (for example, client or switch endpoint). The format is an unsigned integer.

Total Undersized Frames Received The number of frames received by the OSA since the last time the OSA port was reset that passed address filtering, and were smaller than the minimum size of 64 bytes (regardless of whether the cyclic redundancy check (CRC) was valid). Packets shorter than 64 bytes have to be padded and may indicate that the LAN is incorrectly configured and not performing up to capacity. The format is an unsigned integer.

Undersized Frames Received The number of frames received by the OSA during the most recent time interval that passed address filtering and were smaller than the minimum size of 64 bytes (regardless of whether the cyclic redundancy check (CRC) was valid). Packets shorter than 64 have to be padded and may indicate that the LAN is incorrectly configured and not performing up to capacity. The format is an unsigned integer.

OSA 10 Gigabit Ports Summary Attributes

Use the OSA 10 Gigabit Ports Summary attributes to monitor the data associated with a port on an OSA-Express2 10 Gigabit Ethernet feature.

Active MAC Address A 6-byte octet string that contains the current MAC address in use on the OSA. The values are in canonical format. The format is a 12-digit hexadecimal string.

Active Speed Mode The actual speed and mode in which the OSA running. This value is stored as an integer but displayed as a string. The possible values are:

- 1 = unknown
- 8 = tenGigabitFullDuplex

Burned In MAC Address A 6-byte octet string that contains the burned-in MAC address on the OSA. The values are in canonical format. The format is a 12-digit hexadecimal string.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of two hexadecimal characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour

- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Disabled Status A more detailed explanation of the LAN Traffic State attribute value of 5. When the value of ibmOsaExp10GigEthLanTrafficState is not disabled (a value other than 5 in the LAN Traffic State field), the value of this object will be stored as zero and displayed as zeros. When the value of the LAN Traffic State field is 5 (disabled), this object explains the reason for the disabled state. This value is stored as an integer and displayed as a 2-byte hexadecimal number mapped by the bit settings below:

- 0 = reserved0
- 1 = internalPortFailure
- 2 = reserved2
- 3 = reserved3
- 4 = reserved4
- 5 = reserved5
- 6 = portTemporarilyDisabled
- 7 = reserved7
- 8 = reserved8
- 9 = serviceProcessorRequest
- 10 = networkRequest
- 11 = osasfRequest
- 12 = configurationChange
- 13 = linkFailureThresholdExceeded
- 14 = reserved14
- 15 = reserved15

For more information about these values, see the *IBM zSeries Open Systems Adapter-Express Customer's Guide and Reference*.

Good Packets Received The number of good (without error) packets received by the OSA with a length of >= 64 bytes and <= 1518 bytes during the most recent time interval. The format is an unsigned integer.

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Interface Index The interface index associated with this port. The format is an unsigned integer.

LAN Traffic State The LAN state, expressed as a value between 0 and 8 inclusive. A value of 5, disabled, is further explained in the **Disabled Status** field. This value is stored as an integer but displayed as a string. The possible values are:

- 0 = undefined
- 1 = unavailable

- 2 = enabling
- 3 = disabling
- 4 = enabled
- 5 = disabled
- 6 = linkMonitor
- 7 = definitionError
- 8 = configuredOffline

For more information about these values, see the *IBM zSeries Open Systems Adapter-Express Customer's Guide and Reference*.

Octet Rate The average number of octets received or transmitted by the OSA, per minute, during the most recent time interval. The format is an unsigned integer.

Octets Received The number of good (without error) octets received by the OSA during the most recent time interval. The format is an unsigned integer.

Octets Received or Transmitted The number of octets received or transmitted by the OSA during the most recent time interval. The format is an unsigned integer.

Octets Transmitted The total number of octets transmitted by the OSA during the most recent time interval. The format is an unsigned integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Packet Rate The average number of packets received or transmitted by the OSA, per minute, during the most recent time interval. The format is an unsigned integer.

Packets Received The number of packets received by the OSA during the most recent time interval. The format is an unsigned integer.

Packets Received or Transmitted The number of packets received or transmitted by the OSA during the most recent time interval. The format is an unsigned integer.

Packets Transmitted The number of packets transmitted by the OSA during the most recent time interval. The format is an unsigned integer.

Port Interface Index The OSA-Express QDIO port interface index. For interfaces defined by DEVICE and LINK, this is the DEVICE interface index. For interfaces defined by INTERFACE, this is the dynamically generated interface index for the port. This field only applies to the following interface types:

- OSA-Express_QDIO_Ethernet_OSD (external data network type, which is the default value)
- OSA-Express_QDIO_Ethernet_OSM (intra-node management network, which requires IPv6)
- OSA-Express_QDIO_Ethernet_OSX (intra-ensemble data network)

The format is an unsigned integer. For more information about these interface types, see *IBM z/OS Communications Server: IP Configuration Guide*.

Note: This attribute is available only when the monitoring agent is running on z/OS v1.12 or later.

Port Name The name of the port as specified by the VTAM Transport Resource List Entry (TRLE). The format is a 16-character alphanumeric string.

Port Number The physical port number for this port. Currently, this value can be only zero (0). The format is an integer.

Port Type The physical port type. The format is an integer. Currently, this value can be only type 145 (displayed as tenGigabitEthernet), indicating that this is a 10 Gigabit adapter.

Service Mode An indicator of whether the processor is in service mode. This value is stored as an integer but displayed as a string. The possible values are:

- 0 = NotInServiceMode

- 1 = InServiceMode

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Good Packets Received The number of good (without error) packets received by the OSA with a length of >= 64 bytes and <= 1518 bytes since the last time the OSA port was reset. When the value in the **Total Good Packets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Good Packets Received (in G)** field, and the remainder is stored in the **Total Good Packets Received** field. The format is an unsigned integer.

Total Good Packets Received (in G) The number of good (without error) packets received by the OSA with a length of >= 64 bytes and <= 1518 bytes since the last time the OSA port was reset, expressed in G. When the value in the **Total Good Packets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Good Packets Received (in G)** field, and the remainder is stored in the **Total Good Packets Received** field. The format is an unsigned integer.

Total Octets The number of octets received or transmitted by the OSA since the last time the OSA port was reset. When the value in the **Total Octets** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Octets (in G)** field, and the remainder is stored in the **Total Octets** field. The format is an unsigned integer.

Total Octets (in G) The number of octets received or transmitted by the OSA since the last time the OSA port was reset, expressed in G. When the value in the **Total Octets** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Octets (in G)** field, and the remainder is stored in the **Total Octets** field. The format is an unsigned integer.

Total Octets Received The number of good (without error) octets received by the OSA since the last time the OSA port was reset. When the value in the **Total Octets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Octets Received (in G)** field, and the remainder is stored in the **Total Octets Received** field. The format is an unsigned integer.

Total Octets Received (in G) The number of good (without error) octets received by the OSA since the last time the OSA port was reset, expressed in G. When the value in the **Total Octets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Octets Received (in G)** field, and the remainder is stored in the **Total Octets Received** field. The format is an unsigned integer.

Total Octets Transmitted The number of octets transmitted by the OSA since the last time the OSA port was reset. When the value in the **Total Octets Transmitted** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Octets Transmitted (in G)** field, and the remainder is stored in the **Total Octets Transmitted** field. The format is an unsigned integer.

Total Octets Transmitted (in G) The number of octets transmitted by the OSA since the last time the OSA port was reset, expressed in G. When the value in the **Total Octets Transmitted** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Octets Transmitted (in G)** field, and the remainder is stored in the **Total Octets Transmitted** field. The format is an unsigned integer.

Total Packets The number of packets received or transmitted by the OSA since the last time the OSA port was reset. When the value in the **Total Packets** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Packets (in G)** field, and the remainder is stored in the **Total Packets** field. The format is an unsigned integer.

Total Packets (in G) The number of packets received or transmitted by the OSA since the last time the OSA port was reset, expressed in G. When the value in the **Total Packets** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Packets (in G)** field, and the remainder is stored in the **Total Packets** field. The format is an unsigned integer.

Total Packets Received The number of packets received by the OSA since the last time the OSA port was reset. When the value in the **Total Packets Received** field exceeds 1,073,741,823 (1 G), the number is

divided by 1,073,741,824. The quotient is stored in the **Total Packets Received (in G)** field and the remainder is stored in the **Total Packets Received** field. The format is an unsigned integer.

Total Packets Received (in G) The number of packets that received by the OSA since the last time the OSA port was reset, expressed in G. When the value in the **Total Packets Received** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Packets Received (in G)** field, and the remainder is stored in the **Total Packets Received** field. The format is an unsigned integer.

Total Packets Transmitted This is the number of packets transmitted by the OSA since the last time the OSA port was reset. When the value in the **Total Packets Transmitted** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Packets Transmitted (in G)** field, and the remainder is stored in the **Total Packets Transmitted** field. The format is an unsigned integer.

Total Packets Transmitted (in G) This is the number of packets transmitted by the OSA since the last time the OSA port was reset, expressed in G. When the value in the **Total Packets Transmitted** field exceeds 1,073,741,823 (1 G), the number is divided by 1,073,741,824. The quotient is stored in the **Total Packets Transmitted (in G)** field, and the remainder is stored in the **Total Packets Transmitted** field. The format is an unsigned integer.

zOS Release IBM internal use only.

OSA 10 Gigabit Ports Throughput Attributes

Use the OSA 10 Gigabit Ports Throughput attributes to monitor a port on an OSA-Express2 10 Gigabit Ethernet feature.

Broadcast Packets Received The number of good (without error) broadcast packets received by the OSA during the most recent time interval. The format is an unsigned integer.

Broadcast Packets Transmitted The number of broadcast packets transmitted by the OSA during the most recent time interval. The format is an unsigned integer.

Channel Number The channel path identifier (CHPID) corresponding to this device. The format is a string of two hexadecimal characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second

- m = Millisecond

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Jumbo Packets Received The number of good (without error) packets of jumbo size (defined as > 1518 bytes and <= maxFrameSize) received by the OSA during the most recent time interval. The format is an unsigned integer.

The maximum transmission unit (MTU) is the maximum packet size, in bytes, that can be sent on an interface. In queued direct I/O (QDIO) mode, the MTU size used by the OSA feature is 8992 bytes. In non-QDIO mode, the MTU size used by the OSA is 1492 bytes. You can set the MTU size (as long as you stay within the limits and maximum values of the OSA) using TCP/IP profile statements. You can also set the parameters of the neighboring network interface card (NIC) and port (usually a port on a switch, but could be another OSA). For information about setting maximum size for OSA devices, see the *IBM z/OS Communications Server: IP Configuration Reference.*

Jumbo Packets Transmitted The number packets of jumbo size (defined as > 1518 bytes and <= maxFrameSize) transmitted by the OSA during the current collection period. The format is an unsigned integer.

The maximum transmission unit (MTU) is the maximum packet size, in bytes, that can be sent on an interface. In queued direct I/O (QDIO) mode, the MTU size used by the OSA feature is 8992 bytes. In non-QDIO mode, the MTU size used by the OSA is 1492 bytes. You can set the MTU size (as long as you stay within the limits and maximum values of the OSA) using TCP/IP profile statements. You can also set the parameters of the neighboring network interface card (NIC) and port (usually a port on a switch, but could be another OSA). For information about setting maximum size for OSA devices, see the *IBM z/OS Communications Server: IP Configuration Reference.*

Multicast Packets Received The number of good (without error) multicast packets received by the OSA during the most recent time interval. The format is an unsigned integer.

Multicast Packets Transmitted The number of multicast packets transmitted by the OSA during the most recent time interval. The format is an unsigned integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Port Name The name of the port as specified by the VTAM Transport Resource List Entry (TRLE). The format is a 16-character alphanumeric string.

Port Number The physical port number for this port. Currently, this value can be only zero (0). The format is an integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Broadcast Packets Received The number of good (without error) broadcast packets received by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

Total Broadcast Packets Transmitted The number of broadcast packets transmitted by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

Total Jumbo Packets Received The number of good (without error) packets of jumbo size (defined as >1518 bytes and <= maxFrameSize) received by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

The maximum transmission unit (MTU) is the maximum packet size, in bytes, that can be sent on an interface. In queued direct I/O (QDIO) mode, the MTU size used by the OSA feature is 8992 bytes. In non-QDIO mode, the MTU size used by the OSA is 1492 bytes. You can set the MTU size (as long as you stay within the limits and maximum values of the OSA) using TCP/IP profile statements. You can also set the parameters of the neighboring network interface card (NIC) and port (usually a port on a switch, but could be another OSA). For information about setting maximum size for OSA devices, see the *IBM z/OS Communications Server: IP Configuration Reference.*.

Total Jumbo Packets Transmitted The number packets of jumbo size (defined as > 1518 bytes and <= maxFrameSize) transmitted by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

The maximum transmission unit (MTU) is the maximum packet size, in bytes, that can be sent on an interface. In queued direct I/O (QDIO) mode, the MTU size used by the OSA feature is 8992 bytes. In non-QDIO mode, the MTU size used by the OSA is 1492 bytes. You can set the MTU size (as long as you stay within the limits and maximum values of the OSA) using TCP/IP profile statements. You can also set the parameters of the neighboring network interface card (NIC) and port (usually a port on a switch, but could be another OSA). For information about setting maximum size for OSA devices, see the *IBM z/OS Communications Server: IP Configuration Reference.*

Total Multicast Packets Received The number of good (without error) multicast packets received by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

Total Multicast Packets Transmitted The number of multicast packets transmitted by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

Total Unicast Packets Received The number of good (without error) Unicast packets received by the OSA since the last time the OSA port was reset. The number does not include Pause packets with matching Unicast destination addresses. The format is an unsigned integer.

Total Unicast Packets Transmitted The number of Unicast packets transmitted by the OSA since the last time the OSA port was reset. The format is an unsigned integer.

Total VLAN Packets Received The number of good (without error) packets received by the OSA over a virtual LAN (VLAN) since the last time the OSA port was reset. The format is an unsigned integer.

Total VLAN Packets Transmitted The number of virtual LAN (VLAN) packets transmitted by the OSA since the last time the OSA port was reset. This number does not include flow-control or MAC-control packets. The format is an unsigned integer.

Unicast Packets Received The number of good (without error) Unicast packets received by the OSA during the most recent time interval. This number does not include Pause packets with matching Unicast destination addresses. The format is an unsigned integer.

Unicast Packets Transmitted The number of Unicast packets transmitted by the OSA during the most recent time interval. The format is an unsigned integer.

VLAN Packets Received The number of good (without error) packets received by the OSA over a virtual LAN during the most recent time interval. The format is an unsigned integer.

VLAN Packets Transmitted The number of virtual LAN (VLAN) packets transmitted by the OSA during the most recent time interval. This number does not include flow-control or MAC-control packets. The format is an unsigned integer.

TCP Listener Attributes

Use the TCP Listener attributes to display performance and identifying information for a specific listener connection.

Accepted Connections The number of connections accepted by this listener during the most recent time interval. The format is an integer.

Active Connections The number of current connections. The format is an integer.

Active Connection High Water Mark The high-water mark, which is the highest value recorded in the active connections field, for this listener. The format is an integer.

APPLDATA The result of an SIOCSAPPLDATA ioctl query. Use the APPLDATA attribute to enable applications to associate 40 bytes of application-specific information with TCP sockets that they own. This information can assist problem determination, capacity planning, and accounting applications. The format is a string of up to 40 bytes.

For additional information, see the application data appendix in the *IBM z/OS Communications Sever: IP Configuration Reference.*

Application Name The job name associated with the application address space that opened and bound the socket. The format is a string up to 8 characters in length.

ASID The z/OS address space ID of the address space that opened the socket. This value is displayed as a 4-digit hexadecimal value.

Backlog Connections Rejected The number of connections rejected during the most recent time interval because the backlog limit was exceeded before the listener was able to accept the waiting connections. z/OS Communications Server rejects a new connection when the number of connections waiting to be accepted exceeds the backlog limit for a listener. The format is an integer.

Backlog Connections Rejected Time Stamp The date and time that a connection was most recently rejected because the backlog limit was exceeded. The format of date and time is determined by the date and time formats specified in User Preferences. The time stamp reflects the time zone specified in User Preferences. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

This value is stored as a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

When no connections have been rejected, this value is stored as a character string of zeros and displayed as blank.

Backlog Limit The maximum number of connections allowed in backlog at one time. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Connection Rate The average number of accepted connections, per minute, during the most recent time interval. The format is an integer.

Connections in Backlog The current number of connections in backlog. The format is an integer.

DVIPA Whether the listener socket supports Dynamic Virtual IP Addressing (DVIPA). This value is stored as an integer and displayed as a string. The following values are valid:

- 0 = [blank] Not available
- 1 = Yes
- 2 = No

DVIPA Quiesced Whether or not Dynamic Virtual IP Addressing (DVIPA) associated with the listener socket has quiesced. This value is stored as an integer and displayed as a string. The following are valid:

- 0 = [blank] Not available
- 1 = Yes
- 2 = No

Established Connections in Backlog The number of Connections in Backlog that are established. The format is an unsigned integer.

FRCA Connections in Backlog The number of Connections in Backlog that are established Fast Response Cache Accelerator (FRCA) connections not presented to be accepted by the application. The format is an unsigned integer.

Hex Connection Number The hexadecimal representation of the connection number. The format is an 8-digit hexadecimal string.

Idle Time Since Last Accept The amount of time, in hours, that the server has been idle since the most recent connection was accepted. This value is stored in hundreds of an hour (for example, one hour is stored as 100) and displayed as a real number.

Listener Type Indicates whether this listener is for a TN3270 server. A value of 1 indicates that the listener is for a TN3270 Server. The format is an unsigned integer. The following are valid values:

- 0 = Unknown
- 1 = TN3270_Server

Local IP Address The local IP address for this connection. This IP address is 0 (zero) when the application accepts connections to any local IP address. The format is a string up to 45 characters in length.

Local Port The local port for this connection. The format is a four-byte integer.

Local Port (deprecated) The local port for this connection, as a two-byte integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is a string up to 32 characters in length.

Percent Active Connections The number of active connections in this collection interval as a percentage of the active connections high-water mark. The format is an integer.

Server Up Time The amount of time, in hours, that the listener has been active. The format is a real number.

Sysplex Name The name of the sysplex that the monitored system is part of. The format is a string of up to 8 characters.

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Time Stamp for Active Connections High Water Mark The date and time when the highest value was recorded for the active connections. This time is displayed on the interface in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Total Backlog Connections Rejected The total number of connections rejected because the backlog limit was exceeded before the listener was able to accept the waiting connections. z/OS Communications Server rejects a new connection when the number of connections waiting to be accepted exceeds the backlog limit for a listener. The format is an unsigned integer.

TCPIP Address Space Attributes

Use these attributes to view information about TCP/IP stack conditions, find and correct problems in your network, or create situations that monitor information for a selected TCP/IP stack.

Note: If the address space being monitored is running on z/OS v1.11 or earlier, the values for these attributes are retrieved by using SNMP. If the address space being monitored is running on z/OS v1.12 or later, the values for these attributes are retrieved by using the z/OS Communications Server callable network management interface (NMI)

Application Count The number of active TCP/IP applications when the most recent time interval ended. The format is an integer.

Byte Rate The number of bytes received or sent, per minute, during the most recent time interval. When the measured value exceeds 2,147,483,647 (the maximum value), the attribute will be set to 2,147,483,647. The format is an integer.

Collection Interval The time, in minutes, between successive samples; the sampling interval. The format is an integer between 1 and 60.

The Collection Interval was set in the Configuration Tool SPECIFY COMPONENT CONFIGURATION panel by specifying a value for the "TCP/IP sample interval" field or in PARMGEN using the KN3_TCP_SAMPLE_INTERVAL parameter. The Collection Interval controls collection of all TCP/IP data plus Communication Storage Manager (CSM), Enterprise Extender (EE), and High Performance Routing (HPR) data.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Connection Count The number of TCP/IP connections. This number represents the total number of rows in the TCP Connections table, the UDP Endpoints table, and the TCP Listener table. The format is an integer.

CPU Percentage The percentage of CPU in use when the sampling interval ended. The range for this value is from 0% to 100%.

CSA Percent Below 16MB The percentage of Common System Area (CSA) storage below the 16MB line in use when the last sampling interval ended. The range for this value is from 0% to 100%.

CSA Usage Below 16MB Currently Allocated The amount of Common System Area (CSA) storage below the 16MB line in use when the last sampling interval ended. The format is an integer.

Device Count The number of devices defined for the TCP/IP stack. The format is an integer.

Fragmentation Count The number of IP segments requiring fragmentation that were successfully fragmented. The format is an integer.

Note: Segments require fragmentation when they are too large for the next network hop.

Fragmentation Failure Percentage The percentage of IP segments requiring fragmentation that were not successfully fragmented. The range for this value is from 0% to 100%.

Fragmentation Failures The number of IP segments requiring fragmentation that were not successfully fragmented. The format is an integer.

Fragmentation Percentage The percentage of IP segments successfully fragmented since TCP/IP initialization. The range for this value is from 0% to 100%.

Gateway Count The number of gateways defined for the TCP/IP stack. Gateways are routers to other physical networks. The format is an integer.

Host IP Address The IP address of the host. The format is a text string no longer than 45 characters.

Host IP Address (IPv4 only) The IP address of the host. The format is a 15 character string. This attribute value is set only if the character representation of the host's IP address fits within 15 characters. This attribute is not displayed by default.

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Input Discard Percentage The percentage of IP segments this TCP/IP address space received from the network that were undeliverable and therefore discarded. The range for this value is from 0% to 100%.

Input Discards The number of IP segments this TCP/IP address space received that were undeliverable and therefore discarded since TCP/IP initialization. The format is an integer.

Reasons for discarding input segments include the following:

- Hardware errors
- Addressing errors
- Unknown protocols

Input Packet Count (deprecated) The number of IP packets (including those received in error) that this TCP/IP address space received from the network since TCP/IP initialization. When the value in the Input Packet Count field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the Input Packet Count (In G) field and the remainder is stored in the Input Packet Count field. The format is an integer.

Input Packet Count (In G) (deprecated) The number of IP packets (including those received in error) that this TCP/IP address space received from the network since TCP/IP initialization, divided by 1,073,741,824. When the value in the Input Packet Count field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the Input Packet Count (in G) field and the remainder is stored in the Input Packet Count field. The format is an integer.

Input Packets Since TCP/IP initialization, the number of IP packets that this TCP/IP address space received from the network. The format is a long long integer.

Interface Count The number of interfaces defined for the TCP/IP stack. The format is an integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Output Discard Percentage The percentage of all IP output segments from this TCP/IP address space that were undeliverable and therefore discarded. The range for this value is from 0% to 100%.

Output Discards The number of IP segments this address space did not send and therefore discarded since TCP/IP initialization. The format is an integer.

Reasons for discarding output segments include the following:

- No available routes
- Segment needs fragmentation, but the Do Not Frag Bit was set

Output Packet Count (deprecated) The number of IP packets that local IP user-protocols supplied to IP since TCP/IP initialization. When the value in the **Output Packet Count** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Output Packet Count (In G)** field and the remainder is stored in the **Output Packet Count** field. The format is an integer.

Note: This count does not include any packets counted in Input Datagrams Forwarded.

Output Packet Count (in G) (deprecated) The number of IP packets that local IP user-protocols supplied to IP since TCP/IP initialization, divided by 1,073,741,824. When the value in the **Output Packet Count**

field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Output Packet Count (in G)** field and the remainder is stored in the **Output Packet Count** field. The format is an integer.

Note: This count does not include any packets counted in Input Datagrams Forwarded.

Output Packets Since TCP/IP initialization, the number of IP packets that this TCP/IP address space sent to the network. The format is a long long integer.

Paging Rate The paging rate when the last sampling interval ended. The range for this value is from 0% to 100%.

Reassembly Count The number of IP segments received that were successfully reassembled since TCP/IP initialization. The format is an integer.

Reassembly Failure Count The number of IP segments requiring reassembly that were not reassembled since TCP/IP initialization. A reassembly fails when all segments that compose the fragmented datagram are not received. The format is an integer.

Reassembly Failure Percentage The percentage of IP segments requiring reassembly that were not reassembled. A reassembly fails when all segments that compose the fragmented datagram are not received. The range for this value is from 0% to 100%.

The percentage is calculated as follows:

(Reassembly Failure Pct) = (Reassembly Failures) divided by (Reassemblies Requested)

Reassembly Percentage The percentage of IP segments that were reassembled since TCP/IP initialization. The range for this value is from 0% to 100%.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCP Input Segment Count (deprecated) The count of TCP segments this TCP/IP address space received from the network since TCP/IP initialization. When the value in the **TCP Input Segment Count** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **TCP Input Segment Count (in G)** field and the remainder is stored in the **TCP Input Segment Count** field. The format is an integer.

TCP Input Segment Count (in G) (deprecated) The count of TCP segments this TCP/IP address space received from the network since TCP/IP initialization, divided by 1,073,741,824. When the value in the **TCP Input Segment Count** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **TCP Input Segment Count (in G)** field and the remainder is stored in the **TCP Input Segment Count** field. The format is an integer.

TCP Input Segments The count of TCP segments that this TCP/IP address space received from the network since TCP/IP initialization. The format is a long long integer.

TCP Output Segment Count (deprecated) The count of TCP segments this TCP/IP address space delivered to the network since TCP/IP initialization. When the value in the **TCP Output Segment Count** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **TCP Output Segment Count (in G)** field and the remainder is stored in the **TCP Output Segment Count** field. The format is an integer.

TCP Output Segment Count (in G) (deprecated) The count of TCP segments this TCP/IP address space delivered to the network since TCP/IP initialization, divided by 1,073,741,824. When the value in the **TCP Output Segment Count** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **TCP Output Segment Count (in G)** field and the remainder is stored in the **TCP Output Segment Count** field. The format is an integer.

TCP Output Segments The count of TCP segments that this TCP/IP address space delivered to the network since TCP/IP initialization. The format is a long long integer.

TCP Retransmit Percentage The percentage of TCP segments that required retransmission. A TCP segment is retransmitted whenever the receiver does not acknowledge receipt, and a timeout occurs. The range for this value is from 0% to 100%.

The percentage is calculated as follows:

(TCP Retransmit Pct) = (Retransmitted TCP Segments) divided by (TCP Segments Out)

TCP Retransmitted Segments The number of TCP segments this host retransmitted since TCP/IP initialization. A segment is retransmitted whenever the receiver does not acknowledge receipt, and a timeout occurs. The format is an integer.

TCP Session Count The number of TCP sessions currently established to this TCP/IP address space. The format is an integer.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Telnet Connection Count The total number of Telnet connections. The format is an unsigned integer.

Telnet Pool Percentage The percentage of Telnet pool entries in use. The range for this value is from 0% to 100%.

Telnet Pool Size The number of entries in the Telnet pool. Each Telnet user is allocated one entry from the pool. When the pool is exhausted, no new Telnet sessions can be started. The format is an integer.

Telnet Session Count The number of Telnet connections that are currently in session with an application. The format is an integer.

Total CSA Percentage The percentage of Common System Area (CSA) used when the last sampling interval ended. The range for this value is from 0% to 100%.

Total CSA Usage The total amount of Common System Area (CSA) used when the last sampling interval ended. The format is an integer.

UDP Discard Percentage The percentage of user datagram protocol (UDP) datagrams discarded as undeliverable because they were received in error (including No Port Found errors). The range for this value is from 0% to 100%.

The percentage is calculated as

(UDP Discard Pct) = (UDP No Port Errors + UDP Other Errors) divided by (UDP Datagrams Received)

UDP Input Datagram Count (deprecated) The number of user datagram protocol (UDP) datagrams received since TCP/IP initialization. When the value in the **UDP Input Datagram Count** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **UDP Input Datagram Count (in G)** field and the remainder is stored in the **UDP Input Datagram Count** field. The format is an integer.

UDP Input Datagram Count (in G) (deprecated) The number of user datagram protocol (UDP) datagrams received since TCP/IP initialization, divided by 1,073,741,824. When the value in the **UDP Input Datagram Count** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **UDP Input Datagram Count (in G)** field and the remainder is stored in the **UDP Input Datagram Count** field. The format is an integer.

UDP Input Datagrams Since TCP/IP initialization, the number of UDP datagrams received. The format is a long long integer.

UDP Input Errors The number of datagrams discarded as undeliverable because they were received in error (excluding No Port Found errors) since TCP/IP initialization. The format is an integer.

UDP No Port Count The number of user datagram protocol (UDP) datagrams discarded as undeliverable because the port number specified did not match that of any active applications. The format is an integer.

UDP Output Datagram Count (deprecated) The number of datagrams this host sent since TCP/IP initialization. When the value in the **UDP Output Datagram Count** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **UDP Output Datagram Count (in G)** field and the remainder is stored in the **UDP Output Datagram Count** field. The format is an integer.

UDP Output Datagram Count (in G) (deprecated) The number of datagrams this host sent since TCP/IP initialization, divided by 1,073,741,824. When the value in the **UDP Output Datagram Count** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the

UDP Output Datagram Count (in G) field and the remainder is stored in the **UDP Output Datagram Count** field. The format is an integer.

UDP Output Datagrams The number of datagrams this host sent since TCP/IP initialization. The format is a long long integer.

zOS Release IBM internal use only.

TCPIP Applications Attributes

Use the TCPIP Applications attributes to measure performance statistics for the TCP/IP applications that were active when the last sampling interval ended.

Accepted Connections The total number of connections that were accepted by this application during the most recent interval. The format is an integer.

Active Connections The number of current connections. The format is an integer.

Active Connection High Water Mark The high-water mark (the highest value recorded for this listener in the active connections field) for active connections. The format is an integer.

Application Name The job name associated with the application address space that opened and bound the socket. The format is an alphanumeric string no longer than 8 characters.

Application Type Indicates whether this application is a TN3270 server. A value of 1 indicates that the application is acting as a TN3270 Server. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Unknown
- 1 = TN3270_Server

Backlog Connections Rejected The total number of connections that were rejected during the most recent time interval because the backlog limit was exceeded before the application was able to accept the waiting connections. z/OS Communications Server rejects a new connection when the number of connections waiting to be accepted exceeds the backlog limit for a listener. The format is an integer.

Backlog Connections Rejected Time Stamp The date and time that a connection was most recently rejected because the backlog limit was exceeded. The format of date and time is determined by the date and time formats specified in User Preferences. The time stamp reflects the time zone specified in User Preferences. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

This time is stored as a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute

- S = Second
- m = Millisecond

When no connections have been rejected, this value is stored as a character string of zeros and displayed as blank.

Byte Rate_32 (Deprecated) The number of bytes (both sent and received), per minute, during the most recent time interval. The format is an integer.

Byte Rate The number of bytes per minute transmitted to or sent from this application during the most recent time interval. The format is a long long integer.

Bytes Received_32 (Deprecated) The number of bytes received on all connections for this application that existed at the end of the most recent time interval. The format is an integer.

Bytes Received The number of bytes received on all connections for this application that existed at the end of the most recent time interval. The format is a long long integer.

Bytes Sent_32 (Deprecated) The number of bytes sent on all connections for this application that existed at the end of the most recent time interval. The format is an integer.

Bytes Sent The number of bytes sent on all connections for this application that existed at the end of the most recent time interval. The format is a long long integer.

Bytes Sent or Received_32 (Deprecated) The number of bytes sent or received on all connections for this application that existed at the end of the most recent time interval. The format is an integer.

Bytes Sent or Received The number of bytes sent or received on all connections for this application that existed at the end of the most recent time interval. The format is a long long integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Connection Count The number of connections established for this application at the end of the most recent interval. This number represents the total number of TCP Connections, UDP Connections, and TCP Listeners associated with this application. The format is an integer.

Connection Rate The number of connections that were accepted, per minute, during the most recent time interval. The format is an integer.

Connections in Backlog The current number of connections that are in backlog. Connections in backlog are waiting to be accepted. The format is an integer.

Datagram Rate The average number of datagrams (both sent and received), per minute, for this application during the most recent time interval. The average is derived by dividing all datagrams transmitted or received during the current interval by the size of the interval. The format is an integer.

Datagrams Discarded The number of received datagrams that were discarded because a receive queue limit was exceeded during the most recent interval. The format is an integer.

Datagrams Queued The number of datagrams that are in the read queue. The format is an integer.

Datagrams Received The number of datagrams received during the most recent time interval. The format is an integer.

Datagrams Sent The number of datagrams sent during the most recent time interval. The format is an integer.

Datagrams Sent or Received The total number of datagrams (both sent and received) during the most recent time interval. The format is an integer.

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string up to 255 characters in length.

Idle Time Since Last Accept The amount of time, in hours, that the server has been idle since the most recent connection was accepted. This value is stored in hundreds of an hour (for example, one hour is stored as 100) and displayed as a real number.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Out of Order Segments The number of TCP data segments received that did not contain the next expected sequence number during the most recent time interval. The format is an integer.

Percent Datagrams Discarded The percentage of received datagrams that was discarded because a receive queue limit was exceeded during the most recent time interval. The range for this value is from 0% to 100%.

Percent Out of Order Segments The percentage of segments received that did not contain the next expected sequence number during the most recent time interval. The range for this value is from 0% to 100%.

Percent Segments Retransmitted The percentage of TCP segments that was retransmitted during the most recent time interval. The range for this value is from 0% to 100%.

Queued Datagram Bytes The number of data bytes that are in the datagrams in the read queue. The format is an integer.

Receive Byte Rate_32 (deprecated) The number of bytes that was received, per minute, during the most recent time interval. The format is an integer.

Receive Byte Rate The number of bytes that was received, per minute, during the most recent time interval. The format is a long long integer.

Receive Datagram Rate The number of datagrams that was received, per minute, during the most recent time interval. The format is an integer.

Receive Segment Rate The number of segments that was received, per minute, during the most recent time interval. The format is an integer.

Retransmission Rate The number of segments that was retransmitted, per minute, during the most recent time interval. The format is an integer.

Segment Rate The number of segments (both sent and received), per minute, during the most recent time interval. The format is an integer.

Segments Received The number of segments received during the most recent time interval. This number includes the segments received on currently established connections and segments received in error. The format is an integer.

Segments Retransmitted The number of segments retransmitted during the most recent time interval. The format is an integer.

Segments Sent The number of segments sent during the most recent time interval. This number includes the segments on current connections, and excludes those segments that contain only retransmitted octets. The format is an integer.

Segments Sent or Received The total number of segments that was sent or received during the most recent time interval. This number includes the segments on current connections, and segments received in error. This number excludes those segments that contain only retransmitted octets. The format is an integer.

Server Up Time The amount of time, in hours, that the listener has been active. The format is a real number.

Sysplex Name The name of the sysplex that the monitored system is part of. The format is a string of up to 8 characters.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Time Since Last Activity The amount of time, in seconds, since the most recent activity on any connection for this application that existed at the end of the most recent time interval. This value is stored in hundreds of a second (for example, one second is stored as 100) and displayed as a time value (for example, 4.17000s or 4m 20s).

Time Stamp for Active Connections High Water Mark The date and time during which the value for the high-water mark (or highest value) was recorded. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

When the application has had no active connections, this value is stored as a string of zeros and displayed as blank.

Total Backlog Connections Rejected The total number of connections rejected because the backlog limit was exceeded before the listener was able to accept the waiting connections. z/OS Communications Server rejects a new connection when the number of connections waiting to be accepted exceeds the backlog limit for a listener. The format is an unsigned integer.

Total Bytes The total number of bytes sent or received on all connections for this application that existed at the end of the most recent time interval. The format is a long long integer.

Total Bytes_32 (deprecated) The total number of bytes both received and sent on all connections that were active at the end of the most recent time interval for this application. When the value in the **Total Bytes** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes (in GB)** field and the remainder is stored in the Total Bytes field. The format is an integer.

Total Bytes (in GB) (deprecated) The total number of bytes (both sent and received) on all connections that were active at the end of the most recent time interval for this application, divided by 1,073,741,824. When the value in the **Total Bytes** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes (in GB)** field and the remainder is stored in the Total Bytes field. The format is an integer.

Total Bytes Received The total number of bytes received on all connections for this application that existed at the end of the most recent time interval. The format is a long long integer.

Total Bytes Received_32 (deprecated) The total number of bytes received on all connections that was active at the end of the most recent time interval for this application. When the value in the **Total Bytes Received** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Received (in GB)** field and the remainder is stored in the **Total Bytes Received** field. The format is an integer.

Total Bytes Received (in GB) (deprecated) The total number of bytes received on all connections that were active at the end of the most recent time interval for this application, divided by 1,073,741,824. When the value in the **Total Bytes Received** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Received (in GB)** field and the remainder is stored in the **Total Bytes Received** field. The format is an integer.

Total Bytes Sent The total number of bytes sent on all connections for this application that existed at the end of the most recent time interval. The format is a long long integer.

Total Bytes Sent_32 (deprecated) The total number of bytes sent on all connections that was active at the end of the most recent time interval for this application. When the value in the Total Bytes Sent field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Sent (in GB)** field and the remainder is stored in the **Total Bytes Sent** field. The format is an integer.

Total Bytes Sent (in GB) (deprecated) The total number of bytes sent on all connections that was active at the end of the most recent time interval for this application, divided by 1,073,741,824. When the value in the **Total Bytes Sent** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Sent (in GB)** field and the remainder is stored in the **Total Bytes Sent** field. The format is an integer.

Total Datagrams The total number of datagrams received or sent on all connections for this application that existed at the end of the most recent time interval. The format is an integer.

Total Datagrams Received The total number of datagrams received on all connections for this application that existed at the end of the most recent time interval. The format is an integer.

Total Datagrams Sent The total number of datagrams sent on all connections for this application that existed at the end of the most recent time interval. The format is an integer.

Total Out of Order Segments The total number of TCP data segments received that did not contain the next expected sequence number on all connections for this application that existed at the end of the most recent time interval. The format is an integer.

Total Segments The total number of segments sent and received on all connections for this application that existed at the end of the most recent time interval. The format is an integer.

Total Segments Received The total number of segments received on all connections for this application that existed at the end of the most recent time interval. The format is an integer.

Total Segments Retransmitted The total number of segments retransmitted on all connections for this application that existed at the end of the most recent time interval. The format is an integer.

Total Segments Sent The total number of segments sent on all connections for this application that existed at the end of the most recent time interval. The format is an integer.

Transmit Byte Rate The number of bytes that was transmitted, per minute, during the most recent time interval. The format is a long long integer.

Transmit Byte Rate_32 (Deprecated) The number of bytes that was transmitted, per minute, during the most recent time interval. The format is an integer.

Transmit Datagram Rate The number of datagrams that was transmitted, per minute, during the most recent time interval. The format is an integer.

Transmit Segment Rate The number of segments that was transmitted, per minute, during the most recent interval. The format is an integer.

TCPIP Connections Attributes

Use the TCPIP Connections attributes to display performance and identifying information for each connection.

Application Name The job name associated with the application address space that opened and bound the socket. The format is an alphanumeric string no longer than 8 characters.

Application Name and Port The Application Name and Local Port are combined in this attribute, separated by a colon. The format is a string up to 15 characters in length.

Byte Rate The number of bytes sent or received, per minute, during the most recent time interval. Throughput rate is expressed in kilobytes per minute. The format is an integer.

Bytes Received The number of bytes received over a connection during the most recent sampling interval. The format is an integer.

Bytes Sent The number of bytes sent over a connection during the most recent time interval. The format is an integer.

Bytes Sent or Received The total number of bytes sent and received during the most recent time interval. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month

- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Connection Number A unique number that identifies a connection to a TCP/IP stack. The format is an integer. This value is stored as an integer and displayed as a hexadecimal number.

Connection State The state of the connection. The format is an alphanumeric string no longer than 12 characters. The TCP/IP connection states that OMEGAMON XE monitors can be very brief, with normal durations in milliseconds, where the following states are possible:

- **CLOSED** The end state of a TCP connection; this state means the TCP connection no longer exists.
- **CLOSE_WAIT** A state in which the connection is waiting for a connection termination request from the local port.
- **CLOSING** A state in which the connection is waiting for a connection termination request acknowledgment from the remote TCP.
- **ESTABLISHED** A state in which the connection is established.
- **FIN_WAIT_1** A state in which the connection is waiting for a connection termination request from the remote TCP or an acknowledgement of the connection termination request.
- **FIN_WAIT_2** A state in which the connection is waiting for a connection termination request from the remote TCP.
- **LAST_ACK** A state in which the connection is waiting for an acknowledgment of the connection termination request it sent to the remote TCP.
- **LISTEN** A state in which the connection is waiting for a connection request from any remote TCP and port.
- **SYN_RECEIVED** A state in which the connection is waiting for a confirming connection request acknowledgement after receiving and sending a connection request.
- **SYN_SENT** A state in which the connection is waiting for a matching connection request after a connection request was sent. If a connection is in this state for two successive sample intervals, an exception is generated.
- **TIME_WAIT** A state in which the host waits to ensure that a remote TCP has received a connection termination request. After the wait time is over, the socket pair that uniquely defines the connection is available for reuse.
- **UDP** A state in which a UDP endpoint exists between the stack and the remote IP address and port.

Connection Type Specifies the type of connection that is either a UDP endpoint, TCP connection or TCP listener. This is specified as one of the following:

- L = TCP_Listener
- T = TCP_Connection
- U = UDP_Endpoint

Datagram Rate The number of datagrams, per minute, transmitted to or from this connection during the most recent time interval. The format is an integer.

Datagrams Received The total number of datagrams the local port received during the most recent time interval. The format is an integer.

Datagrams Sent The total number of datagrams the local port transmitted during the most recent time interval. The format is an integer.

Datagrams Sent or Received The total number of datagrams (both sent and received) on the local port during the most recent time interval. The format is an integer.

DVIPA Identifies when the Local IP Address is a Dynamic Virtual IP Addressing (DVIPA) address. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = [blank] Not available
- 1 = Yes
- 2 = No

Foreign IP Address The IP address of the remote end of the connection, which might be in the same host or in another host. The format is an alphanumeric string no longer than 45 characters.

Foreign Port The port number to which the remote end of the connection is bound. The format is an unsigned integer.

Foreign Port String The port number to which the remote end of the connection is bound. The format is an alphanumeric string no longer than 6 characters.

Foreign Socket The remote end of the connection, which might be in the same host or in another host. The format is an alphanumeric string no longer than 23 characters.

Hex Connection Number A unique hexadecimal number that identifies a connection to a TCP/IP stack. This value is displayed as a 8-digit hexadecimal string.

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Local IP Address The local IP address for this connection. For UDP endpoints, a value of 0.0.0.0 (or ::) in this field indicates that the UDP endpoint is accepting datagrams from any local IP address. For TCP listeners, this IP address is 0.0.0.0 (or ::) when the application is accepting connections to any local IP address. The format is a string up to 45 characters in length.

Local Port The local port for this connection. The format is an alphanumeric string no longer than 6 characters. The Local Port attribute is displayed as an unsigned integer and not a string. This field no longer displays in the product-provided workspace.

Local Port The local port for this connection. The format is an unsigned integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Percent Segments Retransmitted The percentage of TCP segments that required retransmission over this connection. A segment is retransmitted whenever the receiver does not acknowledge receipt and a timeout occurs.

The percentage is calculated as:

(TCP ReXmit Pct) = (Retransmitted TCP Segments) divided by (TCP Segments Out)

Response Time The elapsed time (in tenths of a second) from when the segment was sent to when the acknowledgment was received. The format is a real number.

Response Time Variance The statistical variation of round trip times since the connection was established. The format is a real number.

Segments Retransmitted The number of segments retransmitted over this connection during the most recent sampling interval.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Telnet Appl Name The VTAM application name that Telnet uses. The remote TCP/IP application and the local Telnet to permit VTAM and TCP/IP applications to communicate over TCP/IP networks. The format is an alphanumeric string no longer than 8 characters.

Telnet LU Name The VTAM logical unit name that Telnet uses to communicate with a VTAM application on this host. When a TCP/IP application requests a session with a VTAM application, a VTAM LU is

assigned from the Telnet pool to allow TCP/IP and VTAM to communicate. The format is an alphanumeric string no longer than 8 characters.

Time Since Last Activity The amount of time since the most recent activity on this connection. This value is stored in hundreds of a second (for example, one second is stored as 100) and displayed as a time value (for example, 4.17000s or 4m 20s).

Total Bytes The total number of bytes sent and received since the connection started. The format is a long long integer.

Total Bytes (deprecated) The total number of bytes sent and received since the connection started. When the value in the Total Bytes field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes (in GB)** field and the remainder is stored in the **Total Bytes** field. The format is an integer.

Total Bytes (in GB) (deprecated) The total number of bytes sent and received since the connection started, divided by 1,073,741,824. When the value in the **Total Bytes** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes (in GB)** field and the remainder is stored in the **Total Bytes** field. The format is an integer.

Total Bytes Received The total number of bytes received since the connection started. The format is a long long integer.

Total Bytes Received (deprecated) The total number of bytes received since the connection started. When the value in the **Total Bytes Received** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Received (in GB)** field and the remainder is stored in the **Total Bytes Received** field. The format is an integer.

Total Bytes Received (in GB) (deprecated) The total number of bytes received since the connection started, divided by 1,073,741,824. When the value in the **Total Bytes Received**field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Received (in GB)** field and the remainder is stored in the **Total Bytes Received** field. The format is an integer.

Total Bytes Sent (deprecated) The total number of bytes sent since the connection started. When the value in the **Total Bytes Sent** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Sent (in GB)** field and the remainder is stored in the **Total Bytes Sent** field. The format is an integer.

Total Bytes Sent The total number of bytes sent since the connection started. The format is a long long integer.

Total Bytes Sent (in GB) (deprecated) The total number of bytes sent since the connection started, divided by 1,073,741,824. When the value in the **Total Bytes Sent** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Sent (in GB)** field and the remainder is stored in the **Total Bytes Sent** field. The format is an integer.

Total Datagrams The total number of all datagrams this connection sent and received since the connection started. The format is an integer.

Total Datagrams Received The total number of datagrams this connection received since the connection started. The format is an integer.

Total Datagrams Sent The total number of datagrams this connection sent since the connection started. The format is an integer.

Total Segments Retransmitted The total number of segments retransmitted over this connection. Retransmissions occur when a TCP segment is sent, but the receiving host does not acknowledge it within a specified timeout period. Hardware errors and network congestion can cause time-outs. The format is an integer.

TCPIP Details Attributes

Use the TCPIP Details attributes to display performance and identifying information for a specific connection.

Agent STC Name The IBM Z OMEGAMON Network Monitor started task name. The default is CANSN3. The format is a string of up to 8 characters.

APPLDATA The result of a SIOCSAPPLDATA ioctl query. APPLDATA enables applications to associate 40 bytes of application-specific information with TCP sockets that they own. This information can assist problem determination, capacity planning, and accounting applications. The format is a string of up to 40 bytes.

For additional information, see the application data appendix in the *IBM z/OS Communications Sever: IP Configuration Reference.*

Application Name The job name associated with the application address space that opened and bound the socket. The format is a string up to 8 characters in length.

Application Name and Port The Application Name and Local Port are combined in this attribute, separated by a colon. The format is a string up to 15 characters in length.

ASID The z/OS address space ID of the address space that opened the socket. This value is displayed as a 4-digit hexadecimal number.

AT-TLS Policy Status The current Application Transparent Transport Layer Security (AT-TLS) policy status for the connection. The value returned defines the current runtime status of the AT-TLS policy for the connection. This value is stored and displayed as a string. Valid values for this integer are:

- 0 = Unknown
- 1 = Off
- 2 = None
- 3 = Not_Enabled
- 4 = Enabled
- 5 = ApplicationControlled

AT-TLS Status The current Application Transparent Transport Layer Security (AT-TLS) status for the connection. This value indicates whether the SSL handshake has completed successfully for the connection. This value has dependency on the value of AT-TLS Policy Status attribute. This value is stored and displayed as a string. Valid values for this integer are:

- 0 = blank
- 1 = Not_Secure
- 2 = Handshake_In_Progress
- 3 = Secure

Byte Rate The number of bytes sent or received per minute during the most recent time interval. The format is an integer.

Bytes Received The number of bytes received during the most recent time interval. The format is an integer.

Bytes Sent The number of bytes sent during the most recent time interval. The format is an integer.

Bytes Sent or Received The number of sent or received bytes during the most recent time interval. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour

- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Congestion Window Size The congestion window size for this connection. Congestion window size is the maximum amount of data that is sent without waiting for an acknowledgment from the remote socket. The format is an unsigned integer.

The value that is used when congestion is detected in the network to limit the amount of data that is sent by the local stack.

Connection Duration The amount of time, in seconds, since this connection was created. This value is displayed as a time value (for example, 22.0000s or 4m 20s).

Connection Start Time The time and date when this connection was created. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Connection State The state of the connection. The following are valid values:

- **CLOSED** The end state of a TCP connection; this state means the TCP connection no longer exists.
- **CLOSE_WAIT** A state in which the connection is waiting for a connection termination request from the local port.

- **CLOSING** A state in which the connection is waiting for a connection termination request acknowledgment from the remote TCP.
- **ESTABLISHED** A state in which the connection is established.
- **FIN_WAIT_1** A state in which the connection is waiting for a connection termination request from the remote TCP or an acknowledgement of the connection termination request.
- **FIN_WAIT_2** A state in which the connection is waiting for a connection termination request from the remote TCP.
- **LAST_ACK** A state in which the connection is waiting for an acknowledgment of the connection termination request it sent to the remote TCP.
- **LISTEN** A state in which the connection is waiting for a connection request from any remote TCP and port.
- **SYN_RECEIVED** A state in which the connection is waiting for a confirming connection request acknowledgement after receiving and sending a connection request.
- **SYN_SENT** A state in which the connection is waiting for a matching connection request after a connection request was sent. If a connection is in this state for two successive sample intervals, an exception is generated.
- **TIME_WAIT** A state in which the host waits to ensure that a remote TCP has received a connection termination request. After the wait time is over, the socket pair that uniquely defines the connection is available for reuse.

DVIPA Identifies when the Local IP Address is a Dynamic Virtual IP Addressing (DVIPA) address. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = [blank] Not available
- 1 = Yes
- 2 = No

Duplicate ACKs The number of duplicate ACKs (TCP acknowledgements) received for this connection. The format is an unsigned integer.

Hex Connection Number The hexadecimal representation of the connection number. The format is an 8-digit hexadecimal string.

Inbound Bytes Buffered The number of incoming bytes buffered by this connection. The format is an unsigned integer.

Inbound Interface Name The link name of the receiving interface for this connection. The format is a string up to 16 characters in length.

Notes:

- This attribute is available only on systems running z/OS v1.12 or later. On systems before z/OS v1.12, this attribute will display as blank.
- This attribute applies to connections that are registered to an ancillary input queue (such as the OSA-Express bulk data queue). For all other connections, this attribute will display as blank.

Inbound Queued Data Time Stamp The time stamp of the oldest inbound data that was queued. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute

- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Local IP Address The local IP address for this connection. The format is a string up to 45 characters in length.

Local Port The local port for this connection. The format is a four-byte integer.

Local Port (deprecated) The local port for this connection, as a two-byte integer.

Local Port String The local port for this connection as a string. The format is a string up to five characters in length.

Local Window Size Frequency The number of times the local window size was set to zero during the most recent time interval. The format is an integer.

Maximum Segment Size The maximum segment size the connection can send. The largest amount of data the local socket can send in a single packet. The format is an unsigned integer.

Maximum Send Window Size The maximum send window size for the connection. The format is an unsigned integer.

Negotiated Cipher The negotiated cipher that is in use by the secure connection. This value is used for the data encryption or decryption. See the description of the TTLSCipherParms statement in the "Policy Agent and Policy Applications" chapter of the *IBM z/OS Communications Server: IP Configuration Reference* v1.12 or later book for a list of possible cipher values. This value is applicable only if the value for AT-TLS Status is **Secure**. This value is stored and displayed as a string. Valid values for this integer are:

- blank = 0X00000000
- TLS_RC4_128_WITH_MD5 = 0X0002F0F1
- TLS_RC4_128_EXPORT40_WITH_MD5 = 0X0002F0F2
- TLS_RC2_CBC_128_CBC_WITH_MD5 = 0X0002F0F3
- TLS_RC2_CBC_128_CBC_EXPORT40_WITH_MD5 = 0X0002F0F4
- TLS_DES_64_CBC_WITH_MD5 = 0X0002F0F6
- TLS_DES_192_EDE3_CBC_WITH_MD5 = 0X0002F0F7
- TLS_NULL_WITH_NULL_NULL=0X0003F0F0
- TLS_RSA_WITH_NULL_MD5 = 0X0003F0F1
- TLS_RSA_WITH_NULL_SHA = 0X0003F0F2
- TLS_RSA_EXPORT_WITH_RC4_40_MD5 = 0X0003F0F3
- TLS_RSA_WITH_RC4_128_MD5 = 0X0003F0F4
- TLS_RSA_WITH_RC4_128_SHA = 0X0003F0F5
- TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 = 0X0003F0F6
- TLS_RSA_WITH_DES_CBC_SHA = 0X0003F0F9
- TLS_RSA_WITH_3DES_EDE_CBC_SHA = 0X0003F0C1

- TLS_DH_DSS_WITH_DES_CBC_SHA = 0X0003F0C3
- TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA = 0X0003F0C4
- TLS_DH_RSA_WITH_DES_CBC_SHA = 0X0003F0C6
- TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA = 0X0003F1F0
- TLS_DHE_DSS_WITH_DES_CBC_SHA = 0X0003F1F2
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA = 0X0003F1F3
- TLS_DHE_RSA_WITH_DES_CBC_SHA=0X0003F1F5
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA = 0X0003F1F6
- TLS_RSA_WITH_AES_128_CBC_SHA = 0X0003F2C6
- TLS_DH_DSS_WITH_AES_128_CBC_SHA = 0X0003F3F0
- TLS_DH_RSA_WITH_AES_128_CBC_SHA = 0X0003F3F1
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA = 0X0003F3F2
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA=0X0003F3F3
- TLS_RSA_WITH_AES_256_CBC_SHA = 0X0003F3F5
- TLS_DH_DSS_WITH_AES_256_CBC_SHA = 0X0003F3F6
- TLS_DH_RSA_WITH_AES_256_CBC_SHA = 0X0003F3F7
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA = 0X0003F3F8
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA = 0X0003F3F9

Negotiated SSL Protocol The negotiated SSL protocol in use by the connection. This value is applicable only when the value for AT-TLS Status is **Secure**. This value is stored and displayed as a string. Valid values for this integer are:

- 0 = Unsecured
- 512 = SSL_Version_2
- 768 = SSL_Version_3=768
- 769 = TLS_Version_1
- 770 = TLS_Version_1.1

Open Type The type of open performed for this connection. This value is stored and displayed as a string. Valid values for this integer are:

- 0 = Passive
- 1 = Active

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Out of Order Segments The number of out-of-order segments received during the most recent time interval. The format is an integer.

Outbound Bytes Buffered The number of outgoing bytes buffered by this connection. The format is an unsigned integer.

Outbound Interface Name The name of the interface used to send the most recent segment. The format is a string up to 16 characters in length.

Outbound Queued Data Time Stamp The time and date of the oldest queued data waiting to be sent. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month

- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Partner User ID The user ID associated with the partner's certificate. This value is applicable only if the value for AT-TLS Status is **Secure**. The format is a string of up to 8 characters.

Percent Out of Order Segments The percentage of segments received that was out of order during the most recent time interval. The range for this value is from 0% to 100%.

Percent Segments Retransmitted The percentage of TCP segments that required retransmission over this connection. This value may exceed 100% when more segments are retransmitted than are successfully sent during the sampling interval.

Receive Buffer Size The receive buffer size for the connection. The format is an unsigned integer.

Receive Byte Rate The number of bytes received, per minute, during the most recent time interval. The format is an integer.

Receive Segment Rate The number of segments received, per minute, during the most recent time interval. The format is an integer.

Registered Ancillary Inbound Queue An indicator of whether the TCP connection is registered with a TCP bulk data ancillary inbound queue. Valid values for this integer are:

- blank = Pre z/OS v1.12
- 1 = Yes
- 2 = No

Note: The attribute is available in a z/OS v1.12 and later environment only.

Remote IP Address The remote IP address for this connection. The format is an alphanumeric string up to 45 characters in length.

Remote Port The remote port for this connection. The format is a four-byte integer.

Remote Port (deprecated) The remote port for this connection, as a two-byte integer.

Remote Port String The remote port for this connection as a string. The format is a string up to five characters in length.

Remote Window Size Frequency The number of times the remote window size was set to zero during the most recent time interval. The format is an integer.

Response Time The elapsed time (in tenths of a second) from when the segment was sent to when the acknowledgment was received. The format is an integer.

Response Time Variance The statistical variation of round trip times since the connection was established. The format is an integer.

Retransmission Rate The number of segments retransmitted, per minute, during the most recent time interval. The format is an integer.

Segment Rate The number of segments sent or received, per minute, during the most recent time interval. The format is an integer.

Segments Received The number of segments received during the most recent time interval. The format is an integer.

Segments Retransmitted The number of segments retransmitted over this connection during most recent time interval. The format is an integer.

Segments Sent The number of segments sent during the most recent time interval. The format is an integer.

Segments Sent or Received The number of segments sent and received during the most recent time interval. The format is an integer.

Send Buffer Size The send buffer size for the connection. The format is an unsigned integer.

Send Window Size The send window size for the connection. The format is an unsigned integer.

Server Resource ID The numeric identification of the server (that is, the listener connection) associated with this client connection. This value applies only to load-balancing servers that have bound to a port number for which SHAREPORT was specified on the PORT/PORTRANGE profile statement. This value is zero (0) for client connections to servers that are not load-balancing servers. The format is an unsigned integer displayed as an 8-character hexadecimal string.

Slow Start Threshold The slow-start threshold for this connection. The format is an unsigned integer.

The slow-start threshold is used to determine whether the connection is recovering from congestion. If the congestion window is smaller than the slow-start threshold, the connection takes actions to more quickly recover from congestion.

SSL Session Type The type of System SSL secure session defined in AT-TLS policy in use by the connection. These values are specified in AT-TLS policy configuration with the HandshakeRole and ClientAuthType parameters. This value is applicable only when the value for AT-TLS Policy Status is **Enabled** or **ApplicationControlled**; otherwise, this value is **SSL_Not_Applicable**. This value is stored and displayed as a string. Valid values for this integer are:

- 0 = SSL_Not_Applicable
- 1 = SSL_Handshake_Client
- 2 = SSL_Handshake_Server
- 3 = Client_Cert_Bypassed
- 4 = Client_Cert_Full
- 5 = Client_Cert_Reqd
- 6 = Client_Cert_with_UserID

Sysplex Cluster Connection Type The sysplex cluster connection types for this connection. This value is stored and displayed as a string. Valid values for this integer are:

- 0 = blank
- 1 = No_Cluster
- 2 = Same_Cluster
- 4 = Same_Image
- 8 = Internal_Cluster

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The TCP/IP job name. The format is an alphanumeric string no longer than 8 characters.

Telnet Appl Name The VTAM application name that Telnet uses. The format is a string no longer than 8 characters.

Telnet Session Type The type of open performed for this connection. This value is stored and displayed as a string. Valid values for this integer are:

- 0 = blank
- 1 = Line_Mode
- 2 = TN3270_Mode
- 4 = TN3270E_Mode

Telnet LU Name The VTAM logical unit name that Telnet uses to communicate with a VTAM application on this host. The format is a string no longer than 8 characters.

Time Since Last Activity The amount of time since the most recent activity on this connection. This value is stored in hundreds of a second (for example, one second is stored as 100) and displayed as a time value (for example, 4.17000s or 4m 20s).

TN3270 Client User ID The client user ID if the TCP connection is for a TN3270 or TN3270E session with an application whose access is restricted by a TN3270 profile RESTRICTAPPL parameter. This attribute is available only if the TN3270 client is in session with an application listed in a RESTRICTAPPL statement on the TN3270 server's profile. For more information about this parameter, see the *IBM z/OS Communications Server IP Configuration Reference.* The format is a string up to 8 characters in length.

TN3270 Logmode Name The VTAM Logmode if the TCP connection is for a TN3270 or TN3270E session. The format is a string up to 8 characters in length.

Total Bytes The total number of bytes sent and received since the connection started. The format is a long long integer.

Total Bytes (deprecated) The total number of bytes sent and received since the connection started. When the value in the Total Bytes field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes (in GB)** field and the remainder is stored in the **Total Bytes** field. The format is an integer.

Total Bytes (in GB) (deprecated) The total number of bytes sent and received since the connection started, divided by 1,073,741,824. When the value in the **Total Bytes** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes (in GB)** field and the remainder is stored in the **Total Bytes** field. The format is an integer.

Total Bytes Received The total number of bytes received since the connection started. The format is a long long integer.

Total Bytes Received (deprecated) The total number of bytes received since the connection started. When the value in the **Total Bytes Received** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Received (in GB)** field and the remainder is stored in the **Total Bytes Received** field. The format is an integer.

Total Bytes Received (in GB) (deprecated) The total number of bytes received since the connection started, divided by 1,073,741,824. When the value in the **Total Bytes Received** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Received (in GB)** field and the remainder is stored in the Total Bytes Received field. The format is an integer.

Total Bytes Sent The total number of bytes sent since the connection started. The format is a long long integer.

Total Bytes Sent (deprecated) The total number of bytes sent since the connection started. When the value in the **Total Bytes Sent** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Sent (in GB)** field and the remainder is stored in the **Total Bytes Sent** field. The format is an integer.

Total Bytes Sent (in GB) (deprecated) The total number of bytes sent since the connection started, divided by 1,073,741,824. When the value in the **Total Bytes Sent** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Sent (in GB)** field and the remainder is stored in the **Total Bytes Sent** field. The format is an integer.

Total Out of Order Segments The total number of out-of-order segments received since the connection started. The format is an integer.

Total Segments The total number of segments sent or received since the connection started. The format is an integer.

Total Segments Received The total number of segments received since the connection started. The format is an integer.

Total Segments Retransmitted The total number of segments retransmitted over this connection since the connection started. The format is an integer.

Total Segments Sent The total number of segments sent since the connection started. The format is an integer.

Transmit Byte Rate The number of bytes transmitted, per minute, during the most recent time interval. The format is an integer.

Transmit Segment Rate The number of segments transmitted, per minute, during the most recent time interval. The format is an integer.

TCPIP Devices Attributes

Use the TCPIP Devices attributes to monitor network devices defined for a selected address space.

Note: If the address space being monitored is running on z/OS v1.11 or earlier, the values for this attribute group are retrieved using SNMP. If the address space being monitored is running on z/OS v1.12 or later, the values for this attribute group are retrieved using the z/OS Communications Server callable network management interface (NMI). Only these attributes in this workspace will show data for non-strategic interfaces:

- Link Name
- Link type
- Interface Index

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour

- M = Minute
- S = Second
- m = Millisecond

Device Address The address of the network device. This is the base address, except for ELANS and ILANS, which use the control port address. The format is an alphanumeric string no longer than eight characters.

Note: If the address space being monitored is running on z/OS v1.11 or earlier, the value for this attribute is retrieved using SNMP, and this field displays an accurate, non-zero value. If the address space being monitored is running on z/OS v1.12 or later, the value for this attribute is retrieved using the z/OS Communications Server callable network management interface (NMI), and the field displays valid, non-zero values for strategic interfaces only. Non-strategic interfaces always display a value of 0000.

Device Name The name of the TCP/IP device associated with this channel. The format is an alphanumeric string no longer than 16 characters.

Device Status The status of the network device, indicating whether the device or datapath is operational. The format is an alphanumeric string no longer than 18 characters, one of the following:

- dormant
- down
- lowerLayerDown
- notPresent
- testing
- unknown
- up

Device Type The type of physical network device being monitored. The format is an alphanumeric string no longer than 8 characters.

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Interface Index The interface index associated with this device. The format is an unsigned integer.

Job Name The name of the job associated with the network device. The format is an alphanumeric string no longer than 8 characters.

Link Name The link name associated with this network device. The format is an alphanumeric string no longer than 16 characters.

Link Type The type of link associated with this network device. The format is an alphanumeric string no longer than eight characters.

Network Number The network to which the device is attached. This attribute is significant for links on library control system (LCS) devices only. The format is an alphanumeric string no longer than eight characters.

Note: If the address space being monitored is running on z/OS v1.11 or earlier, the value for this attribute is retrieved using SNMP, and this field displays an accurate, non-zero value. If the address space being monitored is running on z/OS v1.12 or later, the value for this attribute is retrieved using the z/OS Communications Server callable network management interface (NMI) and the field applies to CTC devices only. For all other Device Types, the field displays a value of zero, meaning that data is not available.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Port Interface Index The interface port index associated with an OSA device or interface. The format is an integer.

Program Name The program name associated with the network device. The format is an alphanumeric string no longer than eight characters.

Queue Size The size of the queue associated with the network device. The format is an alphanumeric string no longer than eight characters.

Note: If the address space being monitored is running on z/OS v1.11 or earlier, the value for this attribute is retrieved using SNMP, and this field displays an accurate, non-zero value. If the address space being monitored is running on z/OS v1.12 or later, the value for this attribute is retrieved using the z/OS Communications Server callable network management interface (NMI) and the field applies to the following devices types:

- ATM (IPv4 only)
- LCS
- OSA-Express QDIO interfaces (IPv6 only).

For all other Interface Types, this field displays a value of zero, meaning that data is not available.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

TCPIP FTP Attributes

Use the TCPIP FTP attributes to create situations that monitor performance data for FTP data transfers between a z/OS FTP client and a remote FTP server and between a remote FTP client and a z/OS FTP server. A local IP address and port number and a remote IP address and port number uniquely define the FTP data connection for this FTP transfer.

Application Name The name of the FTP application. The format is a string of up to 8 characters.

Bytes Transferred The number of bytes that was transferred for this file. The format is a long long integer.

Bytes Transmitted (deprecated) The number of bytes that was transmitted. When the value in the Bytes Transmitted field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Transmitted (in GB)** field and the remainder is stored in the **Bytes Transmitted** field. The format is an integer.

Bytes Transmitted (in GB) (deprecated) The number of bytes that was transmitted, divided by 1,073,741,824. When the value in the **Bytes Transmitted** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Transmitted (in GB)** field and the remainder is stored in the **Bytes Transmitted** field. The format is an integer.

Cipher Specification The current cipher specification for this connection when the security mechanism is TLS or AT-TLS. This value is used for the data encryption or decryption. See the description of the TTLSCipherParms statement in the "Policy Agent and Policy Applications" chapter of the *IBM z/OS Communications Server: IP Configuration Reference* v1.12 or later book for a list of possible cipher values. This value is stored as a long integer and displayed as a string. Valid values for this integer are:

- blank = 0X00000000
- SSL_RC4_US = 0X0000F0F1
- SSL_RC4_EXPORT = 0X0000F0F2
- SSL_RC2_US = 0X0000F0F3
- SSL_RC2_EXPORT = 0X0000F0F4
- SSL_DES_US = 0X0000F0F6
- SSL_3DES_US = 0X0000F0F7
- SSL_NULL_MD5 = 0X0001F0F1
- SSL_NULL_SHA = 0X0001F0F2

- SSL_RC4_MD5_EX = 0X0001F0F3
- SSL_RC4_MD5 = 0X0001F0F4
- SSL_RC4_SHA = 0X0001F0F5
- SSL_RC2_MD5_EX = 0X0001F0F6
- SSL_DES_SHA = 0X0001F0F9
- SSL_3DES_SHA = 0X0001F0FA
- SSL_AES_128_SHA = 0X0001F2C6
- SSL_AES_256_SHA = 0X0001F3F5
- TLS_RC4_128_WITH_MD5 = 0X0002F0F1
- TLS_RC4_128_EXPORT40_WITH_MD5 = 0X0002F0F2
- TLS_RC2_CBC_128_CBC_WITH_MD5 = 0X0002F0F3
- TLS_RC2_CBC_128_CBC_EXPORT40_WITH_MD5 = 0X0002F0F4
- TLS_DES_64_CBC_WITH_MD5 = 0X0002F0F6
- TLS_DES_192_EDE3_CBC_WITH_MD5 = 0X0002F0F7
- TLS_NULL_WITH_NULL_NULL = 0X0003F0F0
- TLS_RSA_WITH_NULL_MD5 = 0X0003F0F1
- TLS_RSA_WITH_NULL_SHA = 0X0003F0F2
- TLS_RSA_EXPORT_WITH_RC4_40_MD5 = 0X0003F0F3
- TLS_RSA_WITH_RC4_128_MD5 = 0X0003F0F4
- TLS_RSA_WITH_RC4_128_SHA = 0X0003F0F5
- TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 = 0X0003F0F6
- TLS_RSA_WITH_DES_CBC_SHA = 0X0003F0F9
- TLS_RSA_WITH_3DES_EDE_CBC_SHA = 0X0003F0C1
- TLS_DH_DSS_WITH_DES_CBC_SHA = 0X0003F0C3
- TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA = 0X0003F0C4
- TLS_DH_RSA_WITH_DES_CBC_SHA = 0X0003F0C6
- TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA = 0X0003F1F0
- TLS_DHE_DSS_WITH_DES_CBC_SHA = 0X0003F1F2
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA = 0X0003F1F3
- TLS_DHE_RSA_WITH_DES_CBC_SHA = 0X0003F1F5
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA = 0X0003F1F6
- TLS_RSA_WITH_AES_128_CBC_SHA = 0X0003F2C6
- TLS_DH_DSS_WITH_AES_128_CBC_SHA = 0X0003F3F0
- TLS_DH_RSA_WITH_AES_128_CBC_SHA = 0X0003F3F1
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA = 0X0003F3F2
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA = 0X0003F3F3
- TLS_RSA_WITH_AES_256_CBC_SHA = 0X0003F3F5
- TLS_DH_DSS_WITH_AES_256_CBC_SHA = 0X0003F3F6
- TLS_DH_RSA_WITH_AES_256_CBC_SHA = 0X0003F3F7
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA = 0X0003F3F8
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA = 0X0003F3F9

Client User ID The local user name (login name) of the client. This column applies to client transfers only. The format is an alphanumeric string no longer than 8 characters.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Command The FTP command that initiated the transfer. The command can be one of the following:

- 1 = Append
- 2 = Delete
- 3 = Rename (only possible when Role is server)
- 4 = Retrieve
- 5 = Store
- 6 = Store Unique

Data Set Type The type of data set for the file that is being transferred. The following values are valid:

- S = Sequential
- P = Partitioned data set
- H = Hierarchical file system

Data Structure The data structure of the file that is being transferred. The following values are valid:

- F = File
- R = Record

Data Type The data type of the file that is being transferred. The following values are valid:

- A = ASCII
- B = Double byte
- E = EBCDIC
- I = Image
- U = UCS-2

Data Set Name The name of the data set that is being transferred. The format is an alphanumeric string with a maximum of 1024 characters.

File Type The type of file that is being transferred. The following three-character values are valid:

- SEQ = Sequential
- JES = Job Entry System
- SQL = Structured Query Language

FTP Session ID The unique identifier for the FTP session associated with this transfer. The format is a string up to 16 characters.

Last Reply to Client The most recent reply that was sent from the server to the client. This value is stored and displayed as a string. Valid values for this integer are:

- 200: Command OK
- 202: Command not implemented
- 211: System status
- 212: Directory status
- 213: File status
- 214: Help message
- 215: System type
- 220: Service ready for new user
- 221: Service closing control connection
- 225: Data connection open -- no transfer in progress
- 226: Closing data connection -- requested file action successful
- 227: Entering passive mode
- 230: User logged in -- proceed
- 250: Requested file action OK -- completed
- 257: Path created
- 331: User name OK -- need password
- 332: Need account for login
- 350: Requested file action pending further information
- 421: Service not available -- closing control connection
- 425: Cannot open data connection
- 426: Connection closed -- transfer aborted
- 450: Requested file action not taken -- file unavailable
- 451: Requested action aborted -- local error in processing
- 452: Requested action not taken -- insufficient system storage
- 500: Syntax error -- command unrecognized
- 501: Syntax error in parameters or arguments
- 502: Command not implemented
- 503: Bad sequence of commands
- 504: Command not implemented for that parameter
- 530: Not logged in
- 532: Need account for storing files
- 550: Requested action not taken -- file unavailable
- 551: Requested action aborted -- page type unknown
- 552: Requested file action aborted -- exceeded storage allocation
- 553: Requested action not taken -- file name not allowed

Last Reply to Client Description Description of the most recent reply that was sent from the server to the client. This value is stored as a string and displayed as a number. Valid values are:

- Command OK = 200
- Command not implemented = 202
- System status = 211
- Directory status = 212
- File status = 213
- Help message = 214
- System type = 215
- Service ready for new user = 220
- Service closing control connection = 221
- Data connection open -- no transfer in progress = 225
- Closing data connection -- requested file action successful = 226
- Entering passive mode = 227
- User logged in -- proceed = 230
- Requested file action OK -- completed = 250
- Path created = 257
- User name OK -- need password = 331
- Need account for login = 332
- Requested file action pending further information = 350
- Service not available -- closing control connection = 421
- Cannot open data connection = 425
- Connection closed -- transfer aborted = 426
- Requested file action not taken -- file unavailable = 450
- Requested action aborted -- local error in processing = 451
- Requested action not taken -- insufficient system storage = 452
- Syntax error -- command unrecognized = 500
- Syntax error in parameters or arguments = 501
- Command not implemented = 502
- Bad sequence of commands = 503
- Command not implemented for that parameter = 504
- Not logged in = 530
- Need account for storing files = 532
- Requested action not taken -- file unavailable = 550
- Requested action aborted -- page type unknown = 551
- Requested file action aborted -- exceeded storage allocation = 552
- Requested action not taken -- file name not allowed = 553

Local IP Address The local IP address for this FTP data connection. The format is a string up to 45 characters in length.

Local IP Port (deprecated) The local port number for this FTP data connection. The format is a two-byte integer.

Local IP Port String The local port for this FTP data connection as a string. The format is a string up to five characters in length.

Local Port The local port for the FTP data connection. The format is a four-byte integer.

Login Method The current login method for this connection. This value is stored as a single character and displayed as a string. The following are valid:

- C= Certificate
- P = Password
- T= Kerberos_Ticket
- U= Undefined

New Data Set Name The name of the second data set involved in the transfer. This column is completed for records associated with an FTP Rename function only. The format is an alphanumeric string no longer than 1024 characters.

New PDS Member Name The name of the member of the second data set involved in the transfer. This column is completed only for records associated with an FTP Rename function. The format is an alphanumeric string no longer than 8 characters.

NMI FTP Enhancements IBM internal use only.

Origin Node The unique identifier of the monitored TCP/IP stack. The format is an alphanumeric string no longer than 32 characters.

PDS Member Name The name of the member of the partitioned data set (PDS) that is being transferred. The format is an alphanumeric string no longer than 8 characters.

Remote IP Address The remote IP address for this FTP data connection. This is the IP address associated with the FTP connection partner session of the TCP/IP stack. The format is an alphanumeric string no longer than 45 characters.

Remote IP Port (deprecated) The remote IP port for this FTP data connection. This is the remote port number, that is the port number associated with the FTP connection partner session of the TCP/IP stack. The format is a two-byte integer.

Remote IP Port String The remote port for this FTP data connection as a string. The format is a string up to five characters in length.

Remote Port The remote port for the FTP data connection. The format is a four-byte integer.

Role The role of the z/OS server that indicates whether the TCP/IP stack is acting as the Client or as the Server in this FTP connection. The following are valid values for this switch:

- 0 = Client
- 1 = Server

Security Mechanism The current security mechanism for this connection. This value is stored as a single character and displayed as a string. The following are valid:

- A = AT_TLS
- G = GSSAPI
- N = None
- T = TLS

Security Protocol Level The current security protocol level for this connection when the security mechanism is TLS or AT-TLS. The format is a character string.

Session Protection Level The current session protection level for this connection. This value is stored as a character and displayed as a string. Valid values are:

- **C** = Clear
- **N** = None
- **P** = Private
- **S** = Safe
- **U** = Unknown

Server Logging Session ID The ID that uniquely identifies sessions between z/OS FTP servers and FTP clients. The format is a 15-character string. The identifier is generated from FTP daemon job name, followed by a 5-digit number in range 00000-99999. The value is displayed in the SYSLOGD file log entries when FTP activity logging is enabled.

State The status of this FTP transfer. This value is stored as an integer and displayed as a number. The following are valid values:

- **0** Unknown - In the history file, the value was Active during historical collection.
- **1** Inactive - A close record was received for this open record.
- **2** Active - No close record was received.
- **4** Complete - The record was closed.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCP Control Connection ID The TCP connection ID of the connection being used for the FTP control connection. This value is displayed as a 8-digit hexadecimal number.

This value is displayed as a hexadecimal number that uniquely identifies the TCP connection being used for the FTP control connection. The TCP connection ID (or resource ID) is displayed under the Local Socket column adjacent to the IP address in the output of a NETSTAT command.

TCP Data Connection ID The TCP connection ID for the connection being used for the FTP data connection. This value is displayed as a 8-digit hexadecimal number.

This value is displayed as a hexadecimal number that uniquely identifies the TCP connection being used for the FTP data connection. The TCP connection ID, sometimes referred to as the resource ID, is displayed under the Local Socket column adjacent to the IP address in the output of a NETSTAT command.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Transfer Protection Level The current transfer protection level for this connection. This value is stored as a single character and displayed as a string. The following are valid:

- C = Clear
- N = None
- P = Private
- S = Safe
- U = Unknown

Transmission Duration The amount of time required for the transfer or command to be completed. This value is stored in milliseconds and displayed as a time value (for example, 4.17300s or 4m 20s).

Transmission End The date and time the transmission ended. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

When the transmission has not ended, this value is stored as a character string of zeros and displayed as blank.

Transmission Mode The transmission mode that is used for this transmission. The following alphabetic characters are valid:

- B = Block
- C = Compressed
- S = Stream

Transmission Start The date and time the transmission started. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

User ID on Server The user name that was used to log in to the server. The format is an alphanumeric string no longer than 8 characters. When the actual user ID is longer then 8 characters, it is truncated. See the **User ID on Server Extended** attribute for longer user IDs.

User ID on Server Extended The user name that was used to log in to the server. The format is an alphanumeric string no longer than 63 characters.

TCPIP Gateways Attributes

Use the TCPIP Gateways attributes to monitor the gateways defined to a selected address space.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Dynamic Route Indicates whether the route used by this gateway was dynamically created (valid for IPv4 only). This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes
- 2 = (blank)

First Hop (Deprecated) The first router in the path to the remote host. The format is an alphanumeric string no longer than 15 characters.

First Hop The first router in the path to the remote network. The format is an alphanumeric string no longer than 45 characters. This special value may be displayed as follows:

<direct> - First Hop is a host IP address.

Host Name The name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Interface Index The interface index associated with this gateway. The format is an unsigned integer.

IP Version The IP version of the route used by this gateway. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4
- 1 = IPv6

Link or Interface Name The link or interface name associated with this gateway (router). The format is an alphanumeric string no longer than 16 characters.

Notes:

- This attribute is not available under z/OS v1.12 if Interface Statistics data collection has been disabled.

- Under z/OS v1.12, this attribute is blank for DVIPA routes. If a row in the Gateways table shows a value of blank for Link or Interface Name attribute under z/OS v1.12 or later, then this row represents a DVIPA route.

Link or Interface Status The status of the gateway link or interface, which indicates if the link is ready or not ready. If a link drops out of **Ready** status, you might lose connectivity to crucial network resources, and you might not be able to access needed applications. The gateway link can be in one of the following states:

- Ready
- Down
- Testing
- DAD_Pending

Notes:

- This attribute is not available under z/OS v1.12 if Interface Statistics data collection has been disabled.
- Under z/OS v1.12, this attribute is blank for DVIPA routes. If a row in the Gateways table shows a value of blank for Link or Interface Status attribute under z/OS v1.12 or later, then this row represents a DVIPA route.

MTU Value The maximum transmission unit (MTU) in bytes for the route. The format of this is an integer with a valid value of up to 65,535.

Network Address (Deprecated) The network address of this gateway. The format is an alphanumeric string no longer than 15 characters.

Network Address The network address of this gateway. The format is an alphanumeric string no longer than 45 characters. Special values may be displayed as follows:

- Defaultnet - The Network Address is a host IP address.
- Default - The Network Address is 0.

Link-local IPv6 addresses are displayed in the following format:

FE80::<interface ID>%<interface name>

Network Route Indicates whether the route used by this gateway was defined as a network route. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = No
- 1 = Yes
- 2 = (blank)

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Packet Size (Deprecated) The length of the packet in which the PING command sends the ECHO request message. The format is an alphanumeric string no longer than eight characters.

Route Status The status of route used by this gateway. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = (blank)
- 1 = Active
- 2 = Inactive

Route Type The type of route used by this gateway. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = (blank)
- 1 = Other
- 2 = Static

- 4 = ICMP
- 8 = RIP
- 13 = OSPF
- 129 = Router Advertisement
- 130 = Replaceable Static

Subnet Mask (Deprecated) The 32-bit mask for the subnetwork address in the IP address host portion. The format is an alphanumeric string no longer than 15 characters.

Subnet Mask The 32-bit (for IPv4 addresses) or 128-bit (for IPv6 addresses) mask for the subnetwork address in the IP address host portion. The format is an alphanumeric string no longer than 45 characters.

The following special values are displayed:

- <none> - Subnet Mask contains zeros
- HOST - Subnet Mask is a host IP address

Subnet Value (Deprecated) The subnet identifier. A subnet composes a group of nodes within the same network ID. The format is an alphanumeric string no longer than 15 characters.

Subnet Value The subnet identifier. A subnet composes a group of nodes within the same network ID. The format is an alphanumeric string no longer than 45 characters.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

TCPIP Memory Statistics Attributes

Use the TCP/IP Memory Statistics attributes to create situations that monitor memory statistics.

64bit Common Storage Allocated The current number of 64-bit common storage bytes allocated. A value of 0 (zero) indicates that this field is not supported. The format is an integer.

Note: This attribute is available only on systems running z/OS V1.11 or later

64bit Common Storage Free The current number of 64-bit common storage bytes free. A value of 0 indicates that this field is not supported. The format is an integer.

Note: This attribute is available only on systems running z/OS V1.11 or later

64bit Common Storage In Use The current number of 64-bit common storage bytes in use. A value of 0 indicates that this field is not supported. The format is an integer.

Note: This attribute is available only on systems running z/OS V1.11 or later.

Authorized Private Storage Allocated The current number of authorized private subpool storage bytes that has been allocated. A value of 0 indicates that this field is not supported. The format is an integer.

Authorized Private Storage Free The current number of authorized private subpool storage bytes free. A value of 0 indicates that this field is not supported. The format is an integer.

Authorized Private Storage In Use The current number of authorized private subpool storage bytes in use. A value of 0 indicates that this field is not supported. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month

- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

ECSA Storage Allocated The current number of Extended Common System Area (ECSA) storage bytes allocated. The format is an integer.

ECSA Storage Free The current number of Extended Common System Area (ECSA) storage bytes free. A value of 0 indicates that this field is not supported. The format is an integer.

ECSA Storage In Use The current number of Extended Common System Area (ECSA) storage bytes in use. A value of 0 indicates that this field is not supported. The format is an integer.

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

IP Address The IP address of the TCP/IP stack. The format is an alphanumeric string no longer than 45 characters.

Maximum 64bit Common Storage Allocated The maximum number of 64-bit common storage bytes allocated. A value of 0 indicates that this field is not supported. The format is an integer.

Note: This attribute is available only on systems running z/OS V1.11 or later

Maximum Authorized Private Storage Allocated The maximum number of authorized private subpool storage bytes allocated since the TCP/IP stack was started. The format is an integer.

Maximum Authorized Private Storage Allowed The maximum number of authorized private subpool storage bytes allowed. This number is specified on the GLOBALCONFIG statement in the TCP/IP profile. A value of zero indicates that there is no limit. The format is an integer.

Maximum ECSA Storage Allocated The maximum number of Extended Common System Area (ECSA) storage bytes that have been allocated since the TCP/IP stack was started. The format is an integer.

Maximum ECSA Storage Allowed The maximum number of Extended Common System Area (ECSA) storage bytes that are allowed. This number is specified on the GLOBALCONFIG statement in the TCP/IP profile. A value of zero indicates that there is no limit. The format is an integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Percent 64bit Common Storage In Use The percentage of 64-bit common storage that is currently in use compared to the current 64-bit common storage that is allocated. The range for this value is from 0% to 100%.

Note: This attribute is available only on systems running z/OS V1.11 or later

Percent Authorized Private Storage Allocated The percentage of authorized private storage currently allocated compared to the maximum authorized storage that is allowed. The range for this value is from 0% to 100%.

Note: The percentage of private storage allocated is always zero (0) if the Maximum Authorized Private Storage Allowed is zero (0).

Percent Authorized Private Storage In Use The percentage of authorized private storage that is currently in use compared to the current authorized private storage that is allocated. The range for this value is from 0% to 100%.

Percent ECSA Allocated Storage The percentage of Extended Common System Area (ECSA) storage currently allocated compared to the maximum ECSA storage that is allowed. The range for this value is from 0% to 100%.

Percent ECSA Storage In Use The percentage of Extended Common System Area (ECSA) storage that is currently in use compared to the current ECSA storage that is allocated. The range for this value is from 0% to 100%.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

TCPIP Stack Layer Attributes

Use the TCPIP Stack Layer attributes to monitor performance data for the layers of a selected TCP/IP stack.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Fragmentation Count The number of IP segments requiring fragmentation that was successfully fragmented. The format is an integer.

Fragmentation Failure Percentage The percentage of IP segments requiring fragmentation that was not successfully fragmented. The range for this value is from 0% to 100%.

Fragmentation Failures The number of IP segments requiring fragmentation that was not successfully fragmented. The format is an integer.

Fragmentation Percentage The percentage of IP segments that was successfully fragmented since TCP/IP initialization. The range for this value is from 0% to 100%.

Fragments To Be Reassembled The number of IP fragments received that needed to be reassembled by the IP layer during the most recent sample. The format is an integer.

Host Name The host name of the TCP/IP stack. The format is a string up to 255 characters in length.

Input Datagram Delivery Rate The rate at which input datagrams were delivered during the most recent sample. The format is an integer.

Input Datagram Forward Rate The rate at which datagrams were forwarded during the last sample. The format is an integer.

Input Datagrams Delivered The number of input datagrams successfully delivered to IP user-protocols (including ICMP) during the most recent sample. The format is an integer.

Input Datagrams Forwarded The number of input datagrams being routed through this host (which was not their final IP destination) and forwarded to the final destination during the most recent sample. The format is an integer.

Input Datagrams in Error The number of input datagrams discarded since TCP/IP initialization because of errors. Datagrams have been discarded because of one of the following errors:

- No route could be found to transmit them to their destination.
- The datagram frame did not carry enough data.
- Failures were detected by the IP reassembly algorithm.
- Errors were found in the IP headers (for example bad checksums , version number mismatch, other format errors, time-to-live exceeded, or errors discovered in processing their IP options).
- The IP address in the destination field of the IP header is not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E).
- The locally addressed datagram was received successfully but discarded because of an unknown or unsupported protocol.

Input Discard Percentage The percentage of IP segments this TCP/IP address space received from the network that was undeliverable and therefore discarded. The range for this value is from 0% to 100%.

Input Discards The number of IP segments that this TCP/IP address space received which were undeliverable and therefore discarded since TCP/IP initialization. The format is an integer.

Input Packet Count The number of IP segments that this TCP/IP address space received from the network since TCP/IP initialization. The format is a long long integer.

Input Packet Count (deprecated) The number of IP packets (including those received in error) that this TCP/IP address space received from the network since TCP/IP initialization, as an integer. When the value in the **Input Packet Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Input Packet Count (In G)** field and the remainder is stored in the **Input Packet Count** field. The format is an integer.

Input Packet Count (in G) (deprecated) The number of IP packets (including those received in error) that this TCP/IP address space received from the network since TCP/IP initialization, divided by 1,073,741,824. When the value in the **Input Packet Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Input Packet Count (in G)** field and the remainder is stored in the **Input Packet Count** field. The format is an integer.

Origin Node This is the unique identifier for the TCP/IP stack being displayed. The format is a string up to 32 characters in length.

Output Discard Percentage The percentage of all IP output segments sent from this TCP/IP address space to the network that was undeliverable and discarded. The range for this value is from 0% to 100%.

Output Discards The number of IP segments that this address space did not send that was undeliverable and therefore discarded since TCP/IP initialization. The format is an integer.

Output No Routes The number of IP segments that this address space did not forward because there was no available route to the destination since TCP/IP initialization. The format is an integer.

Output Packet Count The number of IP segments that this TCP/IP address space sent to the network since TCP/IP initialization. The format is a long long integer.

Output Packet Count (deprecated) The number of IP packets that local IP user-protocols (including ICMP) supplied to IP since TCP/IP initialization, as an integer. When the value in the **Output Packet Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Output Packet Count (In G)** field and the remainder is stored in the **Output Packet Count** field. The format is an integer. **Note:** This count does not include any packets counted in **Input Datagrams Forwarded**.

Output Packet Count (in G) (deprecated) The number of IP packets that local IP user-protocols (including ICMP) supplied to IP since TCP/IP initialization, divided by 1,073,741,824. When the value in the **Output Packet Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Output Packet Count (in G)** field and the remainder is stored in the **Output Packet Count** field. The format is an integer.

Note: This count does not include any packets counted in **Input Datagrams Forwarded**.

Reassembly Count The number of IP segments received that was successfully reassembled since TCP/IP initialization. The format is an integer.

Reassembly Failure Count The number of IP segments requiring reassembly that was not reassembled since TCP/IP initialization. A reassembly fails when all segments that compose the fragmented datagram are not received. The format is an integer.

Reassembly Failure Percentage The percentage of IP segments requiring reassembly that was not reassembled. The range for this value is from 0% to 100%.

Reassembly Percentage The percentage of IP segments reassembled since TCP/IP initialization. The range for this value is from 0% to 100%.

Receive Datagram Rate The number of datagrams received, per minute, during the most recent sample.

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCP Connection Accept Rate The number of connections accepted, per minute, during the most recent sample. The format is an integer.

TCP Connections Accepted The number of connections accepted during the most recent sample. The format is an integer.

TCP Connections Accepted High-Water Mark The high-water mark (the highest value recorded in the TCP Connections Accepted field) for active connections. The format is an integer.

TCP Connections Dropped The total number of connections that was lost by this listener during the most recent interval. The format is an integer. The connections were lost because of one of the following reasons:

- The retransmit threshold was exceeded.
- There was no response while sending window probe requests.
- There was no response while sending keep-alive probe requests.
- The FINWAIT2 timer expired before the FIN segment was received.

TCP FINWAIT2 Timeouts The number of TCP connections that was dropped because the FINWAIT2 timer expired before receiving the FIN segment during the most recent sample. The format is an integer.

TCP Input Segment Count The count of TCP segments that this TCP/IP address space received from the network since TCP/IP initialization. The format is a long long integer.

TCP Input Segment Count (deprecated) The count of TCP segments that this TCP/IP address space received from the network since TCP/IP initialization, as an integer. When the value in the **TCP Input Segment Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **TCP Input Segment Count (in G)** field and the remainder is stored in the **TCP Input Segment Count** field. The format is an integer.

TCP Input Segment Count (in G) (deprecated) The count of TCP segments that this TCP/IP address space received from the network since TCP/IP initialization, divided by 1,073,741,824. When the value in the **TCP Input Segment Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **TCP Input Segment Count (in G)** field and the remainder is stored in the **TCP Input Segment Count** field. The format is an integer.

TCP Keep-Alive Drops The number of TCP connections that was dropped, because there was no response, while sending TCP keepalive probe requests during the most recent sample. The format is an integer.

TCP Out-of-Order Segments The number of out-of-order segments received during the most recent sample. The format is an integer.

TCP Output Segment Count The count of TCP segments that this TCP/IP address space delivered to the network since TCP/IP initialization. The format is a long long integer.

TCP Output Segment Count (deprecated) The count of TCP segments that this TCP/IP address space delivered to the network since TCP/IP initialization, as an integer. When the value in the **TCP Output Segment Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **TCP Output Segment Count (in G)** field and the remainder is stored in the TCP Output Segment Count field. The format is an integer.

TCP Output Segment Count (in G) (deprecated) The count of TCP segments that this TCP/IP address space delivered to the network since TCP/IP initialization, divided by 1,073,741,824. When the value in the **TCP Output Segment Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the TCP Output Segment Count (in G) field and the remainder is stored in the **TCP Output Segment Count** field. The format is an integer.

TCP Percent Out-of-Order Segments The percentage of segments received that was out-of order during the most recent sample. The range for this value is from 0% to 100%.

TCP Receive Segment Rate The number of segments received, per minute, during the most recent sample. The format is an integer.

TCP Received Segment Error Rate The rate at which segments in error were received during the most recent sample. The format is an integer.

TCP Received Segment Errors The number of segments received in error (for example, bad TCP checksums) since TCP/IP initialization. The format is an integer.

TCP Retransmit Percentage The percentage of TCP segments that required retransmission. The range for this value is from 0% to 100%.

TCP Retransmit Threshold Exceeded The number of TCP connections that was dropped, during the most recent sample, because the retransmit threshold was exceeded. The format is an integer.

TCP Retransmitted Segments The number of TCP segments this host retransmitted since TCP/IP initialization. The format is an integer.

TCP Segment Retransmission Rate The rate at which TCP segments were retransmitted during the most recent sample. The format is an integer.

TCP Session Count The number of TCP sessions currently established to this TCP/IP address space. The format is an integer.

TCP Transmit Segment Rate The number of segments transmitted, per minute, during the most recent sample. The format is an integer.

TCP Window Probe Drops The number of TCP connections dropped, because no response was received, while sending window probe requests during the most recent sample. The format is an integer.

TCP Window Probes Sent The number of window probe requests sent during the most recent sample. The format is an integer.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Transmit Datagram Rate Number of datagrams requested to be transmitted, per minute, during the most recent sample. The format is an integer.

UDP Discard Percentage The percentage of UDP datagrams that was discarded as undeliverable (including No Port Found errors) because they were received in error. The range for this value is from 0% to 100%.

UDP Input Datagram Count The number of UDP datagrams received since TCP/IP initialization. The format is a long long integer.

UDP Input Datagram Count (deprecated) The number of UDP datagrams received since TCP/IP initialization, as an integer. When the value in the **UDP Input Datagram Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **UDP Input Datagram Count (in G)** field and the remainder is stored in the **UDP Input Datagram Count** field. The format is an integer.

UDP Input Datagram Count (in G) deprecated) The number of UDP datagrams received since TCP/IP initialization, divided by 1,073,741,824. When the value in the **UDP Input Datagram Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **UDP Input Datagram Count (in G**) field and the remainder is stored in the **UDP Input Datagram Count** field. The format is an integer.

UDP Input Errors The number of datagrams discarded as undeliverable because they were received in error (excluding No Port Found errors) since TCP/IP initialization. The format is an integer.

UDP No Port Count The number of UDP datagrams discarded as undeliverable because the port number specified did not match that of any active applications. The format is an integer.

UDP Output Datagram Count The number of datagrams this host sent since TCP/IP initialization. The format is a long long integer.

UDP Output Datagram Count (deprecated) The number of datagrams this host sent since TCP/IP initialization as an integer. When the value in the **UDP Output Datagram Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **UDP Output Datagram Count (in G)** field and the remainder is stored in the **UDP Output Datagram Count** field. The format is an integer.

UDP Output Datagram Count (in G) (deprecated) The number of datagrams that this TCP/IP address space sent since TCP/IP initialization, divided by 1,073,741,824. When the value in the **UDP Output Datagram Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **UDP Output Datagram Count (in G)** field and the remainder is stored in the UDP Output Datagram Count field. The format is an integer.

UDP Receive Datagram Rate The datagrams received, per minute, during the most recent sample. The format is an integer.

UDP Total Datagrams Received The total number of UDP datagrams received, including those with errors, since TCP/IP initialization. The format is a long long integer.

UDP Total Datagrams Received (deprecated) The total number of UDP datagrams received, including those with errors, since TCP/IP initialization, as an integer. When the value in the UDP Total Datagrams Received field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **UDP Total Datagrams Received (in G)** field and the remainder is stored in the **UDP Total Datagrams Received** field. The format is an integer.

UDP Total Datagrams Received (in G) The total number of UDP datagrams received, including those with errors, since TCP/IP initialization, divided by 1,073,741,824. When the value in the **UDP Total Datagrams Received** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **UDP Total Datagrams Received (in G)** field and the remainder is stored in the **UDP Total Datagrams Received** field. The format is an integer.

UDP Transmit Datagram Rate The number of datagrams transmitted, per minute, during the most recent sample. The format is an integer.

TCPIP Summary Attributes

Use the TCPIP Summary attributes to show the general health and activity of the TCP/IP stack at a glance.

Note: If the address space being monitored is running on z/OS v1.11 or earlier, these attributes are retrieved using SNMP. If the address space being monitored is running on z/OS v1.12 or later, these attributes are retrieved using the z/OS Communications Server callable network management interface (NMI).

Application Count The number of active TCP/IP applications when the most recent time interval ended. The format is an integer.

Byte Rate The number of bytes received or sent, per minute, during the most recent time interval. When the measured value exceeds 2,147,483,647 (the maximum value), the attribute will be set to 2,147,483,647. The format is an integer.

Collection Interval The time, in minutes, between successive samples; the sampling interval. The format is an integer between 1 and 60.

The Collection Interval was set in the Configuration Tool SPECIFY COMPONENT CONFIGURATION panel by specifying a value for the "TCP/IP Sample Interval" field or in PARMGEN using the KN3_TCP_SAMPLE_INTERVAL parameter. The Collection Interval controls collection of all TCP/IP data plus Communication Storage Manager (CSM), Enterprise Extender (EE), and High Performance Routing (HPR) data.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Connection Count The number of active connections at the end of the most recent time interval. This number represents the total number of rows in the TCP Connections table, the UDP Endpoints table, and the TCP Listener table. The format is an integer.

CPU Percentage The percentage of CPU in use when the sampling interval ended. The range for this value is from 0% to 100%.

CSA Percent Below 16MB The percentage of Common System Area (CSA) storage below the 16MB line in use when the last sampling interval ended. The range for this value is from 0% to 100%.

CSA Usage Below 16MB Currently Allocated The amount of Common System Area (CSA) storage below the 16MB line in use when the last sampling interval ended. The format is an integer.

Device Count The number of devices defined for the TCP/IP stack. The format is an integer.

Note: If the address space being monitored is running on z/OS v1.11 or earlier, these attributes are retrieved using SNMP. If the address space being monitored is running on z/OS v1.12 or later, these attributes are retrieved using the z/OS Communications Server callable network management interface (NMI).

Fragmentation Count The number of IP segments requiring fragmentation that was successfully fragmented. The format is an integer.

Note: Segments require fragmentation when they are too large for the next network hop.

Fragmentation Failure Percentage The percentage of IP segments requiring fragmentation that was not successfully fragmented. The range for this value is from 0% to 100%.

Fragmentation Failures The number of IP segments requiring fragmentation that was not successfully fragmented. The format is an integer.

Fragmentation Percentage The percentage of IP segments successfully fragmented since TCP/IP initialization. The range for this value is from 0% to 100%.

Gateway Count The number of gateways defined for the TCP/IP stack. Gateways are routers to other physical networks. The format is an integer.

Host IP Address The IP address of the host. The format is a text string no longer than 45 characters.

Host IP Address (IPv4 only) The IP address of the host. The format is a 15 character string. This attribute value is set only if the character representation of the host's IP address fits within 15 characters. This attribute is not displayed by default.

Host Name The host name of the TCP/IP stack. The format is an alphanumeric string no longer than 255 characters.

Input Discard Percentage The percentage of IP segments this TCP/IP address space received from the network that was undeliverable and therefore discarded. The range for this value is from 0% to 100%.

Input Discards The number of IP segments this TCP/IP address space received that was undeliverable and therefore discarded since TCP/IP initialization. The format is an integer.

Reasons for discarding input segments include

- Hardware errors
- Addressing errors
- Unknown protocols

Input Packet Count The number of IP packets, including those found in error, that this TCP/IP address space received from the network since TCP/IP initialization. When the value in the **Input Packet Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Input Packet Count (In G)** field and the remainder is stored in the **Input Packet Count** field. The format is an integer.

Input Packet Count (In G) (deprecated) The number of IP packets (including those received in error) that this TCP/IP address space received from the network since TCP/IP initialization, divided by 1,073,741,824. When the value in the Input Packet Count field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the Input Packet Count (in G) field and the remainder is stored in the Input Packet Count field. The format is an integer.

Interface Count The number of interfaces defined for the TCP/IP stack. The format is an integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Output Discard Percentage The percentage of all IP output segments from this TCP/IP address space that was undeliverable and therefore discarded. The range for this value is from 0% to 100%.

Output Discards The number of IP segments this address space did not send and therefore discarded since TCP/IP initialization. The format is an integer.

Reasons for discarding output segments include

- No available routes
- Segment needs fragmentation, but the Do Not Frag Bit was set

Output Packet Count The number of IP packets that local IP user-protocols (including ICMP) supplied to IP since TCP/IP initialization. When the value in the **Output Packet Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Output Packet Count (In G)** field and the remainder is stored in the **Output Packet Count** field. The format is an integer.

Note: This count does not include any packets counted in **Input Datagrams Forwarded**.

Output Packet Count (in G) The number of IP packets that local IP user-protocols (including ICMP) supplied to IP since TCP/IP initialization, divided by 1,073,741,824. When the value in the **Output Packet Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Output Packet Count (in G)** field and the remainder is stored in the **Output Packet Count** field. The format is an integer.

Note: This count does not include any packets counted in **Input Datagrams Forwarded**.

Paging Rate The paging rate when the last sampling interval ended. The range for this value is from 0% to 100%.

Reassembly Count The number of IP segments received that was successfully reassembled since TCP/IP initialization. The format is an integer.

Reassembly Failure Count The number of IP segments requiring reassembly that was not reassembled since TCP/IP initialization. A reassembly fails when all segments that compose the fragmented datagram are not received. The format is an integer.

Reassembly Failure Percentage The percentage of IP segments requiring reassembly that was not reassembled. A reassembly fails when all segments that compose the fragmented datagram are not received. The range for this value is from 0% to 100%.

The percentage is calculated as follows:

(Reassembly Failure Pct) = (Reassembly Failures) divided by (Reassemblies Requested)

Reassembly Percentage The percentage of IP segments that was reassembled since TCP/IP initialization. The range for this value is from 0% to 100%.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCP Input Segment Count The count of TCP segments this TCP/IP address space received from the network since TCP/IP initialization. When the value in the **TCP Input Segment Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **TCP Input Segment Count (in G)** field and the remainder is stored in the **TCP Input Segment Count** field. The format is an integer.

TCP Input Segment Count (in G) The count of TCP segments this TCP/IP address space received from the network since TCP/IP initialization, divided by 1,073,741,824. When the value in the **TCP Input Segment Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **TCP Input Segment Count (in G)** field and the remainder is stored in the TCP Input Segment Count field. The format is an integer.

TCP Output Segment Count The count of TCP segments this TCP/IP address space delivered to the network since TCP/IP initialization. When the value in the TCP Output Segment Count field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **TCP Output Segment Count (in G)**field and the remainder is stored in the **TCP Output Segment Count** field. The format is an integer.

TCP Output Segment Count (in G) The count of TCP segments this TCP/IP address space delivered to the network since TCP/IP initialization, divided by 1,073,741,824. When the value in the **TCP Output**

Segment Count field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **TCP Output Segment Count (in G)** field and the remainder is stored in the **TCP Output Segment Count** field. The format is an integer.

TCP Retransmit Percentage The percentage of TCP segments that required retransmission. A TCP segment is retransmitted whenever the receiver does not acknowledge receipt, and a timeout occurs. The range for this value is from 0% to 100%.

The percentage is calculated as follows:

(TCP Retransmit Pct) = (Retransmitted TCP Segments) divided by (TCP Segments Out)

TCP Retransmitted Segments The number of TCP segments this host retransmitted since TCP/IP initialization. A segment is retransmitted whenever the receiver does not acknowledge receipt, and a timeout occurs. The format is an integer.

TCP Session Count The number of TCP sessions currently established to this TCP/IP address space. The format is an integer.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Telnet Pool Percentage The percentage of Telnet pool entries in use. The range for this value is from 0% to 100%.

Telnet Pool Size The number of entries in the Telnet pool. Each Telnet user is allocated one entry from the pool. When the pool is exhausted, no new Telnet sessions can be started. The format is an integer.

Telnet Session Count The number of Telnet pool entries in use. Each Telnet user is allocated one entry from the pool. When the pool is exhausted, no new Telnet sessions can be started. The format is an integer.

Total CSA Percentage The percentage of Common System Area (CSA) used when the last sampling interval ended. The range for this value is from 0% to 100%.

Total CSA Usage The total amount of Common System Area (CSA) used when the last sampling interval ended. The format is an integer.

UDP Discard Percentage The percentage of UDP datagrams discarded as undeliverable because they were received in error (including No Port Found errors). The range for this value is from 0% to 100%.

The percentage is calculated as:

(UDP Discard Pct) = (UDP No Port Errors + UDP Other Errors) divided by (UDP Datagrams Received)

UDP Input Datagram Count The number of UDP datagrams received since TCP/IP initialization. When the value in the **UDP Input Datagram Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **UDP Input Datagram Count (in G)** field and the remainder is stored in the **UDP Input Datagram Count** field. The format is an integer.

UDP Input Datagram Count (in G) The number of UDP datagrams received since TCP/IP initialization, divided by 1,073,741,824. When the value in the **UDP Input Datagram Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **UDP Input Datagram Count (in G)** field and the remainder is stored in the **UDP Input Datagram Count** field. The format is an integer.

UDP Input Errors The number of datagrams discarded as undeliverable because they were received in error (excluding No Port Found errors) since TCP/IP initialization. The format is an integer.

UDP No Port Count The number of UDP datagrams discarded as undeliverable because the port number specified did not match that of any active applications. The format is an integer.

UDP Output Datagram Count The number of datagrams this host sent since TCP/IP initialization. When the value in the **UDP Output Datagram Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **UDP Output Datagram Count (in G)** field and the remainder is stored in the **UDP Output Datagram Count** field. The format is an integer.

UDP Output Datagram Count (in G) The number of datagrams this host sent since TCP/IP initialization, divided by 1,073,741,824. When the value in the **UDP Output Datagram Count** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **UDP Output Datagram Count (in G)** field and the remainder is stored in the **UDP Output Datagram Count** field. The format is an integer.

zOS Release IBM internal use only.

TN3270 Response Time Buckets Attributes

Use the TN3270 Response Time Buckets attributes to view bucket counts and ranges for the TN3270 sessions from a remote TN3270 client to a z/OS TN3270 server.

Bucket Number A number in the range of 1-5 that identifies which response time bucket count is contained in this row. The format is an integer.

Bucket Range The range of response times that are counted in this bucket. The format is a string.

This range is expressed as a character string which shows the lower and upper bounds used to determine which bucket a response time was counted in. This range is expressed as one of the following (based on the Bucket Number value):

- 0 - [Bucket 1 Upper Boundary] msec
- [Bucket 1 Upper Boundary] - [Bucket 2 Upper Boundary] msec
- [Bucket 2 Upper Boundary] - [Bucket 3 Upper Boundary] msec
- [Bucket 3 Upper Boundary] - [Bucket 4 Upper Boundary] msec
- [Bucket 4 Upper Boundary] - [Bucket 5 Upper Boundary] msec
- > [Bucket 5 Upper Boundary] msec

Bucket Response Times Count A count of response times falling into the specified Bucket Number. The format is an integer.

Bucket Response Times Percent The percentage of the total number of response times falling into this bucket. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second

- m = Millisecond

Connection Number A unique number that identifies the connection to a TCP/IP stack. The format is an integer. This value is stored as an integer and displayed as a hexadecimal number.

Local IP Address The local IP address for this Telnet session. The format is an alphanumeric string no longer than 45 characters.

Local Port The local port for this Telnet session. The format is an integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Remote IP Address The remote IP address for this Telnet session. The format is an alphanumeric string no longer than 45 characters.

Remote Port The remote port for this Telnet session. The format is an integer.

SNA Application Name The LU name of the SNA application for this Telnet session. The format is an alphanumeric string no longer than 8 characters.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Telnet LU Name The LU name representing the client for this Telnet session. The format is an alphanumeric string no longer than 8 characters.

TN3270 Server Sess Avail Attributes

Use the TN3270 Server Session attributes to create situations that monitor TN3270 sessions from a remote TN3270 client to a z/OS TN3270 server.

Average IP Response Time The average IP response time over the last Response Times Collection Interval. This value is stored in milliseconds and displayed as a time value (for example, 4.17300s or 4m 20s).

Average SNA Response Time The average SNA response time over the last Response Times Collection Interval. This value is stored in milliseconds and displayed as a time value (for example, 4.17300s or 4m 20s).

Average Total Response Time The average total response time over the last Response Times Collection Interval. This value is stored in milliseconds and displayed as a time value (for example, 4.17300s or 4m 20s).

Average Transaction Count The sliding transaction count used for calculating the values of the Average Total Response Time, Average IP Response Time, and Average SNA Response Time. The format is an integer.

Bucket 1 Response Times Count The number of response times falling into Bucket 1. The format is an integer.

Bucket 1 Response Time Percent The percentage of total number of response times falling into Bucket 1. The range of this value is between 0 and 100%.

Bucket 1 Upper Boundary The range of transaction response times counted in Bucket 1, those less than or equal to this field. The format is an integer.

Bucket 2 Response Times Count The number of response times falling into Bucket 2. The format is an integer.

Bucket 2 Response Time Percent The percentage of total number of response times falling into Bucket 2. The range of this value is between 0 and 100%.

Bucket 2 Upper Boundary This field, together with Bucket 1 Upper Boundary, defines the range of transaction response times counted in Bucket 2: those greater than the value of Bucket 1 upper boundary and less than or equal to the value in this field. The format is an integer.

Bucket 3 Response Times Count The number of response times falling into Bucket 3. The format is an integer.

Bucket 3 Response Time Percent The percentage of total number of response times falling into Bucket 3. The range of this value is between 0 and 100%.

Bucket 3 Upper Boundary This field, together with Bucket 2 Upper Boundary, defines the range of transaction response times counted in Bucket 3: those greater than the value of Bucket 2 upper boundary and less than or equal to the value in this field. The format is an integer.

Bucket 4 Response Times Count The number of response times falling into Bucket 4. The format is an integer.

Bucket 4 Response Time Percent The percentage of total number of response times falling into Bucket 4. The range of this value is between 0 and 100%.

Bucket 4 Upper Boundary This field, together with Bucket 3 Upper Boundary, defines the range of transaction response times counted in Bucket 4: those greater than the value of Bucket 3 upper boundary and less than or equal to the value in this field. This field also defines the range of transaction response times counted in Bucket 5: those greater than this field. The format is an integer.

Bucket 5 Response Times Count The number of response times falling into Bucket 5. The format is an integer.

Bucket 5 Response Time Percent The percentage of total number of response times falling into Bucket 5. The range of this value is between 0 and 100%.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Connection Number A unique number that identifies the connection to a TCP/IP stack. The format is an integer. This value is stored as an integer and displayed as a hexadecimal number.

Data Source Level Identifies the data that is available on the monitored system. The format is an integer. It is displayed as a hexadecimal number. Valid values are:

- 0 = Data available with the original z/OS Communications Server network management interface (NMI) enhancements.

- 1 = Data available with z/OS Communications Server V1.8 network management interface (NMI) enhancements if you have defined the buckets and monitoring group in your TCP/IP profile. For this table, sliding window and bucket count data are available.

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

Definite Responses Detected The number of definite responses or timemarks detected for monitoring purposes. The format is an integer.

IP Response Time Standard Deviation The standard deviation for IP round trip times. The format is an integer.

Variance and standard deviation of response time averages help you understand the dispersion of the response time data. The variance is a measure of how spread out the data is. The square root of the variance is the standard deviation. Knowing the standard deviation allows you make assumptions based on normal distribution. For more information, see the *IBM z/OS Communications Server: IP Configuration Guide*.

IP Response Time Variance The variance of IP round trip response times. The format is an integer.

Variance and standard deviation of response time averages help you understand the dispersion of the response time data. The variance is a measure of how spread out the data is. The square root of the variance is the standard deviation. Knowing the standard deviation allows you make assumptions based on normal distribution. For more information, see the *z/OS Communications Server: IP Configuration Guide*.

Local IP Address The local IP address for this Telnet session. The format is an alphanumeric string no longer than 45 characters.

Local Port The local port for this Telnet session. The format is an integer.

Local Port String The local port for this Telnet session as a string. The format is a string up to five characters in length.

Logmode Name The VTAM logmode. The format is an alphanumeric string no longer than 8 characters.

In an open row, this data is not available. Blanks are displayed.

LU Selection Method The method that was used to select the LU. This value is stored as an integer and displayed as a string. The valid values for LU Selection Method are:

- 0 = Chosen by server
- 1 = Chosen by client
- 9 = Unknown

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Remote IP Address The remote IP address for this Telnet session. The format is an alphanumeric string no longer than 45 characters.

Remote Port The remote port for this Telnet session. The format is an integer.

Remote Port String The remote port for this Telnet session as a string. The format is a string up to five characters in length.

Response Time Collection Time The date and time that the Average Total Response Time, Average IP Response Time, Average SNA Response Time, and Average Transaction Count were calculated by z/OS. The format is an alphanumeric string.

Response Time Standard Deviation The standard deviation for round trip times. The format is an integer.

Variance and standard deviation of response time averages help you understand the dispersion of the response time data. The variance is a measure of how spread out the data is. The square root of the variance is the standard deviation. Knowing the standard deviation allows you make assumptions based on normal distribution. For more information, see the *IBM z/OS Communications Server: IP Configuration Guide*.

Response Time Variance The variance of round trip response times. The format is an integer.

Variance and standard deviation of response time averages help you understand the dispersion of the response time data. The variance is a measure of how spread out the data is. The square root of the variance is the standard deviation. Knowing the standard deviation allows you make assumptions based on normal distribution. For more information, see the *IBM z/OS Communications Server: IP Configuration Guide*.

Session End The date and time when this session ended. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

When the session is active, this value is stored as a character string of zeros and displayed as blank.

Session Indicator Indicates whether the Telnet connection has a session with an application and the status of the session. This value is stored as an integer and displayed as a string. The following values are valid:

- 0 = None
- 1 = Active
- 2 = Completed

Session Start The date and time when this session started. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Session Type The session type. While a TN3270 session is active, the Session Type attribute always displays as Unknown if the session is not monitored by means of a MONITORGROUP definition. At session termination, more granular descriptions of the Session Type are available and will be updated to reflect the session's type. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Unknown
- 1 = TN3270
- 2 = TN3270E
- 3 = Linemode
- 4 = DBCSTransform
- 5 = Binary

SNA Application Name The LU name of the SNA application for this Telnet session. This is not the fully qualified name. The format is an alphanumeric string no longer than 8 characters.

SNA Response Time Standard Deviation The standard deviation for SNA round trip times. The format is an integer.

Variance and standard deviation of response time averages help you understand the dispersion of the response time data. The variance is a measure of how spread out the data is. The square root of the variance is the standard deviation. Knowing the standard deviation allows you make assumptions based on normal distribution. For more information, see the *IBM z/OS Communications Server: IP Configuration Guide*.

SNA Response Time Variance The variance of SNA round trip response times. The format is an integer.

Variance and standard deviation of response time averages help you understand the dispersion of the response time data. The variance is a measure of how spread out the data is. The square root of the variance is the standard deviation. Knowing the standard deviation allows you make assumptions based on normal distribution. For more information, see the *IBM z/OS Communications Server: IP Configuration Guide*.

SSL Status The Secure Sockets Layer (SSL) status for the session. This value is stored as an integer and displayed as a string. While a TN3270 session is active, the SSL status will show as either SECURE, NON_SSL, or Unknown. The SECURE and NON_SSL statuses are only available if the session is monitored by means of a MONITORGROUP definition. At session termination, more granular descriptions of the SSL status are available and the SECURE session's status will be updated to reflect the session's status. The valid values are:

- 0 = NON_SSL
- 1 = SERVER_AUTH
- 2 = NO_SAF
- 3 = SAF
- 9 = Unknown

- 128 = SECURE. This is an interim state that can be displayed while a session or connection is active. The session termination record updates the rows with more granular security information when the session or connection ends.

State The status of this TN3270 sever session. This value is stored as an integer and displayed as a number. Valid values are:

- **0** Unknown - In the history file, the value was Active during historical collection.
- **1** Inactive - A close record was received for this open record.
- **2** Active - No close record was received.
- **4** Complete - The record was closed.

Sysplex Name The name of the sysplex that the monitored system is part of. The format is a string of up to 8 characters.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Telnet LU Name The LU name representing the client for this Telnet session. The format is an alphanumeric string no longer than 8 characters.

TN3270 Server Name The TN3270 Server job name. The format is an alphanumeric string.

Total Bytes The number of bytes sent or received by the server for this session. The format is a long long integer.

Total Bytes (deprecated) The total number of bytes (both received and sent) by the server for this session, as an integer. When the value in the **Total Bytes** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes (in GB)** field and the remainder is stored in the **Total Bytes** field. The format is an integer.

Total Bytes (in GB) (deprecated) The total number of bytes (both received and sent) by the server for this session, divided by 1,073,741,824. When the value in the **Total Bytes** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes (in GB)** field and the remainder is stored in the Total Bytes field. The format is an integer.

Total Bytes Received The number of bytes received by the server for this session. The format is a long long integer.

Total Bytes Received (deprecated) The total number of bytes received by the server for this session, as an integer. When the value in the Total Bytes Received field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Received (in GB)** field and the remainder is stored in the **Total Bytes Received** field. The format is an integer.

Total Bytes Received (in GB) (deprecated) The total number of bytes received by the server for this session, divided by 1,073,741,824. When the value in the **Total Bytes Received** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Bytes Received (in GB)** field and the remainder is stored in the **Bytes Received** field. The format is an integer.

Total Bytes Sent The number of bytes sent by the server for this session. The format is a long long integer.

Total Bytes Sent (deprecated) The total number of bytes sent by the server for this session, as an integer. When the value in the **Total Bytes Sent** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Sent (in GB)** field and the remainder is stored in the **Total Bytes Sent** field. The format is an integer.

Total Bytes Sent (in GB) (deprecated) The total number of bytes sent by this server for this session, divided by 1,073,741,824. When the value in the **Total Bytes Sent** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Sent (in GB)** field and the remainder is stored in the **Total Bytes Sent** field. The format is an integer.

Total Transactions Detected The count of the total number of transactions detected. The format is an integer.

UDP Connections Attributes

Use the UDP Connections attributes to view and filter TCP/IP stack UDP connections.

Application Name The job name associated with the application address space that opened and bound the socket. The format is a string up to 8 characters in length.

ASID The z/OS address space ID of the address space that opened the socket. This value is displayed as a 4-digit hexadecimal number.

Byte Rate The number of bytes sent or received, per minute, during the most recent time interval. The format is an integer.

Bytes Received The number of bytes received during the most recent time interval. The format is an integer.

Bytes Sent The number of bytes sent during the most recent time interval. The format is an integer.

Bytes Sent or Received The number of sent or received bytes during the most recent time interval. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Connection Start Time The time and date when this connection was created. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year

- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Datagram Rate The number of datagrams, per minute, transmitted to or from the connection during the most recent time interval. The format is an integer.

Datagrams Discarded The number of datagrams received that was discarded, because of queue limits, during the most recent time interval. The format is an integer.

Datagrams Queued The number of datagrams on the read queue. The format is an integer.

Datagrams Received The total number of datagrams the local port received during the most recent time interval. The format is an integer.

Datagrams Sent The total number of datagrams the local port sent during the most recent time interval. The format is an integer.

Datagrams Sent or Received The total number of datagrams sent or received on the local port during the most recent time interval. The format is an integer.

Hex Connection Number The hexadecimal representation of the connection number. The format is an 8-digit hexadecimal string.

Inbound Queued Data Time Stamp The time stamp of oldest queued data to receive. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour

- M = Minute
- S = Second
- m = Millisecond

Last Activity Time Stamp The last time of connection activity. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Local IP Address The local IP address for this connection. A value of 0.0.0.0 in this field indicates that the UDP endpoint accepts datagrams from any local IP address. The format is an string up to 45 characters in length.

Local Port The local port for this connection. The format is an integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters.

Percent Datagrams Discarded The percentage of datagrams received that was discarded, because of queue limits, during the most recent time interval. The range for this value is 1 to 100%.

Queued Datagram Bytes The number of data bytes on the read queue. The format is an integer.

Receive Byte Rate The number of bytes received, per minute, during the most recent time interval. The format is an integer.

Receive Datagram Rate The number of datagrams received, per minute, during the most recent time interval. The format is an integer.

Receive Datagram Size Limit The maximum receive datagram size. The format is an integer.

Receive Queue Limit (Bytes) The maximum number of data bytes allowed on the read queue. The format is an integer.

Receive Queue Limit (Datagrams) The maximum number of datagrams allowed on the read queue. The format is an integer.

Remote IP Address The remote IP address for this connection. The format is an string up to 45 characters in length.

Remote Port The remote port for this connection. The format is an integer.

Send Datagram Size Limit The maximum transmit datagram size. The format is an integer.

System ID The SMF system ID. The format is a string up to 4 characters in length.

TCPIP STC Name The TCP/IP job name. The format is a string up to 8 characters in length.

Total Bytes The total number of bytes sent and received since the UDP endpoint started. The format is a long long integer.

Total Bytes (deprecated) The total number of bytes sent and received since the UDP endpoint started. When the value in the **Total Bytes** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes (in GB)** field and the remainder is stored in the **Total Bytes** field. The format is an integer.

Total Bytes (in GB) (deprecated) The total number of bytes sent and received since the UDP endpoint started, divided by 1,073,741,824. When the value in the **Total Bytes** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes (in GB)** field and the remainder is stored in the **Total Bytes** field. The format is an integer.

Total Bytes Received The total number of bytes received since the UDP endpoint started. The format is a long long integer.

Total Bytes Received (deprecated) The total number of bytes received since the UDP endpoint started. When the value in the **Total Bytes Received** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Received (in GB)** field and the remainder is stored in the **Total Bytes Received** field. The format is an integer.

Total Bytes Received (in GB) (deprecated) The total number of bytes received since the UDP endpoint started, divided by 1,073,741,824. When the value in the **Total Bytes Received** field exceeds 1,073,741,823 (1 GB), the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Received (in GB)** field and the remainder is stored in the **Total Bytes Received** field. The format is an integer.

Total Bytes Sent The total number of bytes sent since the UDP endpoint started. The format is a long long integer.

Total Bytes Sent (deprecated) The total number of bytes sent since the UDP endpoint started. When the value in the Total Bytes Sent field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Sent (in GB)** field and the remainder is stored in the **Total Bytes Sent** field. The format is an integer.

Total Bytes Sent (in GB) (deprecated) The total number of bytes sent since the UDP endpoint started, divided by 1,073,741,824. When the value in the **Total Bytes Sent** field exceeds 1,073,741,823, the number is divided by 1,073,741,824. The quotient is stored in the **Total Bytes Sent (in GB)** field and the remainder is stored in the **Total Bytes Sent** field. The format is an integer.

Total Datagrams The total number of datagrams the connection sent or received since the connection started. The format is an integer.

Total Datagrams Received The number of datagrams the connection received since the connection started. The format is an integer.

Total Datagrams Sent The total number of datagrams the connection sent since the connection started. The format is an integer.

Transmit Byte Rate The number of bytes transmitted, per minute, during the most recent time interval. The format is an integer.

Transmit Datagram Rate The number of datagrams transmitted, per minute, during the most recent time interval. The format is an integer.

VTAM Address Space Attributes

Use the VTAM Address Space attributes to monitor information for a selected VTAM host.

CDRM Manager The name of the cross-domain resource manager (CDRM). The CDRM is the part of a system services control point (SSCP) that supports cross-domain session setup and takedown. The format is an alphanumeric string.

Collection Interval The time between successive samples; the sampling interval. This value is expressed as a whole number between 1 and 60, indicating the collection interval in minutes. The Collection Interval was set in the Configuration Tool SPECIFY VTAM APPLID VALUES panel by specifying a value for the "SNA data collection interval" field or in PARMGEN using the KN3_SNA_VTAM_SNAC_SNACINTV parameter.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

CPU Percentage The percentage of CPU in use when the sampling interval ended. The range for this value is from 0% to 100%.

CSA Below 16MB High Water Mark The maximum amount of Common System Area (CSA) below the 16MB line used by VTAM since the last CNM RU. This value is displayed in bytes.

CSA Below 16MB High Water Mark Timestamp The timestamp of the largest value for CSA below 16MB line usage by VTAM since the last CNM RU was sent to VTAM. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

CSA Below 16MB Low Water Mark The lowest amount of CSA below the 16MB line used by VTAM since the last COLLECT CNM RU. The value is displayed in bytes.

CSA Below 16MB Low Water Mark Timestamp The timestamp of the smallest value for CSA below 16MB line usage by VTAM since the last CNM RU was sent to VTAM. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

CSA Currently Allocated The total amount of Common System Area (CSA) used when the last sampling interval ended. The format is an integer.

CSA High Water Mark The largest amount of total CSA (CSA below the 16MB line plus Extended CSA) used by VTAM since the last COLLECT CNM RU. The value is displayed in bytes.

CSA High Water Mark Timestamp The timestamp of the largest value for total CSA usage by VTAM since the last CNM RU was sent to VTAM. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year

- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

CSA Low Water Mark The lowest amount of total CSA (CSA below the 16MB line plus Extended CSA) used by VTAM since the last COLLECT CNM RU. The value is displayed in bytes.

CSA Low Water Mark Timestamp The timestamp of the smallest value for total CSA usage by VTAM since the last CNM RU was sent to VTAM. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

CSA Percent Below 16MB The percentage of CSA storage below the 16MB line in use at the end of the most recent sampling interval. The range for this value is from 0% to 100%.

CSA Percentage The percentage of CSA used when the most recent sampling interval ended. The range for this value is from 0% to 100%.

CSA Usage Below 16MB Currently Allocated The amount of CSA storage below the 16MB line in use when the most recent sampling interval ended. The format is an integer.

CTC SIO Per Sec The SIO rate for all channel to channel adapters (CTCAs) over the most recent sample interval. The rate is expressed as SIOs per second. The format is an integer.

Current Private Storage Allocated The current private storage allocated to the VTAM address space. This value is expressed as an integer.

DASD SIO Per Sec The SIO rate for all DASD devices over the most recent sample interval. The rate is expressed as SIOs per second. The format is an integer.

Local SNA SIO Per Sec The SIO rate for all local SNA controllers over the most recent sample interval. The rate is expressed as SIOs per second. The format is an integer.

Local Non-SNA SIO Per Sec The SIO rate for local non-SNA devices over the most recent sample interval. The rate is expressed as SIOs per second. The format is an integer.

Max CSA Allowed The maximum amount of total CSA (CSA below the 16MB line plus Extended CSA) that VTAM can use in bytes. The format is an integer.

The CSALIMIT start option in SYS1.VTAMLST(ATCSTRnn) sets this value. If you code CSALIMIT=0, allow CSALIMIT to default to 0, or code a value for CSALIMIT that exceeds the amount of available CSA, no limit is enforced on the amount of total CSA used by VTAM.

Max CSA Below 16MB Allowed The maximum amount of CSA below the 16MB line that can be used by VTAM. The CSA2 start option in SYS1.VTAMLST(ATCSTRnn) sets this value. The value displays in bytes. If the user codes a value of 0 or an invalid value in the ATCSTRxx startup parms, a value of 16777215 is shown (which is 16M -1).

Max CSA Below 16MB Used The maximum CSA below the 16MB line used since VTAM initialization. The format is an integer.

Max CSA Used The value of maximum total CSA used since VTAM initialization. The format is an integer.

Max Private Storage Allocated The maximum private storage allocated to the VTAM address space since VTAM initialization. This value is expressed as an integer.

NCP SIO Per Sec The SIO rate for all NCPs over the most recent sample interval. The rate is expressed as SIOs per second. The format is an integer.

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Other SIO Per Sec The SIO rate for all other devices over the most recent sample interval. The rate is expressed as SIOs per second. The format is an integer.

Paging Rate The paging rate when the most recent sampling interval ended. The range for this value is from 0% to 100%.

SIO Rate Pct of System The relative percentage of the VTAM SIO rate compared against the overall system SIO rate. The range for this value is from 0% to 100%.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

VTAM NetID The VTAM Network ID. The format is an alphanumeric string no longer than 8 characters.

VTAM STC Name The VTAM job name. The format is an alphanumeric string no longer than 8 characters.

VTAM Version The VTAM version. The format is an alphanumeric string no longer than 8 characters.

VTAM Buffer Pool Attributes

Use VTAM Buffer Pool attributes to create situations for monitoring performance data related to VTAM buffer pools.

VTAM uses buffer pools to control the buffering of data. It dynamically allocates and de-allocates space in these buffer pools for the VTAM control blocks, I/O buffers, and channel programs that control the transmission of data. When you tune a buffer pool, you optimize the trade-off between CPU usage and the amount of storage allocated for a pool. If you specify a large buffer pool, you might waste storage but conserve CPU usage. If you specify a small pool, you might conserve storage but use the CPU for frequent expansion and contraction. With proper tuning, you can achieve a balance between storage use and performance that is suitable for your system.

Active Extents The current number of active extents. The format is an integer. When dynamic expansion is enabled, then VTAM creates an extent each time it expands the buffer pool. An extent remains active as long as any of its buffers are in use. An extent becomes inactive when VTAM frees the group of pages in that extent to contract the buffer pool.

Available Buffers in Extents The total number of available buffers residing in all active extents. The format is an integer.

Base Buffer Allocation The base number of buffers defined at VTAM initialization. The format is an integer.

This base number of buffers is defined as the number of buffers allocated for the static portion of the buffer pool at VTAM startup. This number is specified in the VTAM start options (for example, SYS1.VTAMLST(ATCSTRxx)). To determine what this number should be, compare the base allocation to the total number of buffers in use. If the total number of buffers in use is consistently greater than the base allocation, consider increasing the base allocation to avoid excessive buffer pool expansion and contraction.

Buffer Pool Fetch Protected Storage Specifies whether storage for this buffer pool is fetch protected. Valid responses for this field are:

- **Yes** this buffer is fetch protected
- **No** this buffer is not fetch protected

Fetch protection limits access to sensitive data by unauthorized programs in the system. To manage real storage, z/OS associates a storage protection key with each page and with the program status word (PSW).

Generally, if both keys match, the program can read or write on the page. If the keys do not match, the program can read the page only if the fetch protection bit is off. If the fetch protection bit is on and the keys do not match, a program exception occurs. Generally, if a program executes with a PSW key of zero, it can read or write to the page regardless of its fetch protection status.

Buffer Pool Fixed Storage Specifies whether the buffer pool storage is fixed or pageable. Valid responses for this field are:

- Fixed
- Pageable

Programs and data are always allocated in virtual storage, which is then mapped to real storage when accessed by a program. Pageable storage frames can reside on DASD and be paged in as needed. Although paging delays access to the storage and slows the program, it conserves real storage. Fixed storage frames are always resident in real storage; the program can access the data without a page in operation. However, when more fixed frames are in use, less real storage is available for any frames that must be paged in.

In most cases, using fixed storage for certain pools helps overall response time and is worth the cost of real storage.

Buffer Pool Name The name of the VTAM buffer pool. This value is displayed as a one of these character strings:

- IO00 - Input/Output message storage pool
- LP00 - Large pageable storage pool 2K buffers
- CRPL - Copied RPL storage pool
- SP00 - Small pageable storage pool
- LF00 - Large fixed storage pool
- SF00 - Small fixed storage pool
- AP00 - Buffer pool below the 16MB line
- XD00 - Pool XDBUF provides common storage for the I/O buffers used in exchange ID (XID) contact processing

- BS00 - Pool BSBUF provides common storage for the boundary Type 2.1, Type 2, and Type 1 peripheral node session control blocks
- CRA4 - Large pageable storage 4k buffers
- CRA8 - Large pageable storage 8k buffers
- TI00 - Input/Output control areas
- T100 - Input/Output control areas, including packing area for iQDIO
- T200 - Input/Output control areas, including a larger packing area than T100

Buffer Pool Subpool The z/OS subpool number from which buffer pool storage is allocated. The format is an integer.

This field displays the number of the z/OS subpool in which the storage is allocated. The number indicates the subpool's specific characteristics, as defined by z/OS.

Buffer Size The size of each buffer in the pool (in bytes). The format is an integer.

You can define the buffer size for the IO00 buffer pool only; VTAM sets all other buffer sizes.

VTAM determines the buffer size by taking the size, rounding it to a doubleword boundary, and adding a 16-byte header. VTAM also adds an additional 55-byte header to the buffers in the I/O pool.

Buffers Available The total number of available buffers in the named pool. The format is an integer.

This field displays the number of buffers that are not being used. These buffers can be allocated as required. VTAM determines the condition of the buffer pool based on this value.

Buffers For Queued Requests The number of available buffers that would be necessary to satisfy the currently queued storage requests. The format is an integer.

Buffers In Use The total number of buffers in the pool that are allocated and in use. The format is an integer. The number is less than or equal to the total number of buffers in the pool.

Buffers Over Expansion The number of available buffers over the expansion threshold. The format is an integer. If dynamic expansion is enabled and the number of buffers falls below the expansion threshold, the pool will expand. The expansion threshold is specified in the VTAM start options (for example, SYS1.VTAMLST(ATCSTRxx)).

Buffers Over Slowdown The number of available buffers over the slowpoint threshold. The format is an integer. A zero indicates that the buffer is currently in slowdown mode. The slowdown threshold is specified in the VTAMLST data set.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day

- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Contraction Threshold The point at which dynamic contraction occurs. The format is an integer. If the number of available buffers is greater than this value, VTAM attempts to contract the buffer pool.

To do this, VTAM locates an inactive extent and frees its pages. VTAM frees the pages in an extent as a group; an extent remains active and allocated as long as any of its buffers are in use.

Expansion Size (Buffers) The number of buffers that VTAM will allocate to each new extent if dynamic expansion is enabled. The format is an integer.

Dynamic expansion expands and contracts the buffer pool as needed to satisfy the demands of VTAM processes. The actual value reflects the number of buffers in each extent after VTAM rounds the value to full pages. For example, if 30 buffers fit on one page of storage and XPANNO is specified as 32, each extent will contain 2 pages of 30 buffers each.

Expansion Size (Bytes) The number of bytes VTAM will allocate to each new extent if dynamic expansion is enabled. The format is an integer.

Expansion Threshold The point at which dynamic expansion occurs. If the number of available buffers is equal to or less than this value, VTAM expands the buffer pool. The format is an integer.

Expansion Threshold Flag Specifies whether the Buffers Available is less than or equal to the Expansion Threshold. Valid responses for this field are:

- **Yes** the Buffers Available setting is less than or equal to the Expansion Threshold.
- **No** the Buffers Available setting is greater than the Expansion Threshold.

IO Buffer Expansion Limit The maximum number of buffers allowed in the buffer pool. The format is an integer.

This field displays the maximum number of buffers allowed for IOBUF. It sets a limit on the amount of CSA that VTAM may use for IOBUF expansions. This number is calculated by VTAM from XPANLIM value specified in IOBUF statement in ATCSTRxx member of SYS1.VTAMLST library.

When calculating VTAM takes into account how many buffers fit on a page. If XPANLIM is not specified in buffer definition or is coded 0, buffer expansion is not limited, and the value 2,147,483,647 is displayed in the field.

IO Expansion Limit Percent The percentage of the total number of I/O buffers compared to expansion limit (xpanlim). The format is an integer.

Max Bytes Allocated The maximum number of bytes allocated since last COLLECT CNM RU command was sent. The format is an integer.

Max Requests Queued The maximum number of queued requests since the last COLLECT CNM RU command was sent. The format is an integer.

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Pool Status The current buffer pool status. The format is an integer. The current buffer pool status can be one of the following:

- **Slowdown**, meaning the number of available buffers is below than the defined slowdown point and expansion is not allowed
- **Expanded**, meaning that the buffer pool has been dynamically expanded
- **Normal**, meaning that dynamic expansion is enabled or and the pool has been neither expanded nor contracted
- **Contracted**, meaning that the buffer pool has been dynamically contracted

Pool Thrashing This column indicates whether the buffer pool is thrashing. The format is a string. Valid responses for this field are:

- **Yes** - The buffer pool is thrashing.
- **No** - The buffer pool is not thrashing.

Queued Requests The number of storage requests that are currently queued (RPHs). The format is an integer.

VTAM honors requests for storage dynamically, as permitted by buffer availability. If buffers are not available, VTAM queues the requests until enough storage is available.

Slowdown Threshold The slowdown threshold value. The format is an integer. If the number of available buffers in the pool is equal to or less than this value the buffer pool enters slowdown mode.

Slowdown mode queues all non-priority requests for buffers and stops the flow on a virtual route. To avoid slowdown mode, increase the XPANPT value.

Static Buffers Available The number of buffers from the base allocation that are currently available. The format is an integer.

Storage Allocated Below 16MB Line Specifies whether storage for this buffer pool is allocated below the 16MB line. Valid responses for this field are:

- **Yes** this buffer pool is allocated below the 16MB line.
- **No** this buffer pool is not allocated below the 16MB line.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

Times Expanded If dynamic expansion is enabled, this field displays the number of pool expansions since the last SMS trace record was written. The format is an integer.

If the SMS trace has not been used, this field displays the number of expansions since VTAM was last started.

Total Buffers The total number of buffers currently in the pool. The format is an integer.

If dynamic expansion is enabled, this number may change and will include the base allocation as well as any dynamic allocation.

If dynamic expansion is not enabled, this field displays a constant value equal to the base allocation.

User Specified Base Buffers The user-defined value for the base number of buffers in the buffer pool (BASENO). This is the value coded in the ATCSTRxx member of SYS1.VTAMLST library. The format an integer.

User Specified Expansion Buffers The user-defined value for the number of buffers VTAM is allowed to acquire when expanding the buffer pool (XPANNO). This is the value coded in the ATCSTRxx member of SYS1.VTAMLST library. The format is an integer.

VTAM Buffer Pool Extents Attributes

Use the VTAM Buffer Pool Extents attributes to display the characteristics and status of the buffer pool extents.

Buffer Pool Name The name of the VTAM buffer pool. This value is displayed as a one of these character strings:

- IO00 - Input/Output message storage pool
- LP00 - Large pageable storage pool 2K buffers
- CRPL - Copied RPL storage pool
- SP00 - Small pageable storage pool
- LF00 - Large fixed storage pool
- SF00 - Small fixed storage pool

- AP00 - Buffer pool below the 16MB line
- XD00 - Pool XDBUF provides common storage for the I/O buffers used in exchange ID (XID) contact processing
- BS00 - Pool BSBUF provides common storage for the boundary Type 2.1, Type 2, and Type 1 peripheral node session control blocks
- CRA4 - Large pageable storage 4k buffers
- CRA8 - Large pageable storage 8k buffers
- TI00 - Input/Output control areas
- T100 - Input/Output control areas, including packing area for iQDIO
- T200 - Input/Output control areas, including a larger packing area than T100

Buffers Per Extent The number of buffers in the extent. The format is an integer.

Bytes Per Buffer The number of bytes per buffer. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

End Address The ending address of the buffer pool extent. The format is a hexadecimal address.

Extent Block Address The pointer to the PXB control block. The format is a hexadecimal address.

Extent Number The relative extent number. The number starts at 1 and is incremented by 1 for each subsequent Pool Extension Block (PBX) on the chain. The format is an integer.

Free Buffers The number of free buffers in the extent. The format is an integer.

Pages Per Extent The number of pages per extent. The format is an integer.

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Percent Used The buffer utilization percentage. The format is an integer.

Start Address The address where the buffers begin in virtual storage for that extent. The format is a hexadecimal address.

Status The status of the extent. An extent is active as long as any its buffers are in use. An extent becomes inactive when VTAM frees the pages in that extent as a group. VTAM does not delete an inactive Pool Extension Block (PBX) but retains it for future reuse. Valid responses for this field are:

- Inactive
- Active

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

VTAM Buffer Usage by Address Space Attributes

Use the VTAM Buffer Usage by Address Space attributes to determine buffer pool utilization by address space.

Address Space Name Name of the address space. The format is an 8-character alphanumeric string.

Buffer Pool Name The name of the VTAM buffer pool. This value is displayed as one of these character strings:

- IO00 - Input/Output message storage pool
- CRPL - Copied RPL storage pool

Buffers The number of buffers used by the address space. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Percent Usage The percentage of buffer pool utilization by the address space. The format is an integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

VTAM Buffer Usage By Application for Address Space Attributes

Use the VTAM Buffer Pool Usage By Application for Address Space attributes to determine the usage of IO00 buffer pools by application logical unit (LU) name for the designated single address space. An address space can be a batch job, started task, or TSO user.

Address Space Name Name of the address space. The format is an 8-character alphanumeric string.

Applid Name of an application logical unit (LU) that appears as the origin or destination element in one or more buffers currently in use by this address space. The format is an 8-character alphanumeric string.

Buffer Pool Name The name of the VTAM buffer pool. This value is always IO00 in this attribute group.

Buffers The number of buffers used by the applid. The format is an integer.

This field contains the number of buffers in which the application LU appears as either an origin or destination element. OMEGAMON examines the PIU within each IO00 buffer currently in use by this address space. From the PIU, OMEGAMON determines the origin and destination element addresses which are then used to determine the element names. This field contains the number of buffers in which this application LU was found.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Percent Usage The relative percentage of buffers used by the particular APPLID relative to the total number of buffers in use by the address space. The format is an integer.

This field contains the number of buffers in which this application LU appears as either an origin or destination element, expressed as a percentage of the total number of buffers currently in use by this address space. The number of buffers is shown in the **Buffers** column

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

VTAM Buffer Usage By Category Attributes

Use the VTAM Buffer Pool Usage By Category attributes to monitor the usage of the IO00 buffer pool based on contents.

The IO00 buffer pool manages the storage of all network input/output messages sent from application programs and across channel connections. All network traffic passes through this pool, regardless of its destination. This buffer pool also contains channel programs used to service locally attached devices.

Because a great deal of activity takes place in the IO00 buffer pool, it is very sensitive to dynamic fluctuations in traffic rates. Consequently, it is a prime candidate for tuning. Examining the contents of this buffer pool can help a network capacity planner plan for more common storage area (CSA), understand how applications are using the pool, and understand the network traffic activity.

The values reported in this attribute table are obtained by processing the contents of the buffers themselves, and the VTAM control blocks are examined to determine which of the two categories each of the buffers in the IO00 pool is to be associated with.

Buffer Pool Category The VTAM IO00 buffer pool usage category. Valid responses are **User Category** or **User Category 2**. Use the information below to determine the types of buffers in each user category:

User Category: Each buffer in the IO00 buffer pool is examined to determine if it falls into each of the following areas.

- Unallocated buffers
- Read channel program buffers
- Buffers with a Transmission Subsystem Control Block (TSCB)
- Miscellaneous category consisting of buffers that do not meet any of the criteria of the previously listed categories

The relative percentage of buffers for each of these categories is calculated and displayed.

User Category 2: Each buffer in the IO00 Buffer Pool which contains a TSCB is examined to determine if it falls into each of the following areas.

- SSCP traffic
- Virtual route pacing response traffic
- APPL(PLU) to same subarea resource traffic
- APPL(PLU) to a different subarea resource traffic
- APPL(SLU) to a different subarea resource traffic
- Local SNA resource to a different subarea APPL traffic
- Local non-SNA to a different subarea
- Intermediate routing node traffic

The relative percentage of buffers for each of these categories is calculated and displayed.

Buffer Pool Name The name of the VTAM buffer pool. This value is always IO00 in this attribute group.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Description The description of the buffer based on the contents of the buffer. The format is an alphanumeric string no longer than 40 characters. This field can have the following values:

- **APPL (PLU) to Different Subarea Resource**: I/O buffers being used for traffic flowing between a primary logical unit (PLU) application and a secondary logical unit (SLU) source in another subarea.
- **APPL (PLU) to Same Subarea Resource**: I/O buffers being used for traffic flowing between a primary logical unit (PLU) application and a secondary logical unit (SLU) resource (both in this host).
- **APPL (SLU) to Different Subarea Resource:** I/O buffers being used for traffic flowing between a secondary logical unit (SLU) application on this host and a primary logical unit (PLU) application in another subarea.
- **Intermediate Routing Node Traffic:** I/O buffers being used for traffic flowing between two resources, neither of which is in this subarea
- **Local Non-SNA to Different Subarea APPL:** I/O buffers being used for traffic flowing between a local non-SNA terminal and an application in another subarea.
- **Local SNA to Different Subarea APPL:** I/O buffers being used for traffic flowing between a local SNA terminal and an application in another subarea.
- **Misc**: I/O buffers that could not be categorized. This number includes path information units (PIUs) that could not be classified because of state changes in VTAM, as well as channel programs (other than read).
- **Read Channel Programs:** I/O buffers being used to hold read channel programs. VTAM uses read channel programs to transfer data from the NCP or local cluster control units and perform a read channel operation. A read channel program consists of a string of channel command words (CCWs), each allocated at the beginning of an I/O buffer. VTAM transfers the data in blocks, each the size of an I/O Buffer.
- **SSCP Traffic**: I/O buffers being used for traffic to and from the System Services Control Point (SSCP). The SSCP provides resource management and control for the network. This field does not include the virtual route pacing response traffic.
- **TSCBs**: This is the total number of Transmission Subsystem Control Blocks (TSCBs) in the IO00 buffer pool. Each TSCB contains a Path Information Unit (PIU).
- **Unallocated Buffers**: Buffers currently unallocated and available.
- **Virtual Route Pacing Response Traffic:** I/O buffers being used for virtual route pacing responses (VRPRSs). A VRPRS flows in response to a request to send another full window of path information units (PIUs). If this value is high, the maximum window size might be too small. Or, there might be a large number of virtual routes defined and active.

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Percent Percentage of the described buffer (which is based on its content) relative to the other buffers within its user category. The format is an integer.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

VTAM IO Attributes

Use the VTAM IO attributes to retrieve additional I/O statistics for a selected VTAM address space.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Delta SIO Count The SIO count for one of the six types of SIOs over the last collection interval. The format is an integer.

Device The type of SIO. The format is a string. Possible SIO types are:

- DASD
- NCP
- CTC (channel to channel adapter)
- Local SNA (local SNA controllers)
- Local Non-SNA (all local non-SNA devices)
- Other (all other devices)

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Relative Frequency Distribution The relative distribution of one of the six types of SIO tracked. The format is an integer. Possible SIO types are:

- DASD
- NCP
- CTC (channel to channel adapter)
- Local SNA (local SNA controllers)
- Local Non-SNA (all local non-SNA devices)
- Other (all other devices)

SIOs per Second The SIO rate (number of SIOs per second) over the last collection period for one of the six types of SIOs tracked. The format is an integer. Possible SIO types are:

- DASD
- NCP
- CTC (channel to channel adapter)
- Local SNA (local SNA controllers)
- Local Non-SNA (all local non-SNA devices)
- Other (all other devices)

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

Total SIO Count The total SIO count for one of six types of SIOs tracked. The format is an integer.

VTAM Summary Statistics Attributes

Use the VTAM Summary Statistics attributes to create situations that monitor VTAM data, including Enterprise Extender (EE) connections, High Performance Routing (HPR) connections, and storage allocations.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss (Tivoli Enterprise Portal) or yy/mm/dd hh:mm:ss (3270)
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Maximum ECSA Storage Allowed The maximum number of Extended Common System Area (ECSA) storage, stored in kilobytes, allowed. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Number of Enterprise Extender Connections The number of Enterprise Extender connections that existed at the end of the most recent time interval. The format is an integer.

Number of High Performance Routing Connections The number of High Performance Routing (HPR) connections that existed at the end of the most recent time interval. The format is an integer.

Origin Node The unique identifier for the VTAM job being displayed. The format is an alphanumeric string no longer than 32 characters.

Storage Allocated Across DSP Pools The cumulative storage, stored in kilobytes, allocated across all Data Space Pool (DSP) pools. The format is an integer. The format is an integer. The default display units

is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

Storage Allocated Across ECSA Pools The cumulative storage, stored in kilobytes, allocated across all Extended Common System Area (ECSA) pools. The format is an integer. The default display units is kilobytes. The units may be specified as K for kilobytes, M for megabytes, G for gigabytes, or T for terabytes.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters.

Disk space requirements for historical data tables

You can calculate the amount of DASD required to support the persistent data store for storing historical data in Tivoli Data Warehouse.

This section provides the information you will need to determine space allocations in the persistent data store for each monitoring agent. Therefore, the disk space requirements in the tables in this section are for short-term history, which is stored on z/OS systems in the OMEGAMON XE persistent data store.

Network size and the type of network resources managed vary widely between enterprises. The amount and type of historical data that you choose to retain will greatly affect the amount of storage required. Wide differences between networks make it difficult to provide one size for the persistent data store that reflects the needs of most enterprises.

The default storage allocation is efficient for a very small network. Most users will need to allocate additional storage and data sets. Increase the default number of data sets from 3 to 5 or more. Increasing the number of data sets, using the **Group Count** parameter in the Control Program, is explained in the following section under "Allocating additional storage and data sets" on page 510.

This appendix provides you with the following information:

- Alternative methods for determining storage
- Effective allocation of additional storage and data sets (if needed)
- A list of attribute tables supported by short-term history
- Record size for each attribute table
- Worksheets to help you estimate the storage required

Note: If you are upgrading from V4.1 or 4.2 and did this exercise for one of these releases, it is recommended that you do it again for V5.1. The upgraded versions contain new attribute tables, and new attributes are included in existing tables.

Alternative methods of determining storage requirements

One way to determine the amount of DASD required for your persistent data is trial and error.

Many users who estimate the storage requirements for collecting historical data do it by trial and error. The main problems with this approach are twofold:

1. Every time you adjust storage parameters (number of cylinders and number of data sets), you must stop the agent. This might be unacceptable if implemented in a production network.
2. The network you use to determine storage parameters might not be comparable in size to the network where you will collect short-term history

If trial and error is not an acceptable approach in your environment, then you can use the information in this appendix to estimate storage size.

Trial and error approach
Use this information to understand how to effectively execute a trial and error approach for computing storage requirements.

About this task

To compute space requirements by trial and error, start historical collection for all resources you need to store in short-term history, and collect at least 25 hours of data. If you cannot draw a report containing the last 24 hours of data, for any attribute table, then you need to allocate additional storage or data sets or both.

If you are collecting short-term history, you can also create a rough estimate of the hours of measurement data you can store by looking in the RKPDLOG log of the IBM Z OMEGAMON Network Monitor monitoring agent. This log can be viewed from MVS/TSO in the SDSF Status window. To perform this estimate, do the following:

1. Examine the RKPDLOG log.
2. Record the elapsed time between the message:

   ```
   KPDIFIL: Initial output file selection completed successfully for group KN3
   ```

   And the message:

   ```
   KPDDSTR:  File rhilev.&midlev.RKN3HIS3 is full
   ```

This rough estimator works whether you have the default 3 history data sets (RKN3HIS1 – RKN3HIS3) or more data sets. Short-term history first fills the data set with the highest suffix (for example, RKN3HIS7) and then works its way down to RKN3HIS1, before it wraps back to the data set with the highest suffix.

If the elapsed time is 24 hours or greater, you should have enough storage allocated for users to view reports with 24 hours of data. If the elapsed time is less than 24 hours, then you need to allocate additional storage or data sets or both.

If you need to increase space allocation, and estimate how much to allocate, you should understand the relationship between the two configurable storage parameters: allocated Cylinders and Group Count, explained under “Allocating additional storage and data sets” on page 510.

Estimating approach
The information and worksheets in this section can be used to estimate storage requirements.

You will need to know the following:

1. Resource types (attribute tables) that need to be collected for history.
2. Approximate quantity of each resource type that will be monitored. If the number of monitored resources varies widely between different LPARs, and different TCP/IP stacks, you might want to estimate the different storage requirements for each LPAR and each TCP/IP stack.
3. Historical collection interval.

Allocating additional storage and data sets

You can override the default storage sizes that the PARMGEN method provided for short-term history data sets. Understand the varied roles that short-term history plays and how to change the size of your persistent data store.

The PARMGEN method provides default storage size values for short-term history data sets in the persistent data store. You can override these defaults. The IBM Z OMEGAMON Network Monitor monitoring agent storage size defaults are shown in Table 41 on page 511.

Table 41. Definition and default values for cylinders and group count parameters	
Storage parameters	**Default values**
Cylinders *Cylinders* is a measure of storage capacity on a disk drive. Considering control blocks and indexing, the persistent data store can store approximately 717 KB of measurement data on one cylinder of 3390 disk drive. After you determine the number of cylinders you need for your environment, add 37 to it to account for the RN3SGRPx data sets. This value is then entered into the **Est Cyl Space** field of the Persistent Datastore Specifications panel.	420 (for the persistent data stores, 383 for the RKN3HISx data sets + 37 for the RN3SGRPx data sets)
Group Count *Group Count* refers to the number of persistent data store data sets. Each persistent data store dataset will be allocated with (Cylinders / Group Count) number of cylinders. A Group Count of 6 means that 6 RKN3HISx data sets will be allocated for measurement data.	6

Short-term history is more than a place to store data. It enables:

- Continuous operations without manual attention to pruning outdated data
- Dynamic data set switching (data wrapping without losing data)
- Display of a full 24 hours of data, in a Tivoli Enterprise Portal report, at any point in time
- Access to 72 or more hours of data from the OMEGAMON Enhanced 3270 User Interface

These features require that one of the data sets be temporarily unavailable in preparation for data set switching. In addition, preserving the ability to display data from the last 24, 72, or more hours at any time of day might require that an additional data set be allocated to accommodate when the data set being written to is almost empty.

To account for the extra data sets needed to enable these features, apply a *Group Count factor* to the total number of cylinders required to store 24, 72, or more hours of data in your network. The Group Count factor expresses the storage relationship of Group Count to the number of cylinders to allocate. That is:

```
Cylinders to Allocate = Cylinders needed for 24, 72, or more hours data
X  Group Count Factor
```

Where:

```
Group Count Factor = (Group Count / (Group Count - 2))
```

These two examples illustrate the effect of the Group Count Factor. These examples show how increasing the Group Count value can use the allocated cylinders of space more efficiently (that is, requires less space for the same amount of data). Note that warehousing (exporting data to Tivoli Data Warehouse) and short-term historical queries are more efficient in smaller persistent data store data sets (that is, higher group count).

This formula is used to calculate DASD for both examples:

```
Cylinders to Allocate = Cylinders needed for 24, 72, or more hours data
X  (Group Count / (Group Count - 2))
Cylinders to Allocate = 10 X (3/(3-2)  = 30
```

Figure 3. Formula for calculating DASD

Modelling some alternate Group Count values illustrates the impact that modifying this parameter has on the amount of DASD (Cylinders of 3390) to be allocated.

Table 42. Sample group count and cylinders to allocate to enable viewing of 24 hours of data			
Cylinders needed for 24 hours of data	**Group count**	**Group count factor**	**Cylinders to allocate**
Example 1: a very small test network requiring only 70 cylinders of 3390 DASD for 24 hours of data			
70	3	3.00	210
70	4	2.00	140
70	5	1.67	119
70	6	1.50	105
70	7	1.40	105
70	8	1.33	91
70	9	1.29	91
70	10	1.25	91
Example 2: a somewhat larger network requiring 500 cylinders of 3390 DASD for 24 hours of data			
500	3	3.00	1500
500	4	2.00	1000
500	5	1.67	830
500	6	1.50	750
500	7	1.40	700
500	8	1.33	670
500	9	1.29	640
500	10	1.25	630

For the small network in Example 1, retaining the default Group Count value of 6 is more than adequate. However, for the larger network in Example 2, you would need to increase group count and cylinders, possibly to 7 and 700. For a monitored network with more than 10,000 TCP/IP connections, consider using a Group Count of at least 8.

When you consider these examples in light of the default values that ship with this product (Cylinders 3390 = 420 and Group Count = 6), you can accept the defaults with no loss of function for the small network. However, for the larger network in Example 2, you could not accept the defaults and confidently expect that users could view a report with 24 hours of data at any time of day. However, if you increased Group Count to at least 7 (and your network size estimate is correct), you should be able to provide this support by allocating 700 cylinders (+37) of additional DASD to short-term history.

Estimating the space requirements

Before providing sizings for historical data collection tables, understand how this data is collected.

You can collect historical data for the IBM Z OMEGAMON Network Monitor attribute tables listed in Table 43 on page 513. The columns in Table 43 on page 513 are explained in the section that follows:

Attribute Table
Is the name of the attribute table in which historical data is stored.

Filename
Is the name of the file that corresponds to the name of the attribute table.

Default
Specifies whether the table is configured if you select **Default Groups** in the Historical Collection dialog.

Estimated Storage Required
Is the estimated space required to store 24 hours of data per monitored resource.

A row stored in short-term history consists of all the attributes in the real-time row, plus 28 bytes per row to account for the additional fields maintained for all historical records. Space requirements for real-time data are described under "Understanding how historical data is collected" on page 14.

For most attribute groups, real-time data is only kept for the most recent measurement. For historical collection, data is stored for each history collection interval.

You might also choose to configure long-term history, and therefore store data for periods longer than 24 hours. Long-term history is stored in the Tivoli Data Warehouse. Fortunately, the space requirements per row of data are the same for a row of data in short-term history (in the persistent data store) and a row of data in long-term history (in a relational database).

Some clients use the archiving feature of short-term history to save backups and to collect more than 24 hours of data for analysis in a third-party statistical software package. Disk space requirements for archives are not included in the basic disk space requirements that are shown in Table 43 on page 513.

Historical data tables

To understand how to size your historical data tables, look at this table, which displays the storage used when monitoring one resource for 24 hours for every attribute group.

Table 43 on page 513 lists the IBM Z OMEGAMON Network Monitor attribute tables available for historical collection. This table displays the storage used when monitoring one resource for 24 hours, assuming collection intervals of 15 minutes.

Table 43. Historical data tables

Attribute table	File name	Default*	Estimated storage required for one data set (in KB)	Estimated storage required for one data set (3390 cylinders; No. of cylinders = KB/717)
Agent				
KN3 Agent Status	KN3AGS	Yes	24	0.0329
KN3 SNA Collector Status	KN3SCS	Yes	12	0.0173
KN3 TCP Collector Status	KN3TCS	Yes	73.5	0.1025
TCP/IP				
Current IP Filters	KN3IFC	No	79	0.1098
Dynamic IP Tunnels	KN3ITD	No	99	0.1376
FTP Sessions	KN3FSE	Yes	0.8	0.0011
Interfaces	KN3TIF	Yes	47	0.0654
IKE Tunnels	KN3ITI	No	65	0.0905
IPSec Status	KN3ISS	Yes	36	0.0507
KN3 ICMP Global Counters	KN3GCG	No	12	0.0167
KN3 ICMP Type Counters	KN3GCT	No	10	0.0141
KN3 Interface Address	KN3IFA	No	15	0.0209
KN3 Interface Read Queue	KN3IFR	No	32	0.0445
KN3 Interface Statistics	KN3IFS	No	31	0.0434

Table 43. Historical data tables (continued)

Attribute table	File name	Default*	Estimated storage required for one data set (in KB)	Estimated storage required for one data set (3390 cylinders; No. of cylinders = KB/717)
KN3 Interface Status	KN3IFE	No	35	0.0486
KN3 Interface Write Queue	KN3IFW	No	21	0.0298
KN3 IP Counter Statistics	KN3GIC	No	24	0.0340
KN3 IP General Statistics	KN3GIG	No	11	0.0146
KN3 OSA-Express5S Ports Control	KN35SC	No	15	0.0209
KN3 OSA-Express5S Ports Errors	KN35SE	No	26	0.0366
KN3 OSA-Express5S Ports Summary	KN35SS	No	34	0.0468
KN3 OSA-Express5S Ports Throughput	KN35ST	No	34	0.0468
KN3 TCP Counter Statistics	KN3GTC	No	29	0.0403
KN3 UDP Counter Statistics	KN3GUC	No	15	0.0204
Manual IP Tunnels	KN3ITM	No	37	0.0513
OSA-Express Channels	KN3TCH	Yes	42	0.0581
OSA-Express LPARS	KN3TLP	Yes	201	0.2803
OSA-Express Ports	KN3TPO	Yes	75	0.1041
OSA 10 Gigabit Ports Control	KN3TTC	No	39	0.0547
OSA 10 Gigabit Ports Errors	KN3TTE	Yes	42	0.0591
OSA 10 Gigabit Ports Summary	KN3TTS	Yes	48	0.0664
OSA 10 Gigabit Ports Throughput	KN3TTT	No	42	0.0586
OSA-Express3 Ports Control	KN3THC	No	39	0.0547
OSA-Express3 Ports Errors	KN3THE	Yes	48	0.0664
OSA-Express3 Ports Summary	KN3THS	Yes	68	0.0947
OSA-Express3 Ports Throughput	KN3THT	No	48	0.0669
TCP Listener	KN3TCL	Yes	28	0.0387

Table 43. Historical data tables (continued)

Attribute table	File name	Default*	Estimated storage required for one data set (in KB)	Estimated storage required for one data set (3390 cylinders; No. of cylinders = KB/717)
TCPIP Address Space	KN3TAS	Yes	61	0.0853
TCPIP Applications	KN3TAP	Yes	64	0.0894
TCPIP Connections	KN3TCN	Yes	62	0.0863
TCPIP Details	KN3TCP	Yes	60	0.0842
TCPIP Devices	KN3TDV	Yes	43	0.0601
TCPIP FTP (FTP transfers)	KN3FTP	Yes	5	0.0068
TCPIP Gateways	KN3TGA	Yes	59	0.0821
TCPIP Memory Statistics	KN3TPV	Yes	47	0.0654
TCPIP Stack Layer	KN3TSL	Yes	60	0.0832
TN3270 Server Sess Avail	KN3TNA	Yes	15	0.0207
UDP Connections	KN3UDP	Yes	36	0.0507
VTAM				
CSM Storage	KN3CSM	Yes	19	0.0267
EE Connections	KN3EEC	Yes	26	0.0361
EE Connection Details	KN3EED	Yes	126	0.1752
HPR RTP Connections	KN3HPR	Yes	56	0.0779
KN3 CSM Storage by Owner	KN3CSO	No	18	0.0256
VTAM Address Space	KN3VAS	Yes	26	0.0356
VTAM Buffer Pool Extents	KN3BPE	No	12	0.0162
VTAM Buffer Pools	KN3BPD	Yes	239	0.3332
VTAM Buffer Usage by Address Space	KN3BPS	Yes	9	0.0131
VTAM Buffer Usage by Application for Address Space	KN3BPA	Yes	10	0.0141
VTAM Buffer Usage by Category	KN3BPG	Yes	108	0.1506
VTAM I/O	KN3VIO	Yes	56	0.0785
VTAM Summary Statistics	KN3SNA	Yes	9	0.0131
Total			2760.6 KB	3.8502 cylinders

*Indicates the attribute groups for which product developers have defined historical views. You must configure these attribute groups if you want to see historical data in the predefined workspaces.

Tools for estimating data storage requirements

Use the worksheets in this section to understand the formula for historical collection, the attribute group record sizes, and the space requirements for the various data types for historical data storage.

The following types of formulas and data type combinations are included in this product:

- Agent historical data storage
- TCP/IP historical data storage
- VTAM historical data storage
- FTP historical data storage
- TN3270 historical data storage

The following formulas and worksheets provide the information needed to estimate storage requirements for each of the data types.

Agent historical data storage

Use this information to understand the formula for historical collection, the attribute group record sizes, and the space requirements for Agent historical data storage.

- **Agent formula**

  Storage assumptions:

  – Historical collection interval: 15 minutes

  – Quantity of each resource types monitored: 1

$$\frac{\text{4 collections per hour} \times \text{24 hours} \times \text{Bytes per record} \times \text{1 monitored resource (agent)} \times \text{1 row per resource}}{1024} = \text{KB per 24-hour period}$$

Which simplifies to:

$$\frac{96 \times \text{Number of bytes per record}}{1024} = \text{KB per 24-hour period}$$

Figure 4. Formula for Agent historical collection data storage

- **Attribute group record sizes**

  This data is collected once every collection interval for the agent. The number of rows returned may vary depending on the table. For example, the number of rows returned for the TCP Collector Status table depends on how many TCP/IP stacks the agent is monitoring.

Table 44. Agent data collected

Type of data	Historical data attribute table	Row size in bytes	Frequency	Subtotal storage required
Agent	KN3 Agent Status	252	1 row	24 KB
	KN3 SNA Collector Status	132	1 row	12 KB
	KN3 TCP Collector Status	784	1 row per monitored stack	73.5 KB

- **Space requirement worksheets**

Use the worksheets shown in Tables 72 through 74 to estimate the disk space requirements for your site. A sample calculation is provided for each historical data collection table.

- Each worksheet is for one agent per LPAR.
- For an LPAR, there can be one VTAM address space and one or more TCP/IP address spaces being monitored by the agent. The number of rows returned for the TCP Collector Status table depends on how many TCP/IP address spaces the agent is monitoring. You will need to multiply the required storage by the number of TCP/IP address spaces being monitored.
- If you are monitoring multiple LPARs, complete a worksheet for each LPAR, or one worksheet that represents the average LPAR.

KN3 Agent Status (KN3AGS) worksheet

Use the KN3 Agent Status (KN3AGS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 45. KN3 Agent Status (KN3AGS) worksheet

Interval	Record size	Formula	Agent	Agent address space	Expected storage required for 24 hours
15 minutes	252	4 x 24 x 252 x1 x 1 / 1024	1	1	24 KB

KN3 TCP Collector Status (KN3TCS) worksheet

Use the KN3 TCP Collector Status (KN3TCS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 46. TCP Collector Status (KN3TCS) worksheet

Interval	Record size	Formula	Agent	Monitored TCP/IP address spaces	Expected storage required for 24 hours
15 minutes	784	4 x 24 x 784 x 1 x 1 / 1024	1	1	73.5 KB

KN3 SNA Collector Status (KN3SCS) worksheet

Use the KN3 SNA Collector Status (KN3SCS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 47. SNA Collector Status (KN3SCS) worksheet

Interval	Record size	Formula	Agent	VTAM address space	Expected storage required for 24 hours
15 minutes	132	4 x 24 x 132 x 1 x 1 / 1024	1	1	12 KB

TCP/IP historical data storage

Use this information to understand the formula for historical collection, the attribute group record sizes, and the space requirements for TCP/IP historical data storage.

- **TCP/IP formula**

  Storage assumptions:

  – Historical collection interval: 15 minutes

  – Quantity of each resource types monitored: 1

$$\frac{\text{4 collections per hour} \times \text{24 hours} \times \text{Bytes per record} \times \text{1 monitored resource} \times \text{1 row per resource} \times \text{1 TCP/IP stack}}{1024} = \text{KB per 24-hour period}$$

Which simplifies to:

$$\frac{96 \times \text{Number of bytes per record}}{1024} = \text{KB per 24-hour period}$$

Figure 5. Formula for TCP/IP historical collection data storage

- **Attribute group record sizes**

  This data is collected once every collection interval for each TCP/IP stack. If you have an LPAR with multiple TCP/IP stacks, combine the storage required for each stack you will monitor.

Table 48. Data collected once every collection interval

Type of data	Real-time data attribute group	Row size in bytes	Frequency per interval	Subtotal storage required (KB)
TCP/IP and VTAM (required collection)	TCPIP Memory Statistics	500	1 row per TCP/IP address space	47
TCP/IP Stack layer Statistics	TCPIP Address Space	652	1 row per TCPIP address space	61
	KN3 ICMP Global Counters	128	1 row per TCP/IP address space	12
	KN3 ICMP Type Counters	108	1 row per ICMP type per ICMP version	10
	KN3 IP Counter Statistics	260	Up to 2 rows per TCP/IP address space	24
	KN3 IP General Statistics	112	1 row per TCP/IP address space	11
	KN3 TCP Counter Statistics	308	1 row per TCP/IP address space	29
	KN3 UDP Counter Statistics	156	1 row per TCP/IP address space	15
	TCPIP Stack Layer	636	1 row per TCP/IP address space	60

Table 48. Data collected once every collection interval (continued)

Type of data	Real-time data attribute group	Row size in bytes	Frequency per interval	Subtotal storage required (KB)
Interfaces statistics	Interfaces	500	1 row per interface	47
	KN3 Interface Address	160	1 row per TCP/IP interface address	15
	KN3 Interface Statistics	332	1 row per active strategic TCP/IP interface	31
	KN3 Interface Status	372	1 row per TCP/IP interface	35
	TCPIP Devices	460	1 row per device	43
Interface Data Link Control statistics collection	KN3 Interface Read Queue	340	1 row per read queue per active OSA Queued Direction I/O (QDIO) or HiperSockets interface	32
	KN3 Interface Write Queue	228	1 row per configured queue priority per OSA-Express Queued Direct I/O (QDIO) or HiperSocket interface	21

Table 48. Data collected once every collection interval (continued)

Type of data	Real-time data attribute group	Row size in bytes	Frequency per interval	Subtotal storage required (KB)
OSA statistics collection	OSA-Express Channels	444	1 row per OSA Channel	42
	OSA-Express LPARS	134	1 row per OSA LPAR	201
	OSA-Express Ports	796	1 row per OSA Port	75
	OSA 10 Gigabit Ports Control	418	1 row per OSA-Express 2 10 Gigabit Port	39
	OSA 10 Gigabit Ports Errors	452	1 row per OSA-Express 2 10 Gigabit Port	42
	OSA 10 Gigabit Ports Summary	508	1 row per OSA-Express 2 10 Gigabit Port	48
	OSA 10 Gigabit Ports Throughput	448	1 row per OSA-Express 2 10 Gigabit Port	42
	OSA-Express3 Ports Control	418	1 row per OSA-Express3 Port	39
	OSA-Express3 Ports Errors	508	1 row per OSA-Express3 Port	48
	OSA-Express3 Ports Summary	724	1 row per OSA-Express3 Port	68
	OSA-Express3 Ports Throughput	512	1 row per OSA-Express3 Port	48
	KN3 OSA-Express5S Ports Control	160	1 row per OSA-Express5S Port	15
	KN3 OSA-Express5S Ports Errors	280	1 row per OSA-Express5S Port	26
	KN3 OSA-Express5S Ports Summary	360	1 row per OSA-Express5S Port	34
	KN3 OSA-Express5S Ports Throughput	358	1 row per OSA-Express5S Port	34
TCP/IP Connection and Application Performance statistics collection	TCPIP Applications	684	1 row per TCP/IP application	64
	TCPIP Connections	660	1 row per TCPIP connection	62
	TCPIP Details	644	1 row per TCP connection	60
	TCP Listener	296	1 row per TCP listener	28
	UDP Connections	388	1 row per UDP endpoint	36
Routing Table Statistics Collection	TCPIP Gateways	628	1 row per TCP/IP gateway collected on Routing Table Collection Frequency	59

Table 48. Data collected once every collection interval (continued)				
Type of data	**Real-time data attribute group**	**Row size in bytes**	**Frequency per interval**	**Subtotal storage required (KB)**
IPSec Security collection	IPSec Status	388	1 row per TCP/IP address space	36
	Current IP Filters	840	1 row per IP filter	79
	Dynamic IP Tunnels	1052	1 row per dynamic IP tunnel	99
	IKE Tunnels	692	1 row per IKE tunnel	65
	Manual IP Tunnels	392	1 row per manual IP tunnel	37

- **Space requirement worksheets**

  Use the worksheets shown in Tables 76 through 109 to estimate the disk space requirements for your site. A sample calculation is provided for each historical data collection table.

  - Each worksheet is for one monitored resource per LPAR or per TCP/IP stack.
  - Typically you are monitoring more than one resource (that is, one TCP/IP address space, connection, or session, for example). You need to multiply the required storage by the number of resources.
  - If you are monitoring multiple LPARs, complete a worksheet for each LPAR, or one worksheet that represents the average LPAR.
  - If you are monitoring more than one TCP/IP stack in an LPAR, multiply by the number of TCP/IP stacks.

Current IP Filters (KN3IFC) worksheet

Use the Current IP Filters (KN3IFC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 49. Current IP Filters (KN3IFC) worksheet					
Interval	**Record size**	**Formula**	**TCP/IP address space resources**	**IP Filters**	**Expected storage required for 24 hours**
15 minutes	840	4 x 24 x 840 x 1 x 1 / 1024	1	1	79 KB

Dynamic IP Tunnels (KN3ITD) worksheet

Use the Dynamic IP Tunnels (KN3ITD) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 50. Dynamic IP Tunnels (KN3ITD) worksheet					
Interval	**Record size**	**Formula**	**TCP/IP address space resources**	**Dynamic IP Tunnels**	**Expected storage required for 24 hours**
15 minutes	1052	4 x 24 x 1052 x 1 x 1 / 1024	1	1	99 KB

Interfaces (KN3TIF) worksheet

Use the Interfaces (KN3TIF) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 51. Interfaces (KN3TIF) worksheet

Interval	Record size	Formula	TCP/IP interface	TCP/IP stack	Expected storage required for 24 hours
15 minutes	500	4 x 24 x 500 x 1 x 1 x 1/ 1024	1	1	47 KB

IKE Tunnels (KN3ITI) worksheet

Use the IKE Tunnels (KN3ITI) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 52. IKE Tunnels (KN3ITI) worksheet

Interval	Record size	Formula	TCP/IP address space resources	Dynamic IP Tunnels	Expected storage required for 24 hours
15 minutes	692	4 x 24 x 692 x 1 x 1 / 1024	1	1	65 KB

IPSec Status (KN3ISS) worksheet

Use the IPSec Status (KN3ISS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 53. IPSec Status (KN3ISS) worksheet

Interval	Record size	Formula	TCP/IP address space resources	TCP/IP stack	Expected storage required for 24 hours
15 minutes	388	4 x 24 x 388 x 1 x 1 / 1024	1	1	36 KB

KN3 ICMP Global Counters (KN3GCG) worksheet

Use the KN3 ICMP Global Counters (KN3GCG) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 54. KN3 ICMP Global Counters (KN3GCG) worksheet

Interval	Record size	Formula	ICMP protocol	ICMP Version	TCP/IP stack	Expected storage required for 24 hours
15 minutes	128	4 x 24 x 128 x 1 x 1 x 1 / 1024	1	1	1	12 KB

KN3 ICMP Type Counters (KN3GCT) worksheet

Use the KN3 ICMP Type Counters (KN3GCT) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 55. KN3 ICMP Type Counters (KN3GCT) worksheet

Interval	Record size	Formula	ICMP type	TCP/IP stack	Expected storage required for 24 hours
15 minutes	108	4 x 24 x 108 x 1 x 1 / 1024	1	1	10 KB

KN3 Interface Address (KN3IFA) worksheet

Use the KN3 Interface Address (KN3IFA) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 56. KN3 Interface Address (KN3IFA) worksheet

Interval	Record size	Formula	TCP/IP interface address	TCP/IP interface	TCP/IP stack	Expected storage required for 24 hours
15 minutes	160	4 x 24 x 160 x 1 x 1 x 1 / 1024	1	1	1	15 KB

KN3 Interface Read Queue (KN3IFR) worksheet

Use the KN3 Interface Read Queue (KN3IFR) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 57. KN3 Interface Read Queue (KN3IFR) worksheet

Interval	Record size	Formula	Read queue	Active TCP/IP QDIO or HiperSockets interface	TCP/IP stack	Expected storage required for 24 hours
15 minutes	340	4 x 24 x 340 x 1 x 1 x 1 / 1024	1	1	1	32KB

KN3 Interface Statistics (KN3IFS) worksheet

Use the KN3 Interface Statistics (KN3IFS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 58. KN3 Interface Statistics (KN3IFS) worksheet

Interval	Record size	Formula	Active TCP/IP strategic interface*	TCP/IP stack	Expected storage required for 24 hours
15 minutes	332	4 x 24 x 332 x 1 x 1 / 1024	1	1	31 KB

* The strategic interfaces have one of the following values for the Interface Type attribute on KN3 workspaces: Loopback, OSA-Express Queued Direct I/O (QDIO) Ethernet, HiperSockets, or Multipath Channel Point-To-Point (MPCPTP)

KN3 Interface Status (KN3IFE) worksheet

Use the KN3 Interface Status (KN3IFE) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 59. KN3 Interface Status (KN3IFE) worksheet

Interval	Record size	Formula	TCP/IP interface	TCP/IP stack	Expected storage required for 24 hours
15 minutes	372	4 x 24 x 372 x 1 x 1 / 1024	1	1	35 KB

KN3 Interface Write Queue (KN3IFW) worksheet

Use the KN3 Interface Write Queue (KN3IFW) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 60. KN3 Interface Write Queue (KN3IFW) worksheet

Interval	Record size	Formula	Write queue	Active TCP/IP QDIO or HiperSockets interface	TCP/IP stack	Expected storage required for 24 hours
15 minutes	228	4 x 24 x 228 x 1 x 1 x 1 / 1024	1	1	1	21 KB

KN3 IP Counter Statistics (KN3GIC) worksheet

Use the KN3 IP Counter Statistics (KN3GIC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 61. KN3 IP Counter Statistics (KN3GIC) worksheet

Interval	Record size	Formula	IP counter statistics	IP version	TCP/IP stack	Expected storage required for 24 hours
15 minutes	260	4 x 24 x 260 x 1 x 1 x 1 / 1024	1	1	1	24 KB

KN3 IP General Statistics (KN3GIG) worksheet

Use the KN3 IP General Statistics (KN3GIG) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 62. IP General Statistics (KN3GIG) worksheet

Interval	Record size	Formula	IP protocol	TCP/IP stack	Expected storage required for 24 hours
15 minutes	112	4 x 24 x 112 x 1 x 1 / 1024	1	1	11 KB

KN3 OSA-Express5S Ports Control (KN35SC) worksheet

Use the KN3 OSA-Express5S Ports Control (KN35SC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 63. OSA-Express5S Ports Control (KN35SC) worksheet

Interval	Record size	Formula	OSA-Express channels	TCP/IP stack	Expected storage required for 24 hours
15 minutes	160	4 x 24 x 160 x 1 x 1 x 1 / 1024	1	1	15 KB

KN3 OSA-Express5S Ports Errors (KN35SE) worksheet

Use the KN3 OSA-Express5S Ports Errors (KN35SE) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 64. OSA-Express5S Ports Errors (KN35SE) worksheet

Interval	Record size	Formula	OSA-Express channels	TCP/IP stack	Expected storage required for 24 hours
15 minutes	280	4 x 24 x 280 x 1 x 1 x 1 / 1024	1	1	26 KB

KN3 OSA-Express5S Ports Summary (KN35SS) worksheet

Use the KN3 OSA-Express5S Ports Summary (KN35SS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 65. OSA-Express5S Ports Summary (KN35SS) worksheet

Interval	Record size	Formula	OSA-Express channels	TCP/IP stack	Expected storage required for 24 hours
15 minutes	360	4 x 24 x 360 x 1 x 1 x 1 / 1024	1	1	34 KB

KN3 OSA-Express5S Ports Throughput (KN35ST) worksheet

Use the KN3 OSA-Express5S Ports Throughput (KN35ST) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 66. OSA-Express5S Ports Throughput (KN35ST) worksheet

Interval	Record size	Formula	OSA-Express channels	TCP/IP stack	Expected storage required for 24 hours
15 minutes	358	4 x 24 x 358 x 1 x 1 x 1 / 1024	1	1	34 KB

KN3 TCP Counter Statistics (KN3GTC) worksheet

Use the KN3 TCP Counter Statistics (KN3GTC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 67. KN3 TCP Counter Statistics (KN3GTC) worksheet

Interval	Record size	Formula	TCP/IP protocol	TCP/IP stack	Expected storage required for 24 hours
15 minutes	308	4 x 24 x 308 x 1 x 1 / 1024	1	1	29 KB

KN3 UDP Counter Statistics (KN3GUC) worksheet

Use the KN3 UDP Counter Statistics (KN3GUC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 68. KN3 UDP Counter Statistics (KN3GUC) worksheet

Interval	Record size	Formula	UDP protocol	TCP/IP stack	Expected storage required for 24 hours
15 minutes	156	4 x 24 x 156 x 1 x 1 / 1024	1	1	15 KB

Manual IP Tunnels (KN3ITM) worksheet

Use the Manual IP Tunnels (KN3ITM) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 69. Manual IP Tunnels (KN3ITM) worksheet

Interval	Record size	Formula	TCP/IP address space resources	Manual IP Tunnels	Expected storage required for 24 hours
15 minutes	392	4 x 24 x 392 x 1 x 1 / 1024	1	1	37 KB

OSA-Express Channels (KN3TCH) worksheet

Use the OSA-Express Channels (KN3TCH) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 70. OSA-Express Channels (KN3TCH) worksheet

Interval	Record size	Formula	OSA-Express channels	TCP/IP stack	Expected storage required for 24 hours
15 minutes	444	4 x 24 x 444 x 1 x 1 x 1 / 1024	1	1	42 KB

OSA-Express LPARS (KN3TLP) worksheet

Use the OSA-Express LPARS (KN3TLP) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 71. OSA-Express LPARS (KN3TLP) worksheet

Interval	Record size	Formula	OSA-Express Channels	OSA Express LPARS	TCP/IP stack	Expected storage required for 24 hours
15 minutes	134	4 x 24 x 134 x 1 x 16 x 1 / 1024	1	16	1	201

OSA-Express Ports (KN3TPO) worksheet

Use the OSA-Express Ports (KN3TPO) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 72. OSA-Express Ports (KN3TPO) worksheet

Interval	Record size	Formula	OSA-Express port	TCP/IP stack	Expected storage required for 24 hours
15 minutes	796	4 x 24 x 796 x 1 x 1 x 1 / 1024	1	1	75 KB

OSA 10 Gigabit Ports Control (KN3TTC) worksheet

Use the OSA 10 Gigabit Ports Control (KN3TTC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 73. OSA 10 Gigabit Ports Control (KN3TTC) worksheet

Interval	Record size	Formula	OSA 10 Gigabit ports control	TCP/IP stack	Expected storage required for 24 hours
15 minutes	418	4 x 24 x 418 x 1 x 1 x 1 / 1024	1	1	39

OSA 10 Gigabit Ports Errors (KN3TTE) worksheet

Use the OSA 10 Gigabit Ports Errors (KN3TTE) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 74. OSA 10 Gigabit Ports Errors (KN3TTE) worksheet

Interval	Record size	Formula	OSA 10 Gigabit ports errors	TCP/IP stack	Expected storage required for 24 hours
15 minutes	452	4 x 24 x 452 x 1 x 1 x 1 / 1024	1	1	42 KB

OSA 10 Gigabit Ports Summary (KN3TTS) worksheet

Use the OSA 10 Gigabit Ports Summary (KN3TTS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 75. OSA 10 Gigabit Ports Summary (KN3TTS) worksheet

Interval	Record size	Formula	OSA 10 Gigabit port	TCP/IP stack	Expected storage required for 24 hours
15 minutes	508	4 x 24 x 508 x 1 x 1 x 1 / 1024	1	1	48 KB

OSA 10 Gigabit Ports Throughput (KN3TTT) worksheet

Use the OSA 10 Gigabit Ports Throughput (KN3TTT) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 76. OSA 10 Gigabit Ports Throughput (KN3TTT) worksheet

Interval	Record size	Formula	OSA 10 Gigabit ports throughput	TCP/IP stack	Expected storage required for 24 hours
15 minutes	448	4 x 24 x 448 x 1 x 1 x 1 / 1024	1	1	42

OSA-Express3 Ports Control (KN3THC) worksheet

Use the OSA-Express3 Ports Control (KN3THC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 77. OSA-Express3 Ports Control (KN3THC) worksheet

Interval	Record size	Formula	OSA-Express3 ports control	TCP/IP stack	Expected storage required for 24 hours
15 minutes	418	4 x 24 x 418 x 1 x 1 x 1 / 1024	1	1	39

OSA-Express3 Ports Errors (KN3THE) worksheet

Use the OSA-Express3 Ports Errors (KN3THE) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 78. OSA-Express3 Ports Errors (KN3THE) worksheet

Interval	Record size	Formula	OSA-Express3 ports errors	TCP/IP stack	Expected storage required for 24 hours
15 minutes	508	4 x 24 x 508 x 1 x 1 x 1 / 1024	1	1	48 KB

OSA-Express3 Ports Summary (KN3THS) worksheet

Use the OSA-Express3 Ports Summary (KN3THS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 79. OSA-Express3 Ports Summary (KN3THS) worksheet

Interval	Record size	Formula	OSA-Express3 port	TCP/IP stack	Expected storage required for 24 hours
15 minutes	724	4 x 24 x 724 x 1 x 1 x 1 / 1024	1	1	68 KB

OSA-Express3 Ports Throughput (KN3THT) worksheet

Use the OSA-Express3 Ports Throughput (KN3THT) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 80. OSA-Express3 Ports Throughput (KN3THT) worksheet

Interval	Record size	Formula	OSA-Express3 ports throughput	TCP/IP stack	Expected storage required for 24 hours
15 minutes	512	4 x 24 x 512 x 1 x 1 x 1 / 1024	1	1	48

TCP Listener (KN3TCL) worksheet

Use the TCP Listener (KN3TCL) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 81. TCP Listener (KN3TCL) worksheet

Interval	Record size	Formula	TCP listeners	TCP/IP stack	Expected storage required for 24 hours
15 minutes	296	4 x 24 x 296 x 1 x 1 / 1024	1	1	28 KB

TCPIP Address Space (KN3TAS) worksheet

Use the TCPIP Address Space (KN3TAS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 82. TCPIP Address Space (KN3TAS) worksheet

Interval	Record size	Formula	TCP/IP address space resources	TCP/IP stack	Expected storage required for 24 hours
15 minutes	652	4 x 24 x 652 x 1 x 1 / 1024	1	1	61 KB

TCPIP Applications (KN3TAP) worksheet

Use the TCPIP Applications (KN3TAP) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 83. TCPIP Applications (KN3TAP) worksheet

Interval	Record size	Formula	TCP/IP applications	TCP/IP stack	Expected storage required for 24 hours
15 minutes	684	4 x 24 x 684 x 1 x 1 / 1024	1	1	64 KB

TCPIP Connections (KN3TCN) worksheet

Use the TCPIP Connections (KN3TCN) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 84. TCPIP Connections (KN3TCN) worksheet

Interval	Record size	Formula	TCP/IP connections	TCP/IP stack	Expected storage required for 24 hours
15 minutes	660	4 x 24 x 660 x 1 x 1 / 1024	1	1	62 KB

TCPIP Details (KN3TCP) worksheet

Use the TCPIP Details (KN3TCP) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 85. TCPIP Details (KN3TCP) worksheet

Interval	Record size	Formula	TCP connections	TCP/IP stack	Expected storage required for 24 hours
15 minutes	644	4 x 24 x 644 x 1 x 1 / 1024	1	1	60 KB

TCPIP Devices (KN3TDV) worksheet

Use the TCPIP Devices (KN3TDV) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 86. TCPIP Devices (KN3TDV) worksheet

Interval	Record size	Formula	TCP/IP devices	TCP/IP stack	Expected storage required for 24 hours
15 minutes	460	4 x 24 x 460 x 1 x 1 / 1024	1	1	43 KB

TCPIP Gateways (KN3TGA) worksheet

Use the TCPIP Gateways (KN3TGA) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 87. TCPIP Gateways (KN3TGA) worksheet

Interval	Record size	Formula	Gateways	TCP/IP stack	Expected storage required for 24 hours
15 minutes	628	4 x 24 x 628 x 1 x 1 x 1 / 1024	1	1	59 KB

TCPIP Memory Statistics (KN3TPV) worksheet

Use the TCPIP Memory Statistics (KN3TPV) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 88. TCPIP Memory Statistics (KN3TPV) worksheet

Interval	Record size	Formula	TCP/IP address spaces	TCP/IP stack	Expected storage required for 24 hours
15 minutes	500	4 x 24 x 500 x 1 x 1 x 1 / 1024	1	1	47 KB

TCPIP Stack Layer (KN3TSL) worksheet

Use the TCPIP Stack Layer (KN3TSL) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 89. TCPIP Stack Layer (KN3TSL) worksheet

Interval	Record size	Formula	TCP/IP address spaces	TCP/IP stack	Expected storage required for 24 hours
15 minutes	636	4 x 24 x 636 x 1 x 1 x 1 / 1024	1	1	60 KB

UDP Connections (KN3UDP) worksheet

Use the UDP Connections (KN3UDP) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 90. UDP Connections (KN3UDP) worksheet

Interval	Record size	Formula	UDP connections	TCP/IP stack	Expected storage required for 24 hours
15 minutes	388	4 x 24 x 388 x 1 x 1 / 1024	1	1	36 KB

VTAM historical data storage

Use this information to understand the formula for historical collection, the attribute group record sizes, and the space requirements for VTAM historical data storage.

- **VTAM formula**

  Storage assumptions:

  – Historical collection interval: 15 minutes

  – Quantity of each resource types monitored: 1

$$\frac{\text{4 collections per hour} \times \text{24 hours} \times \text{Bytes per record} \times \text{1 monitored resource} \times \text{1 row per resource}}{1024} = \text{KB per 24-hour period}$$

Which simplifies to:

$$\frac{96 \times \text{Number of bytes per record}}{1024} = \text{KB per 24-hour period}$$

Figure 6. Formula for VTAM historical collection data storage

- **Attribute group record sizes**

  The following data is collected once every historical collection interval. This data is collected for each LPAR you will monitor.

Table 91. Data collected once every collection interval

Type of data	Real-time data attribute group	Row size in bytes	Frequency per interval	Subtotal storage required in KB
TCP/IP and VTAM (required collection)	VTAM Summary Statistics	100	1 row	9
Enterprise Extender (EE) and High Performance Routing (HPR) statistics collection	EE Connections	276	1 row per EE connection	26
	EE Connections Details	268	5 rows per EE connection	126
	HPR RTP Connections	596	1 row per HPR RTP connection	56

Table 91. Data collected once every collection interval (continued)				
Type of data	**Real-time data attribute group**	**Row size in bytes**	**Frequency per interval**	**Subtotal storage required in KB**
Communications Storage Manager (CSM) buffer reporting	CSM Storage	204	1 row	19
	KN3 CSM Storage by Owner	196	1 row per address space that owns CSM storage	18
Buffer Pool and VTAM environment collection	VTAM Address Space	272	1 row	26
	VTAM I/O	100	1 row for each of 6 resources	56
	VTAM Buffer Pools	182	1 row for each of 14 resources	239
	VTAM Buffer Pool Extents	124	1 row per buffer pool extent	12
	VTAM Buffer Usage by Address Space	100	1 row per address space using IO00 or CRPL buffers	9
	VTAM Buffer Usage by Application for Address Space	108	1 row per application per address space using IO00 buffers	10
	VTAM Buffer Usage by Category	96	1 row for each of 12 resources	108

- **Space requirement worksheets**

  Use the worksheets shown in Tables 111 through 121 to estimate the disk space requirements for your site. A sample calculation is provided for each historical data collection table.

  - Each worksheet is for one monitored resource per LPAR.
  - Typically you are monitoring more than one resource (that is, one connection). You need to multiply the required storage by the number of resources.
  - If you are monitoring multiple LPARs, complete a worksheet for each LPAR, or one worksheet that represents the average LPAR.

CSM Storage (KN3CSM) worksheet

Use the CSM Storage (KN3CSM) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 92. CSM Storage (KN3CSM) worksheet				
Interval	**Record size**	**Formula**	**CSM storage resources**	**Expected storage required for 24 hours**
15 minutes	204	4 x 24 x 204 x 1 x 1/ 1024	1	19 KB

EE Connection Details (KN3EED) worksheet

Use the EE Connection Details (KN3EED) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 93. EE Connection Details (KN3EED) worksheet

Interval	Record size	Formula	EE connection resources	Expected storage required for 24 hours
15 minutes	268	4 x 24 x 268 x 1 x 5 / 1024	1	126 KB

EE Connections (KN3EEC) worksheet

Use the EE Connections (KN3EEC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 94. EE Connections (KN3EEC) worksheet

Interval	Record size	Formula	EE connection resources	Expected storage required for 24 hours
15 minutes	276	4 x 24 x 276 x 1 x 5 / 1024	1	26 KB

HPR RTP Connections (KN3HPR) worksheet

Use the HPR RTP Connections (KN3HPR) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 95. HPR RTP Connections (KN3HPR) worksheet

Interval	Record size	Formula	HPR RTP connection resources	Expected storage required for 24 hours
15 minutes	596	4 x 24 x 596 x 1 x 1/ 1024	1	56 KB

KN3 CSM Storage by Owner (KN3CSO) worksheet

Use the KN3 CSM Storage by Owner (KN3CSO) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 96. KN3 CSM Storage by Owner (KN3CSO) worksheet

Interval	Record size	Formula	CSM Storage by Owner resources	Expected storage required for 24 hours
15 minutes	196	4 x 24 x 196 x 1 x 1/ 1024	1	18 KB

VTAM Address Space (KN3VAS) worksheet

Use the VTAM Address Space (KN3VAS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 97. VTAM Summary Statistics (KN3VAS) worksheet

Interval	Record size	Formula	VTAM address space resources	Expected storage required for 24 hours
15 minutes	272	4 x 24 x 272 x 1 / 1024	1	26 KB

VTAM Buffer Pool Extents (KN3BPE) worksheet

Use the VTAM Buffer Pool Extents (KN3BPE) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 98. VTAM Buffer Pool Extents (KN3BPE) worksheet

Interval	Record size	Formula	Number of resources	Expected storage required for 24 hours
15 minutes	124	4 x 24 x 124 x 1 x 1 / 1024	1	12 KB

VTAM Buffer Pools (KN3BPD) worksheet

Use the VTAM Buffer Pools (KN3BPD) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 99. VTAM Buffer Pools (KN3BPD) worksheet

Interval	Record size	Formula	Number of resources	Expected storage required for 24 hours
15 minutes	182	4 x 24 x 182 x 14 x 1 / 1024	14	239 KB

VTAM Buffer Usage by Address Space (KN3BPS) worksheet

Use the VTAM Buffer Usage by Address Space (KN3BPS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 100. VTAM Buffer Usage by Address Space (KN3BPS) worksheet

Interval	Record size	Formula	Number of resources	Expected storage required for 24 hours
15 minutes	100	4 x 24 x 100 x 1 x 1 / 1024	1	9 KB

VTAM Buffer Usage by Application for Address Space (KN3BPA) worksheet

Use the VTAM Buffer Usage by Application by Address Space (KN3BPA) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 101. VTAM Buffer Usage by Application for Address Space (KN3BPA) worksheet

Interval	Record size	Formula	Number of resources	Expected storage required for 24 hours
15 minutes	108	4 x 24 x 108 x 1 x 1 / 1024	1	10 KB

VTAM Buffer Usage by Category (KN3BPG) worksheet

Use the VTAM Buffer Usage by Category (KN3BPG) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 102. VTAM Buffer Usage by Category (KN3BPG) worksheet

Interval	Record size	Formula	Number of resources	Expected storage required for 24 hours
15 minutes	96	4 x 24 x 96 x 12 x 1 / 1024	12	108 KB

VTAM I/O (KN3VIO) worksheet

Use the VTAM I/O (KN3VIO) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 103. VTAM I/O (KN3VIO) worksheet

Interval	Record size	Formula	Number of resources	Expected storage required for 24 hours
15 minutes	100	4 x 24 x 100x 6 x 1 / 1024	6	56 KB

VTAM Summary Statistics (KN3SNA) worksheet

Use the VTAM Summary Statistics (KN3SNA) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 104. VTAM Summary Statistics (KN3SNA) worksheet

Interval	Record size	Formula	SNA resources	Expected storage required for 24 hours
15 minutes	100	4 x 24 x 100 x 1 / 1024	1	10 KB

FTP historical data storage

Use this information to understand the formula for historical collection, the attribute group record sizes, and the space requirements for FTP historical data storage.

- **FTP formula**

  Storage assumptions:

  – Historical collection interval: 15 minutes

  – Quantity of each resource types monitored: 1

$$\frac{\text{Bytes per record} \times \text{1 monitored resource} \times \text{2 rows per session or transfer} \times \text{1 TCP/IP stack}}{1024} = \text{KB per 24-hour period}$$

Figure 7. Formula for FTP historical collection data storage

- **Attribute group record sizes**

  The following FTP data is collected when a new session or transfer is opened or when an existing session or transfer is closed. This data is collected when z/OS Communications Server notifies the monitoring agent that there is data available and therefore does not adhere to a collection interval. For these three attribute tables, storage per monitored resource is relatively low because only one record is stored per active session or transfer, plus one record per completed session or transfer. However, you might have thousands of sessions or transfers in 24 hours, and thus storage cost for FTP sessions could be significant.

  FTP data is collected for each TCP/IP stack. If you have LPARs with multiple TCP/IP stacks, total the storage required for each stack you will monitor.

Table 105. FTP data collected

Type of data	Historical data attribute table	Row size in bytes	Frequency	Subtotal storage required
FTP Data Collection	FTP Sessions	412	2 rows per FTP session	0.8 KB
	TCPIP FTP	2464	2 rows per FTP transfer	5 KB

- **Space requirement worksheets**

  Use the worksheets shown in Tables 124 and 125 to estimate the disk space requirements for your site. A sample calculation is provided for each historical data collection table.

  – Each worksheet applies to one monitored resource per TCP/IP stack.

  – Typically you are monitoring more than one resource (that is, one session or transfer, for example). You need to multiply the required storage by the number of resources.

  – If you are monitoring multiple LPARs, complete a worksheet for each LPAR, or one worksheet that represents the average LPAR.

  – If you are monitoring more than one TCP/IP stack in an LPAR and each TCP/IP stack has an FTP server, multiply by the number of TCP/IP stacks.

FTP Sessions (KN3FSE) worksheet

Use the FTP Sessions (KN3FSE) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 106. FTP Sessions (KN3FSE) worksheet

Record size	Formula	FTP sessions	TCP/IP stack	Expected storage required for 24 hours
412	412 x 1 x 2 x 1 / 1024	1	1	0.8 KB

TCPIP FTP (KN3FTP) worksheet

Use the TCPIP FTP (KN3FTP) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 107. TCPIP FTP (KN3FTP) worksheet

Record size	Formula	FTP transfers	TCP/IP stack	Expected storage required for 24 hours
2464	(2464 x 1 x 2 x 1) / 1024	1	1	5 KB

TN3270 historical data storage

Use this information to understand the formula for historical collection, the attribute group record sizes, and the space requirements for 3270 historical data storage.

- **TN3270 formula**

  Storage assumptions:

  - Historical collection interval: 15 minutes
  - Quantity of each resource types monitored: 1
  - TN3270 session is active for 8 hours, and then is closed

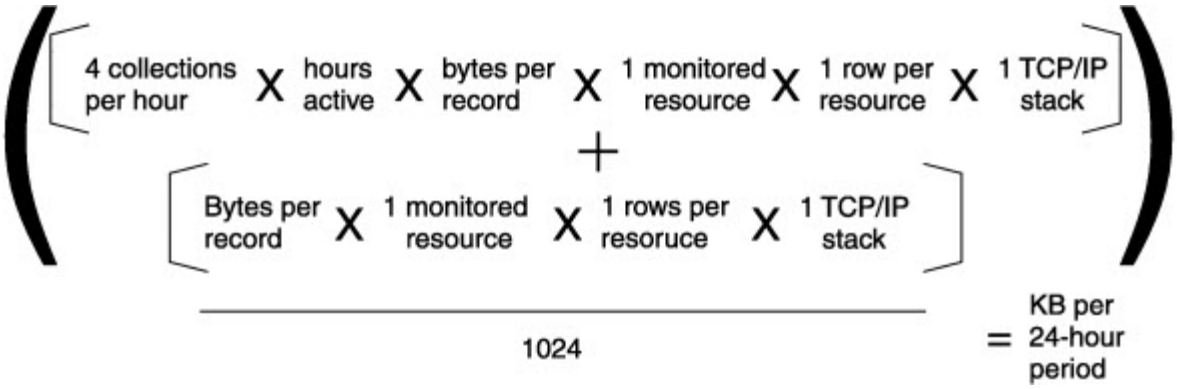


Figure 8. Formula for TN3270 historical collection data storage

- **Attribute group record sizes**

  The TN3270 data provides information about open, closed and active TN3270 sessions for a TCP/IP address space. A record is stored for each TN3270 session that closed since historical data was last collected or that is active when historical data is collected. The record for a TN3270 session will be stored when new data is available at the time that historical data is collected (i.e. the same, unchanged

record will not be stored twice). New data is available each collection interval starting when the session opened until the collection interval after the session closed.

Thirty-two (32) records a day (4 per hour for 8 hours) will be stored for each active TN3270 session.

Table 108. TN3270 data collected

Type of data	Historical data attribute table	Row size in bytes	Frequency	Subtotal storage required
TN3270 Server Statistics Data Collection	TN3270 Server Sess Avail	460	1 row per active TN3270 server session **+** 1 row per closed TN3270 server session	15 KB

- **Space requirement worksheets**

  Use the worksheet shown in Table 127 to estimate the disk space requirements for your site. A sample calculation is provided for each historical data collection table.

  - Each worksheet is for one monitored resource per TCP/IP stack.
  - Typically you are monitoring more than one resource (that is, one session). You need to multiply the required storage by the number of resources.
  - If you are monitoring multiple LPARs, complete a worksheet for each LPAR, or one worksheet that represents the average LPAR.
  - If you are monitoring more than one TCP/IP stack in an LPAR and each TCP/IP stack has a TN3270 server, multiply by the number of TCP/IP stacks.

TN3270 Server Sess Avail (KN3TNA) worksheet

Use the TN3270 Server Sess Avail (KN3TNA) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 109. TN3270 Server Sess Avail (KN3TNA) worksheet

Record size	Formula	TN3270 server sessions	TCP/IP stack	Expected storage required for 24 hours
460	((4 x 8 x 460 x 1 x 1 x 1) + (460 x 1 x 1 x 1)) / 1024	1	1	15 KB

IBM Z OMEGAMON Network Monitor disk space summary worksheet

Use this worksheet to summarize the historical database calculations you have made in previous attribute group-specific worksheets.

The disk space summary worksheet for IBM Z OMEGAMON Network Monitor follows.

Table 110. Disk space summary

Historical attribute table	Historical attribute table size in KB (for a 24-hour period)	Subtotal of storage required in cylinders
Agent Historical Data Collection Interval		
Agent Status		

Table 110. Disk space summary (continued)

Historical attribute table	Historical attribute table size in KB (for a 24-hour period)	Subtotal of storage required in cylinders
SNA Collector Status		
TCP Collector Status		
TCP/IP and VTAM (required collection		
TCPIP Memory Statistics		
TCP/IP Stack Layer Statistics		
TCPIP Address Space		
KN3 ICMP Global Counters		
KN3 ICMP Type Counters		
KN3 IP Counter Statistics		
KN3 IP General Statistics		
KN3 TCP Counter Statistics		
KN3 UDP Counter Statistics		
TCPIP Stack Layer		
Interfaces statistics collection		
Intterfaces		
KN3 Interface Address		
KN3 Interface Statistics		
KN3 Interface Status		
TCPIP Devices		
KN3 Interface ReadQueue		
KN3 Interface Write Queue		
OSA statistics collection		
OSA-Express Channels		
OSA-Express LPARS		
OSA-Express Ports		
OSA 10 Gigabit Ports Control		
OSA 10 Gigabit Ports Errors		
OSA 10 Gigabit Ports Summary		
OSA 10 Gigabit Ports Throughput		
OSA-Express3 Ports Control		
OSA-Express3 Ports Errors		
OSA-Express3 Ports Summary		
OSA-Express3 Ports Throughput		

Table 110. Disk space summary (continued)

Historical attribute table	Historical attribute table size in KB (for a 24-hour period)	Subtotal of storage required in cylinders
KN3 OSA-Express5S Ports Control		
KN3 OSA-Express5S Ports Errors		
KN3 OSA-Express5S Ports Summary		
KN3 OSA-Express5S Ports Throughput		
TCP/IP Connection and Application Performance statistics collection		
TCPIP Applications		
TCPIP Connections		
TCPIP Details		
TCP Listener		
UDP Connections		
Routing Table statistics collection		
TCPIP Gateways		
IPSec Security collection		
IPSec Status		
Current IP Filters		
Dynamic IP Tunnels		
IKE Tunnels		
Manual IP Tunnels		
VTAM Historical Data Collection Interval		
VTAM Summary Statistics		
EE Connections		
EE Connections Details		
HPR RTP Connections		
CSM Storage		
VTAM Address Space		
VTAM I/O		
VTAM Buffer Pools		
VTAM Buffer Pool Extents		
VTAM Buffer Pool Usage by Address Space		
VTAM Buffer Pool Usage by Application		

Table 110. Disk space summary (continued)		
Historical attribute table	**Historical attribute table size in KB (for a 24-hour period)**	**Subtotal of storage required in cylinders**
VTAM Buffer Pool Usage by Category		
FTP Data Storage		
FTP Sessions		
TCPIP FTP		
TN3270 Data Storage		
TN3270 Server Sess Avail		
Total Storage Required		

Estimating the storage required per LPAR
These formulas help you estimate the amount of storage required for historical data tables on a per LPAR basis.

Use the following formula to estimate the cylinders of 3390 DASD required.

$$\text{Storage to allocate} = \frac{\text{Total storage required in KB}}{\text{717 KB per cylinder}} \times \frac{\text{Group Count}}{(\text{Group Count} - 2)}$$

Figure 9. KB formula for total storage required per LPAR for cylinders of 3390 DASD

If you estimated in cylinders, you can use the following formula:

$$\text{Storage to allocate} = \text{Total storage in cylinders} \times \frac{\text{Group Count}}{(\text{Group Count} - 2)}$$

Figure 10. Cylinder formula for total storage required per LPAR in cylinders of 3390 DASD

Format of the SNMP configuration file

Since V4.2, SNMP data collection in the IBM Z OMEGAMON Network Monitor monitoring agent was enhanced to give you greater flexibility when communicating with the SNMP agents.

SNMP data collection supports the use of IPv6 interfaces in the configuration.

Before you can use this enhanced SNMP function, you must configure it. This section describes the syntax of the SNMP manager configuration file.

Note: Do not modify or point your PROCs to this sample copy. This copy will be regenerated when the RTE is loaded. Make a copy of this sample and modify it to your needs.

When to create the SNMP configuration file

Create your site's SNMP configuration file after you run the Configuration Tool or PARMGEN, but before you start the IBM Z OMEGAMON Network Monitor monitoring agent.

Sample files are generated by the PARMGEN method when the **Create Runtime Members** job is run and are stored in *&hilev.&midlev.&rtename.*RKANSAMU. This sample files is named KN3SNMP.

For PARMGEN, the sample file is created when you run the KCIJPW2R JCL job. The member is stored in *&hilev.&midlev.&rtename.*RKANSAMU.

The SNMP configuration file can be a sequential data set or a member of a partitioned data set. The SNMP configuration file does not have to have the same attributes as the *&rhilev.&midlev.&rtename.*RKANSAMU

data set. The data set might have fixed or variable record format with a record length of up to and including 2048 bytes.

Format of the SNMP manager configuration file

Information entered into the SNMP configuration file should be in this format.

For each SNMP agent with which IBM Z OMEGAMON Network Monitor will communicate when monitoring one or more TCP/IP stacks, you must add a line to the SNMP manager configuration files in the format shown in the following section:

```
ip_address   port_number   snmp_version   community_name
```

Where:

ip_address
Is the IP address of the SNMP agent associated with the TCP/IP stack being monitored. In IBM Z OMEGAMON Network Monitor, the IP address can be an IPv6 address. This parameter is required because there is no default value.

port_number
Is the port number on which the SNMP agent is listening for SNMP requests. The port number can be between 1-65535, inclusive. The parameter is required, but a hyphen (dash) may be coded to indicate that the default value of 161 is to be used.

snmp_version
Is the version of SNMP protocol to be used when communicating with the SNMP agent. This parameter is required as there is no default value. Code snmpv2.

community_name
Is the community name (password) to be used to request data from the SNMP agent. The value is a character string that is between 1 and 255 characters, inclusive, in length. This parameter is required, but a hyphen (dash) may be coded to indicate that the default value of **public** is to be used.

When creating this configuration file, these rules apply:

- All parameters for an entry must be contained on one line in the configuration file.
- You may insert comments into this file. Comments begin with a # character in column 1.

Sample configuration file

Here is a sample configuration file:

```
################################################################################
#                                                                              #
# NAME:         KN3SNMP                                                        #
#                                                                              #
# PURPOSE:      Sample Simple Network Management Protocol (SNMP)      #
#               configuration file                                             #
#                                                                              #
# This sample provides information for configuring SNMP manager        #
# functions used by TCP/IP data collection.  The entries define SNMP   #
# agents with which the SNMP manager functions may communicate.  They #
# also provide additional information to enable the communication.     #
#                                                                              #
# It is possible to share a single SNMP configuration file among       #
# OMEGAMON for Networks started task procedures. Sharing a single      #
# SNMP configuration file could make it easier for an administrator an#
# to maintain the list of TCP/IP stacks that OMEGAMON for Networks     #
# monitors.  A shared KN3SNMP configuration can be acheived            #
# by altering the KN3SNMP DD card in the OMEGAMON for Networks         #
# started task procedures to use the same SNMP configuration file.     #
#                                                                              #
# This file may have fixed or variable record format and a record      #
# length up to and including 2048 bytes.                              #
#                                                                              #
# The rules for the entries in this file are as follows.               #
#                                                                              #
#   - Comments begin with a # character in column 1                    #
#   - All parameters for an entry must be contained on one line        #
```

```
#                                                                      #
# An entry in this file is made up of the following positional         #
# parameters.                                                          #
#                                                                      #
#   - SNMP agent address                                               #
#                                                                      #
#     IP address of an SNMP agent with which the SNMP manager          #
#     functions of TCP/IP data collection may communicate.             #
#     This parameter is required and there is no default value.        #
#                                                                      #
#   - SNMP agent port number                                           #
#                                                                      #
#     Port number on which an SNMP agent is listening for              #
#     requests.  The value may be between 1 and 65535, inclusive.      #
#     This parameter is required; however, a dash (-) may be           #
#     coded to indicate that the conventional SNMP request             #
#     port number 161 is to be used.                                   #
#                                                                      #
#   - SNMP version                                                     #
#                                                                      #
#     Version of the SNMP protocol whose requests are being used       #
#     to communicate with an SNMP agent.  This parameter is            #
#     required.  "snmpv2" is the only supported value.                 #
#                                                                      #
#   - Community name                                                   #
#                                                                      #
#     The community name (password) to be used in requests sent to     #
#     an SNMP agent.  The value may be between 1 and 255               #
#     characters, inclusive, in length.  This parameter is             #
#     required; however, a dash (-) may be coded to indicate that      #
#     the default community name of "public" is to be used.            #
#                                                                      #
# Sample definitions for SNMP agents appear below.  They are for       #
# illustrative purposes only.                                          #
#                                                                      #
########################################################################
########################################################################
# Member: KN3$SNMP                                                     #
# Master Source: TDZOST.IZMS110A.TKANSAM(KN3PRMLB)                     #
# KCIJPUP1 or KCIJPCFG/KCIJPPRF Batch Job Output:                      #
#   TDZOST.IZMS110A.M5PBRSB6.IKANSAMU(KN3$SNMP) - IBM Default Copy     #
#   TDZOST.IZMS110A.M5PBRSB6.WCONFIG(KN3$SNMP)  - Customer Copy        #
# Purpose:                                                             #
#   WCONFIG(KN3$SNMP) SNMP configuration file input to the             #
#   xKANSAMU(KN3SNMP) and xKANSAMU(KONSNMP) members for both           #
#   OMEGAMON for Networks CUA and Agent components.                    #
#                                                                      #
#   xKANSAMU(KN3SNMP) is the default value for the                     #
#   KN3_SNMP_CONFIG_FILE LPAR RTE profile parameter.  The              #
#   KN3_SNMP_CONFIG_FILE dataset value is concatenated in the KN3SNMP  #
#   DD of the OMEGAMON for Networks Agent address space and CUA        #
#   address space. CUA is supported in v5.3.0 and below.               #
#                                                                      #
#   Ensure that you customize the KN3_SNMP_CONFIG_FILE parameter with  #
#   the KN3SNMP member of your choice (whether it is the default       #
#   KN3SNMP member supplied by PARMGEN in the xKANSAMU dataset, or     #
#   your own user controlled member.                                   #
# Instructions:                                                        #
#   1. Add a configuration statement for each SNMP agent from which    #
#      data will be collected (one per TCP/IP stack).                  #
#      Sample definitions for SNMP agents appear below.  They are for  #
#      illustrative purposes only.                                     #
#   2. Refer to topic "Format of the SNMP manager configuration file"  #
#      in the product Knowledge Center for more information about      #
#      this file format.                                               #
#      Refer to "Appendix F. Format of the SNMP configuration file"    #
#      for v5.3.0 and below.                                           #
#   3. WCONFIG(KCIJPCCF) "Clone customized WCONFIG members" job may    #
#      also be used to copy this imbed to other RTEs' WCONFIG          #
#      libraries so the cloned RTE also starts using this imbed in     #
#      the runtime member where $PARSE* "Create runtime members and    #
#      jobs" would imbed it.                                           #
#   4. Sample placeholder entries for user-defined system variables    #
#      have been set-up for modeling if this RTE will be enabled for   #
#      for system variables.                                           #
#      TDZOST.IZMS110A.PARMGEN.JCL(M5PBRSB6)                           #
#      System Variables profile has the corresponding symbols          #
#      defined to resolve to the sample SNMP agent entry.              #
#      If you choose to use these entries, customize the               #
#      TDZOST.IZMS110A.PARMGEN.JCL(M5PBRSB6)                           #
#      System Variables profile accordingly and enable the             #
#      "&SNMP_ENTRYn." entries by uncommenting out the user-defined    #
```

```
#      symbol to use (remove the "#" on column 1).                    #
#                                                                     #
#&SNMP_ENTRY1.
#&SNMP_ENTRY2.
#&SNMP_ENTRY3.
#&SNMP_ENTRY4.
#&SNMPIPADDR. &SNMPPORT. snmpv2 &SNMPCOMM.
#   Note: By default, the auto-discovered IP address (in the system   #
#         where the PARMGEN KCIJPUP1 job was submitted) is provided   #
#         for your convenience.                                       #
#######################################################################################
127.0.0.1                                    -    snmpv2     -
192.168.54.96                                -    snmpv2     -
10.10.3.72                                 2161   snmpv2  public
10.10.3.73                                   -    snmpv2     -
FF01::0001                                 8161   snmpv2  publicv6
FE80:1234:5678:9ABC:DEF0:1234:5678:9ABC   65161   snmpv2     -
```

Appendix B. Disk space requirements for historical data tables

You can calculate the amount of DASD required to support the persistent data store for storing historical data in Tivoli Data Warehouse.

This section provides the information you will need to determine space allocations in the persistent data store for each monitoring agent. Therefore, the disk space requirements in the tables in this section are for short-term history, which is stored on z/OS systems in the OMEGAMON XE persistent data store.

Network size and the type of network resources managed vary widely between enterprises. The amount and type of historical data that you choose to retain will greatly affect the amount of storage required. Wide differences between networks make it difficult to provide one size for the persistent data store that reflects the needs of most enterprises.

The default storage allocation is efficient for a very small network. Most users will need to allocate additional storage and data sets. Increase the default number of data sets from 3 to 5 or more. Increasing the number of data sets, using the **Group Count** parameter in the Control Program, is explained in the following section under “Allocating additional storage and data sets” on page 510.

This appendix provides you with the following information:

- Alternative methods for determining storage
- Effective allocation of additional storage and data sets (if needed)
- A list of attribute tables supported by short-term history
- Record size for each attribute table
- Worksheets to help you estimate the storage required

Note: If you are upgrading from V4.1 or 4.2 and did this exercise for one of these releases, it is recommended that you do it again for V5.1. The upgraded versions contain new attribute tables, and new attributes are included in existing tables.

Alternative methods of determining storage requirements

One way to determine the amount of DASD required for your persistent data is trial and error.

Many users who estimate the storage requirements for collecting historical data do it by trial and error. The main problems with this approach are twofold:

1. Every time you adjust storage parameters (number of cylinders and number of data sets), you must stop the agent. This might be unacceptable if implemented in a production network.
2. The network you use to determine storage parameters might not be comparable in size to the network where you will collect short-term history

If trial and error is not an acceptable approach in your environment, then you can use the information in this appendix to estimate storage size.

Trial and error approach

Use this information to understand how to effectively execute a trial and error approach for computing storage requirements.

About this task

To compute space requirements by trial and error, start historical collection for all resources you need to store in short-term history, and collect at least 25 hours of data. If you cannot draw a report containing the last 24 hours of data, for any attribute table, then you need to allocate additional storage or data sets or both.

If you are collecting short-term history, you can also create a rough estimate of the hours of measurement data you can store by looking in the RKPDLOG log of the IBM Z OMEGAMON Network Monitor monitoring agent. This log can be viewed from MVS/TSO in the SDSF Status window. To perform this estimate, do the following:

1. Examine the RKPDLOG log.
2. Record the elapsed time between the message:

   ```
   KPDIFIL: Initial output file selection completed successfully for group KN3
   ```

   And the message:

   ```
   KPDDSTR:  File rhilev.&midlev.RKN3HIS3 is full
   ```

This rough estimator works whether you have the default 3 history data sets (RKN3HIS1 – RKN3HIS3) or more data sets. Short-term history first fills the data set with the highest suffix (for example, RKN3HIS7) and then works its way down to RKN3HIS1, before it wraps back to the data set with the highest suffix.

If the elapsed time is 24 hours or greater, you should have enough storage allocated for users to view reports with 24 hours of data. If the elapsed time is less than 24 hours, then you need to allocate additional storage or data sets or both.

If you need to increase space allocation, and estimate how much to allocate, you should understand the relationship between the two configurable storage parameters: allocated Cylinders and Group Count, explained under “Allocating additional storage and data sets” on page 510.

Estimating approach

The information and worksheets in this section can be used to estimate storage requirements.

You will need to know the following:

1. Resource types (attribute tables) that need to be collected for history.
2. Approximate quantity of each resource type that will be monitored. If the number of monitored resources varies widely between different LPARs, and different TCP/IP stacks, you might want to estimate the different storage requirements for each LPAR and each TCP/IP stack.
3. Historical collection interval.

Allocating additional storage and data sets

You can override the default storage sizes that the PARMGEN method provided for short-term history data sets. Understand the varied roles that short-term history plays and how to change the size of your persistent data store.

The PARMGEN method provides default storage size values for short-term history data sets in the persistent data store. You can override these defaults. The IBM Z OMEGAMON Network Monitor monitoring agent storage size defaults are shown in Table 111 on page 548.

Table 111. Definition and default values for cylinders and group count parameters

Storage parameters	Default values
Cylinders *Cylinders* is a measure of storage capacity on a disk drive. Considering control blocks and indexing, the persistent data store can store approximately 717 KB of measurement data on one cylinder of 3390 disk drive. After you determine the number of cylinders you need for your environment, add 37 to it to account for the RN3SGRPx data sets. This value is then entered into the **Est Cyl Space** field of the Persistent Datastore Specifications panel.	420 (for the persistent data stores, 383 for the RKN3HISx data sets + 37 for the RN3SGRPx data sets)

Table 111. Definition and default values for cylinders and group count parameters (continued)	
Storage parameters	**Default values**
Group Count *Group Count* refers to the number of persistent data store data sets. Each persistent data store dataset will be allocated with (Cylinders / Group Count) number of cylinders. A Group Count of 6 means that 6 RKN3HISx data sets will be allocated for measurement data.	6

Short-term history is more than a place to store data. It enables:

- Continuous operations without manual attention to pruning outdated data
- Dynamic data set switching (data wrapping without losing data)
- Display of a full 24 hours of data, in a Tivoli Enterprise Portal report, at any point in time
- Access to 72 or more hours of data from the OMEGAMON Enhanced 3270 User Interface

These features require that one of the data sets be temporarily unavailable in preparation for data set switching. In addition, preserving the ability to display data from the last 24, 72, or more hours at any time of day might require that an additional data set be allocated to accommodate when the data set being written to is almost empty.

To account for the extra data sets needed to enable these features, apply a *Group Count factor* to the total number of cylinders required to store 24, 72, or more hours of data in your network. The Group Count factor expresses the storage relationship of Group Count to the number of cylinders to allocate. That is:

```
Cylinders to Allocate = Cylinders needed for 24, 72, or more hours data
X  Group Count Factor
```

Where:

```
Group Count Factor = (Group Count / (Group Count - 2))
```

These two examples illustrate the effect of the Group Count Factor. These examples show how increasing the Group Count value can use the allocated cylinders of space more efficiently (that is, requires less space for the same amount of data). Note that warehousing (exporting data to Tivoli Data Warehouse) and short-term historical queries are more efficient in smaller persistent data store data sets (that is, higher group count).

This formula is used to calculate DASD for both examples:

```
Cylinders to Allocate = Cylinders needed for 24, 72, or more hours data
X  (Group Count / (Group Count - 2))
Cylinders to Allocate = 10 X (3/(3-2)  = 30
```

Figure 11. Formula for calculating DASD

Modelling some alternate Group Count values illustrates the impact that modifying this parameter has on the amount of DASD (Cylinders of 3390) to be allocated.

Table 112. Sample group count and cylinders to allocate to enable viewing of 24 hours of data			
Cylinders needed for 24 hours of data	**Group count**	**Group count factor**	**Cylinders to allocate**
Example 1: a very small test network requiring only 70 cylinders of 3390 DASD for 24 hours of data			
70	3	3.00	210
70	4	2.00	140
70	5	1.67	119

Table 112. Sample group count and cylinders to allocate to enable viewing of 24 hours of data (continued)

Cylinders needed for 24 hours of data	Group count	Group count factor	Cylinders to allocate
70	6	1.50	105
70	7	1.40	105
70	8	1.33	91
70	9	1.29	91
70	10	1.25	91
Example 2: a somewhat larger network requiring 500 cylinders of 3390 DASD for 24 hours of data			
500	3	3.00	1500
500	4	2.00	1000
500	5	1.67	830
500	6	1.50	750
500	7	1.40	700
500	8	1.33	670
500	9	1.29	640
500	10	1.25	630

For the small network in Example 1, retaining the default Group Count value of 6 is more than adequate. However, for the larger network in Example 2, you would need to increase group count and cylinders, possibly to 7 and 700. For a monitored network with more than 10,000 TCP/IP connections, consider using a Group Count of at least 8.

When you consider these examples in light of the default values that ship with this product (Cylinders 3390 = 420 and Group Count = 6), you can accept the defaults with no loss of function for the small network. However, for the larger network in Example 2, you could not accept the defaults and confidently expect that users could view a report with 24 hours of data at any time of day. However, if you increased Group Count to at least 7 (and your network size estimate is correct), you should be able to provide this support by allocating 700 cylinders (+37) of additional DASD to short-term history.

Estimating the space requirements

Before providing sizings for historical data collection tables, understand how this data is collected.

You can collect historical data for the IBM Z OMEGAMON Network Monitor attribute tables listed in Table 43 on page 513. The columns in Table 43 on page 513 are explained in the section that follows:

Attribute Table
Is the name of the attribute table in which historical data is stored.

Filename
Is the name of the file that corresponds to the name of the attribute table.

Default
Specifies whether the table is configured if you select **Default Groups** in the Historical Collection dialog.

Estimated Storage Required
Is the estimated space required to store 24 hours of data per monitored resource.

A row stored in short-term history consists of all the attributes in the real-time row, plus 28 bytes per row to account for the additional fields maintained for all historical records. Space requirements for real-time data are described under "Understanding how historical data is collected" on page 14.

For most attribute groups, real-time data is only kept for the most recent measurement. For historical collection, data is stored for each history collection interval.

You might also choose to configure long-term history, and therefore store data for periods longer than 24 hours. Long-term history is stored in the Tivoli Data Warehouse. Fortunately, the space requirements per row of data are the same for a row of data in short-term history (in the persistent data store) and a row of data in long-term history (in a relational database).

Some clients use the archiving feature of short-term history to save backups and to collect more than 24 hours of data for analysis in a third-party statistical software package. Disk space requirements for archives are not included in the basic disk space requirements that are shown in Table 43 on page 513.

Historical data tables

To understand how to size your historical data tables, look at this table, which displays the storage used when monitoring one resource for 24 hours for every attribute group.

Table 113 on page 551 lists the IBM Z OMEGAMON Network Monitor attribute tables available for historical collection. This table displays the storage used when monitoring one resource for 24 hours, assuming collection intervals of 15 minutes.

Table 113. Historical data tables

Attribute table	File name	Default*	Estimated storage required for one data set (in KB)	Estimated storage required for one data set (3390 cylinders; No. of cylinders = KB/717)
Agent				
KN3 Agent Status	KN3AGS	Yes	24	0.0329
KN3 SNA Collector Status	KN3SCS	Yes	12	0.0173
KN3 TCP Collector Status	KN3TCS	Yes	73.5	0.1025
TCP/IP				
Current IP Filters	KN3IFC	No	79	0.1098
Dynamic IP Tunnels	KN3ITD	No	99	0.1376
FTP Sessions	KN3FSE	Yes	0.8	0.0011
Interfaces	KN3TIF	Yes	47	0.0654
IKE Tunnels	KN3ITI	No	65	0.0905
IPSec Status	KN3ISS	Yes	36	0.0507
KN3 ICMP Global Counters	KN3GCG	No	12	0.0167
KN3 ICMP Type Counters	KN3GCT	No	10	0.0141
KN3 Interface Address	KN3IFA	No	15	0.0209
KN3 Interface Read Queue	KN3IFR	No	32	0.0445
KN3 Interface Statistics	KN3IFS	No	31	0.0434
KN3 Interface Status	KN3IFE	No	35	0.0486

Table 113. Historical data tables (continued)

Attribute table	File name	Default*	Estimated storage required for one data set (in KB)	Estimated storage required for one data set (3390 cylinders; No. of cylinders = KB/717)
KN3 Interface Write Queue	KN3IFW	No	21	0.0298
KN3 IP Counter Statistics	KN3GIC	No	24	0.0340
KN3 IP General Statistics	KN3GIG	No	11	0.0146
KN3 OSA-Express5S Ports Control	KN35SC	No	15	0.0209
KN3 OSA-Express5S Ports Errors	KN35SE	No	26	0.0366
KN3 OSA-Express5S Ports Summary	KN35SS	No	34	0.0468
KN3 OSA-Express5S Ports Throughput	KN35ST	No	34	0.0468
KN3 TCP Counter Statistics	KN3GTC	No	29	0.0403
KN3 UDP Counter Statistics	KN3GUC	No	15	0.0204
Manual IP Tunnels	KN3ITM	No	37	0.0513
OSA-Express Channels	KN3TCH	Yes	42	0.0581
OSA-Express LPARS	KN3TLP	Yes	201	0.2803
OSA-Express Ports	KN3TPO	Yes	75	0.1041
OSA 10 Gigabit Ports Control	KN3TTC	No	39	0.0547
OSA 10 Gigabit Ports Errors	KN3TTE	Yes	42	0.0591
OSA 10 Gigabit Ports Summary	KN3TTS	Yes	48	0.0664
OSA 10 Gigabit Ports Throughput	KN3TTT	No	42	0.0586
OSA-Express3 Ports Control	KN3THC	No	39	0.0547
OSA-Express3 Ports Errors	KN3THE	Yes	48	0.0664
OSA-Express3 Ports Summary	KN3THS	Yes	68	0.0947
OSA-Express3 Ports Throughput	KN3THT	No	48	0.0669
TCP Listener	KN3TCL	Yes	28	0.0387
TCPIP Address Space	KN3TAS	Yes	61	0.0853

Table 113. Historical data tables (continued)

Attribute table	File name	Default*	Estimated storage required for one data set (in KB)	Estimated storage required for one data set (3390 cylinders; No. of cylinders = KB/717)
TCPIP Applications	KN3TAP	Yes	64	0.0894
TCPIP Connections	KN3TCN	Yes	62	0.0863
TCPIP Details	KN3TCP	Yes	60	0.0842
TCPIP Devices	KN3TDV	Yes	43	0.0601
TCPIP FTP (FTP transfers)	KN3FTP	Yes	5	0.0068
TCPIP Gateways	KN3TGA	Yes	59	0.0821
TCPIP Memory Statistics	KN3TPV	Yes	47	0.0654
TCPIP Stack Layer	KN3TSL	Yes	60	0.0832
TN3270 Server Sess Avail	KN3TNA	Yes	15	0.0207
UDP Connections	KN3UDP	Yes	36	0.0507
VTAM				
CSM Storage	KN3CSM	Yes	19	0.0267
EE Connections	KN3EEC	Yes	26	0.0361
EE Connection Details	KN3EED	Yes	126	0.1752
HPR RTP Connections	KN3HPR	Yes	56	0.0779
KN3 CSM Storage by Owner	KN3CSO	No	18	0.0256
VTAM Address Space	KN3VAS	Yes	26	0.0356
VTAM Buffer Pool Extents	KN3BPE	No	12	0.0162
VTAM Buffer Pools	KN3BPD	Yes	239	0.3332
VTAM Buffer Usage by Address Space	KN3BPS	Yes	9	0.0131
VTAM Buffer Usage by Application for Address Space	KN3BPA	Yes	10	0.0141
VTAM Buffer Usage by Category	KN3BPG	Yes	108	0.1506
VTAM I/O	KN3VIO	Yes	56	0.0785
VTAM Summary Statistics	KN3SNA	Yes	9	0.0131
Total			2760.6 KB	3.8502 cylinders

*Indicates the attribute groups for which product developers have defined historical views. You must configure these attribute groups if you want to see historical data in the predefined workspaces.

Tools for estimating data storage requirements

Use the worksheets in this section to understand the formula for historical collection, the attribute group record sizes, and the space requirements for the various data types for historical data storage.

The following types of formulas and data type combinations are included in this product:

- Agent historical data storage
- TCP/IP historical data storage
- VTAM historical data storage
- FTP historical data storage
- TN3270 historical data storage

The following formulas and worksheets provide the information needed to estimate storage requirements for each of the data types.

Agent historical data storage

Use this information to understand the formula for historical collection, the attribute group record sizes, and the space requirements for Agent historical data storage.

- **Agent formula**

  Storage assumptions:

  – Historical collection interval: 15 minutes
  – Quantity of each resource types monitored: 1

$$\frac{\text{4 collections per hour} \times \text{24 hours} \times \text{Bytes per record} \times \text{1 monitored resource (agent)} \times \text{1 row per resource}}{1024} = \text{KB per 24-hour period}$$

Which simplifies to:

$$\frac{96 \times \text{Number of bytes per record}}{1024} = \text{KB per 24-hour period}$$

Figure 12. Formula for Agent historical collection data storage

- **Attribute group record sizes**

  This data is collected once every collection interval for the agent. The number of rows returned may vary depending on the table. For example, the number of rows returned for the TCP Collector Status table depends on how many TCP/IP stacks the agent is monitoring.

Table 114. Agent data collected

Type of data	Historical data attribute table	Row size in bytes	Frequency	Subtotal storage required
Agent	KN3 Agent Status	252	1 row	24 KB
	KN3 SNA Collector Status	132	1 row	12 KB
	KN3 TCP Collector Status	784	1 row per monitored stack	73.5 KB

- **Space requirement worksheets**

Use the worksheets shown in Tables 72 through 74 to estimate the disk space requirements for your site. A sample calculation is provided for each historical data collection table.

- Each worksheet is for one agent per LPAR.
- For an LPAR, there can be one VTAM address space and one or more TCP/IP address spaces being monitored by the agent. The number of rows returned for the TCP Collector Status table depends on how many TCP/IP address spaces the agent is monitoring. You will need to multiply the required storage by the number of TCP/IP address spaces being monitored.
- If you are monitoring multiple LPARs, complete a worksheet for each LPAR, or one worksheet that represents the average LPAR.

KN3 Agent Status (KN3AGS) worksheet
Use the KN3 Agent Status (KN3AGS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 115. KN3 Agent Status (KN3AGS) worksheet

Interval	Record size	Formula	Agent	Agent address space	Expected storage required for 24 hours
15 minutes	252	4 x 24 x 252 x1 x 1 / 1024	1	1	24 KB

KN3 TCP Collector Status (KN3TCS) worksheet
Use the KN3 TCP Collector Status (KN3TCS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 116. TCP Collector Status (KN3TCS) worksheet

Interval	Record size	Formula	Agent	Monitored TCP/IP address spaces	Expected storage required for 24 hours
15 minutes	784	4 x 24 x 784 x 1 x 1 / 1024	1	1	73.5 KB

KN3 SNA Collector Status (KN3SCS) worksheet
Use the KN3 SNA Collector Status (KN3SCS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 117. SNA Collector Status (KN3SCS) worksheet

Interval	Record size	Formula	Agent	VTAM address space	Expected storage required for 24 hours
15 minutes	132	4 x 24 x 132 x 1 x 1 / 1024	1	1	12 KB

TCP/IP historical data storage

Use this information to understand the formula for historical collection, the attribute group record sizes, and the space requirements for TCP/IP historical data storage.

- **TCP/IP formula**

  Storage assumptions:

  – Historical collection interval: 15 minutes

  – Quantity of each resource types monitored: 1

$$\frac{\text{4 collections per hour} \times \text{24 hours} \times \text{Bytes per record} \times \text{1 monitored resource} \times \text{1 row per resource} \times \text{1 TCP/IP stack}}{1024} = \text{KB per 24-hour period}$$

Which simplifies to:

$$\frac{96 \times \text{Number of bytes per record}}{1024} = \text{KB per 24-hour period}$$

Figure 13. Formula for TCP/IP historical collection data storage

- **Attribute group record sizes**

  This data is collected once every collection interval for each TCP/IP stack. If you have an LPAR with multiple TCP/IP stacks, combine the storage required for each stack you will monitor.

Table 118. Data collected once every collection interval

Type of data	Real-time data attribute group	Row size in bytes	Frequency per interval	Subtotal storage required (KB)
TCP/IP and VTAM (required collection)	TCPIP Memory Statistics	500	1 row per TCP/IP address space	47
TCP/IP Stack layer Statistics	TCPIP Address Space	652	1 row per TCPIP address space	61
	KN3 ICMP Global Counters	128	1 row per TCP/IP address space	12
	KN3 ICMP Type Counters	108	1 row per ICMP type per ICMP version	10
	KN3 IP Counter Statistics	260	Up to 2 rows per TCP/IP address space	24
	KN3 IP General Statistics	112	1 row per TCP/IP address space	11
	KN3 TCP Counter Statistics	308	1 row per TCP/IP address space	29
	KN3 UDP Counter Statistics	156	1 row per TCP/IP address space	15
	TCPIP Stack Layer	636	1 row per TCP/IP address space	60

Table 118. Data collected once every collection interval (continued)

Type of data	Real-time data attribute group	Row size in bytes	Frequency per interval	Subtotal storage required (KB)
Interfaces statistics	Interfaces	500	1 row per interface	47
	KN3 Interface Address	160	1 row per TCP/IP interface address	15
	KN3 Interface Statistics	332	1 row per active strategic TCP/IP interface	31
	KN3 Interface Status	372	1 row per TCP/IP interface	35
	TCPIP Devices	460	1 row per device	43
Interface Data Link Control statistics collection	KN3 Interface Read Queue	340	1 row per read queue per active OSA Queued Direction I/O (QDIO) or HiperSockets interface	32
	KN3 Interface Write Queue	228	1 row per configured queue priority per OSA-Express Queued Direct I/O (QDIO) or HiperSocket interface	21

Table 118. Data collected once every collection interval (continued)

Type of data	Real-time data attribute group	Row size in bytes	Frequency per interval	Subtotal storage required (KB)
OSA statistics collection	OSA-Express Channels	444	1 row per OSA Channel	42
	OSA-Express LPARS	134	1 row per OSA LPAR	201
	OSA-Express Ports	796	1 row per OSA Port	75
	OSA 10 Gigabit Ports Control	418	1 row per OSA-Express 2 10 Gigabit Port	39
	OSA 10 Gigabit Ports Errors	452	1 row per OSA-Express 2 10 Gigabit Port	42
	OSA 10 Gigabit Ports Summary	508	1 row per OSA-Express 2 10 Gigabit Port	48
	OSA 10 Gigabit Ports Throughput	448	1 row per OSA-Express 2 10 Gigabit Port	42
	OSA-Express3 Ports Control	418	1 row per OSA-Express3 Port	39
	OSA-Express3 Ports Errors	508	1 row per OSA-Express3 Port	48
	OSA-Express3 Ports Summary	724	1 row per OSA-Express3 Port	68
	OSA-Express3 Ports Throughput	512	1 row per OSA-Express3 Port	48
	KN3 OSA-Express5S Ports Control	160	1 row per OSA-Express5S Port	15
	KN3 OSA-Express5S Ports Errors	280	1 row per OSA-Express5S Port	26
	KN3 OSA-Express5S Ports Summary	360	1 row per OSA-Express5S Port	34
	KN3 OSA-Express5S Ports Throughput	358	1 row per OSA-Express5S Port	34
TCP/IP Connection and Application Performance statistics collection	TCPIP Applications	684	1 row per TCP/IP application	64
	TCPIP Connections	660	1 row per TCPIP connection	62
	TCPIP Details	644	1 row per TCP connection	60
	TCP Listener	296	1 row per TCP listener	28
	UDP Connections	388	1 row per UDP endpoint	36
Routing Table Statistics Collection	TCPIP Gateways	628	1 row per TCP/IP gateway collected on Routing Table Collection Frequency	59

Table 118. Data collected once every collection interval (continued)				
Type of data	**Real-time data attribute group**	**Row size in bytes**	**Frequency per interval**	**Subtotal storage required (KB)**
IPSec Security collection	IPSec Status	388	1 row per TCP/IP address space	36
	Current IP Filters	840	1 row per IP filter	79
	Dynamic IP Tunnels	1052	1 row per dynamic IP tunnel	99
	IKE Tunnels	692	1 row per IKE tunnel	65
	Manual IP Tunnels	392	1 row per manual IP tunnel	37

- **Space requirement worksheets**

  Use the worksheets shown in Tables 76 through 109 to estimate the disk space requirements for your site. A sample calculation is provided for each historical data collection table.

  – Each worksheet is for one monitored resource per LPAR or per TCP/IP stack.
  – Typically you are monitoring more than one resource (that is, one TCP/IP address space, connection, or session, for example). You need to multiply the required storage by the number of resources.
  – If you are monitoring multiple LPARs, complete a worksheet for each LPAR, or one worksheet that represents the average LPAR.
  – If you are monitoring more than one TCP/IP stack in an LPAR, multiply by the number of TCP/IP stacks.

Current IP Filters (KN3IFC) worksheet
Use the Current IP Filters (KN3IFC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 119. Current IP Filters (KN3IFC) worksheet					
Interval	**Record size**	**Formula**	**TCP/IP address space resources**	**IP Filters**	**Expected storage required for 24 hours**
15 minutes	840	4 x 24 x 840 x 1 x 1 / 1024	1	1	79 KB

Dynamic IP Tunnels (KN3ITD) worksheet
Use the Dynamic IP Tunnels (KN3ITD) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 120. Dynamic IP Tunnels (KN3ITD) worksheet					
Interval	**Record size**	**Formula**	**TCP/IP address space resources**	**Dynamic IP Tunnels**	**Expected storage required for 24 hours**
15 minutes	1052	4 x 24 x 1052 x 1 x 1 / 1024	1	1	99 KB

Interfaces (KN3TIF) worksheet
Use the Interfaces (KN3TIF) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 121. Interfaces (KN3TIF) worksheet

Interval	Record size	Formula	TCP/IP interface	TCP/IP stack	Expected storage required for 24 hours
15 minutes	500	4 x 24 x 500 x 1 x 1 x 1/ 1024	1	1	47 KB

IKE Tunnels (KN3ITI) worksheet
Use the IKE Tunnels (KN3ITI) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 122. IKE Tunnels (KN3ITI) worksheet

Interval	Record size	Formula	TCP/IP address space resources	Dynamic IP Tunnels	Expected storage required for 24 hours
15 minutes	692	4 x 24 x 692 x 1 x 1 / 1024	1	1	65 KB

IPSec Status (KN3ISS) worksheet
Use the IPSec Status (KN3ISS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 123. IPSec Status (KN3ISS) worksheet

Interval	Record size	Formula	TCP/IP address space resources	TCP/IP stack	Expected storage required for 24 hours
15 minutes	388	4 x 24 x 388 x 1 x 1 / 1024	1	1	36 KB

KN3 ICMP Global Counters (KN3GCG) worksheet
Use the KN3 ICMP Global Counters (KN3GCG) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 124. KN3 ICMP Global Counters (KN3GCG) worksheet

Interval	Record size	Formula	ICMP protocol	ICMP Version	TCP/IP stack	Expected storage required for 24 hours
15 minutes	128	4 x 24 x 128 x 1 x 1 x 1 / 1024	1	1	1	12 KB

KN3 ICMP Type Counters (KN3GCT) worksheet
Use the KN3 ICMP Type Counters (KN3GCT) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 125. KN3 ICMP Type Counters (KN3GCT) worksheet

Interval	Record size	Formula	ICMP type	TCP/IP stack	Expected storage required for 24 hours
15 minutes	108	4 x 24 x 108 x 1 x 1 / 1024	1	1	10 KB

KN3 Interface Address (KN3IFA) worksheet
Use the KN3 Interface Address (KN3IFA) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 126. KN3 Interface Address (KN3IFA) worksheet

Interval	Record size	Formula	TCP/IP interface address	TCP/IP interface	TCP/IP stack	Expected storage required for 24 hours
15 minutes	160	4 x 24 x 160 x 1 x 1 x 1 / 1024	1	1	1	15 KB

KN3 Interface Read Queue (KN3IFR) worksheet
Use the KN3 Interface Read Queue (KN3IFR) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 127. KN3 Interface Read Queue (KN3IFR) worksheet

Interval	Record size	Formula	Read queue	Active TCP/IP QDIO or HiperSockets interface	TCP/IP stack	Expected storage required for 24 hours
15 minutes	340	4 x 24 x 340 x 1 x 1 x 1 / 1024	1	1	1	32KB

KN3 Interface Statistics (KN3IFS) worksheet
Use the KN3 Interface Statistics (KN3IFS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 128. KN3 Interface Statistics (KN3IFS) worksheet

Interval	Record size	Formula	Active TCP/IP strategic interface*	TCP/IP stack	Expected storage required for 24 hours
15 minutes	332	4 x 24 x 332 x 1 x 1 / 1024	1	1	31 KB

* The strategic interfaces have one of the following values for the Interface Type attribute on KN3 workspaces: Loopback, OSA-Express Queued Direct I/O (QDIO) Ethernet, HiperSockets, or Multipath Channel Point-To-Point (MPCPTP)

KN3 Interface Status (KN3IFE) worksheet
Use the KN3 Interface Status (KN3IFE) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 129. KN3 Interface Status (KN3IFE) worksheet

Interval	Record size	Formula	TCP/IP interface	TCP/IP stack	Expected storage required for 24 hours
15 minutes	372	4 x 24 x 372 x 1 x 1 / 1024	1	1	35 KB

KN3 Interface Write Queue (KN3IFW) worksheet
Use the KN3 Interface Write Queue (KN3IFW) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 130. KN3 Interface Write Queue (KN3IFW) worksheet

Interval	Record size	Formula	Write queue	Active TCP/IP QDIO or HiperSockets interface	TCP/IP stack	Expected storage required for 24 hours
15 minutes	228	4 x 24 x 228 x 1 x 1 x 1 / 1024	1	1	1	21 KB

KN3 IP Counter Statistics (KN3GIC) worksheet
Use the KN3 IP Counter Statistics (KN3GIC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 131. KN3 IP Counter Statistics (KN3GIC) worksheet

Interval	Record size	Formula	IP counter statistics	IP version	TCP/IP stack	Expected storage required for 24 hours
15 minutes	260	4 x 24 x 260 x 1 x 1 x 1 / 1024	1	1	1	24 KB

KN3 IP General Statistics (KN3GIG) worksheet
Use the KN3 IP General Statistics (KN3GIG) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 132. IP General Statistics (KN3GIG) worksheet

Interval	Record size	Formula	IP protocol	TCP/IP stack	Expected storage required for 24 hours
15 minutes	112	4 x 24 x 112 x 1 x 1 / 1024	1	1	11 KB

KN3 TCP Counter Statistics (KN3GTC) worksheet
Use the KN3 TCP Counter Statistics (KN3GTC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 133. KN3 TCP Counter Statistics (KN3GTC) worksheet

Interval	Record size	Formula	TCP/IP protocol	TCP/IP stack	Expected storage required for 24 hours
15 minutes	308	4 x 24 x 308 x 1 x 1 / 1024	1	1	29 KB

KN3 UDP Counter Statistics (KN3GUC) worksheet
Use the KN3 UDP Counter Statistics (KN3GUC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 134. KN3 UDP Counter Statistics (KN3GUC) worksheet

Interval	Record size	Formula	UDP protocol	TCP/IP stack	Expected storage required for 24 hours
15 minutes	156	4 x 24 x 156 x 1 x 1 / 1024	1	1	15 KB

Manual IP Tunnels (KN3ITM) worksheet
Use the Manual IP Tunnels (KN3ITM) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 135. Manual IP Tunnels (KN3ITM) worksheet

Interval	Record size	Formula	TCP/IP address space resources	Manual IP Tunnels	Expected storage required for 24 hours
15 minutes	392	4 x 24 x 392 x 1 x 1 / 1024	1	1	37 KB

OSA-Express Channels (KN3TCH) worksheet
Use the OSA-Express Channels (KN3TCH) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 136. OSA-Express Channels (KN3TCH) worksheet

Interval	Record size	Formula	OSA-Express channels	TCP/IP stack	Expected storage required for 24 hours
15 minutes	444	4 x 24 x 444 x 1 x 1 x 1 / 1024	1	1	42 KB

OSA-Express LPARS (KN3TLP) worksheet
Use the OSA-Express LPARS (KN3TLP) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 137. OSA-Express LPARS (KN3TLP) worksheet

Interval	Record size	Formula	OSA-Express Channels	OSA Express LPARS	TCP/IP stack	Expected storage required for 24 hours
15 minutes	134	4 x 24 x 134 x 1 x 16 x 1 / 1024	1	16	1	201

OSA-Express Ports (KN3TPO) worksheet
Use the OSA-Express Ports (KN3TPO) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 138. OSA-Express Ports (KN3TPO) worksheet

Interval	Record size	Formula	OSA-Express port	TCP/IP stack	Expected storage required for 24 hours
15 minutes	796	4 x 24 x 796 x 1 x 1 x 1 / 1024	1	1	75 KB

OSA 10 Gigabit Ports Control (KN3TTC) worksheet
Use the OSA 10 Gigabit Ports Control (KN3TTC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 139. OSA 10 Gigabit Ports Control (KN3TTC) worksheet

Interval	Record size	Formula	OSA 10 Gigabit ports control	TCP/IP stack	Expected storage required for 24 hours
15 minutes	418	4 x 24 x 418 x 1 x 1 x 1 / 1024	1	1	39

OSA 10 Gigabit Ports Errors (KN3TTE) worksheet
Use the OSA 10 Gigabit Ports Errors (KN3TTE) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 140. OSA 10 Gigabit Ports Errors (KN3TTE) worksheet

Interval	Record size	Formula	OSA 10 Gigabit ports errors	TCP/IP stack	Expected storage required for 24 hours
15 minutes	452	4 x 24 x 452 x 1 x 1 x 1 / 1024	1	1	42 KB

OSA 10 Gigabit Ports Summary (KN3TTS) worksheet
Use the OSA 10 Gigabit Ports Summary (KN3TTS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 141. OSA 10 Gigabit Ports Summary (KN3TTS) worksheet

Interval	Record size	Formula	OSA 10 Gigabit port	TCP/IP stack	Expected storage required for 24 hours
15 minutes	508	4 x 24 x 508 x 1 x 1 x 1 / 1024	1	1	48 KB

OSA 10 Gigabit Ports Throughput (KN3TTT) worksheet
Use the OSA 10 Gigabit Ports Throughput (KN3TTT) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 142. OSA 10 Gigabit Ports Throughput (KN3TTT) worksheet

Interval	Record size	Formula	OSA 10 Gigabit ports throughput	TCP/IP stack	Expected storage required for 24 hours
15 minutes	448	4 x 24 x 448 x 1 x 1 x 1 / 1024	1	1	42

OSA-Express3 Ports Control (KN3THC) worksheet
Use the OSA-Express3 Ports Control (KN3THC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 143. OSA-Express3 Ports Control (KN3THC) worksheet

Interval	Record size	Formula	OSA-Express3 ports control	TCP/IP stack	Expected storage required for 24 hours
15 minutes	418	4 x 24 x 418 x 1 x 1 x 1 / 1024	1	1	39

OSA-Express3 Ports Errors (KN3THE) worksheet
Use the OSA-Express3 Ports Errors (KN3THE) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 144. OSA-Express3 Ports Errors (KN3THE) worksheet

Interval	Record size	Formula	OSA-Express3 ports errors	TCP/IP stack	Expected storage required for 24 hours
15 minutes	508	4 x 24 x 508 x 1 x 1 x 1 / 1024	1	1	48 KB

OSA-Express3 Ports Summary (KN3THS) worksheet
Use the OSA-Express3 Ports Summary (KN3THS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 145. OSA-Express3 Ports Summary (KN3THS) worksheet

Interval	Record size	Formula	OSA-Express3 port	TCP/IP stack	Expected storage required for 24 hours
15 minutes	724	4 x 24 x 724 x 1 x 1 x 1 / 1024	1	1	68 KB

OSA-Express3 Ports Throughput (KN3THT) worksheet
Use the OSA-Express3 Ports Throughput (KN3THT) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 146. OSA-Express3 Ports Throughput (KN3THT) worksheet

Interval	Record size	Formula	OSA-Express3 ports throughput	TCP/IP stack	Expected storage required for 24 hours
15 minutes	512	4 x 24 x 512 x 1 x 1 x 1 / 1024	1	1	48

TCP Listener (KN3TCL) worksheet
Use the TCP Listener (KN3TCL) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 147. TCP Listener (KN3TCL) worksheet

Interval	Record size	Formula	TCP listeners	TCP/IP stack	Expected storage required for 24 hours
15 minutes	296	4 x 24 x 296 x 1 x 1 / 1024	1	1	28 KB

TCPIP Address Space (KN3TAS) worksheet
Use the TCPIP Address Space (KN3TAS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 148. TCPIP Address Space (KN3TAS) worksheet

Interval	Record size	Formula	TCP/IP address space resources	TCP/IP stack	Expected storage required for 24 hours
15 minutes	652	4 x 24 x 652 x 1 x 1 / 1024	1	1	61 KB

TCPIP Applications (KN3TAP) worksheet
Use the TCPIP Applications (KN3TAP) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 149. TCPIP Applications (KN3TAP) worksheet

Interval	Record size	Formula	TCP/IP applications	TCP/IP stack	Expected storage required for 24 hours
15 minutes	684	4 x 24 x 684 x 1 x 1 / 1024	1	1	64 KB

TCPIP Connections (KN3TCN) worksheet
Use the TCPIP Connections (KN3TCN) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 150. TCPIP Connections (KN3TCN) worksheet

Interval	Record size	Formula	TCP/IP connections	TCP/IP stack	Expected storage required for 24 hours
15 minutes	660	4 x 24 x 660 x 1 x 1 / 1024	1	1	62 KB

TCPIP Details (KN3TCP) worksheet
Use the TCPIP Details (KN3TCP) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 151. TCPIP Details (KN3TCP) worksheet

Interval	Record size	Formula	TCP connections	TCP/IP stack	Expected storage required for 24 hours
15 minutes	644	4 x 24 x 644 x 1 x 1 / 1024	1	1	60 KB

TCPIP Devices (KN3TDV) worksheet
Use the TCPIP Devices (KN3TDV) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 152. TCPIP Devices (KN3TDV) worksheet

Interval	Record size	Formula	TCP/IP devices	TCP/IP stack	Expected storage required for 24 hours
15 minutes	460	4 x 24 x 460 x 1 x 1 / 1024	1	1	43 KB

TCPIP Gateways (KN3TGA) worksheet
Use the TCPIP Gateways (KN3TGA) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 153. TCPIP Gateways (KN3TGA) worksheet

Interval	Record size	Formula	Gateways	TCP/IP stack	Expected storage required for 24 hours
15 minutes	628	4 x 24 x 628 x 1 x 1 x 1 / 1024	1	1	59 KB

TCPIP Memory Statistics (KN3TPV) worksheet
Use the TCPIP Memory Statistics (KN3TPV) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 154. TCPIP Memory Statistics (KN3TPV) worksheet

Interval	Record size	Formula	TCP/IP address spaces	TCP/IP stack	Expected storage required for 24 hours
15 minutes	500	4 x 24 x 500 x 1 x 1 x 1 / 1024	1	1	47 KB

TCPIP Stack Layer (KN3TSL) worksheet
Use the TCPIP Stack Layer (KN3TSL) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 155. TCPIP Stack Layer (KN3TSL) worksheet

Interval	Record size	Formula	TCP/IP address spaces	TCP/IP stack	Expected storage required for 24 hours
15 minutes	636	4 x 24 x 636 x 1 x 1 x 1 / 1024	1	1	60 KB

UDP Connections (KN3UDP) worksheet

Use the UDP Connections (KN3UDP) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 156. UDP Connections (KN3UDP) worksheet

Interval	Record size	Formula	UDP connections	TCP/IP stack	Expected storage required for 24 hours
15 minutes	388	4 x 24 x 388 x 1 x 1 / 1024	1	1	36 KB

VTAM historical data storage

Use this information to understand the formula for historical collection, the attribute group record sizes, and the space requirements for VTAM historical data storage.

- **VTAM formula**

  Storage assumptions:

  – Historical collection interval: 15 minutes

  – Quantity of each resource types monitored: 1

$$\frac{\text{4 collections per hour} \times \text{24 hours} \times \text{Bytes per record} \times \text{1 monitored resource} \times \text{1 row per resource}}{1024} = \text{KB per 24-hour period}$$

Which simplifies to:

$$\frac{96 \times \text{Number of bytes per record}}{1024} = \text{KB per 24-hour period}$$

Figure 14. Formula for VTAM historical collection data storage

- **Attribute group record sizes**

  The following data is collected once every historical collection interval. This data is collected for each LPAR you will monitor.

Table 157. Data collected once every collection interval

Type of data	Real-time data attribute group	Row size in bytes	Frequency per interval	Subtotal storage required in KB
TCP/IP and VTAM (required collection)	VTAM Summary Statistics	100	1 row	9
Enterprise Extender (EE) and High Performance Routing (HPR) statistics collection	EE Connections	276	1 row per EE connection	26
	EE Connections Details	268	5 rows per EE connection	126
	HPR RTP Connections	596	1 row per HPR RTP connection	56

Table 157. Data collected once every collection interval (continued)

Type of data	Real-time data attribute group	Row size in bytes	Frequency per interval	Subtotal storage required in KB
Communications Storage Manager (CSM) buffer reporting	CSM Storage	204	1 row	19
	KN3 CSM Storage by Owner	196	1 row per address space that owns CSM storage	18
Buffer Pool and VTAM environment collection	VTAM Address Space	272	1 row	26
	VTAM I/O	100	1 row for each of 6 resources	56
	VTAM Buffer Pools	182	1 row for each of 14 resources	239
	VTAM Buffer Pool Extents	124	1 row per buffer pool extent	12
	VTAM Buffer Usage by Address Space	100	1 row per address space using IO00 or CRPL buffers	9
	VTAM Buffer Usage by Application for Address Space	108	1 row per application per address space using IO00 buffers	10
	VTAM Buffer Usage by Category	96	1 row for each of 12 resources	108

- **Space requirement worksheets**

  Use the worksheets shown in Tables 111 through 121 to estimate the disk space requirements for your site. A sample calculation is provided for each historical data collection table.

  – Each worksheet is for one monitored resource per LPAR.
  – Typically you are monitoring more than one resource (that is, one connection). You need to multiply the required storage by the number of resources.
  – If you are monitoring multiple LPARs, complete a worksheet for each LPAR, or one worksheet that represents the average LPAR.

CSM Storage (KN3CSM) worksheet
Use the CSM Storage (KN3CSM) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 158. CSM Storage (KN3CSM) worksheet

Interval	Record size	Formula	CSM storage resources	Expected storage required for 24 hours
15 minutes	204	4 x 24 x 204 x 1 x 1/ 1024	1	19 KB

EE Connection Details (KN3EED) worksheet
Use the EE Connection Details (KN3EED) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 159. EE Connection Details (KN3EED) worksheet

Interval	Record size	Formula	EE connection resources	Expected storage required for 24 hours
15 minutes	268	4 x 24 x 268 x 1 x 5 / 1024	1	126 KB

EE Connections (KN3EEC) worksheet
Use the EE Connections (KN3EEC) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 160. EE Connections (KN3EEC) worksheet

Interval	Record size	Formula	EE connection resources	Expected storage required for 24 hours
15 minutes	276	4 x 24 x 276 x 1 x 5 / 1024	1	26 KB

HPR RTP Connections (KN3HPR) worksheet
Use the HPR RTP Connections (KN3HPR) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 161. HPR RTP Connections (KN3HPR) worksheet

Interval	Record size	Formula	HPR RTP connection resources	Expected storage required for 24 hours
15 minutes	596	4 x 24 x 596 x 1 x 1/ 1024	1	56 KB

KN3 CSM Storage by Owner (KN3CSO) worksheet
Use the KN3 CSM Storage by Owner (KN3CSO) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 162. KN3 CSM Storage by Owner (KN3CSO) worksheet

Interval	Record size	Formula	CSM Storage by Owner resources	Expected storage required for 24 hours
15 minutes	196	4 x 24 x 196 x 1 x 1/ 1024	1	18 KB

VTAM Address Space (KN3VAS) worksheet
Use the VTAM Address Space (KN3VAS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 163. VTAM Summary Statistics (KN3VAS) worksheet

Interval	Record size	Formula	VTAM address space resources	Expected storage required for 24 hours
15 minutes	272	4 x 24 x 272 x 1 / 1024	1	26 KB

VTAM Buffer Pool Extents (KN3BPE) worksheet
Use the VTAM Buffer Pool Extents (KN3BPE) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 164. VTAM Buffer Pool Extents (KN3BPE) worksheet

Interval	Record size	Formula	Number of resources	Expected storage required for 24 hours
15 minutes	124	4 x 24 x 124 x 1 x 1 / 1024	1	12 KB

VTAM Buffer Pools (KN3BPD) worksheet
Use the VTAM Buffer Pools (KN3BPD) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 165. VTAM Buffer Pools (KN3BPD) worksheet

Interval	Record size	Formula	Number of resources	Expected storage required for 24 hours
15 minutes	182	4 x 24 x 182 x 14 x 1 / 1024	14	239 KB

VTAM Buffer Usage by Address Space (KN3BPS) worksheet
Use the VTAM Buffer Usage by Address Space (KN3BPS) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 166. VTAM Buffer Usage by Address Space (KN3BPS) worksheet

Interval	Record size	Formula	Number of resources	Expected storage required for 24 hours
15 minutes	100	4 x 24 x 100 x 1 x 1 / 1024	1	9 KB

VTAM Buffer Usage by Application for Address Space (KN3BPA) worksheet
Use the VTAM Buffer Usage by Application by Address Space (KN3BPA) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 167. VTAM Buffer Usage by Application for Address Space (KN3BPA) worksheet

Interval	Record size	Formula	Number of resources	Expected storage required for 24 hours
15 minutes	108	4 x 24 x 108 x 1 x 1 / 1024	1	10 KB

VTAM Buffer Usage by Category (KN3BPG) worksheet
Use the VTAM Buffer Usage by Category (KN3BPG) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 168. VTAM Buffer Usage by Category (KN3BPG) worksheet

Interval	Record size	Formula	Number of resources	Expected storage required for 24 hours
15 minutes	96	4 x 24 x 96 x 12 x 1 / 1024	12	108 KB

VTAM I/O (KN3VIO) worksheet
Use the VTAM I/O (KN3VIO) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 169. VTAM I/O (KN3VIO) worksheet

Interval	Record size	Formula	Number of resources	Expected storage required for 24 hours
15 minutes	100	4 x 24 x 100x 6 x 1 / 1024	6	56 KB

VTAM Summary Statistics (KN3SNA) worksheet
Use the VTAM Summary Statistics (KN3SNA) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 170. VTAM Summary Statistics (KN3SNA) worksheet

Interval	Record size	Formula	SNA resources	Expected storage required for 24 hours
15 minutes	100	4 x 24 x 100 x 1 / 1024	1	10 KB

FTP historical data storage

Use this information to understand the formula for historical collection, the attribute group record sizes, and the space requirements for FTP historical data storage.

- **FTP formula**

  Storage assumptions:

  – Historical collection interval: 15 minutes

  – Quantity of each resource types monitored: 1

$$\frac{\text{Bytes per record} \times \text{1 monitored resource} \times \text{2 rows per session or transfer} \times \text{1 TCP/IP stack}}{1024} = \text{KB per 24-hour period}$$

Figure 15. Formula for FTP historical collection data storage

- **Attribute group record sizes**

  The following FTP data is collected when a new session or transfer is opened or when an existing session or transfer is closed. This data is collected when z/OS Communications Server notifies the monitoring agent that there is data available and therefore does not adhere to a collection interval. For these three attribute tables, storage per monitored resource is relatively low because only one record is stored per active session or transfer, plus one record per completed session or transfer. However, you might have thousands of sessions or transfers in 24 hours, and thus storage cost for FTP sessions could be significant.

  FTP data is collected for each TCP/IP stack. If you have LPARs with multiple TCP/IP stacks, total the storage required for each stack you will monitor.

Table 171. FTP data collected

Type of data	Historical data attribute table	Row size in bytes	Frequency	Subtotal storage required
FTP Data Collection	FTP Sessions	412	2 rows per FTP session	0.8 KB
	TCPIP FTP	2464	2 rows per FTP transfer	5 KB

- **Space requirement worksheets**

  Use the worksheets shown in Tables 124 and 125 to estimate the disk space requirements for your site. A sample calculation is provided for each historical data collection table.

  – Each worksheet applies to one monitored resource per TCP/IP stack.

  – Typically you are monitoring more than one resource (that is, one session or transfer, for example). You need to multiply the required storage by the number of resources.

  – If you are monitoring multiple LPARs, complete a worksheet for each LPAR, or one worksheet that represents the average LPAR.

  – If you are monitoring more than one TCP/IP stack in an LPAR and each TCP/IP stack has an FTP server, multiply by the number of TCP/IP stacks.

FTP Sessions (KN3FSE) worksheet
Use the FTP Sessions (KN3FSE) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 172. FTP Sessions (KN3FSE) worksheet

Record size	Formula	FTP sessions	TCP/IP stack	Expected storage required for 24 hours
412	412 x 1 x 2 x 1 / 1024	1	1	0.8 KB

TCPIP FTP (KN3FTP) worksheet
Use the TCPIP FTP (KN3FTP) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 173. TCPIP FTP (KN3FTP) worksheet

Record size	Formula	FTP transfers	TCP/IP stack	Expected storage required for 24 hours
2464	(2464 x 1 x 2 x 1) / 1024	1	1	5 KB

TN3270 historical data storage

Use this information to understand the formula for historical collection, the attribute group record sizes, and the space requirements for 3270 historical data storage.

- **TN3270 formula**

  Storage assumptions:

  - Historical collection interval: 15 minutes
  - Quantity of each resource types monitored: 1
  - TN3270 session is active for 8 hours, and then is closed

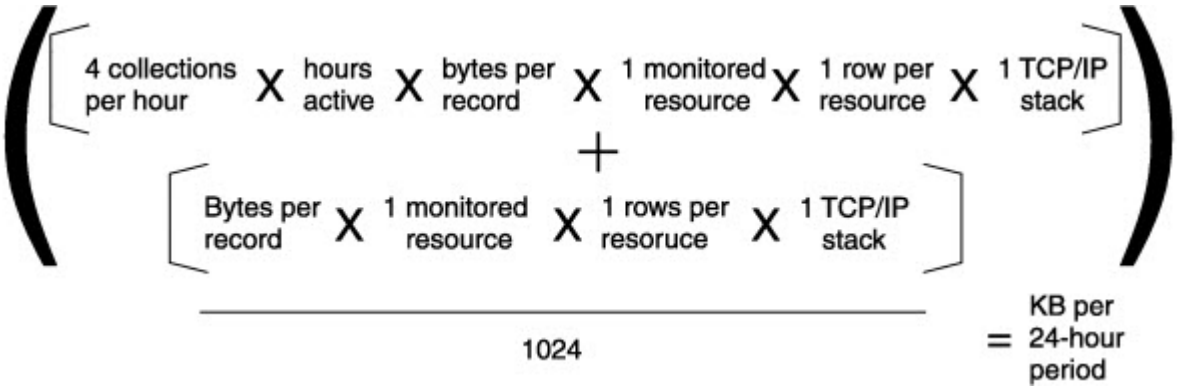


Figure 16. Formula for TN3270 historical collection data storage

- **Attribute group record sizes**

  The TN3270 data provides information about open, closed and active TN3270 sessions for a TCP/IP address space. A record is stored for each TN3270 session that closed since historical data was last collected or that is active when historical data is collected. The record for a TN3270 session will be

stored when new data is available at the time that historical data is collected (i.e. the same, unchanged record will not be stored twice). New data is available each collection interval starting when the session opened until the collection interval after the session closed.

Thirty-two (32) records a day (4 per hour for 8 hours) will be stored for each active TN3270 session.

Table 174. TN3270 data collected

Type of data	Historical data attribute table	Row size in bytes	Frequency	Subtotal storage required
TN3270 Server Statistics Data Collection	TN3270 Server Sess Avail	460	1 row per active TN3270 server session + 1 row per closed TN3270 server session	15 KB

- **Space requirement worksheets**

  Use the worksheet shown in Table 127 to estimate the disk space requirements for your site. A sample calculation is provided for each historical data collection table.

  - Each worksheet is for one monitored resource per TCP/IP stack.
  - Typically you are monitoring more than one resource (that is, one session). You need to multiply the required storage by the number of resources.
  - If you are monitoring multiple LPARs, complete a worksheet for each LPAR, or one worksheet that represents the average LPAR.
  - If you are monitoring more than one TCP/IP stack in an LPAR and each TCP/IP stack has a TN3270 server, multiply by the number of TCP/IP stacks.

TN3270 Server Sess Avail (KN3TNA) worksheet
Use the TN3270 Server Sess Avail (KN3TNA) worksheet to calculate the amount of DASD required by this attribute group in the persistent data store.

Table 175. TN3270 Server Sess Avail (KN3TNA) worksheet

Record size	Formula	TN3270 server sessions	TCP/IP stack	Expected storage required for 24 hours
460	((4 x 8 x 460 x 1 x 1 x 1) + (460 x 1 x 1 x 1)) / 1024	1	1	15 KB

IBM Z OMEGAMON Network Monitor disk space summary worksheet

Use this worksheet to summarize the historical database calculations you have made in previous attribute group-specific worksheets.

The disk space summary worksheet for IBM Z OMEGAMON Network Monitor follows.

Table 176. Disk space summary

Historical attribute table	Historical attribute table size in KB (for a 24-hour period)	Subtotal of storage required in cylinders
Agent Historical Data Collection Interval		
Agent Status		

Table 176. Disk space summary (continued)

Historical attribute table	Historical attribute table size in KB (for a 24-hour period)	Subtotal of storage required in cylinders
SNA Collector Status		
TCP Collector Status		
TCP/IP and VTAM (required collection		
TCPIP Memory Statistics		
TCP/IP Stack Layer Statistics		
TCPIP Address Space		
KN3 ICMP Global Counters		
KN3 ICMP Type Counters		
KN3 IP Counter Statistics		
KN3 IP General Statistics		
KN3 TCP Counter Statistics		
KN3 UDP Counter Statistics		
TCPIP Stack Layer		
Interfaces statistics collection		
Intterfaces		
KN3 Interface Address		
KN3 Interface Statistics		
KN3 Interface Status		
TCPIP Devices		
KN3 Interface ReadQueue		
KN3 Interface Write Queue		
OSA statistics collection		
OSA-Express Channels		
OSA-Express LPARS		
OSA-Express Ports		
OSA 10 Gigabit Ports Control		
OSA 10 Gigabit Ports Errors		
OSA 10 Gigabit Ports Summary		
OSA 10 Gigabit Ports Throughput		
OSA-Express3 Ports Control		
OSA-Express3 Ports Errors		
OSA-Express3 Ports Summary		
OSA-Express3 Ports Throughput		

Table 176. Disk space summary (continued)		
Historical attribute table	**Historical attribute table size in KB (for a 24-hour period)**	**Subtotal of storage required in cylinders**
KN3 OSA-Express5S Ports Control		
KN3 OSA-Express5S Ports Errors		
KN3 OSA-Express5S Ports Summary		
KN3 OSA-Express5S Ports Throughput		
TCP/IP Connection and Application Performance statistics collection		
TCPIP Applications		
TCPIP Connections		
TCPIP Details		
TCP Listener		
UDP Connections		
Routing Table statistics collection		
TCPIP Gateways		
IPSec Security collection		
IPSec Status		
Current IP Filters		
Dynamic IP Tunnels		
IKE Tunnels		
Manual IP Tunnels		
VTAM Historical Data Collection Interval		
VTAM Summary Statistics		
EE Connections		
EE Connections Details		
HPR RTP Connections		
CSM Storage		
VTAM Address Space		
VTAM I/O		
VTAM Buffer Pools		
VTAM Buffer Pool Extents		
VTAM Buffer Pool Usage by Address Space		
VTAM Buffer Pool Usage by Application		

Table 176. Disk space summary (continued)		
Historical attribute table	**Historical attribute table size in KB (for a 24-hour period)**	**Subtotal of storage required in cylinders**
VTAM Buffer Pool Usage by Category		
FTP Data Storage		
FTP Sessions		
TCPIP FTP		
TN3270 Data Storage		
TN3270 Server Sess Avail		
Total Storage Required		

Estimating the storage required per LPAR

These formulas help you estimate the amount of storage required for historical data tables on a per LPAR basis.

Use the following formula to estimate the cylinders of 3390 DASD required.

$$\text{Storage to allocate} = \frac{\text{Total storage required in KB}}{\text{717 KB per cylinder}} \times \frac{\text{Group Count}}{(\text{Group Count} - 2)}$$

Figure 17. KB formula for total storage required per LPAR for cylinders of 3390 DASD

If you estimated in cylinders, you can use the following formula:

$$\text{Storage to allocate} = \text{Total storage in cylinders} \times \frac{\text{Group Count}}{(\text{Group Count} - 2)}$$

Figure 18. Cylinder formula for total storage required per LPAR in cylinders of 3390 DASD

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

IBM Support Assistant
The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination.

Troubleshooting Guide
For more information about resolving problems, see the product's Troubleshooting Guide.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z

Accessibility

Accessibility features help users with physical disabilities, such as restricted mobility or limited vision, to use software products successfully. OMEGAMON XE monitoring products support several user interfaces. Product functionality and accessibility features vary according to the interface.

The major accessibility features in this product enable users in the following ways:

- Use assistive technologies, such as screen-reader software and digital speech synthesizer, to hear what is displayed on the screen. Consult the product documentation of the assistive technology for details on using those technologies with this product.
- Operate specific or equivalent features using only the keyboard.
- Magnify what is displayed on the screen.

In addition, the product documentation was modified to include the following features to aid accessibility:

- All documentation is available in both HTML and convertible PDF formats to give the maximum opportunity for users to apply screen-reader software.
- All images in the documentation are provided with alternative text so that users with vision impairments can understand the contents of the images.

Interface information
The Tivoli Enterprise Portal interface offers the greatest range of functionality, but is not entirely accessible. The OMEGAMON Enhanced 3270 user interface offers more limited functionality, but is entirely accessible. (The enhanced 3270 user interface supports all the accessibility features supported by your emulator. If you are using IBM Personal Communications, you can find information on its accessibility features at http://publib.boulder.ibm.com/infocenter/pcomhelp/v6r0/index.jsp?topic=/com.ibm.pcomm.doc/books/html/quick_beginnings10.htm. If you are using a third-party emulator, see the documentation for that product for accessibility information.)

The OMEGAMON ("classic") and OMEGAMON II (CUA) 3270 interfaces use an ISPF style interface. Standard and custom PF Key settings, menu options, and command line interface options allow for short cuts to commonly viewed screens. While basic customization options allow for highlights and other eye-catcher techniques to be added to the interface, the customization options are limited.

Related accessibility information
You can view the publications for IBM Z OMEGAMON Network Monitor Adobe Portable Document Format (PDF) using the Adobe Acrobat Reader.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

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

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Intel, Intel logo, and Intel Xeon, are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z