GC32-0756-02

IBM Tivoli NetView® for TCP/IP Performance Installation Guide

Version 1.5

Tivoli software

Fifth Edition (July, 2002)

This edition applies to the IBM Tivoli NetView® Performance Monitor for TCP/IP Installation Guide.

APPLIED EXPERT SYSTEMS, INC. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Applied Expert System, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Trademarks

Tivoli and NetView are trademarks or registered trademarks of IBM Corporation in the United States, other countries, or both.

IBM, MVS, SMF, and VSAM are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product, and service names may be the trademarks or service marks of others.

READ THIS FIRST

IBM Tivoli NetView® for TCP/IP Performance (NV4IP) provides network performance measurements for the TCP/IP transaction environment. It provides critical workload information on such services FTP, SNMP, and Telnet as well as the socket-attached TCP/IP based OLTP environment.

Audience

This guide is intended for performance analysts, network system programmers, and capacity planners. It assumes knowledge of the MVS TCP/IP transaction environment.

How To Use This Book

This guide covers the installation of NV4IP in an MVS TCP/IP operating environment. Following is a brief summary:

INTRODUCTION
The Introduction gives a brief description of the NV4IP's architecture, features, functions, and operation.

HOST MONITOR INSTALLATION
The Host Installation section describes the steps involved in installing NV4IP for the Host Monitor, including unloading the target libraries and customizing the installation.

NV4IP MONITOR OPERATION
The Monitor Operation section describes the management of the Monitor portion of NV4IP on the MVS host and contains information on starting and stopping NV4IP on the Host, enabling the submission of VTAM commands, adding critical resources, and managing the historical database.

NV4IP SERVER INSTALLATION
This section will provide you with the necessary steps to complete the installation of the NV4IP Java servlets on any Web server that supports the Java Runtime Environment (JRE). It is recommended that the installation be done first on the Apache HTTP Server. See Appendix A for a sample installation.

VERIFYING THE INSTALLATION

This section explains how to verify the successful installation of NV4IP.

TROUBLESHOOTING YOUR WEB SERVER INSTALLATION

The troubleshooting guide focuses on error messages that might arise during installation. It provides explanations of what might have gone wrong and some steps to take towards resolving the problem

MESSAGES AND CODES

This section contains error messages and codes that you may encounter in the process of installing and using NV4IP. It includes informational, error and warning messages for the NV4IP Host.

APPENDICES

The Appendices include a sample installation of the NV4IP Java Servlets on the Apache Web Server, NV4IP SMF record layouts, and sample JCL, FTP Log, and SMF Log listings.

TABLE OF CONTENTS

INTRODUCTION

NV4IP is a real-time network performance monitor for the TCP/IP transaction environment. It provides critical workload information on such applications as FTP, SMTP, and Telnet, as well as the socket-attached TCP/IP based OLTP environment. NV4IP networking and application workload information is used for:

- establishing TCP/IP mission critical application service level objectives,
- reporting service level performance on a routine basis,
- identifying the high-demand workload periods,
- trending based on historical data for network response time issues and planning purposes,
- identifying performance bottlenecks before users complain,
- monitoring in real time,
- command submission to the mainframe host(s), as well as sending alerts to the operator console, and
- planning for networked mission critical transactions on a proactive basis.

NV4IP is designed to help performance analysts, operations personnel, network system programmers, and capacity planners effectively monitor performance, troubleshoot problems, and plan for the future.

Product Architecture

NV4IP provides network performance measurements for the TCP/IP network environment through data gathering on the mainframe and performance reporting both on the mainframe and on a PC workstation through a browser-based platform. The Monitor and BatchPR are the host portions of the product. The Monitor is installed on each host whose MVS TCP/IP address space is to be monitored. It performs the data collection that is then provided to BatchPR or the PC workstations for reporting purposes. All data for that mainframe is stored locally on that host.

Host Components

The Monitor collects information on host TCP/IP buffers, channel-attached devices, applications workload, and network response time between monitored host and *critical resources* on the IP network, such as UNIX servers, AS/400 computers, Windows/NT/2000/XP servers, network printers, or end-user workstations. The data is written to SMF and also to VSAM databases for historical reporting.

BatchPR provides an option for those users who require a TN3270-like mainframe reporting option. BatchPR is executed from the TSO command line of ISPF or through the submission of JCLs. The reports focus on two aspects of the network performance: response time and availability and workload performance related to application sessions. With BatchPR, one can easily answer such questions as:

- How reliable is network access between Mainframe System A and the branch office System B?
- How available is the Mainframe System to all its major communication nodes?
- Is the Mainframe System providing the level of service that it should to the key users in the Network?
- How are my FTP sessions during last weekend? What is the average session data transfer volume?

Currently, BatchPR provides up to 9 reports. They can be controlled with the parameters specified either in the JCL or interactively using ISPF. See *IBM Tivoli NetView for TCP/IP Performance BatchPR Utilities Reference Guide Version 1.5* for more information.

NV4IP Server

The server must be installed and running in order to access the monitoring/reporting functions available for viewing through NV4IP. Java servlets are installed on a Web server, such as Apache for Windows and WebSphere for z/OS. The Java servlets communicate with the Monitor through a TCP/IP socket interface.

A browser acts as the display platform and runs on any operating system platform that supports the Netscape Navigator browser or the Microsoft Internet Explorer browser. NV4IP is available to an authorized user from any intranetwork enabled device as well as from the Internet.

NV4IP consists of the Master, the Operations Manager functions, and the Performance Manager functions. It provides the historical charts and real-time reports that allow you to monitor the TCP/IP transaction environment, as it occurs and over time, for performance tuning, trending, and resource planning. The browser accesses the Web server using standard URL addresses, which invokes the Java servlets that retrieve the desired information from the host.

User Workstation Operation

NV4IP provides both real-time and historical reporting capabilities to assist in the determination of workload throughput, capacity planning, trending, and network performance. It has three major areas: the Master for administration, the Performance Manager for historical reporting, and the Operations Manager for real-time reporting.

The monitor function determines who gets monitored and how frequently. It is recommended that one Master function be set up per installation. The Master performs configuration and administrative tasks. It can be used to add, change, or delete the configuration data used by any Monitor on any mainframe and authorizes the users who may access that information.

The Manager applications perform data reporting, analysis, real-time monitoring, and command submission for any Monitor on any mainframe. Access to NV4IP Functions is controlled through User IDs, which provide functional authorization to the modules. Regardless of the user's access privileges, the home base is SysPoint and its accompanying functions: LinkView, Connect Expert, and Alerts.

The Performance Manager is used to view the historical TCP/IP network performance from the enterprise level to the remote user connection. Performance indicators for workload and response time are reported in various granularity's: by time, by host, or by application. The Performance Manager uses charts with toolbars and zoom functions for easy manipulation of the data.

The Operations Manager is used to monitor, in real time, network performance, resource availability, buffer pools, Telnet, FTP, user defined applications, or CPU usage. Network performance or operations personnel may use the expert assisted interface or unassisted mode to enter commands to control the Monitor mainframe

SysPoint

SysPoint is the primary entry point for NV4IP, providing a view across all monitored host systems. SysPoint displays a system summary of performance activities and alerts including the stack name and IP address for all monitored hosts and details for those hosts that are active. The details include alerts for link, ports, response time, availability, and buffer utilization; stack workload details, channel link status and connection data for primary protocols.

Note: You must define at least one Host Monitor the first time you use NV4IP to be able to access Host data.

Alerts

SysPoint provides both summary and detail data on alerts by clicking in any alert column. Current alerts are highlighted by displaying in red. The Summary Alert Report provides data for all alerts on the SysPoint screens. The Detail Report is context sensitive and provides data from the Alert selected on the SysPoint Home Page. The Detail data consists of two charts: one shows alerts regarding the most recent occurrence, the last occurrence, and the alerts since midnight, and the second chart shows relevant data for the selected alert. Alerts for Critical Resource Availability and Performance are set in the Master from the PC Workstation. All other alerts are set on the Host (CONF00 member).

LinkView

LinkView provides real-time Channel Processor Monitoring for TCP/IP. LinkView shows all the channel-attached processors and links associated with your TCP/IP address space on one screen. Channel-attached processors include Channel-to-Channel devices, LAN channel stations, ATM devices, CLAW devices (ex: RS 6000s), FDDI devices, or router cards such as the CISCO CIP card. You can also access the Thru24 IP Summary/Detail reports from LinkView, which provide near-time IP throughput information on channel-attached devices. LinkView is accessible to authorized Master and Operations Manager users only.

Connect Expert

The Connect Expert feature allows you to monitor sockets and the connectivity to all your sessions using TCP and UDP (non-EE) in real time. You can also access the Enterprise Extender (EE) Expert report from Connect Expert, which provides information on current EE UDP workload for each of the assigned EE ports in real time. From the UDP Sessions (non EE) table you can zoom in to view UDP (non EE) activity detail in real time. From the TCP Sessions table you can zoom in to any port/application or session to view details. From the detailed display, you can perform functions such as TraceRoute, Drop, or Ping simply by clicking the appropriate hyperlink. The byte count for the session indicates the number of bytes from the last collection interval. The application may be Telnet, e-mail, or any other socket-attached OLTP applications using the selected TCP/IP address space. The data is refreshed periodically at the host according to the interval specified on the parameters to the started task.

Master

Use the Master module to manage and configure parameters for probing and monitoring network devices. The Master also controls user access to the application and for monitoring (addresses, frequencies, and packet sizes for the tests used to collect response time data for the monitored servers). These parameters can be tailored to model application workload. Use the Master to perform the following functions:

- Add/Delete/View User IDs (NV4IP application security only)
- Add/Delete/View Host Definitions
- Add/Delete/View Resource Definitions
- Review Monitoring Status
- Start/Stop Monitoring
- Start/Stop Alerting

Performance Manager

Within NV4IP, there is a grouping of functions that are of performance management in nature. This group is called the Performance Manager. The Performance Manager functions provide a historical TCP/IP network performance view for the enterprise. The Performance Manager functions include Real-Time, History, and SessionLog tabs.

The Performance Manager functions are:

Real-Time Tab	
Real-Time	Real-time graphs and reports provide performance and workload information for applications and clients. Includes graphs and tabular reports for response time, applications, ports, clients, Connect Expert, and workload in terms of bytes transferred and sessions. This information is presented in terms of response time for bytes transferred and number of sessions. Data is available as soon as the Monitor on the host is activated on your network.
History Tab	
Base History Reports	Provides workload, peak/valley, and response time reports for performance and workload historical data.
Thru99 EE History	Allows you to view interval-based throughput summaries of EE UDP data by port.
Thru99 Link History	Allows you to view interval-based throughput summaries of UDP IP data by port.
API Expert	Provides both global and detailed views of API activity. Reports are available in two catagories: address (activity based) and application based.
FTP Performance Expert	Provides both global and detailed views of FTP activity. Reports are address based, data set based, and failure based.
Telnet Expert	Provides both global and detailed views of Telnet activity. Reports are available in two catagories: address (activity based) and application based.
VTAM Buffer Pool Reports	Provides both global and detailed views of VTAM buffer pool activity. Reports are available in two categories: all buffer pools and specific buffer pool activity
CSM Buffer Pool Reports	Provides both global and detailed views of Communications Storage Manager (CSM) buffer pool activity. Reports are available in two categories: usage and Alerts.

SessionLog Tab	
SessionLog	The SessionLog allows viewing of *near time* or current time sessions for FTP, API, Telnet, and SMF records. That is, sessions that are either currently live or have recently happened. The definition of *recently* is up to the installation and may be set in the parameters to the FTP or SMF exits. The records for these sessions are held in memory by the NV4IP Monitor executing on the MVS host.

Operations Manager

Within NV4IP, there is a grouping of functions that are of operational management in nature. This group is called the Operations Manager. The Operations Manager functions provide real-time viewing of events as they happen across the enterprise. The Operations Manager functions include Real-Time, SessionLog, SNMP, StackView, Monitor and Commands tabs

The Operations Manager functions are:

Real-Time Tab	
Real-Time	Real-time graphs and reports provide performance and workload information for applications and clients, in terms of response time for bytes transferred and number of sessions. Data is available as soon as the Monitor on the host is activated on your network.
SessionLog Tab	
SessionLog	The SessionLog allows viewing of *near time* or current time sessions for FTP, API, Telnet, and SMF records. That is, sessions that are either currently live or have recently happened. The definition of *recently* is up to the installation and may be set in the parameters to the FTP or SMF exits. These session records are held in memory by the NV4IP Monitor executing on the Host.
SNMP Tab	
SNMP MIB	Provides tabular and real-time graphs of the public and private MIBs for any SNMP-capable device, including OSA Express, Cisco CIP, IBM 2216, and TN3270 servers.
StackView Tab	
StackView	Tracks CPU usage for the address spaces associated with TCP/IP (TCP/IP, SNALK, FTP server, etc), as well as for any address space associated with a socket-attached application.

Monitor Tab	
Real-Time Monitoring	Monitor response time, availability, Telnet, and channel processors in real time.
Commands Tab	
Commands	Execute commands to diagnose problems and control network activity while within NV4IP. The following commands can be issued: **Netstat** to check the link, foreign port, client, or socket-attached application status. **TraceRoute** to view TCP/IP route and segment information. **D NET,RTPS** to perform a VTAM-based Rapid Transport Protocol (RTP) Route Test across the HPR pipe from any EE connection to a specific RTP endpoint. Only available for z/OS V.1.2 and later. **Ping** to determine if a TCP/IP resource is available. **D NET,APING** to test network connectivity of Enterprise Extender links or to determine APPN availability and response time for a specific APPN Transmission Group (TG) between two APPN endpoints. **VTAM** to display, inactivate, activate, or modify a resource in VTAM. **Storage** to display shared storage, such as CSM or VTAM buffer pools. **OSPF** or **RIP** to specify dynamic routing protocols and **Route Table** to view Route Table configuration. These commands are implemented with the **OMPRoute** program application. **D OMVS** to display and diagnose current OMVS-based settings and associated processes.

Product Requirements

Listed below are the minimum system configurations required for the effective operation of this product.

System	Hardware	Software
Host	IBM S390 architecture 200 3390-type device tracks for the product libraries 600 3390-type device cylinders for historical databases	OS/390 V2R10, z/OS V1R1 or later, or z/OS.e. Tivoli NetView for OS/390 C Runtime or equivalent SAS/C run time library, for example ISP.SISPSASC (ISPF).
Server	For Windows/Linux: 256 MB of RAM IBM PC compatible Model Pentium 500MHz or above 200 MB of hard disk space	Operating Systems: OS/390 V2R10, z/OS V1R1 or later, z/OS.e. Windows NT 4.0 SP6a, Windows 2000, Windows XP. RedHat Linux 7.2. Web Servers: WebSphere for OS/390 3.5. WebSphere for z/OS 4.0.1. Apache HTTP Server 1.3.26 for Windows and Apache Tomcat for Windows 4.0.4. Apache HTTP Server 1.3.26 for Linux and Apache Tomcat for Linux. 4.0.4. The Servlet/JSP containers must support JSP 1.1 and Servlet 2.2 specifications. The JDK classes must be Java Development Kit 1.3.1_04 or higher (prior releases will not work).
PC Workstation	256 MB RAM IBM PC compatible Model Pentium 500MHz or above 200 MB of hard disk space	Operating Systems: Windows 98/Me, Windows NT 4.0 SP6a, Windows 2000, Windows XP. Browser Applications: Internet Explorer 5.5 or 6.0. Netscape 6.2 or 7.0.

Installation Package

The distribution tape (e.g., 3480 Cartridge) contains all of the files necessary to install the Host portion of this product.

The NV4IP installation package consists of:

- Mainframe Distribution Tape
- One CD-ROM for Server Installation
- Installation Manual

Product Components

The product components shipped on the CD-ROM for the browser-based version are:

- setup.exe
- apache_1.3.26-win32-x86-no_src.exe (Apache HTTP Server 1.3.26)
- jakarta-tomcat-4.0.4.exe (Apache Tomcat 4.0.4)
- mod_jk.dll (Apache/Tomcat connector)
- pja.jar (Pure Java AWT Java classes)
- pjatools.jar (Pure Java AWT Toolkit)
- Program file:
  - nvip.war - web application containing jsps, servlets, all necessary Java classes and resource bundles, and the deployment descriptor
- Program Directory
  - htdocs
    - nvip
      - chart - contains jar file for the charting applets
      - webhelp - contains web files for the online help system
      - images - graphics files(.jpg, .gif)
      - javascript - javascript files
- Linux Installation Directory
      - apache_1.3.26.tar.gz (Apache HTTP Server 1.3.26 Linux source)
      - jakarta-tomcat-4.0.4.tar.gz (Apache Tomcat 4.0.4 Linux binaries)
      - jakarta-tomcat-connectors-4.0.4.tar.gz (Apache/Tomcat connector source)
      - setup.tar

Note: If the Java Software Development Kit is not already installed on the server, it must be downloaded from: http://java.sun.com/products

Product Support

If you have a question or a problem with the NV4IP product family, contact Customer Support by visiting the Website at

www-3.ibm.com/software/sysmgmt/products/support/

They are ready to give you the assistance you need to get the most from this product. Customer Support or your distributor can assist you with problem resolution, information on product enhancements, and tips/techniques for the most effective use of the product family.

When sending an email to Customer Support, please be sure to include as much specific information as possible so that your inquiry may be addressed quickly and accurately. Please use the information below as a guide.

CUSTOMER ID:		
CUSTOMER NAME:		
PROBLEM DESCRIPTION:		
ERROR CODE / MESSAGES: (or SYSTEM ABEND CODE)		
ERROR MODULES TRACEBACK (if presented)		
TIVOLI VERSION/RELEASE LEVELS:		
SYSTEM INFORMATION VERSION/RELEASE LEVELS:		
Host OS/390	**Browser**: Netscape Internet Explorer	**Web Server:** Operating System: Server software:

WHAT'S NEW IN NV4IP V1.5?

This section describes changed general user interfaces, functions, and data fields in NV4IP V1.5.

Changed User Interfaces and Functions in V1.5

The following general user interfaces and functions have been changed in V1.5.

1. The default User ID is changed to "TCPIP" if SECURITY=0 is specified.
2. The "Reports" tab has been changed to "Real-Time."
3. Grouping of functions is added to the SessionLog, History, Monitor and Commands tabs. Detailed function descriptions have been removed.
4. If an option is not applicable, it will be grayed out.
5. When deleting a critical resource from the Master, both the monitored and unmonitored resources are listed separately. If a monitored resource is to be deleted, its monitoring status will be turned off first.
6. The User ID group on the Master menu is grayed out if SECURITY=1 or SECURITY=2 is specified.
7. The SNMP MIB Browser's option bar has been changed to look more like the menu bar on the main page, and it is always accessible from the SNMP MIB Browser.
8. When viewing a graph, you may move a graph proportionally by dragging the image. You may resize a graph either vertically or horizontally by double-clicking and dragging the mouse. You may move the legend by double-clicking on the legend box and move it to a different area.
9. NV4IP has a new option (FPING statement in CONFxx) for monitoring critical resources behind a firewall that blocks ICMP messages.

Changed Data Fields in NV4IP V1.5

The following data fields have been changed in V1.5.

1. The "Bytes In" and "Bytes Out" fields for TCP Sessions in Connect Expert are delta values. They represent byte counts since the last sampling interval. In previous versions (V1.3 and V1.4), they were cumulative values, representing byte counts since the TCP sessions were started.
2. The "Bytes Sent" and "Bytes Received" fields in NV4IP's workload SMF record are delta values. In previous versions, they were cumulative values. See "Workload SMF Record Layout" on page 100.

3. Host names and critical resource names are changed from 16 bytes to 48 bytes in length.

HOST MONITOR INSTALLATION

The NV4IP installation package contains the software for the host Monitor and the server. The installation steps for the Host components are listed below.

The Monitor

NV4IP Monitor runs as three started tasks:

- Main started task
- Network Statistics Collector
- Command Processor

The main started task handles requests from the users and also collects performance information about a TCP/IP address space. The Network Statistics Collector collects the workload information about the TCP/IP address space. The performance and workload data is written to SMF and also saved in VSAM databases for historical reporting. The Command Processor issues TCP/IP commands per user's request or for real-time data collection.

To install the Monitor, you must have authority to APF-authorize a load library and have access to SYS1.PARMLIB and SYS1.PROCLIB or their equivalents. To install the Monitor on the MVS host, complete the following steps:

1. Unload the target libraries. See the Program Directory for instructions.
2. Customize the Installation. This step is described in detail below.

Notes for Migration from an Earlier Version (NV4IP V1.4 or V1.3)

Migrating from an earlier version of NV4IP requires that you modify the installation procedures for your current NV4IP operating environment. You may continue to use the existing VSAM databases. To allocate new VSAM databases, See "Allocate and Initialize VSAM Databases for the Historical Data" on page 30. Specific steps for migrating from Version 1.4 and 1.3 follow.

Migrating from NV4IP 1.4 to NV4IP 1.5

If you are migrating from NV4IP V1.4, you will need to make a few minor adjustments. Please perform the following tasks in order to complete the migration:

- Use the new PROCS AESTCPIP, AESTNETS and AESTCMDS in the V1.5 SAEDJCL to start the host monitor tasks. The following default parameters in the AESTCPIP PROC have been changed:
    - NINT=90 (old value=60)

    - R=210 (old value=28)
- Customize member CONFxx in SAEDSLIB to use the following new options: DEVLINKEXCEPTION, FPING, FTPOSTPR, IPV6, SMF119. Copy any parameters that were modified in your NV4IP V1.4 CONF00 member to the NV4IP V1.5 CONF00 member.
- Define the new FTP Exit FTPOSTPR. FTPOSTPR is called upon completion of the FTP commands RETR, STOR, STOU, APPE, DELE and RNTO. See "FTP Exit Installation" on page 32.
- The new NV4IP V1.5 SMF Exit AESSMF00 must be defined, replacing the exiting AESSMF83 and AESSMF84 exits. A new SMF Exit AESSMF85 must also be defined. See "Step 2 Specify SMF exits" on page 25.
- The NV4IP V1.5 SAEDLINK library must be authorized. See "Step 3 Authorize SAEDLINK" on page 26.
- If you are using RACF Program Control security (WHEN(PROGRAM)), you must issue the following commands to allow the FTP exit programs to be fetched from the NV4IP V1.5 library:

```
RALTER PROGRAM FTCHKIP ADDMEM('hilevel.SAEDLINK'/volser/NOPADCHK) UACC(READ)
RALTER PROGRAM FTCHKPWD ADDMEM('hilevel.SAEDLINK'/volser/NOPADCHK) UACC(READ)
RALTER PROGRAM FTCHKCMD ADDMEM('hilevel.SAEDLINK'/volser/NOPADCHK) UACC(READ)
RALTER PROGRAM FTPOSTPR ADDMEM('hilevel.SAEDLINK'/volser/NOPADCHK) UACC(READ)
SETR WHEN(PROGRAM) REFRESH
```

  where hilevel is the NV4IP V1.5 dataset qualifier.
- Your FTP daemon Proc (FTPD) must be changed to point to the NV4IP V1.5 SAEDLINK. See "Process 1: NV4IP FTP Exits Only", step 1 or step 2 on page 32
- If you had to re-link the NV4IP V1.4 FTP exits with your own FTP exits, you will need to follow the instructions in section "Process 2: NV4IP FTP Exits with Existing User Exits" on page 33.
- The SAEDCONF library contains NV4IP configuration data; e.g., host definitions and critical resource definitions, etc. To retain configuration data during a migration, copy the following members from your V1.4 SAEDCONF library to the V1.5 supplied library, replacing any existing members: AUTOMON, HOSTS, SERVERS, USER1, USER2, USER3. Then, run job CONVNAME from SAEDJCL. This job will convert existing host names and critical resource names to UTF-8 encoding, and change their length from 16 bytes to 48 bytes in support of internationalization.
- The SAEDVSM0 VSAM cluster contains NV4IP user options; e.g., auto-refresh interval and graphing options, etc. To retain user options during a migration, use the existing SAEDVSM0 in the AESTCPIP (or equivalent) PROC.
- Both the Host component and the Server component must be at V1.5 level. NV4IP V1.5 Host component will not work with NV4IP V1.4 Server component, and NV4IP V1.5 Server component will not work with NV4IP V1.4 Host component.

Migrating from NV4IP 1.3 to NV4IP 1.5

If you are migrating from NV4IP V1.3, you will need to make a few minor adjustments. Please perform the following tasks in order to complete the migration:

- Use the PROCS AESTCPIP, AESTNETS, and AESTCMDS in the V1.5 SAEDJCL to start the host monitor tasks. The following default parameters in the AESTCPIP PROC have been changed:
  - NINT=90 (old value=60)
  - REFRESH=15 (old value=5)
  - R=210 (old value=27)

  There is also a new parameter TCPXLBIN in the AESTCMDS and AESTNETS PROCs.
- Customize member CONFxx in SAEDSLIB to use the following new options: CSMALERT, DEVLINKMON, DEVLINKEXCEPTION, FPING, FTPOSTPR, IPV6, SMF119, TCPPORTMON, TCPPORTMONINTERVAL, VTAMBUFINTERVAL. Copy any parameters that were modified in your NV4IP V1.3 CONF00 member to the NV4IP V1.5 CONF00 member.
- Define the new FTP Exit FTPOSTPR. FTPOSTPR is called upon completion of the FTP commands RETR, STOR, STOU, APPE, DELE and RNTO. See "FTP Exit Installation" on page 32.
- The new NV4IP V1.5 SMF Exit AESSMF00 must be defined, replacing the exiting AESSMF83 and AESSMF84 exits. A new SMF Exit AESSMF85 must also be defined. See "Step 2 Specify SMF exits" on page 25
- The NV4IP V1.5 SAEDLINK library must be authorized. See "Step 3 Authorize SAEDLINK" on page 26.
- If you are using RACF Program Control security (WHEN(PROGRAM)), you must issue the following commands to allow the FTP exit programs to be fetched from the NV4IP V1.5 library:

```
RALTER PROGRAM FTCHKIP ADDMEM('hilevel.SAEDLINK'/volser/NOPADCHK) UACC(READ)
RALTER PROGRAM FTCHKPWD ADDMEM('hilevel.SAEDLINK'/volser/NOPADCHK) UACC(READ)
RALTER PROGRAM FTCHKCMD ADDMEM('hilevel.SAEDLINK'/volser/NOPADCHK) UACC(READ)
RALTER PROGRAM FTPOSTPR ADDMEM('hilevel.SAEDLINK'/volser/NOPADCHK) UACC(READ)
SETR WHEN(PROGRAM) REFRESH
```

  where hilevel is the NV4IP V1.5 dataset qualifier.

- Your FTP daemon Proc (FTPD) must be changed to point to the NV4IP V1.5 SAEDLINK. See "Process 1: NV4IP FTP Exits Only", step 1 or step 2 on page 32.
- If you had to re-link the NV4IP V1.3 FTP exits with your own FTP exits, you will need to follow the instructions in "Process 2: NV4IP FTP Exits with Existing User Exits" on page 33.
- The SAEDCONF library contains NV4IP configuration data; e.g., host definitions and critical resource definitions, etc. To retain configuration data during a

migration, copy the following members from your V1.3 SAEDCONF library to the V1.5 supplied library, replacing any existing members: AUTOMON, HOSTS, SERVERS, USER1, USER2, USER3. Then, run job CONVNAME from SAEDJCL. This job will convert existing host names and critical resource names to UTF-8 encoding, and change their length from 16 bytes to 48 bytes in support of internationalization.

- The SAEDVSM0 VSAM cluster contains NV4IP user options; e.g., auto-refresh interval and graphing options, etc. To retain user options during a migration, use the existing SAEDVSM0 in the AESTCPIP (or equivalent) PROC.
- Both the Host component and the Server component must be at V1.5 level. NV4IP V1.5 Host component will not work with NV4IP V1.3 Server component, and NV4IP V1.5 Server component will not work with NV4IP V1.3 Host component.

Required Target Libraries

Library	Description	Directory Blocks	Tracks 3390
SAEDCLIB	CLIST library	10	5
SAEDJCL	Sample JCL library	20	5
SAEDLINK	Load library	60	160
SAEDSLIB	Skeleton/System library and Panels	50	15
SAEDCMDS	Work File For Command Processing	N/A	30
SAEDCONF	Configuration File	40	15
SAEDOPT1	Product Options File	N/A	10
SAEDOPT2	Product Options File	N/A	10
Totals		180	3640

C Runtime Library

The Tivoli NetView for OS/390 C Runtime (Program Number 5697-B82) is required by NV4IP. If the C Runtime library (or its equivalent) is not in your LNKLST concatenation, you must STEPLIB the C Runtime library in all the PROCs and JCLs in SAEDJCL. The C Runtime library must be APF-authorized.

SAEDCONF

SAEDCONF contains the product configuration data, host definitions, and critical resource definitions for the system being monitored. The host definitions are contained in the *HOSTS* member and the critical resource definitions are contained in the *SERVERS* member. If the host definitions need to be reset, copy the member *MODLHOST* to *HOSTS*. If the critical resource definitions need to be reset, copy the member *MODLSERV* to *SERVERS*.

WARNING: DO NOT edit or delete any members in the SAEDCONF library!

Required VSAM Databases

The required VSAM databases per monitored TCP/IP stack are:

Suffix	Description	Cylinders (Initial Allocation)
SAEDVSM0	User Profiles and Report Database	100
SAEDVSM1	NV4IP Performance Database and Alerts Database	100
SAEDVSM2	NV4IP Workload Database	100
SAEDVSM3	IBM TCP/IP FTP SMF and LinkView Database	100
SAEDVSM4	IBM TCP/IP Telnet and API SMF Database	100
	Alternate Index for SAEDVSM4	30
SAEDVSM5	CSM, VTAM Buffer Pool, Alerts, and TraceRoute Database	100
Totals		630

User Ids

Using NV4IP requires a User Id and password. User Ids and passwords are saved on the host. The level of security used by NV4IP is determined by the SECURITY option in the CONFxx member of the SAEDSLIB data set during installation. The default member is CONF00. An installation may choose to use either NV4IP's own security authorization or a System Authorization Facility (SAF) product such as RACF, CA-ACF2, or CA-TopSecret. Security authorization option is specified by the SECURITY statement in CONFxx. The default security level is NV4IP security authorization (SECURITY=0). The available options and their operation are described below:

<table>
<tr><th>Security Option</th><th colspan="2">Description</th></tr>
<tr><td><b>0</b></td><td colspan="2">NV4IP security authorization. User IDs and passwords are defined by the Master component on the Server.</td></tr>
<tr><td><b>1</b></td><td colspan="2">SAF User Id and password authorization. A verified user has full access to the Master, Performance Manager and Operations Manager.</td></tr>
<tr><td rowspan="6"><b>2</b></td><td colspan="2">SAF User Id and password authorization with GROUP access verification. Group names as defined in your SAF product determine the authority of the user. A user may be connected to more than one group. The group names are:</td></tr>
<tr><td><b>Group name</b></td><td><b>Description</b></td></tr>
<tr><td>AESMSTR</td><td>Full access to the Master, Performance Manager, and Operations Manager functions.</td></tr>
<tr><td>AESPM</td><td>Access to the Performance Manager functions.</td></tr>
<tr><td>AESOM1</td><td>Access to the Operations Manager functions and informational command authority for Expert Commands.</td></tr>
<tr><td>AESOM2</td><td>Access to the Operations Manager functions and full command authority for Expert Commands.</td></tr>
</table>

Customize The Installation

The worksheets that follow provide a quick reference to be used when installing NV4IP. The Installation Preparation Worksheet provides a list of the datasets and naming conventions required for installing the application while the Installation Worksheets provide a checklist of the steps to be taken when installing NV4IP.

Installation Preparation Worksheet

Fill in the following information to be used during installation. It is recommended that you photocopy this worksheet and have it on hand during the installation so that you may refer back to it more easily.

Required Name/Information:		**Installation Standard**
Naming convention for: • SMP/E datasets (SMP/E HLQ) • production datasets (production HLQ)		
PROCLIB concatenation from the JES2 proc (PROC00)		
Name of TCPIP started task (e.g.: TCPIP)		
Name of TCPIP proc PROFILE dataset		
Name of TCPIP proc SYSTCPD dataset		
FTP server proc from PROFILE dataset (e.g.. FTPD)		
SYSFTPD name from FTP server proc		
LOAD member and IPLPARM dataset (from output of "D IPLINFO" command)		
IEASYS list (from output of "D IPLINFO" command)		
PARMLIB concatenation (from IPLPARM LOADxx member)		
Suffixes (from PARMLIB and IEASYS info.)	SMFPRM	
	BPXPRM	

Required Name/Information:		**Installation Standard**
	IKJTSO	
	PROG	
	LNKLST	
SMF system (SID) from SMFPRMxx		
Name of VTAM proc		
Suffix of the ATCCONxx member (from VTAM proc or start of VTAM proc - could be in COMMNDxx member of PARMLIB)		
Name of the VTAMLST dataset (from VTAM proc or start of VTAM proc - could be in COMMNDxx member of PARMLIB)		

After NV4IP has been successfully downloaded into target libraries, perform the following customization tasks:

1. Allocate non-SMP/E datasets and copies of SMP/E target files.
2. Specify SMF exits.
3. Authorize SAEDLINK.
4. Copy and modify NV4IP's PROCs.
5. Set up security administration.
6. Specify authorized TSO/E Commands.
7. Allocate and initialize VSAM databases for the historical data.
8. Enable TCP/IP SMF recording.
9. Install SMF and FTP exits.
10. Set Up AESVTCMD.
11. Set up NV4IP run-time options in CONF00.

Installation Checklist

The following is the first time installation checklist.

Item	Status	Notes
Allocate non-SMP/E datasets and copies of SMP/E target files		
Specify SMF exits		
Authorize SAEDLINK and Specify SMF Exits to the Dynamic Exits Facility		
Copy and modify NV4IP's PROCs. Copy the following PROCs from SAEDJCL to SYS1.PROCLIB (or equivalent) and modify: AESTCPIP, AESTNETS, and AESTCMDS		
Set up security administration		
Setup authorized TSO/E commands		
Allocate and initialize VSAM databases for the historical data		
Enable TCP/IP SMF recording		
Install SMF and FTP exits		
Set Up AESVTCMD. Copy the AESVTCMD member of SAEDJCL to the VTAMLST and activate the VTAM application.		
Set up NV4IP run-time options in CONF00		

Step 1. Allocate non-SMP/E datasets and copies of SMP/E target files.

Run job AEDSALO from SAEDJCL. This job allocates the non-SMP/E datasets required by NV4IP (SAEDCMDS, SAEDOPT1, SAEDOPT2) and also creates copies of the SMP/E target source libraries SAEDCLIB, SAEDCONF, SAEDJCL, and SAEDSLIB. Use the high-level qualifiers from the installation preparation worksheet. (For example: SMP/E HLQ, production HLQ.)

Each member beginning with AED has an alias that does not begin with AED. For example, in SAEDSLIB, member AEDCONF0 has an alias of CONF00. After you run the AEDSALO job, the CONF00 member in your production SAEDSLIB may be modified but you should NEVER edit the CONF00 member in your SMP/E target, SAEDSLIB, directly. When you apply SMP/E maintenance to SAEDCLIB, SAEDCONF, SAEDJCL, or SAEDSLIB, ensure that the changes made to the target libraries are merged into your production libraries.

NOTE: Never edit members in the SMP/E target libraries mentioned above! Editing a member will break the alias link between the members and future maintenance release will not apply correctly.

Step 2. Specify SMF Exits

NV4IP provides two standard SMF Record Exits: AESSMF00 and AESSMF85, which are explained below.

AESSMF00	This is the IEFU83 and IEFU84 SMF Record Exit. IEFU83 receives control when TCP/IP invokes either the SMFWTM macro or the SMFEWTM macro and specifies BRANCH=NO. IEFU84 receives control when TCP/IP invokes the SMFEWTM macro specifying BRANCH=YES.
AESSMF85	This is the IEFU85 SMF Record Exit. IEFU85 receives control when TCP/IP invokes the SMFEWTM macro, specifying BRANCH=YES and MODE=XMEM and when ASCB does not equal PSAAOLD.

Use the SMFPRM member suffix as listed in the installation preparation worksheet. The EXITS option of the SYS parameter in SMFPRMxx (in SYS1.PARMLIB) specifies which SMF exits are to be invoked for the entire system. If the EXITS option is not specified, all SMF exits are invoked. If an exit is not specified, it is not invoked. To define the SMF exits to SMF, complete the following steps:

1. Code the EXITS parameter:
    a. If you have NOEXITS specified for the SYS statement, replace it with EXITS(IEFU83,IEFU84,IEFU85). If you have coded an EXITS parameter, make sure that IEFU83, IEFU84 and IEFU85 are specified. Otherwise, no change is required.

   b. If you have a SUBSYS statement and you have coded an EXITS parameter, make sure that IEFU83, IEFU84 and IEFU85 are specified for SUBSYS STC, OMVS and TSO. Otherwise, no change is required.

2. Specify DDCONS(NO) in the SMFPRMxx member.

   The Network Statistics Collector and the Command Processor started tasks are long-running jobs. They invoke NETSTAT to collect workload data both for historical reporting and for real-time monitoring. NETSTAT may generate a lot of EXCP counts and dynamic allocations. When the Monitor is terminated, SMF will take a long time to perform DD consolidation for SMF Type 30 records and may impact the system's performance. DDCONS(NO) specifies that DD consolidation be bypassed, resulting in a reduction in system overhead when the Monitor is terminated.

3. Make sure that SMF record types 118/119 and 251 (or their equivalent user SMF record types, if 251 is already being used) are being recorded.

   Note: NV4IP requires that the following SMF records be written to Type 118/119: Telnet Server, Telnet Client, FTP Server, FTP Client, and API.

4. Issue command SET SMF=xx to dynamically modify the SMF recording options if you made any changes to the SMFPRMxx member.

   Here are some sample SMFPRMxx modifications for NV4IP:

Original SMFPRMxx	**Modified SMFPRMxx**
`SYS(TYPE(1:118,241,251))`	`No changes required`
`SYS(TYPE(1:255),EXITS(IEFUJI))`	`SYS(TYPE(1:255),EXITS(IEFU83,IEFU84,IEFU85,IEFUJI))`

`SYS(TYPE(1:255))`
`SUBSYS(STC,EXITS(IEFACTRT))`
	`SYS(TYPE(1:255))`
	`SUBSYS(STC,EXITS(IEFU83,IEFU84,IEFU85,IEFACTRT))`

Step 3. Authorize SAEDLINK and Specify SMF Exits to the Dynamic Exits Facility

SAEDLINK must be APF-authorized. To authorize SAEDLINK, complete the following steps:

1. Edit the PROGxx member in SYS1.PARMLIB to add an entry for SAEDLINK:

```
APF ADD DSNAME(highlevel.SAEDLINK) VOLUME(volser)
```

   Where volser is the volume serial for SAEDLINK.

   IBM has defined the SMF exits to the dynamic exits facility. Through the PROGxx parmlib member, you can associate multiple exit routines with SMF exits, at IPL or while the system is running.

2. To define SMF exits to the dynamic exits facility, add the following statements in the PROGxx member in SYS1.PARMLIB :

```
EXIT ADD EXITNAME(SYS.IEFU83) MODNAME(AESSMF00)
DSNAME(highlevel.SAEDLINK)

EXIT ADD EXITNAME(SYS.IEFU84) MODNAME(AESSMF00)
DSNAME(highlevel.SAEDLINK)
```

```
EXIT ADD EXITNAME(SYS.IEFU85) MODNAME(AESSMF85)
DSNAME(highlevel.SAEDLINK)
```

3. If IEFU83, IEFU84 and IEFU85 are specified in the EXITS option of the SUBSYS parameter(s) in SMFPRMxx, you must also define matching EXIT ADD statements for the following SUBSYS in PROGxx: STC, TSO, and OMVS. For example, if you specify the following in SMFPRMxx,

```
SUBSYS(STC,EXITS(IEFU83,IEFU84,IEFU85,…)…)

SUBSYS(OMVS,EXITS(IEFU83,IEFU84,IEFU85,…)…)

SUBSYS(TSO,EXITS(IEFU83,IEFU84,IEFU85,…)…)
```

You also need to specify the following in PROGxx:

```
EXIT ADD EXITNAME(SYSSTC.IEFU83)  MODNAME(AESSMF00) DSNAME(highlevel.SAEDLINK)

EXIT ADD EXITNAME(SYSSTC.IEFU84)  MODNAME(AESSMF00) DSNAME(highlevel.SAEDLINK)

EXIT ADD EXITNAME(SYSSTC.IEFU85)  MODNAME(AESSMF85) DSNAME(highlevel.SAEDLINK)

EXIT ADD EXITNAME(SYSOMVS.IEFU83) MODNAME(AESSMF00) DSNAME(highlevel.SAEDLINK)

EXIT ADD EXITNAME(SYSOMVS.IEFU84) MODNAME(AESSMF00) DSNAME(highlevel.SAEDLINK)

EXIT ADD EXITNAME(SYSOMVS.IEFU85) MODNAME(AESSMF85) DSNAME(highlevel.SAEDLINK)

EXIT ADD EXITNAME(SYSTSO.IEFU83)  MODNAME(AESSMF00) DSNAME(highlevel.SAEDLINK)

EXIT ADD EXITNAME(SYSTSO.IEFU84)  MODNAME(AESSMF00) DSNAME(highlevel.SAEDLINK)

EXIT ADD EXITNAME(SYSTSO.IEFU85)  MODNAME(AESSMF85) DSNAME(highlevel.SAEDLINK)
```

4. Make sure that the PROGxx member you updated is listed in the IEASYSxx member to allow these changes to be activated automatically after an IPL. Issue the SET PROG=xx operator command to dynamically change the APF list and SMF exits.

Step 4. Copy and Modify NV4IP's PROCs

NV4IP Monitor runs as three started tasks. The main started task (AESTCPIP) starts the other 2 started tasks, the Network Statistics Collector (AESTNETS), and the Command Processor (AESTCMDS). Refer to the installation preparation worksheet for PROCLIB names.

Copy the members **AESTCPIP, AESTNETS** and **AESTCMDS** in SAEDJCL to SYS1.PROCLIB (or its equivalent) and specify the required parameters in the PROCs.

The important parameters for the AESTCPIP PROC include the following:

CMDPROC	Specifies the started task name for the Command Processor. Default is AESTCMDS. If you renamed the AESTCMDS PROC name, you must code the new name in this parameter.
HOSTPORT	Specifies a TCP/IP port number for NV4IP Monitor to communicate with its users. The default number is 5050. The port number specified cannot be used or reserved by another application. Use the TCP/IP command NETSTAT PORTLIST to see if this port is reserved for another TCP/IP application.

See installation preparation worksheet for BPXPRM suffix.

Also check the INADDRANYPORT and INADDRANYCOUNT values coded in BPXPRMxx. If the port number (e.g., 5050) falls between the value coded for INADDRANYPORT and INADDRANYPORT+INADDRANYCOUNT, then this port is reserved for OMVS and you need to specify a different port number.

You may also reserve NV4IP's port number in the TCP/IP profile data set. For example:

PORT 5050 TCP AESTCPIP

NETSPROC	Specifies the started task name for the Network Statistics Collector. Default is AESTNETS. If you renamed the AESTNETS PROC name, you must code the new name in this parameter.
REFRESH	Default is 15 minutes. Specifies how often the data sampling counters are cleared and indicates the reporting interval for alerts on the SysPoint Home Page.
SMFSYSID	System Identification for SMF records.
SMFRECID	Specifies the SMF record type for NV4IP's SMF records. The default is 251. Please use the "D SMF,O" operator command to verify that this record type is available. If it is being excluded, then you need to modify SYS1.PARMLIB(SMFPRMxx) to include this record type.

Step 5. Set Up Security Administration

If you have a security manager such as RACF or ACF2, the three started tasks (AESTCPIP, AESTNETS, and AESTCMDS) or their equivalents must belong to a started task group that has READ/WRITE authorization to all the target libraries and VSAM databases. The AESTCIP started task must also have proper authority to Start/Stop the other two started tasks.

The AESTCMDS task must have update access to MVS.VARY.TCPIP.DROP or its equivalent in order to allow an NV4IP user to issue the NETSTAT DROP command from within NV4IP. Please consult with your site's security administrator prior to setting up the authorized group to ensure that task name assignments and authorizations follow site security procedures.

All socket applications must have an OMVS segment definition. Typically, the OMVS segment definition is defined by your installation's security administrator. It may be set up to use a default OMVS segment so that a unique OMVS segment is not required for each application.

1. Create an OMVS segment.
   a. Issue an LU (list user) command for your TCPIP started task name (ex: LU TCPIP) and note the value for DEFAULT-GROUP. For example:

```
       USER=TCPIP  NAME=UNKNOWN  OWNER=IBMUSER   CREATED=01.050

       DEFAULT-GROUP=OMVS      PASSDATE=N/A     PASS-INTERVAL=N/A
```

   b. Define the started task ids (AESTCPIP AESTCMDS AESTNETS or equivalents) using the same default group as TCPIP. From the above example, the ADDUSER command syntax would be:

```
       ADDUSER AESTCPIP  DFLTGRP(OMVS)       .
```

2. Set up the OMVS segments for *each* started task. Each OMVS segment must have the appropriate UID, GID, home directory, and initial program location. Note that if the OMVS segment definition is missing or incorrect, the Monitor will not start up and the following error message will be received:

```
LSCX470 **** WARNING **** ERRNO = ESYS
.....  Vendor-specific TCP/IP error condition (IBM TCP/IP: errno=156).
socket() call failed in AEST001: Operating system interface failure
```

Step 6.   Setup Authorized TSO/E Commands

Add the following commands to the AUTHCMD list in SYS1.PARMLIB(IKJTSOxx)

See installation preparation worksheet for IKJTSO suffix.

```
AESCNETS
AEST044
AEST049
```

where 0 is zero.

To dynamically add the commands to the AUTHCMD list, use the TSO command PARMLIB. The command syntax for PARMLIB is as follows:

PARMLIB UPDATE(xx)

Where xx is the PARMLIB member suffix that is being updated or used for production. Please verify that this command is available in your operating environment (operating system level and group authority to issue the commands).

The following RACF commands would give USER XXXX authority to issue the PARMLIB command:

```
  permit parmlib class(tsoauth) id(XXXX) acc(upd)

  setropts raclist(tsoauth) refresh
```

Step 7. Allocate and Initialize VSAM Databases for the Historical Data

NV4IP requires six VSAM datasets to be allocated for historical performance, workload, and real-time monitoring data. The default cluster names are SAEDVSM0, SAEDVSM1, SAEDVSM2, SAEDVSM3, SAEDVSM4, and SAEDVSM5.

- If migrating from NV4IP 1.3 or 1.4, you may continue to use the existing VSAM databases.
- For new installs, use the sample JCL **AESTINIV** in SAEDJCL to allocate and initialize these VSAM databases.

Step 8. Enable TCP/IP SMF Recording

Refer to the installation preparation worksheet for TCP/IP started task and PROC names. NV4IP captures TCP/IP's SMF records and reports on activities such as FTP, Telnet, and API based on SMF statistics. Complete the following steps to enable TCP/IP SMF recording:

1. Specify the following statement in the FTP DATA dataset (DD statement SYSFTPD in the FTP daemon(FTPD) proc) for FTP Server records:

```
SMF STD
SMF TYPE119[1]
```

2. Specify the following statement in the TCP/IP PROFILE dataset (DD statement PROFILE in the TCP/IP proc) for FTP Client, Telnet Client and API records:

```
SMFCONFIG TCPINIT TCPTERM FTPCLIENT TN3270CLIENT
     TYPE119 TCPINIT TCPTERM FTPCLIENT TN3270CLIENT[2]
```

3. Specify the following statement in the TCP/IP PROFILE dataset(DD statement PROFILE in the TCP/IP proc) for Telnet Server records:

```
TELNETPARMS
…
…
SMFINIT STD
SMFINIT TYPE119
SMFTERM STD
SMFTERM TYPE119
…
…
ENDTELNETPARMS
```

NOTE: If you made any changes to the FTP DATA dataset or the TCP/IP PROFILE dataset, you will need to restart TCP/IP.

---

[1] To have all type 119 FTP server records created.

[2] To enable type 119 records recorded.

Step 9. Install SMF and FTP Exits

NV4IP provides two types of user exits: NV4IP SMF exits and NV4IP FTP exits. The use of the SessionLog Expert requires the completion of the following steps:

1. Enable the SMF exits.
2. Enable the FTP exits.
3. Set the parameters for the exits in the CONFxx (Default is CONF00) member in the *high-level.SAEDSLIB* data set.

NOTE: If you are running multiple NV4IP Monitors in the same LPAR, FTP and SMF exits may be activated for only one Monitor.

SMF Exit

Configure CONFxx to specify the logging options by setting the SMFXTELNET, SMFXFTP, and SMFXAPI parameters. Specify the SMF record subtypes and the SMFXN parameter if required. Sample CONF00 statements include the following:

```
SMFXTELNET LOG=YES,WTO=NO
SMFXFTP    LOG=YES,WTO=NO
SMFXAPI    LOG=YES,WTO=NO
```

Default Sub-Types

If you are not using the default subtypes for your TCP/IP SMF records, use the following statements to specify the subtypes in CONFxx:

Statement Syntax	*Record subtype*	*Default Value*
TCPINIT=n	API INIT record	1
TCPTERM=n	API TERM record	2
FTPCLIENT=n	FTP Client record	3
TN3270CLIENT=n	Telnet Client record	4
TCPIPSTATISTICS=n	TCP/IP statistics record	5
TELNETSMFINIT=n	Telnet Server INIT record	20
TELNETSMFTERM=n	Telnet Server TERM record	21
SMFAPPE=n	FTP Server Append record	70
SMFDEL=n	FTP Server Delete record	71
SMFLOGN=n	FTP Server Login Failure record	72
SMFREN=n	FTP Server Rename record	73
SMFRETR=n	FTP Server Retrieve record	74
SMFSTOR=n	FTP Server Store record	75

FTP Exit Installation

Two processes are defined below for the FTP Exit Installation. Complete process 1 if your installation does not have any of the following exits defined: FTCHKIP, FTCHKPWD, FTCHKCMD or FTPOSTPR. If your installation already has one or more of these exits defined; for example, one or more of these modules are in a STEPLIB of the FTP Server PROC or in a LNKLST library (refer to installation preparation worksheet), complete process 2 to re-link the NV4IP FTP exits with your installation's FTP exit(s). Your FTP exit will then be invoked after NV4IP's FTP exit has finished processing.

Use the SETROPTS LIST command to see if the RACF Program Control is active. If the RACF Program Control *is* active, that is, if you have issued the SETROPTS WHEN(PROGRAM) RACF command, you ***must*** define FTP Exits to RACF class *PROGRAM* as follows:

```
RDEFINE PROGRAM FTCHKIP ADDMEM('hilevel.SAEDLINK'/volser/NOPADCHK) UACC(READ)
RDEFINE PROGRAM FTCHKPWD ADDMEM('hilevel.SAEDLINK'/volser/NOPADCHK) UACC(READ)
RDEFINE PROGRAM FTCHKCMD ADDMEM('hilevel.SAEDLINK'/volser/NOPADCHK) UACC(READ)
RDEFINE PROGRAM FTPOSTPR ADDMEM('hilevel.SAEDLINK'/volser/NOPADCHK) UACC(READ)
SETR WHEN(PROGRAM) REFRESH
```

The volume serial of the target library SAEDLINK is *volser*. An asterisk may be specified instead of the actual volser to indicate that the volser where SAEDLINK is cataloged should be used. for example: 'hilevel.SAEDLINK'/*/NOPADCHK.

NOTE: If the RACF Program Control is active and you did not define FTP Exits to RACF, the FTP client receives the following error message when it tries to log into FTP:

```
550 PASS COMMAND FAILED - _PASSWD() ERROR: EDC5157I AN INTERNAL ERROR OCURRED
```

Process 1: NV4IP FTP Exits Only

To set up the FTP exits, complete the following steps:

1. Add SAEDLINK to your FTP Server Proc (FTPD):
   //STEPLIB DD DISP=SHR,DSN=*highlevel*.SAEDLINK

2. Recycle the FTP Server (stop and then re-start it) to make the NV4IP FTP exits accessible to the FTP Server. This is necessary because the FTPCHKIP user exit is loaded at FTP daemon initialization time only.
3. Configure CONFxx to specify the logging options via the FTCHKIP, FTCHKPWD, FTCHKCMD and FTPOSTPR statements. Specify FTPXN as well, if required.

Process 2: NV4IP FTP Exits with Existing User Exits

If your installation already has one or more of these FTP exits (FTCHKCMD, FTCHKIP, FTCHKPWD, FTPOSTPR), please perform the following procedures to re-link NV4IP's FTP exit(s) with your installation's FTP exit(s). Your FTP exit will then be invoked after NV4IP's FTP exit has finished processing.

NOTE: If you are re-linking non-reentrant load modules with NV4IP's FTP exits, remove the RENT parameter from the PARM field in the following JCL.

FTCHKCMD

To set up the FTCHKCMD exit, complete the following steps:

1. Copy FTCHKCMD from hilevel.SAEDLINK to another load library (temp-load).
2. Modify your installation's FTCHKCMD:
    - Rename the module to FTCHKCM2.
    - Change the CSECT to FTCHKCM2.
    - Assemble FTCHKCM2 into user-objlib.
3. Relink NV4IP's FTCHKCMD with your FTCHKCM2 by entering the following:

```
// EXEC PGM=IEWL,PARM='LIST,MAP,XREF,RENT'
//SYSLMOD DD DISP=SHR,DSN=hilevel.SAEDLINK
//SAEDLINK DD DISP=SHR,DSN=temp-load
//OBJ     DD DISP=SHR,DSN=user-objlib
//SYSUT1  DD DSN=&&SYSUT1,UNIT=SYSDA,SPACE=(CYL,(2,2))
//SYSLIN  DD DDNAME=SYSIN
//SYSIN   DD *
   INCLUDE SAEDLINK(FTCHKCMD)
   INCLUDE OBJ(FTCHKCM2)
   NAME FTCHKCMD(R)
//
```

FTCHKIP

To set up the FTCHKIP exit, complete the following steps:

1. Copy FTCHKIP from hilevel.SAEDLINK to another load library (temp-load)
2. Modify your installation's FTCHKIP:
    - Rename the module to FTCHKI2.
    - Change the CSECT to FTCHKI2.
    - Assemble FTCHKI2 into user-objlib.

3. Relink NV4IP's FTCHKIP with your FTCHKI2 by entering the following:

```
// EXEC PGM=IEWL,PARM='LIST,MAP,XREF,RENT'
//SYSLMOD DD DISP=SHR,DSN=hilevel.SAEDLINK
//SAEDLINK DD DISP=SHR,DSN=temp-load
//OBJ     DD DISP=SHR,DSN=user-objlib
//SYSUT1  DD DSN=&&SYSUT1,UNIT=SYSDA,SPACE=(CYL,(2,2))
//SYSLIN  DD DDNAME=SYSIN
//SYSIN   DD *
   INCLUDE SAEDLINK(FTCHKIP)
   INCLUDE OBJ(FTCHKI2)
   NAME FTCHKIP(R)
//
```

FTCHKPWD

To set up the FTCHKPWD exit, complete the following steps:

1. Copy FTCHKPWD from hilevel.SAEDLINK to another load library (temp-load)

2. Modify your installation's FTCHKPWD:

- Rename the module to FTCHKPW2.
- Change the CSECT to FTCHKPW2.
- Assemble FTCHKPW2 into user-objlib.

3. Relink NV4IP 's FTCHKPWD with your FTCHKPW2 by entering the following:

```
 // EXEC PGM=IEWL,PARM='LIST,MAP,XREF,RENT'
//SYSLMOD DD DISP=SHR,DSN=hilevel.SAEDLINK
//SAEDLINK DD DISP=SHR,DSN=temp-load
//OBJ     DD DISP=SHR,DSN=user-objlib
//SYSUT1  DD DSN=&&SYSUT1,UNIT=SYSDA,SPACE=(CYL,(2,2))
//SYSLIN  DD DDNAME=SYSIN
//SYSIN   DD *
   INCLUDE SAEDLINK(FTCHKPWD)
   INCLUDE OBJ(FTCHKPW2)
   NAME FTCHKPWD(R)
//
```

FTPOSTPR

To set up the FTPOSTPR exit, complete the following steps:

1. Copy FTPOSTPR from hilevel.SAEDLINK to another load library (temp-load)

2. Modify your installation's FTPOSTPR:

- Rename the module to FTPOSTP2.
- Change the CSECT to FTPOSTP2.
- Assemble FTPOSTP2 into user-objlib.

3. Relink NV4IP's FTPOSTPR with your FTPOSTP2 by entering the following:

```
 // EXEC PGM=IEWL,PARM='LIST,MAP,XREF,RENT'
//SYSLMOD DD DISP=SHR,DSN=hilevel.SAEDLINK
//SAEDLINK DD DISP=SHR,DSN=temp-load
//OBJ     DD DISP=SHR,DSN=user-objlib
//SYSUT1  DD DSN=&&SYSUT1,UNIT=SYSDA,SPACE=(CYL,(2,2))
//SYSLIN  DD DDNAME=SYSIN
```

```
    //SYSIN    DD *
       INCLUDE SAEDLINK(FTPOSTPR)
       INCLUDE OBJ(FTPOSTP2)
       NAME FTPOSTPR(R)
    //
```

Step 10. Set Up AESVTCMD

The AESVTCMD member in the SAEDJCL dataset must be copied to the VTAM list and activated as an application in order for the VTAM command option to function.

Note: You may change the major and minor node names for AESVTCMD, but you may ***not*** change the ACBNAME.

1. Activate the application by issuing the following VTAM command from the console:

   V NET,ACT,ID=AESVTCMD

2. To ensure that AESVTCMD is activated on subsequent starts of VTAM (or after an IPL) add AESVTCMD to your ATCCONxx member in VTAMLST where xx is the CONFIG=xx parameter in ATCSTR00.

Step 11. Set Up NV4IP Run-Time Options in CONFxx

NV4IP's configuration parameters are specified in the CONFxx (Default is CONF00) member in SAEDSLIB. If you are running multiple Monitors, you may wish to set up a separate CONFxx member for each Monitor. Then, modify the AESTCPIP PROC or its equivalent to point to the correct member in SAEDSLIB.

Here is a sample CONFxx member that includes SMF and FTP exit specifications. The parameters that can be specified are covered in detail following this section. Once you have completed the configuration of the CONFxx member, you are ready to start NV4IP. Refer to *NV4IP Monitor Operation*.

```
SECURITY=1
COMMANDLOG=YES
AUTOALERT=YES
SMFXTELNET,LOG=YES,WTO=WTL
SMFXFTP,LOG=YES,WTO=WTL
SMFXAPI,LOG=YES,WTO=WTL
SMFXN=10000
FTPXINTERVAL=55
FTCHKIP,LOG=YES,WTO=WTL
FTCHKPWD,LOG=YES,WTO=WTL
FTPCHKCMD,LOG=YES,WTO=WTL
FTPOSTPR,LOG=YES,WTO=WTL
APPLMON S,FTPS,I=30,T=80K,S=10000K,P=20
TCPMON=TCPIP
VTAMBUFINTERVAL=60
CSMALERT 1000,1000,10,0,23
CSMINTERVAL=60
MREC=YES
```

```
TCPPORTMON=21
TCPPORTMON=80
TCPPORTMONINTERVAL=600
DEVLINKMON I=600,Q=3
```

Figure 1. Sample CONFxx Member

The **CONFxx** parameters setup and control logging, ftp options, real-time monitoring, security and use of the SMF exits. The parameter and its options are listed below in alphabetical order. Following the table is a description of each CONFxx parameter.

CONFxx Parameter	Description
Command Logging	COMMANDLOG
FTP Exit options	FTCHKCMD FTCHKIP FTCHKPWD FTPOSTPR FTPXINTERVAL FTPXN
Real-Time Monitoring	APPLMON APPLMONHOURS AUTOALERT AUTOTRACEROUTE CSMALERT CSMINTERVAL DEVLINKMON DEVLINKEXCEPTION FPING IPV6 MREC TCPMON TCPPORTMON TCPPORTMONINTERVAL VTAMBUFINTERVAL
Security	SECURITY
SMF Exit	SMF119 SMFXAPI SMFXFTP SMFXN SMFXTELNET

Table 1. CONFxx Parameters

COMMAND LOGGING PARAMETER

COMMANDLOG=YES|NO	Specifies whether to keep track of TCP/IP or VTAM commands issued by NV4IP users. If YES is specified, such commands are logged in the //SYSPRINT DD statement of the main STC PROC (AESTCPIP). Default=NO.

FTP EXIT OPTION PARAMETERS

For the FTP Exit Options, LOG= may be set to YES to force an event to be written to the NV4IP FTP log, AESFTPLG DD. The default is that an event is not recorded in the log. Further, a WTO may be written to the operator console or system log when certain events occur. The default is that an event is not written to the console or to the system log.

FTCHKCMD LOG=YES|NO, WTO=YES|NO|WTL	Activates the FTP Command exit.
FTCHKIP LOG=YES|NO, WTO=YES|NO|WTL	Activates the FTP Open Connection exit.
FTCHKPWD LOG=YES|NO, WTO=YES|NO|WTL	Activates the FTP Password Verification exit.
FTPOSTPR LOG=YES|NO, WTO=YES|NO|WTL	Activates the FTP Command Completion exit.
FTPXINTERVAL=n	Specifies how frequently (in seconds) the Monitor should scan its internal memory buffer for new events to write out to log. Default=60.
FTPXN=n	Specifies the number of FTP Exit events to be kept in memory for real-time analysis. This is a wrapped around buffer located in ECSA. Each buffer entry is 72 bytes. This buffer area will be allocated only if one or more NV4IP's FTP exits are active. Default=10000.

Real-Time Monitoring Parameters

APPLMON C|S,<Application Group>,I=<Interval>,T=<Throughput>,S=<Size>, P=<Port Ranges>

Use the APPLMON statement to monitor a range of ports for hangs, throughput, and data transfer size. This feature is intended to monitor long-running applications whose availability and performance are of critical importance. Up to 8 APPLMON statements may be specified. Please limit the number of application groups to reduce overhead. When an exception occurs, one of the following messages will be displayed: AES914W, AES915W or AES916W. The parameters, listed by subject, are described below.

Parameter	**Description**	
C|S	**C**	specifies that client ports are to be monitored.
	S	specifies that server ports are to be monitored.
<APPLICATION GROUP>	Specifies the name of the application to be monitored. This is a user defined name and can be from one to eight characters.	
I	Specifies the monitoring interval in seconds. The minimum value is 10. Recommended value is 10 through 30. If a value less than 10 is specified, it will be reset to 10.	
T	Specifies the *minimum* throughput in bytes/second that the application must perform. You may add the letter 'K' at the end to denote thousands of bytes, for example, T=55000, or T=55K. If this is not specified, or if T=0 is specified, then throughput exception will not be monitored.	
S	Specifies the *maximum* data size in bytes that the application is allowed to transfer. You may add the letter 'K' at the end to denote thousands of bytes, for example, S=60000000, or S=60000K. If this is not specified, or if S=0 is specified, then data size exception will not be monitored.	
P	Specifies one or more ports to be monitored. You may specify a single port, e.g., P=23; a range of ports, e.g., P=6060-6070; or a combination of both. E.g., P=23,4000,5000-5003,6000-6060.	

Sample Statements include:

To monitor FTP Server data port	APPLMON S,FTPS,I=12,T=80K,S=10000K,P=20
To monitor FTP Clients	APPLMON C,FTPC,I=10,T=50K,S=20000K,P=20
To monitor application server ports 6000, 6005, 7000-7010, and 8080	APPLMON S,SAMPLE,I=15,T=40K,S=1000K, P=6000,6005,7000-7010,8080

APPLMONHOURS <start hour>,<end hour>

This option specifies the hour range within which APPLMON will be active. The hour range will apply to all application groups specified in the APPLMON statement(s).

Default = APPLMONHOURS 0,23

AUTOALERT=YES|NO

This option specifies whether to start Availability and/or Performance alert monitoring automatically. The Performance alert conditions are set as determined by its last activation settings. Default = NO.

AUTOTRACEROUTE <packet size>,<time out>

This option specifies whether to start TraceRoute automatically when an Availability or Performance alert is triggered. The TraceRoute data will be saved in a VSAM database for later analysis. This option is in effect only if AUTOALERT=YES is specified, or if Availability and/or Performance alert is turned on.

Settings include the following:

<packet size>	specifies the packet size for TraceRoute
<time out>	specifies the time out value (in seconds) for TraceRoute

For example: AUTOTRACEROUTE 32,2

CSMALERT <ECSA Threshold>,<DSP Threshold>,<% Free Threshold>,<Start Hour>,<End Hour>

This option specifies CSM exception monitoring settings. A sample of this would be CSMALERT 1000,1000,10,0,23. WTO messages will be issued when an exception occurs. The CSMINTERVAL option must be specified in order for this to take effect. Exception monitoring settings include the following:

<ECSA Threshold>	specifies the maximum number (KB) of buffer space to be used of ECSA by any address space. If the threshold is exceeded, then the WTO AES918W message will be displayed.
<DSP Threshold>	specifies the maximum number (KB) of buffer space to be used of Data Space by any address space. If the threshold is exceeded, then the WTO AES918W message will be displayed.
<% Free Threshold>	sets the minimum percent free for any CSM buffer area. If the percent free is below the threshold, then the AES919W WTO message will be displayed.
<Start Hour>	starting hour (0 to 23) for the exception monitoring to be active.
<End Hour> active	ending hour (0 to 23) for the exception monitoring to be active.

CSMINTERVAL=n

This option specifies that CSM usage is to be monitored, where n is the monitoring interval (in seconds). The minimum value is 60.

DEVLINKEXCEPTION=<link name>

This option specifies a link name that is NOT to be monitored for availability.

<link name>	specifies a 1 to 16-character link name. A single asterisk ('*') may be specified at the end of a name to indicate 0 or more of any character. Up to 256 DEVLINKEXCEPTION statements may be specified.

Some examples include the following:

DEVLINKEXCEPTION=ETH6

DEVLINKEXCEPTION=TR2*   (This will match any name that starts with "TR2".)

DEVLINKMON I=<Interval>,Q=<Queuesize>

This option specifies how frequently channel-attached processors should be monitored. If the CHPID is not ready, then the AES920W WTO message will be displayed. If the link is not ready, then the AES921W WTO message will be displayed. Optionally, the channel-attached processor's queue size may also be monitored.

<Interval>	specifies monitoring interval in seconds. The minimum value is 60. Default value is 600.
<Queuesize>	specifies the queue size threshold. If the threshold is exceeded, then the AES922W message will be displayed.

FPING <IP Address>,<Port Number>

This option allows NV4IP to monitor a critical resource behind a firewall that blocks ICMP messages. If a monitored critical resource has a matching IP address on the FPING statement, NV4IP will attempt to make a TCP connection to that port. (The critical resource must first be defined by the Master or by the SERVDEF Modify command.) If a TCP connection cannot be established, then the critical resource is considered unavailable. Otherwise, the critical resource is considered available, and the response time is the time that it took to establish the TCP connection. Up to 1,200 FPING statements may be specified.

<IP Address>	specifies the IP address of a monitored critical resource that is behind a firewall.
<Port Number>	specifies a TCP port number on the critical resource. This port must be in listening state and that a TCP connection can be established through the firewall.

IPV6=YES|NO

For z/OS 1.4 or later releases only. This option specifies whether IPV6 is enabled, or if LONG format is specified on the IPCONFIG statement in the TCP/IP Profile. *Note*: NV4IP will only display the low 32 bits of an IPV6 address. Default=NO.

MREC=YES|NO

This option specifies whether the minutely performance records and workload records are to be written to the VSAM databases. You may specify NO to save space in the VSAM databases, but you won't be able to drill down from historical hourly reports to the minutely reports. Default = NO.

TCPMON=<address space name>

This option specifies the TCP/IP and related address space name for StackView to monitor. Up to 8 TCPMON statements can be specified. This is a required parameter for StackView operation. Some examples include the following:

```
TCPMON=TCPIP
TCPMON=CICSX
```

TCPPORTMON=<port number>

This option specifies the TCP port number to be monitored by NV4IP. NV4IP will test the port number to see if a connection can be made. If not, then the AES923W message will be displayed. Up to 128 TCPPORTMON statements may be specified.

TCPPORTMONINTERVAL=<Interval>

This option specifies the TCPPORTMON monitoring interval in seconds. The minimum value is 60. Default is 600.

VTAMBUFINTERVAL=n

This option specifies that VTAM buffer usage is to be monitored, where n is the monitoring interval (in seconds). The minimum value is 60.

Security Parameters

SECURITY = 0 |1|2

This option specifies your security settings. An installation may choose to use either NV4IP's own security authorization or a System Authorization Facility (SAF) product such as RACF, CA-ACF2, or CA-TopSecret. The default security level is NV4IP security authorization (SECURITY=0). SECURITY=1 refers to SAF User Id and password authorization. SECURITY=2 refers to SAF User Id and password authorization with GROUP access verification. For more detailed information, please refer to the section on Host Monitor Installation.

SMF Exit Parameters

SMF119=YES|NO

Specify to use SMF type 119 records or not. If YES is specified, NV4IP only looks for type 119 records. Default is NO.

SMFXAPI LOG=YES|NO, WTO=YES|NO|WTL

Captures API SMF records.

LOG	Specifies whether the event is to be written to NV4IP's SMF logs: AESSTLOG – Telnet records AESSFLOG – FTP records AESSALOG – API records The default is NO.
WTO	Specifies whether the event is to be written to the operator console (WTO=YES), or to the system log (WTO=WTL). The default is NO.

SMFXFTP LOG=YES|NO, WTO=YES|NO|WTL

Captures FTP SMF records.

SMFXN=n

Specifies the number of NV4IP's SMF exit events to be kept in memory for real-time analysis. This is a wrapped around buffer area located in ECSA. Each entry is 130 bytes. This buffer area will be allocated only if one or more SMF exit option statements are specified. Default =10000.

SMFXTELNET LOG=YES|NO, WTO=YES|NO|WTL

Captures Telnet SMF records.

Installing the Monitor on Multiple Systems

If your installation wishes to install and run the Monitor on multiple systems, the steps below must be repeated for *each* system:

1. Customize the PROCS for each system:

   AESTCPIP

   AESTNETS

   AESTCMDS
2. Allocate a unique data set for each system by using a unique *CFGHILVL* qualifier for the following datasets:
   - **SAEDOPT1**
   - **SAEDOPT2**
   - **SAEDCMDS**

   These data sets should have the same attributes as the existing data sets.
3. Allocate and initialize VSAM databases using a different VSMHILVL high-level qualifier per system.
4. Create and copy the target library, **SAEDCONF,** to the **CFGHILVL.SAEDCONF** equivalent

   where *CFGHILVL* is the CFGHILVL parameter value that has the new configuration high-level qualifier in the AESTCPIP and AESTCMDS Procs (or their equivalents) for each system.

   Each instance of NV4IP must have its own SAEDCONF dataset and a unique HOMEIP member (in SAEDCONF) for each LPAR. Do not copy the HOMEIP member from an existing SAEDCONF to a new SAEDCONF. The HOMEIP member will be automatically created when you start NV4IP for the very first time.
5. Create a new CONFxx member in SAEDSLIB and specify the member name in the AESTCPIP Proc. That is, if you defined the new NV4IP parameters in member CONF091, then specify CONF=CONF091 in the AESTCPIP Proc.

Installing Multiple Monitors on a Single LPAR

If you are running more than one TCP/IP stack in a single LPAR and you wish to monitor them all, configure the Monitor as above, but with the following limitations:

1. Only one Monitor may activate the SMF and FTP exits.
2. The Monitor with active SMF and FTP exits will see Session Log activities from all of the TCP/IP stacks in the LPAR.

NV4IP MONITOR OPERATION

The Monitor Operation section describes the management of the Monitor portion of NV4IP on the MVS host. This section contains information on turning on alerts, starting and stopping NV4IP on the Host, enabling the submission of VTAM commands, adding critical resources, and managing the historical database.

NV4IP Alerts Summary

The following table summarizes NV4IP alerts and their related messages. These alerts are shown in SysPoint and may be reviewed through the selection of Historical Reports or Show Detail information at the workstation.

Alert Type	***CONFxx statements and other setup***	***WTO Messages***
CSM Buffer Alert	CSMALERT CSMINTERVAL	AES918W AES919W
Link Alert	DEVLINKMON	AES920W AES921W AES922W
Port Alert	TCPPORTMON TCPPORTMONINTERVAL	AES923W
Session Alert	APPLMON APPLMONHOURS	AES914W AES915W AES916W
Critical Resource Availability Alert	Critical resources are defined by the Master or by the SERVDEF Modify command. Initially, critical resources are monitored by the "Start Monitoring" option in the Master. Availability alerts are also specified by the Master. Subsequently, they may be automatically monitored by specifying AUTOMON=YES in the AESTCPIP Proc. Availability alerting may be started automatically by specifying AUTOALERT=YES in CONFxx.	AES902W
Critical Resource Performance Alert	Initially, performance alerting is specified by the Master. Subsequently, performance alerts may be started by specifying AUTOALERT=YES in CONFxx.	AES901W

Starting NV4IP on the Host

The steps to start the Monitor on the host are:

1. Enable VTAM.
2. Start the Monitor.

Enable VTAM Command Submission

Enabling VTAM Command Submission provides monitoring of the CSM and VTAM buffers and the use of VTAM commands from within the NV4IP application. To enable the submission of VTAM commands, execute the following command from the MVS Operator's console or NetView:

```
VARY NET,ACT,ID=AESVTCMD
```

This allows the use of the Console and Expert-Assist VTAM commands functions from within the Operations Manager. If the application is not activated, these functions are not available.

Start the Monitor

To start the NV4IP Monitor on the host, issue the following system command from the system console, given that the STC PROC is AESTCPIP:

```
S  AESTCPIP
```

This started task automatically starts the Network Statistics Collector (AESTNETS), and the Command Processor (AESTCMDS). AESTCPIP can also be started via the AUTOLOG statement in the TCP/IP Profile data set. This ensures that AESTCPIP is started after TCP/IP is fully initialized.

The AESTCMDS task must have update access to MVS.VARY.TCPIP.DROP or its equivalent in order to allow an NV4IP user to issue the NETSTAT DROP command from within NV4IP.

Warning: Do not start AESTNETS or AESTCMDS manually!!

Stopping NV4IP on the Host

To stop the NV4IP Monitor, issue the following system command:

```
P  AESTCPIP
```

The started task automatically stops the Network Statistics Collector (AESTNETS), and the Remote Command Processor (AESTCMDS) if the Operations Manager is enabled. It may take a few seconds for the Monitor to completely shut down.

Warning: Do not stop AESTNETS or AESTCMDS manually!!

If the Monitor cannot be stopped normally, use the CANCEL command, such as *C AESTNETS*, to cancel individual started tasks.

Adding Critical Resources Using a Host Based Data Set

MVS TCP/IP address spaces and critical resources may be added from a Host input data set or using the Master. The procedures below describe the process used to add resources using the Host component of NV4IP.

MVS TCP/IP Address Spaces

To add new MVS TCP/IP address space definitions from a Host input data set, use the following Modify command:

F aestcpip, HOSTDEF=<dsn>

Where <dsn> specifies the data set that contains the definition. Do not use quotes around the data set name. For example:

```
F AESTCPIP,HOSTDEF=SYS2.TEST.HOSTDEF
F AESTCPIP,HOSTDEF=SYS2.HOSTDEF.PDS(SYSA)
```

Each Data Format statement within the data set has the following syntax:
<host name>; <IP address>; <port number>;

The field values are defined as:

<host name>	MVS TCP/IP Host name; 1 to 16 characters
<IP address>	IP address of the host
<port number>	Port number for running the Monitor

For example, the contents of the SYS2.TEST.HOSTDEF data set are:

```
HOST HT1; 137.72.43.240; 5050;
SYS J; 10.31.109.130; 5050;
```

WTO Messages

The messages displayed are based on the success or failure of the commands. If the command was successful, the following message is displayed:

AES840I HOST DEFINITIONS ADDED

If the command failed, one of the following messages is displayed:

```
AES841E  HOSTDEF INVALID DSN:<dsn>
AES842E  HOSTDEF DYNALLOC FAILED FOR <dsn>
AES843E  HOSTDEF UNABLE TO OBTAIN A SOCKET
AES844E  HOSTDEF SOCKET CONNECTION FAILED
AES845E  HOSTDEF SendRec FAILED
AES846E  HOSTDEF RecvRec FAILED
AES847E  HOSTDEF I/O ERROR
AES848E  HOSTDEF UNKNOWN ERROR: <error code>
```

Critical Resources

To add new Critical Resource definitions from a Host input data set, use the following Modify command:

```
F aestcpip,SERVDEF=<dsn>
```

Where <dsn> specifies the data set that contains the definitions. Do not use quotes around the data set name. Valid command examples are:

```
F AESTCPIP,SERVDEF=SYS2.TEST.SERVDEF
F AESTCPIP,SERVDEF=SYS2.TESTDEF.PDS(SYSA)
```

Each Data Format statement within the data set has the following syntax:
<server name>; <IP address>; <interval in minutes>; <interval in seconds>; <packet size 1>; <packet size 2>; <packet size 3>; <packet size 4>;

The field values are defined as:

<server name>	Critical resource name; 1 to 16 characters
<IP address>	IP address of the critical resource
<interval in minutes>	Monitoring frequency in minutes
<interval in seconds>	Monitoring frequency in seconds
<packet size>	Up to 4 packets may be sent to the critical resource. Specify from the following: 0, 256, 512, 1024, 2048. If 0 is specified, then that packet will not be sent.

For example, the contents of the SYS2.TEST.SERVDEF data set are:

```
ROUTER AS2; 137.72.43.1; 0; 5; 256; 512; 1024; 2048;
ROUTER AS19; 137.72.246.1; 1; 0; 256; 512; 1024; 2048;
```

Figure 2. Adding Critical Resources

WTO Messages

The messages displayed are based on the success or failure of the commands. If the command was successful, the following message is displayed:

AES830I SERVER DEFINITIONS ADDED

If the command failed, one of the following messages is displayed:

AES831E SERVDEF INVALID DSN:<dsn>
AES832E SERVDEF DYNALLOC FAILED FOR <dsn>
AES833E SERVDEF UNABLE TO OBTAIN A SOCKET
AES834E SERVDEF SOCKET CONNECTION FAILED
AES835E SERVDEF SendRec FAILED
AES836E SERVDEF RecvRec FAILED
AES837E SERVDEF I/O ERROR
AES838E SERVDEF UNKNOWN ERROR: <error code>

Historical Database Management

NV4IP Monitor writes summarized SMF data to its databases as follows, where *vshmilvl* is the high-level qualifier for the VSAM databases:

vsmhilvl.SAEDVSM1	Performance (response times) data
vsmhilvl.SAEDVSM2	Workload data
*vsmhilvl.*SAEDVSM3	FTP data
*vsmhilvl.*SAEDVSM4	Telnet and API data
*vsmhilvl.*SAEDVSM5	VTAM buffer pool, CSM and traceroute data

When the database becomes too large, it may be necessary to delete old records from the database in order to control DASD usage. The Monitor may continue to run while records are deleted from its database.

Deleting Records

To delete records in the VSAM files, use the following sample JCL:

VSAM File	**Use the sample JCL:**
SAEDVSM1 and SAEDVSM2	**AESTVSMD/VSAMDEL** in SAEDJCL
SAEDVSM3, SAEDVSM4 and SAEDVSM5	**VSAMDEL3, VSAMDEL4** and **VSAMDEL5** in SAEDJCL

Reclaiming Wasted Space

Use the sample job VSAMEXAM in SAEDJCL to determine how much space is unavailable due to the database's control interval spaces. VSAMEXAM analyzes and reports on the structural integrity and/or size of the databases.

To reclaim the wasted space within the control intervals, periodically run the sample job VSAMREOG in SAEDJCL. The VSAM REORG JOB requires exclusive use of SAEDVSMn. To temporarily free up the allocation(s) from the NV4IP Monitor, use the following operator command:

```
F aestcpip, FREEVSM,n
```

Where n specifies the VSAM database. For example, 1 for SAEDVSM1, 2 for SAEDVSM2, etc.

To reallocate these VSAM datasets to the NV4IP Monitor after the reorganization is finished, use the following operator command:

```
F aestcpip, ALLOCVSM,n
```

Note: When the VSAM dataset is temporarily unallocated, you will not be able to obtain any historical data that is saved in the VSAM database.

Database Maintenance

When the size of the database becomes an issue due to resource utilization or performance, NV4IP offers three options:

1. Archive existing VSAM cluster on tape. Delete. Re-allocate to make it bigger, and re-initialize VSAM. Using this method, you start with a new empty VSAM cluster.
2. Export/Repro the old clusters to tape. Delete. Re-allocate the VSAM clusters with more space, and import/repro the old records from tape back to the new VSAM cluster.
3. Delete the records and reclaim the wasted space using VSAMDEL, VSAMDEL3, VSAMDEL4 and VSAMDEL5. These batch jobs will work with Monitor, delete records and reclaim wasted space in a single run.

NV4IP SERVER INSTALLATION

The following section will provide you with the necessary steps to complete the installation on any web server that supports the Java Runtime Environment (JRE). To allow you to view the Java functions in the minimum amount of time, we ship a version of the Apache HTTP Server that runs under Windows. It is *highly recommended*, however, that you first install NV4IP on the Apache HTTP Server. This should take about 30-60 minutes to install, then you can migrate to the web server of choice at your convenience. Please refer to Appendix A to perform the sample Windows installation for the Apache HTTP Server. Refer to Appendix B for Linux installation and Appendix C for WebSphere installation.

Product Components

The product components shipped on the CD-ROM for the browser-based version are:

- setup.exe
- apache_1.3.26-win32-x86-no_src.exe (Apache HTTP Server 1.3.26)
- jakarta-tomcat-4.0.4.exe (Apache Tomcat 4.0.4)
- mod_jk.dll (Apache/Tomcat connector)
- pja.jar (Pure Java AWT Java classes)
- pjatools.jar (Pure Java AWT Toolkit)
- Program file:
  - nvip.war - web application containing jsps, servlets, all necessary Java classes and resource bundles, and the deployment descriptor
- Program Directory
  - htdocs
    - nvip
      - chart - contains jar file for the charting applets
      - webhelp - contains web files for the online help system
      - images - graphics files(.jpg, .gif)
      - javascript - javascript files
- Linux Installation Directory
  - apache_1.3.26.tar.gz (Apache HTTP Server 1.3.26 Linux source)
  - jakarta-tomcat-4.0.4.tar.gz (Apache Tomcat 4.0.4 Linux binaries)
  - jakarta-tomcat-connectors-4.0.4.tar.gz (Apache/Tomcat connector source)
  - setup.tar

Note: If the Java Software Development Kit is not already installed on the server, it must be downloaded from: http://java.sun.com/products

Java Servlets

NV4IP web browser support consists of Java servlets, jsps, applets, javascipt, and HTML pages. In following the instructions, please remember that Java is case sensitive, and problems may arise if the indicated capitalization is not used. In order to view the function of the servlets/jsps before migrating to a different platform such as Linux or another web server such as IIS, it is recommended that the product be installed on a Windows PC using the Apache HTTP Server. Please see Appendix A for the Windows installation of an Apache HTTP Server.

Requirements

The web server must be enabled to support Java servlets and jsps. Many web servers do not natively support Java servlets/jsps and need an add-on product, known as a Servlet/JSP Container, to provide this support. For example, Apache requires a product such as Tomcat to run servlets/jsps. The add-on product will, in turn, invoke the classes from the Java Development Kit (JDK) as needed. The Servlet/JSP container must support JSP 1.1 and Servlet 2.2 specifications. In addition, you must have the appropriate Java Plugin installed on your browser in order for graphs to display and print correctly. The combination of plugin or JRE and JDK are packaged together in the Java SDK and must be at the following release level:

Java Software Development Kit	Latest version of 1.3.1 or higher

Sample Web Server Directory Structures

For your reference, a sample directory structure of Apache is found below. These may help you in assessing your web server structure

The Apache Directory Structure:

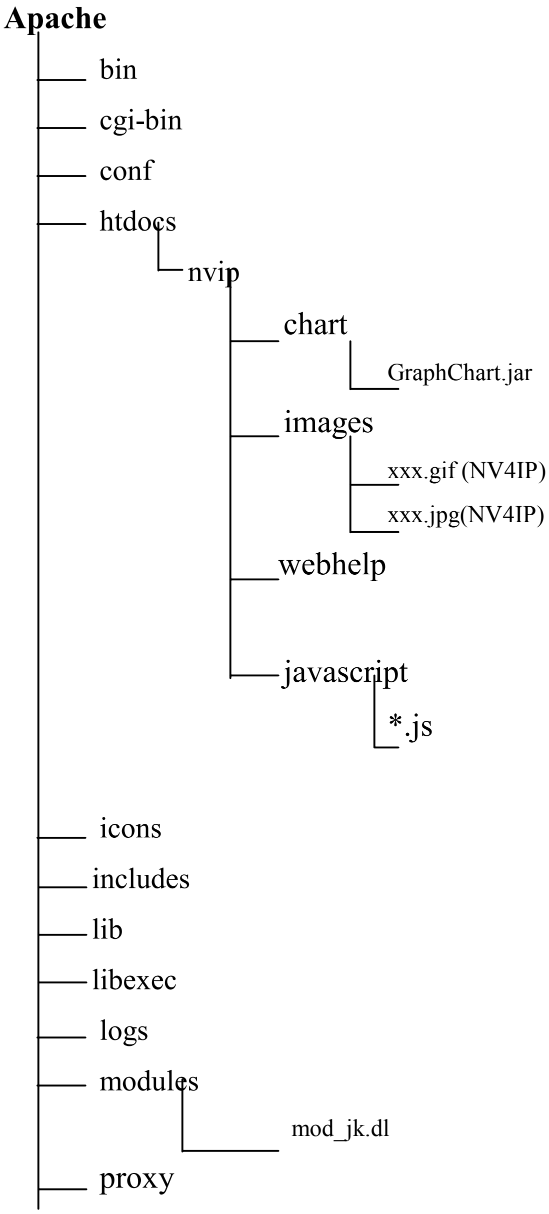


Figure 3. Apache HTTP Server

Apache Tomcat Directory Structure

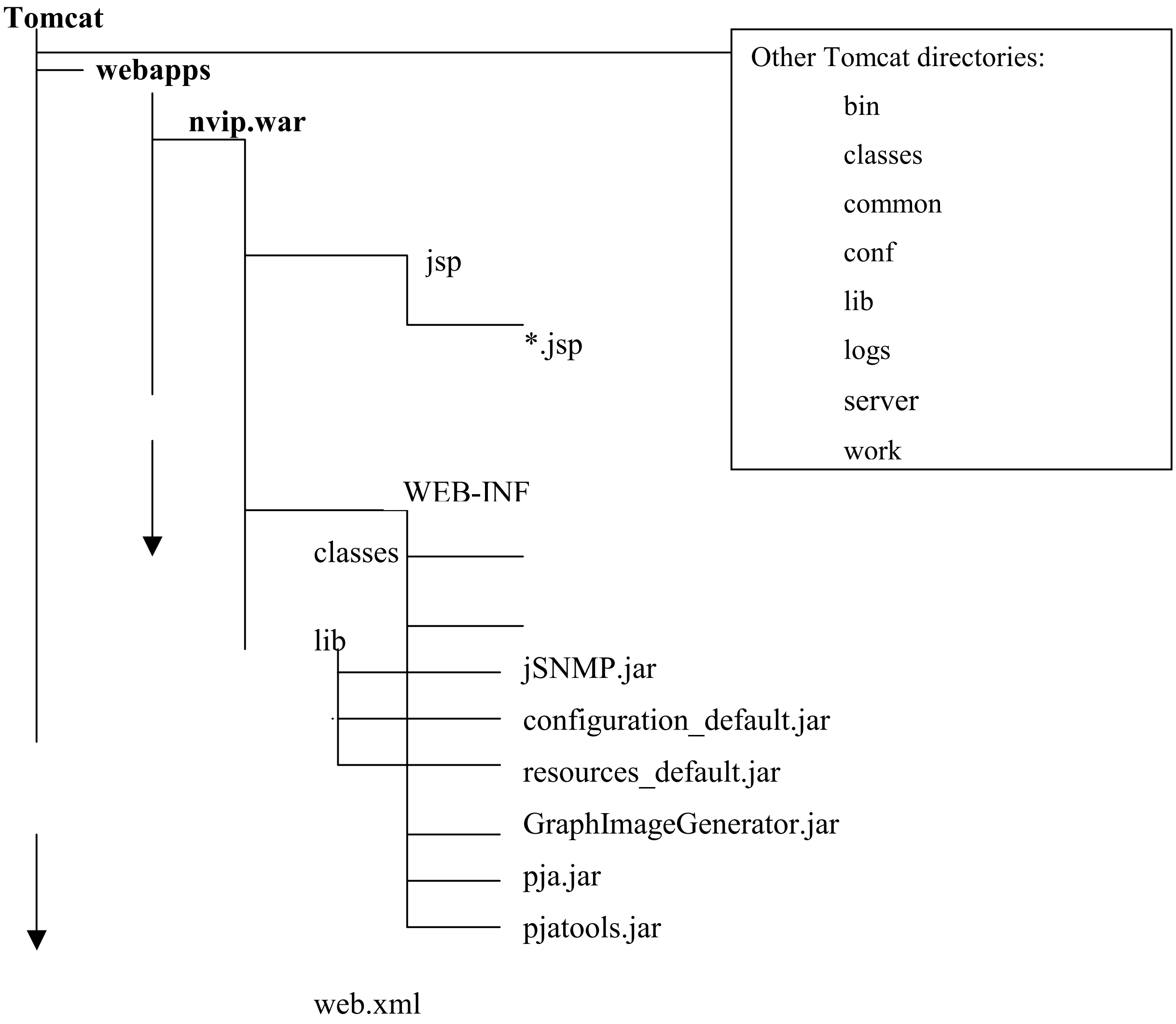


Figure 4. Apache Tomcat Structure

Installation Checklist

Item	Status	Notes
Verify that the installation is compliant with JSP 1.1 and Servlet 2.2 Specs for the Servlet/JSP container.		

Installation Steps

For NV4IP, the main static files are in the nvip subdirectory of the htdocs directory on the CD-ROM. The nvip subdirectory goes where the web server thinks the document root is located. Some web servers define a document root per application, which may be the document root for all applications or the document root for that particular application.

The following section provides instructions on installing NV4IP on any web server that supports the Java Runtime Environment (JRE). It *is* recommended that you complete the installation on the included Apache HTTP Server before migrating to another server. This section details the important steps to consider when migrating to a different web server.

Step 1. Main Static Files

For NV4IP, all static files are placed in their appropriate subdirectories in the nvip directory of the htdocs directory on the CD-ROM. This complete directory, nvip, goes where the web server thinks the document root is located.

To install: Copy the nvip subdirectory in the htdocs directory on the CDROM to the document root of the application on the selected web server.

Step 2. nvip.war

nvip.war contains the following files and directories: jSNMP.jar, servlet and java classes, jsps, necessary resource bundles, and the deployment descriptor file, web.xml. These components are required to install NV4IP on the server. If your web server supports the automatic expansion of .war files, the installation process is complete after copying the nvip.war file into the server's web application directory.

To install: Copy the nvip.war file into the web application directory of your web server. The nvip.war is placed in the webapps directory of the Apache/Tomcat installation.

The installation process is now complete.

Starting NV4IP at Your Workstation

Once the installation is complete, start NV4IP from your workstation in order to access the application. After the Monitor and Server portions of NV4IP have been installed and are operational, you may access the performance and operations functions at this time. To access the web server portion of NV4IP, complete the following steps:

1. Open the browser on your workstation. Supported browsers are Netscape and Internet Explorer.
2. In the URL address field, enter:

   ```
   http://servername/nvip/jsp/logon.jsp
   ```

   where **servername** is the name specified for installation in the Apache server conf file. The servername may be alphanumeric or the IP Address of the server.

NOTE: The server name must be the same as the one specified in the Apache server's conf file. If you are unsure of the name, check the ServerName value in \Apache Group\Apache\conf\httpd.conf.

3. The logon screen appears.
4. Enter your existing user ID and password, if running the SAF security option, or the NV4IP defaults if running the NV4IP security option.
5. Enter the IP address for the host.
6. Enter the designation for the host port. The default is 5050.
7. Click Submit. The SysPoint Home Page appears. The navigation tabs that appear on the top of each screen vary depending upon the level of access permitted by your User ID.
8. Click Logoff before you close the Browser window. This will ensure that session related data be cleaned up on the host.

NOTE: If you are using a proxy server, you need to configure it so that NV4IP's page requests will bypass the proxy server. Alternatively, you may configure your Browser to bypass the proxy server if the URL contains NV4IP's page requests. For example, for Internet Explorer, select Tools -> Internet Options -> Connection -> LAN settings -> Proxy Server Advanced -> Exception list, then specify the servername in the Exception list.

MESSAGES AND CODES

This section contains error messages and codes that you may encounter in the process of installing and using NV4IP. It includes informational, error and warning messages for the NV4IP Host.

NV4IP Host Error Messages

NV4IP Host messages have the following format:

AES*nnn*I	Informational Messages
AES*nnn*E	Error Messages
AES*nnn*W	Warning Messages

AES100I	NV4IP STARTED	NV4IP is started. This message is written to the operator console. It may be used by automation tool
AES101I	NV4IP started: **mm/dd/yyyy hh**:**mm**:**ss**	NV4IP is started on mm/dd/yyyy, at hh:mm:ss.
AES102I	NV4IP is terminating…	NV4IP is going through termination process.
AES103I	NV4IP Terminated.	NV4IP is terminated.
AES105E	Load library is not APF authorized.	The load library SAEDLINK is not APF authorized. NV4IP will terminate.
AES106I	SMF Exit Controller initialized, # of dynamic buffers=**n**	NV4IP's SMF exit controller routine has been initialized. The number of dynamic buffers (as specified in the SMFXN statement in the CONFxx member) is n.
AES107E	SMF Exit Controller initialization failed, RC from IEANTCR=**rc**	NV4IP's SMF exit controller routine was not initialized. The return code from IEANTCR is rc.
AES108I	FTP Exit Controller initialized, # of dynamic buffers=**n**	NV4IP's FTP exit controller routine has been initialized. The number of dynamic buffers (as specified in the FTPXN statement in the CONFxx member) is n.
AES109E	FTP Exit Controller initialization failed, RC from IEANTCR=**rc**	NV4IP's FTP exit controller routine was not initialized. The return code from IEANTCR is rc.
AES110I	IBM Tivoli NetView ® for TCP/IP Performance V1.5 initializing on port # **n**	NV4IP is starting up and is listening on port number n.
AES111I	SMF Record ID = n	NV4IP's SMF record ID is n (default = 251).

AES112E	SMF SYSTEM ID NOT SPECIFIED SMF system ID is not specified on the SMFSYSID parameter in the main started task's PROC. NV4IP will not perform SMF recording of performance or workload activities.
AES113I	SMF System ID = sysid NV4IP will write out SMF records with system ID = sysid.
AES114I	Performance Test Time-out = **n** seconds The time-out value (as specified by the TIMEOUT parameter in the CONFxx member) is n seconds.
AES116E	Calloc for telnet session data failed Internal Error: there is not enough storage for keeping telnet session data.
AES117I	HOMEIP set to ipaddr in AESTHOIP The IP address of the host TCP/IP being monitored is ipaddr. This value is also saved in the member HOMEIP of SAEDCONF for later reference. This message is displayed only when NV4IP is started the very first time.
AES118I	HOMEIP obtained from AESTHOIP: ipaddr (ipaddr_hex) The IP address of the host TCP/IP being monitored is ipaddr; its hex value is ipaddr_hex. This value is obtained from the member HOMEIP of SAEDCONF.
AES119I	Command logging activated "COMMANDLOG=YES" is specified in the CONFxx member. TCP/IP and VTAM command issued by users will be logged in the SYSPRINT DD.
AES120I	VTAM Buffer Monitoring Interval = **n** seconds VTAM buffer monitoring is activated with a sampling interval of n seconds.
AES121I	CSM Monitoring Interval = **n** seconds CSM monitoring is activated with a sampling interval of n seconds.
AES122I	CSM Monitoring Alert: ECSA=e, DSP=d, %Free=f, Start Hour=start_hour, End Hour=end_hour CSM monitoring for exceptions is activated. The ECSA threshold is e; Data Space threshold is d; % free threshold is f. CSM exception monitoring is active between the hours start_hour and end_hour.
AES123E	Maximum number of APPLMON's (n) reached, statement ignored. Maximum of APPLMON statements n has been specified in the CONFxx member. Any subsequent APPLMON statement(s) will be ignored.
AES124E	***ERROR*** APPLMON: 'C' or 'S' missing after 'APPLMON' APPLMON syntax error.
AES125E	***ERROR*** APPLMON: application group name missing Application group name is missing in the APPLMON statement.
AES126I	***WARNING*** APPLMON: Interval (I) set to 30 The interval value is not specified in the APPLMON statement; it is set to 30 seconds.
AES127E	***ERROR*** APPLMON: Ports (P) are not specified Port or ports are not specified in the APPLMON statement.
AES128I	Extended MCS console activated. NV4IP's extended MCS console is activated.

AES129E	Extended MCS console not activated: RC=rc, Reason=rn. NV4IP's extended MCS console is not activated, return code from MCSOPER is rc, reason code is rn.
AES130I	Network statistics interval = n seconds. The Network Statistics Collector's sampling interval (as specified by the NINT parameter in the main started task's PROC) is n seconds.
AES131I	*WARNING* NETSPROC is not specified in the PROC, no network statistics will be collected. The "NETSPROC" parameter is not specified in the main started task's PROC. No network statistics (workload) data will be collected.
AES132I	*WARNING* Network Statistics Collector disabled. The "NETSPROC" parameter is not specified in the main started task's PROC. No network statistics data will be collected.
AES133I	Network Statistics Collector started. The Network Statistics Collector has been started by NV4IP.
AES134E	Network Statistics Collector (procname) could not be started. The Network Statistics Collector (PROC name=procname) could not be started by NV4IP.
AES135I	*WARNING* CMDPROC is not specified in the PROC, TCP/IP command processing will not be available.
AES136I	*WARNING* TCP/IP Command Processor disabled. The CMDPROC parameter is not specified in the main started task's PROC. TCP/IP command processing is not supported.
AES137I	NV4IP Remote Command Processor (procname) started. NV4IP's Remote (TCP/IP) Command Processor (PROC name=procname) is started.
AES138E	TCP/IP Remote Command Processor (procname) could not be started. NV4IP's Remote (TCP/IP) Command Processor could not be started by the main started task.
AES139I	AUTOMON started for n critical resources. AUTOMON has activated n critical resources for Performance and Availability monitoring.
AES140I	VTAM Buffer Pool Monitoring started, interval = n. VTAM buffer pool monitoring is activated with a sampling interval of n seconds.
AES141I	CSM Monitoring started, interval = n. CSM monitoring is activated with a sampling interval of n seconds.
AES142I	Nets_proc and Cmd_proc will be recycled every 24 hours.
AES143I	Nets_proc and Cmd_proc will be recycled every n minutes.
AES144E	ATTACH to AEST002 failed. Internal Error: An ATTACH of a subtask (AEST002) failed.
AES145E	Command Processor not active, APPLMON task terminated. The Remote Command Processor is not active, no APPLMON monitoring is allowed.
AES146I	APPLMON for appl_group (server ports) started, interval=n seconds. APPLMON is activated to monitor the application group appl_group on its server port(s), with a sampling interval of n seconds.

AES147I	APPLMON for appl_group (client ports) started, interval=n seconds. APPLMON is activated to monitor the application group appl_group on its client port(s), with a sampling interval of n seconds.
AES148E	AESFTPLG OPEN failed, FTP Server logging suppressed. The file allocated to the AESFTPLG DD in the main started task could not be opened. FTP Server logging events will not be written.
AES149I	STOP command entered: mm/dd/yyyy hh:mm:ss. The STOP command has been entered.
AES150I	NV4IP Monitor initialized on Host: host_name, Port # n. NV4IP has been initialized on the IP host host_name and is listening on port number n.
AES151E	Bind() failed in AEST001: socket_error_message. Socket Error: bind() failed.
AES152E	Getsockname() failed in AEST001: socket_error_message. Socket Error: getsockname() failed.
AES153E	Gethostname() failed in AEST001: socket_error_message. Socket Error: gethostname() failed.
AES154E	Gethostid() failed in AEST001: socket_error_message. Socket Error: gethostid() failed.
AES155E	Listen() failed in AEST001: socket_error_message. Socket Error: listen() failed.
AES156E	Accept() failed in AEST001: socket_error_message. Socket Error: accept() failed.
AES157E	Givesocket() failed in AEST001: socket_error_message. Socket Error: givesocket() failed.
AES158E	Socket() failed in AEST001: socket_error_message. Socket Error: socket() failed.
AES159E	Getclientid() failed in AEST001: socket_error_message. Socket Error: getclientid() failed.
AES160E	***ERROR*** File AESTPARM OPEN failed, CONFxx options will not be processed Please check the specification for the AESTPARM dataset in the AESTCPIP Proc.
AES161E	CSMALERT: Invalid %Free parameter specified: p, set to 0. The %Free threshold value p for CSMALERT is invalid. It is set to 0.
AES162E	CSMALERT: Invalid Start/End Hours specified: start_hour:end_hour, set to 0:23. The Start Hour (start_hour) and/or End Hour (end_hour) specified on CSMALERT is invalid. The hour range is to be set from hour 0 to hour 23.
AES163E	CSM Monitoring Error: <error text> CSM Monitoring has encountered error from the VTAM command processor. The error is described in the <error text>: AESVTCMD APPL is not active OPEN ACB failed in AESVTCMD SENDCMD failed in AESVTCMD RCVCMD failed in AESVTCMD CLOSE ACB failed in AESVTCMD

AES164E

VTAM Buffer Pool Monitoring Error: <error text>

VTAM Buffer Pool Monitoring has encountered error from the VTAM command processor. The error is described in the <error text>:

AESVTCMD APPL is not active
OPEN ACB failed in AESVTCMD
SENDCMD failed in AESVTCMD
RCVCMD failed in AESVTCMD
CLOSE ACB failed in AESVTCMD

AES165E

calloc for DevLink data failed

There is not enough memory for DevLink data to be collected.

AES166I

DEVLINK Monitoring started, interval = <*i*>

Monitoring for channel-attached devices has started. The monitoring interval is *i* seconds.

AES167W

DEVLINKMON interval is less than 60, reset to 60

The interval specified is less than 60 seconds. It is set to be 60.

AES168E

calloc for TCP PortMon data failed

There is not enough memory for TCP Port monitoring.

AES169E

Maximum number of TCPPORTMON statements (128) reached.

More than 128 TCPPORTMON statements are specified. They will be ignored by NV4IP.

AES170W

TCPPORTMONINTERVAL is less than 60, reset to 60 seconds.

A value less than 60 is specified. It is set to be 60 seconds.

AES171I

TCP Port Monitoring started, interval = *i*

TCP Port Monitoring has started with a monitoring interval of *i* seconds.

AES172E

socket() failed, TCP Port Monitoring disabled.

TCP Port Monitoring could not obtain a socket. This function is disabled.

AES173E

ERROR File SYSTCPD OPEN failed. Please check your TCPDLIB specification in the PROC.

The data set specified in the TCPDLIB parameters is invalid.

AES174E

ERROR Invalid CONFxx Statement:

> <text>

The specified statement in CONFxx is invalid.

SMF Exit Logging Messages

For FTP Server *login failure* record, the following message is displayed:

AES804W	FTP Server Logon Failure,IP=<ip>,PORT=<localport>/<remoteport>,User=<usr>,Time=hh:mm:ss

For other types of FTP Server record, the following messages are displayed:

AES801I	FTPS:<cmd>,IP=<ip>,PORT=<localport>/<remoteport>,RC=<rc>,User=<usr>, Format=<type>/<mode>/<fmt>,ABND=<abndinfo>
AES802I	Start=<starttime>,End=<endtime>,Bytes=<bytes>,Elapsed=<etime>sec, Throughput=<tp>KB/sec
AES803I	DSN1=<dsn1>/<mem1>,DSN2=<dsn2>/<mem2>

For FTP Client record, the following messages are displayed:

AES805I	FTPC:<subcmd>,IP=<ipaddr>,PORT=<portnum>,RC=<reply code>, User=<userid>,RemoteUser=<remote user>,Host=<host name>, Format=[pds]/[mode]/[datafmt]
AES806I	Start=<hh:mm:ss.hsec>,End=<hh:mm:ss.hsec>,Bytes=<byte count>, Elapsed=<elapsed time>,Throughput=<tput>KB/sec
AES807I	DSN=<dsn>

Where the following field values are defined as:

<subcmd>	FTP command
<ipaddr>	Remote FTP Server IP address
<portnum>	Remote port: Port number for the remote FTP Server Local port: Port number of the local FTP client
<reply code>	Last reply sent to this FTP server. The normal return code is 250.
<userid>	Local user id
<remote user>	Remote User Id
<host name>	Local host name.
<pds>/<mode>/<datfmt>	pds: blank for sequential dataset, p for a partitioned dataset mode: S-stream, B-block, C-compressed fmt: A-ASCII, E-EBCDIC
<hh:mm:ss.hsec>	Beginning time and End time of transmission: hh:mm:ss.hsec
<byte count>	Number of bytes transferred

<elapsed time>	Total time of transmission (seconds) for the file transfer
<tput>	Throughput (Kbytes per second)
<dsn>	Dataset name of the file being transferred

For API INIT record, the following message is displayed:

AES820I API:INIT,IP=<ip>,PORT=<localport>/<remoteport>,Job=<job>,ID=<id>, Time=hh:mm:ss

For API TERM record, the following message is displayed:

AES821I API:TERM,IP=<ip>, Job=<job>,ID=<id>,Bin=<bin>,Bout=<bout>, Time=hh:mm:ss

WHERE THE FOLLOWING FIELD VALUES ARE DEFINED AS:

<**BIN**>	Bytes in. This is valid only for termination.
<bout>	Bytes out. This is valid only for termination.
<fmt>	Data format: A-ASCII, E-EBCDIC
<id>	Job ID
<ip>	Remote IP address
<job>	Job name
<localport>	Local port number
<remoteport>	Remote port number

For Telnet Server INIT record, the following message is displayed:

AES810I TELS:LOGN,,IP=<ip>,PORT=<localportstep 7/<remoteport>,LU=<lu>,APPL=<appl>, Dev=<device>,Time=hh:mm:ss

For Telnet Server TERM record, the following message is displayed:

AES811I TELS:LOGF,IP=<ip>,PORT=<localport>/<remoteport>,LU=<lu>,APPL=<appl>, Dev=<device>

AES812I Elapsed=<etime>,Time=hh:mm:ss

For Telnet Client record, the following message is displayed:

AES813I TELC:<subcmd>,IP=<ip>,PORT=<localport>/<remoteport>,STC=<stc>,NJE=<nje>, Time=hh:mm:ss

Where the following field values are defined as:

<APPL>	Application name
<device>	Internal logical device address (same for LOGN or LOGF records)
<etime>	Elapsed session time in hh:mm:ss
<ip>	Remote IP address
<localport>	Local port number
<nje>	NJE node name
<remoteport>	Remote port number
<stc>	Started task qualifier name
<subcmd>	LGON for logon or LGOF for logoff

FTP Exits Logging Messages

AES824I **FTP OPEN CONNECTION,IP=xxx.xxx.xxx.xxx,PORT=nnnnn,TIME=hh:mm:ss.th**

Indicates that an FTP client is making a connection to the FTP server, where xxx… is the IP address of FTP client; nnnnn is the foreign port number.

AES825I **FTP LOGIN,USER=uuuuuuuu,TIME=hh:mm:ss.th**

Indicates that an FTP client is logging on to the FTP server, where uuuuuuu is the user ID.

AES826I **FTP CMD=cccccccc,USER=uuuuuuuu,TIME=hh:mm:ss.th,ARG=xxxxxx…**

Indicates a command entered by an FTP client, where ccccccc is the FTP command; uuuuuuu is the user ID, xxxxxxx is the command argument.

AES827I **FTP POST,CMD=cccccccc,USER=uuuuuuuu,IP=xxx.xxx.xxx.xxx,TYPE=dddd/ffff,RC=mmm,REASON=nn,TIME=hh:mm:ss.th,ARG=xxxxxx…**

Indicates an FTP command completion, where ccccccc is the FTP command; uuuuuuu is the user ID, xxx… is the client's IP address, ddd is the directory type, ffff is the file type, mmm is the FTP reply code, nn is the FTP close reason code.

FTP close reason code:

0 – Transfer completed normally.

4 – Transfer completed with errors; see FTP reply code and reply text string.

8 – Transfer completed with socket communication errors; transfer is ended and no response can be sent to client.

12 – Transfer aborted after data connection was established.

16 – Transfer aborted with SQL file errors after data connection was established.

AES828W	**FTP REPLY**=<reply text string> Displays the FTP reply text string when the FTP close reason code is 4.

SERVDEF Command Responses

AES830I	SERVER DEFINITIONS ADDED
AES831E	SERVDEF INVALID DSN:<dsn>
AES832E	SERVDEF DYNALLOC FAILED FOR <dsn>
AES833E	SERVDEF UNABLE TO OBTAIN A SOCKET
AES834E	SERVDEF SOCKET CONNECTION FAILED
AES835E	SERVDEF SendRec FAILED
AES836E	SERVDEF RecvRec FAILED
AES837E	SERVDEF I/O ERROR
AES838E	SERVDEF UNKNOWN ERROR: <error code>

HOSTDEF Command Responses

AES840I	HOST DEFINITIONS ADDED
AES841E	HOSTDEF INVALID DSN:<dsn>
AES842E	HOSTDEF DYNALLOC FAILED FOR <dsn>
AES843E	HOSTDEF UNABLE TO OBTAIN A SOCKET
AES844E	HOSTDEF SOCKET CONNECTION FAILED
AES845E	HOSTDEF SendRec FAILED
AES846E	HOSTDEF RecvRec FAILED
AES847E	HOSTDEF I/O ERROR
AES848E	HOSTDEF UNKNOWN ERROR: <error code>

Alert Messages

AES901W	IP=**ipaddr** PK=**pksize** RT=**rsp** TH=**th** TIME=hh:mm:ss:hsec Performance Monitoring Alert for critical resource whose IP address is **ipaddr**, packet size is **pksize**, response time is **rsp**.
AES902W	IP=**ipaddr** NOT RESPONDING TMIE=hh:mm:ss:hsec Availability Monitoring Alert for critical resource whose IP address is **ipaddr**.
AES914W	**applname hostname** HUNG IP=**ipaddr** TIME=hh:mm:ss.hsec APPLMON Alert for application hung, where ipaddr is the IP address of the client.
AES915W	**applname hostname** THROUGHPUT **tp**<**threshold** IP=**ipaddr** TIME=hh:mm:ss.hsec APPLMON Alert for application throughput exception, where applname is the application group name, tp is the measured throughput (bytes/second), ipaddr is the IP address of the client.
AES916W	**applname hostname** SIZE **ts**>**threshold** IP=**ipaddr** TIME=hh:mm:ss.hsec APPLMON Alert for application data size exception, where applname is the application group name, ts is the total number of bytes transferred, ipaddr is the IP address of the client.
AES918W	CSM USAGE **asn** ECSA=**e** DSP=**d** HOST=**hostname** TIME=hh:mm:ss CSM Usage Alert for address space asn, where e is the total KB used of ECSA buffers, d is the total KB used of Data Space buffers.
AES919W	CSM **buf** BUFFERS **f**% < **threshld**% HOST=**hostname** TIME=hh:mm:ss CSM Buffer %Free Alert for buffer pool buf, whose % free (f) buffer area is below the threshold.
AES920W	DEVICE NOT READY: NAME=**devname** STATUS=**devstatus** TIME=hh:mm:ss.hsec Channel-attached device **devname** is not READY. Its status is **devstatus**.
AES921W	LINK NOT READY: NAME=**linkname** TIME=hh:mm:ss.hsec Channel link **linkname** is not ready.
AES922W	QUESIZE=**qsize** (**threshold**) LINKNAME=**linkname** DESTADDR=**ipaddr** TIME=hh:mm:ss.hsec The queue size (**qsize**) for Channel link **linkname** has exceeded the threshold value (**threshold**). The DESTADDR for **linkname** is **ipaddr**.
AES923W	TCP PORT NOT READY: PORT=**portnum** TIME=hh:mm:ss.hsec The TCP/IP port **portnum** is not ready for connection.

SAS/C Run-Time Messages

NV4IP uses the SAS/C Run-Time Library. All SAS/C Run-Time messages have the following format:

LSCXnnn ***Message Text***

Here are some of the most common SAS/C Run-Time messages:

LSCX470 **** WARNING **** ERRNO = ESYS

```
... Vendor-specific TCP/IP error condition (IBM TCP/IP:
errno=156).
```

It indicates that NV4IP's PROC's do not have an OMVS segment defined.

LSCX483 **** WARNING **** ERRNO = ENOTCONN

If you also see the following message:

AES151E bind() failed in AEST001: Socket address is already being used

It indicates that the HOSTPORT parameter specified the AESTCPIP PROC is being used or reserved by another application. Use a different port number (e.g., 9050) and restart AESTCPIP.

LSCX716 **** WARNING **** ERRNO = ESYS

If you also see the following message:

```
Command AESCNETS was abnormally terminated with a IKJEFTSR

  Plist error (rc=20) Reason code of 0060
```

Then it indicates that the name AESCNETS was not defined as an authorized TSO command in IKJTSOxx.

(This page intentionally left blank.)

APPENDIX A – SAMPLE INSTALLATION APACHE HTTP SERVER FOR WINDOWS

The following procedure has been verified for an Apache HTTP Server with Tomcat support under Windows. Supported operating systems are: Windows NT SP 6, 2000 and XP. With the exception of Java 2 SDK, the modules required for the installation procedure (Apache and Tomcat etc.) are found on the NV4IP CD-ROM.

Migrating from an Earlier Release of NV4IP

If you are migrating from NV4IP V1.3, V1.4, first uninstall the Apache Web Server and Apache Tomcat (V1.4) or Apache JServ (V1.3). After running the uninstall program, delete the remaining folders created by the installation attempt. A clean install must be performed since a new Apache Web Server and Apache Tomcat are now used by NV4IP. To perform a clean install on a machine that has previously been a server for NV4IP, complete the following steps:

1. Using the Add/Remove Programs function in the Control Panel, REMOVE the following:
    - From V1.4 Installation
        a. Apache 1.3.22 (This version has a vulnerability in the handling of chunked transfer encoding. More information is available at http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0392)
        b. Jakarta Tomcat 3.3
        c. Any Java SDK earlier than version 1.3.1_04
        d. Any Java Plug-in that is listed
    - From V1.3 Installation
        a. JSDK 2.0
        b. JRE 1.3
        c. Apache Server 1.3.12
        d. Apache Jserv
        e. Any Java Plug-in that is listed

2. Using Windows Explorer, DELETE the following directories:
    a. Apache Group folder (V1.3, V1.4)
    b. Apache JServ folder (V1.3)
    c. JSDK 2.0 (V1.3)
    d. jdk folder (V1.4)
    e. jakarta-tomcat folder (V1.4)

Apache HTTP Server Installation for NV4IP 1.5

Complete the following steps to install the Apache HTTP Server for Windows:

1) Download and install the Java 2 SDK (Software Development Kit):

Module	**Default Install Location**
URL: *http://java.sun.com/products/archive/j2se/1.3.1_04/index.html* Module name: **j2sdk-1_3_1_04-windows-i586.exe**	C:\jdk1.3.1_04

   a. Java 2 SDK must be downloaded from the java.sun.com web site. Point your Browser to the following URL: *http://java.sun.com/products/archive/j2se/1.3.1_04/index.html*
   b. Click on *DOWNLOAD* under SDK for Windows(all languages).
   c. Download and save the program file: j2sdk-1_3_1_04-windows-i586.exe.
   d. Double click on the program file to start the installation process.
   e. Select Program Files to install when prompted by the installation program:
   f. Record the directory where Java 2 SDK was installed: ________________________________

2) Install the Apache HTTP Server:

Module Name	**Default Install Location**
apache_1.3.26-win32-x86-no_src.exe	C:\Program Files\Apache Group\Group

   a) Find the module apache_1.3.26-win32-x86-no_src.exe on the CD-ROM provided. Double click on it to start the installation process.
   b) If your server has a valid DNS name, enter your server's DNS name as the Network Domain and Server Name. Otherwise, enter your server's IP address as the Network Domain and Server Name.
   c) If you have a Windows NT, 2000, or XP operating system and would like to install Apache as a service, select "Run as a service for all users".
   d) Select Complete when prompted for the type of installation.
   e) Record the directory where Apache Web Server was installed.
   f) Reboot the server.

3) Install Apache Tomcat 4.0

Module Name	Default Install Location
jakarta-tomcat-4.0.4.exe	C:\Program Files\Apache Tomcat 4.0\

   a) Shutdown any running Apache Tomcat servers on your system.

   b) Find the module jakarta-tomcat-4.0.4.exe on the CD-ROM provided. Double click on it to start the installation process.

   c) If you have an NT, 2000, or XP operating system and would like to run Tomcat as a service, check the "NT Service" installation option. Otherwise, take the default and select Next and Install.

   d) Record the directory where Apache Tomcat was installed.

4) Click and start **setup.exe** from the NV4IP CD-ROM. Setup will:

   a) Prompt you for the installed locations of the following components:
   Java 2 SDK, Apache HTTP Server, and Apache Tomcat.

      i) Install NV4IP.

5) If you have installed Apache Tomcat as a service, you must also set JVM parameters in the registry. From the Start Menu, select Run, and enter *regedit /S "[Path]\bin\tomcat.reg"*, where [Path] is the directory from 3d). The following name and value pairs will be added/modified to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Apache Tomcat\Parameters.**

   a) JVM Option Count = 5

   b) JVM Option Number 2 = -Xbootclasspath/a:C:\pja_2.4\lib\pja.jar

   c) JVM Option Number 3 = -Djava.awt.fonts=%windir%\Fonts

   d) JVM Option Number 4 = -Duser.home=%JAVA_HOME%\jre

6) After a successful installation, start Apache Tomcat and then the Apache HTTP Server. Some operating systems (Windows NT, Windows 2000 and Windows XP) start Apache as a service upon installation. Therefore you would need to restart your

Apache HTTP Server before the changes applied by setup.exe will take place. Refer to *Starting NV4IP Browser-based Version* for further information.

Note: The Windows NT, Windows 2000 and Windows XP operating systems automatically start Apache and Tomcat as a Service if they exist on your system (from installation). Therefore, before starting Apache and Tomcat by issuing a Start command, verify that they have not already been started by the operating system's Task Manager.

Troubleshooting the Installation

Successfully executing **setup.exe** completes the installation. If **setup.exe** fails to execute properly or the server fails to work properly after installation is complete, perform the following steps to shut down Apache:

1. Shut down the Apache HTTP Server (apache –k shutdown), if needed.
2. Uninstall the Apache HTTP Server using the uninstall program.
3. Remember to delete **all** remaining folders created by the installation attempt after completing the uninstall program. For example:

   ```
   \jdk1.3.1_04\
   \Program Files\Apache Group\Group
   \Program Files\Apache Tomcat 4.0\
   ```

4. Begin again from the first step in the preceding installation procedure. Skipping a step or attempting to shortcut the clean install process may result in unpredictable server failures.

Starting NV4IP Browser-based Version

After NV4IP has been successfully installed, complete the following steps to start the application and begin monitoring your network's performance:

1) Start Apache Tomcat.
2) Start Apache HTTP Server.

Starting Apache Tomcat

After successfully installing the web server software and NV4IP, start Apache Tomcat as follows:

1. Open an MS-DOS Prompt window and go to the Apache Tomcat subdirectory ***bin***. For example, enter:

   ```
   cd "c:\program files\Apache Tomcat 4.0\bin\"
   ```

   If the operating system does not support long file names, enter the following:

   ```
   cd "c:\progra~1\jakart~1.4\bin\"
   ```

2. At the command prompt line, type:

   ```
   startup
   ```

3. If Apache Tomcat does not start, please reboot the computer and try again. If Apache Tomcat still does not start, please refer to the *Troubleshooting the Installation* section.

4. Upon successful command completion, minimize the DOS Apache window.

5. To shutdown Apache Tomcat, open a second MS-DOS prompt window, go to the Apache Tomcat subdirectory ***bin*** and enter:

   ```
   Shutdown
   ```

Starting the Apache HTTP Server

After Apache Tomcat is started, start the Apache HTTP Sever by completing the following steps:

1. Open an MS-DOS window and go to the Apache subdirectory. For example, enter:

```
cd "c:\program files\apache group\apache"
```

If the server does not support long file names, enter the following:

```
cd "c:\progra~1\apache~1\apache"
```

2. At the command prompt line, type:

```
Apache
```

3. If Apache HTTP Server does not start, please reboot the computer and try again. If Apache HTTP Server still does not start, please refer to the *Troubleshooting the Installation* section.

4. Upon successful command completion, minimize the DOS Apache window.

5. To shutdown the Apache HTTP Server, open an MS-DOS prompt window, go to Apache subdirectory and enter:

```
apache –k shutdown
```

Installation Verification Checklist

Item	**Status**	**Notes**
To test web server installation, enter at browser address window - **http://*servername*** where the servername is the name specified during the Apache installation. The test page for Apache Installation should appear.		
To test the Tomcat installation, enter at browser address window: **http://*servername:8080*/** The test page for Tomcat Installation should appear.		

If any of these steps resulted in an error message, please refer to the troubleshooting guide for an explanation of what the problem may be and potential solutions.

Verifying Your Apache HTTP Server Installation

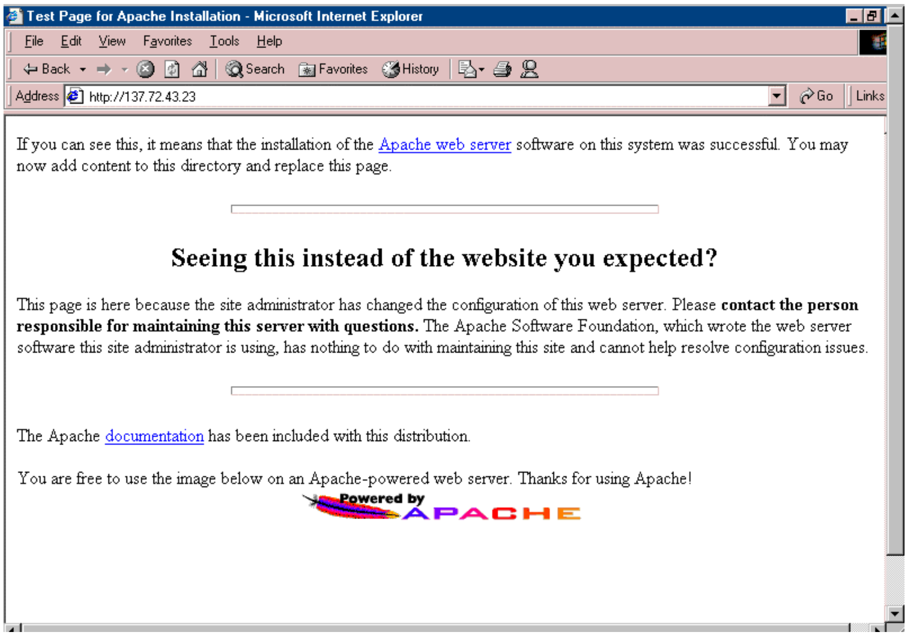
The following example shows the verification of an Apache HTTP Server installation of NV4IP, including troubleshooting guidelines. To verify the success of the NV4IP server installation, answer the following questions by completing the indicated steps:

Step 1: Is the Web Server Installed Properly?

To test whether the Apache HTTP Server is installed properly, enter at browser address window

http://*servername*

If the server has been properly installed, the following screen appears:


Test Page for Apache Installation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Links
Powered by APACHE

Address: http://137.72.43.23

If you can see this, it means that the installation of the Apache web server software on this system was successful. You may now add content to this directory and replace this page.

Seeing this instead of the website you expected?

This page is here because the site administrator has changed the configuration of this web server. Please **contact the person responsible for maintaining this server with questions.** The Apache Software Foundation, which wrote the web server software this site administrator is using, has nothing to do with maintaining this site and cannot help resolve configuration issues.

The Apache documentation has been included with this distribution.

You are free to use the image below on an Apache-powered web server. Thanks for using Apache!

If you see this page, Apache is working and you may go on to the next step.

If you do not see this page, the web server is not working and you need to determine the following:

- Is another web server using port 80? This is the well-known port for HTTP. If another web server is using port 80, you have to change the port number you are using in the *httpd.conf* file to something other than port 80.
- Review the *httpd.conf* file changes. The setup program enters the server IP address in Section 1 after Listen 3000 and in Section 2 after ServerName. Please check that these changes have been done.
- If you do not have a static IP address, verify that the IP address entered in *httpd.conf* is accurate.

If you are getting an error message when you try to start Apache, please check the Apache Website (www.apache.org) for information. The FAQ often has very good explanations.

The following is the Apache Directory Structure:

Apache

- **bin**
- **cgi-bin**
- **conf**
    - **httpd.conf**
- **htdocs**
    - **nvip**
        - **chart**
        - **webhelp**
        - **javascript**
            - ***.js**
        - **images**
            - **xxx.gif (NV4IP)**
            - **xxx.jpg(NV4IP)**
- **icons**
- **include**
- **lib**
- **libexec**
- **logs**
    - **access.log**
    - **nvip_mod_jk.log**
- **modules**
- **proxy**

Step 2: Is Servlet Support Installed Properly?

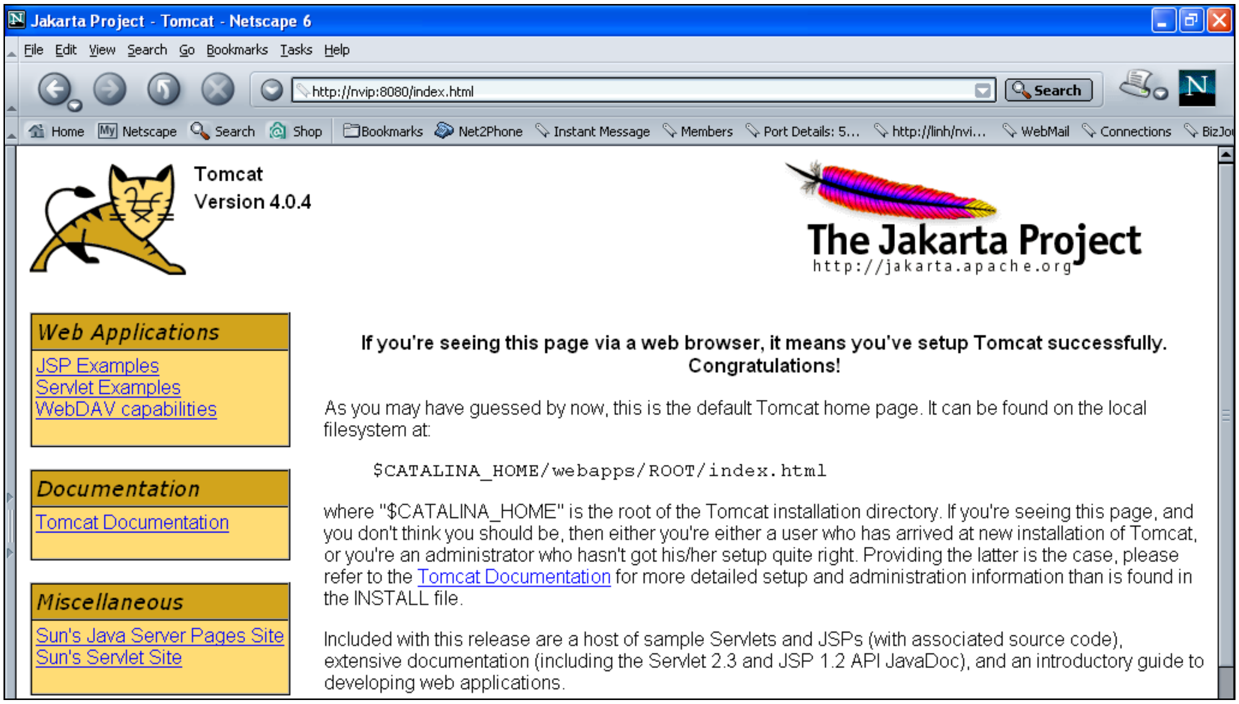
The Apache HTTP Server requires additional support to run servlets. This is provided by the Apache/Tomcat module. This module requires the Java Development Kit.

To test Apache/Tomcat, enter at browser address window:

http://servername:8080

Please remember that the address given here is *case-sensitive*.

If it is working, the following screen appears:



Tomcat
Version 4.0.4

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

```
$CATALINA_HOME/webapps/ROOT/index.html
```

where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Documentation for more detailed setup and administration information than is found in the INSTALL file.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.3 and JSP 1.2 API JavaDoc), and an introductory guide to developing web applications.

If this screen appears, continue to step 3. If this screen does not appear, Apache/Tomcat is not working. Please check the following:

- Was Tomcat started before the Apache HTTP Server?
- Is Tomcat installed properly?

The following is the Apache Tomcat Directory Structure

Apache Tomcat

- **bin**
- **classes**
- **common**
- **conf**
- **lib**
- **logs**
- **server**
- **temp**
- **webapps**
  - **nvip.war**
- **work**

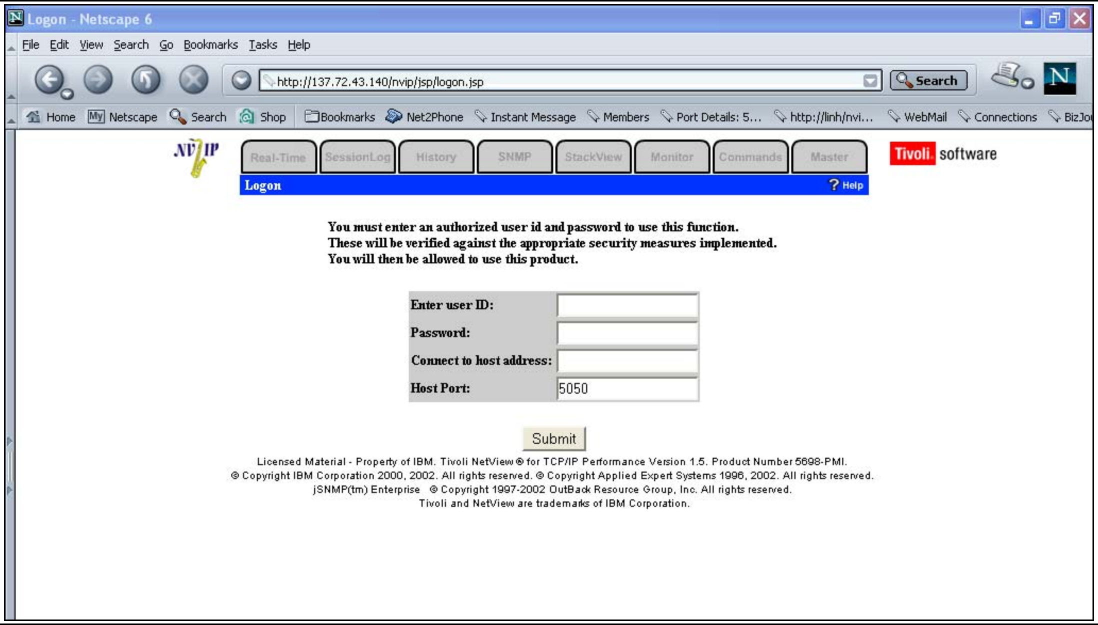
Step 3: Accessing the Program JSPs

nvip.war contains all Servlet Java classes and JSPs that are program modules in archived and compressed format. It needs to be placed in the web application directory. For Apache/Tomcat, this is the webapps subdirectory of the Apache Tomcat installation directory. If nvip.war is being accessed properly, you should be able to access the main page of the NV4IP product (logon.jsp). To test this, enter at browser address window:

http://*servername/nvip/jsp/logon.jsp*

Where servername must match the Server Name that you specified when you installed the Apache HTTP Server. Refer to the Apache HTTP Server Installation at the beginning of this appendix for further information. Remember that the address given here is *case-sensitive*.

If the JSP files of the web application are working properly , the logon screen appears and you may continue to step 4.



http://137.72.43.140/nvip/jsp/logon.jsp

You must enter an authorized user id and password to use this function.
These will be verified against the appropriate security measures implemented.
You will then be allowed to use this product.

Enter user ID:	
Password:	
Connect to host address:	
Host Port:	5050

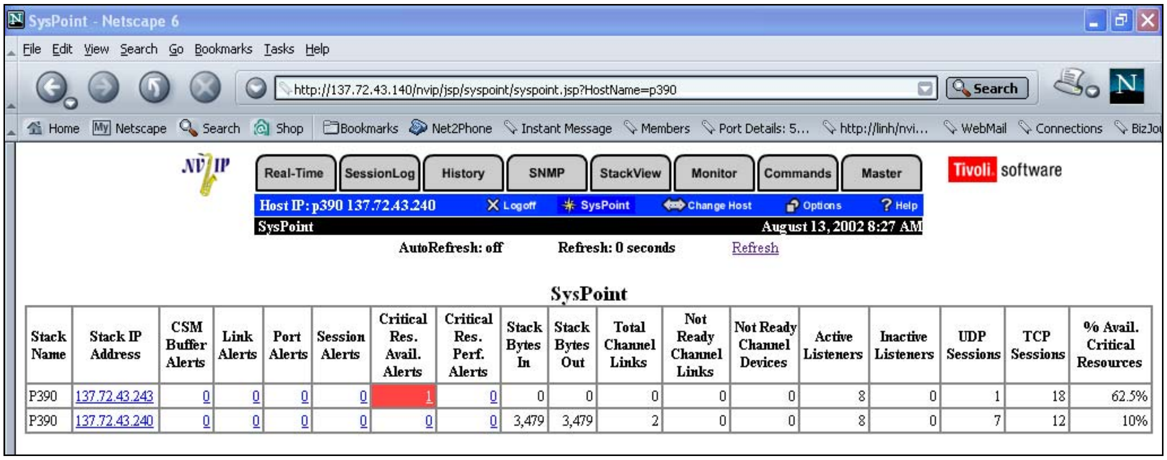
Licensed Material - Property of IBM. Tivoli NetView ® for TCP/IP Performance Version 1.5. Product Number 5698-PMI.
© Copyright IBM Corporation 2000, 2002. All rights reserved. © Copyright Applied Expert Systems 1996, 2002. All rights reserved.
jSNMP(tm) Enterprise © Copyright 1997-2002 OutBack Resource Group, Inc. All rights reserved.
Tivoli and NetView are trademarks of IBM Corporation.

If the logon screen does not appear, the JSP files of the web application are not working properly please do the following:

- Confirm that case sensitivity was observed.
- Verify that there is an nvip subdirectory in the web application directory of the Servlet/Jsp Container.

Step 4: Accessing the Program Servlets

If the servlets from the web application are working properly, you should be able to access the next page of the NV4IP product (SysPoint). To test this, press Submit from the main page. The following page appears:


SysPoint - Netscape 6
File Edit View Search Go Bookmarks Tasks Help
Search
Home Netscape Search Shop Bookmarks Net2Phone Instant Message Members Port Details: 5... http://linh/nvi... WebMail Connections BizJou
NV IP
Real-Time SessionLog History SNMP StackView Monitor Commands Master
Tivoli software
Logoff SysPoint Change Host Options Help

http://137.72.43.140/nvip/jsp/syspoint/syspoint.jsp?HostName=p390

Host IP: p390 137.72.43.240

SysPoint August 13, 2002 8:27 AM

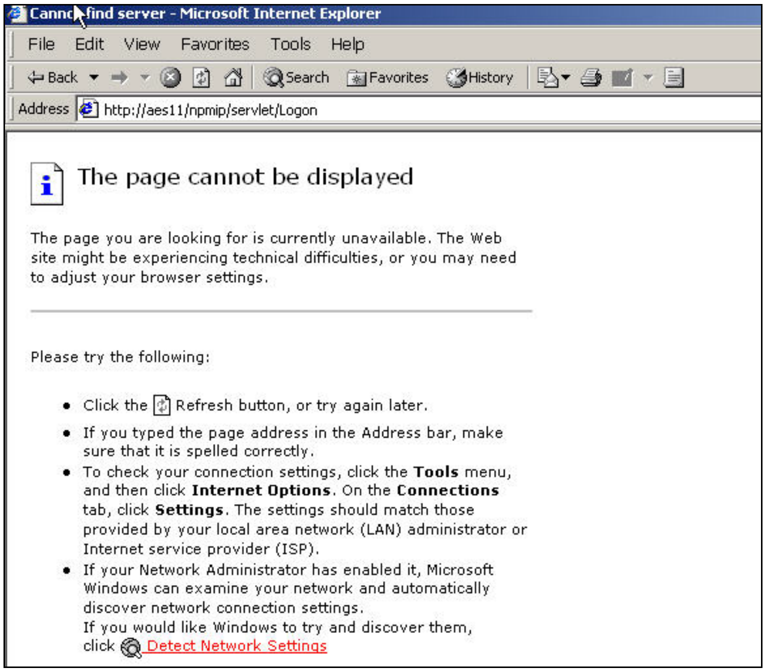
AutoRefresh: off Refresh: 0 seconds Refresh

SysPoint

Stack Name	Stack IP Address	CSM Buffer Alerts	Link Alerts	Port Alerts	Session Alerts	Critical Res. Avail. Alerts	Critical Res. Perf. Alerts	Stack Bytes In	Stack Bytes Out	Total Channel Links	Not Ready Channel Links	Not Ready Channel Devices	Active Listeners	Inactive Listeners	UDP Sessions	TCP Sessions	% Avail. Critical Resources
P390	137.72.43.243	0	0	0	0	1	0	0	0	0	0	0	8	0	1	18	62.5%
P390	137.72.43.240	0	0	0	0	0	0	3,479	3,479	2	0	0	8	0	7	12	10%

If you see this page, then servlets are working properly and you may continue to step 5. If you are not able to access the Program Servlets, your next actions depend on the screen that appears instead.

One screen that may appear is the following:


Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address

http://aes11/npmip/servlet/Logon

The page cannot be displayed

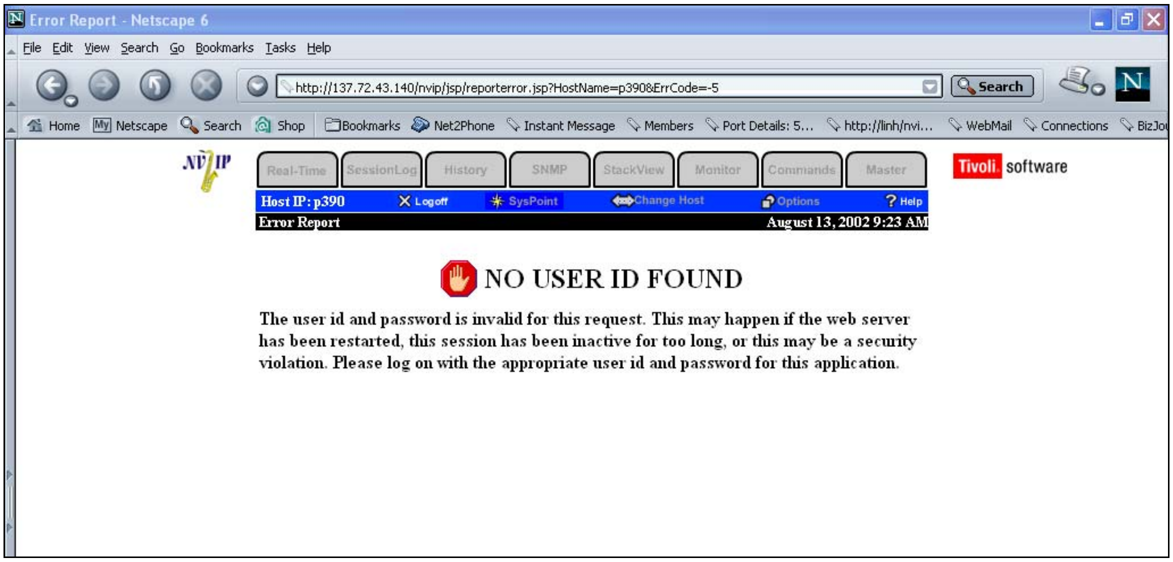
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- If your Network Administrator has enabled it, Microsoft Windows can examine your network and automatically discover network connection settings.
  If you would like Windows to try and discover them, click Detect Network Settings

Check that nvip.war is where the server expects war files to be located. In the case of Apache, this is in the Apache Tomcat/webapps subdirectory.

The following is another screen that may appear:



Host IP: p390

Error Report

August 13, 2002 9:23 AM

NO USER ID FOUND

The user id and password is invalid for this request. This may happen if the web server has been restarted, this session has been inactive for too long, or this may be a security violation. Please log on with the appropriate user id and password for this application.

This screen may appear if the session is dropped before the allotted idle period. There are two possible solutions to this problem, which are as follows:

1) Check the Server Name

Verify that the servername used matches the server name specified in the web server's configuration. For the Apache Web Server, the server name is set in the *httpd.conf* file under the *conf* subdirectory of *Apache* as follows:

```
ServerName=servername
```

2) Press the Help Key

Try pressing the Help key from the main screen, if you see that, then may be a DNS issue. A redirect is done to get to the home page. We have seen this problem where all pages can be accessed on the PC where the server is set up, but not on any other PC. The other PC's can access Help page. The cause was that the PC where the web server is installed was not defined in any DNS. So, no one was able to access it.

Additional Troubleshooting Steps

If you have completed the installation verification and found that you are still having difficulties, you might also check the following files:

access.log	Displays information on who has used NV4IP
nvip_mod_jk.log	Sometimes contains helpful error information

If you are still unable to determine the source of your problem, please contact customer support.

(This page intentionally left blank.)

APPENDIX B - LINUX INSTALLATION

This section is intended to serve as an aid in the installation of NV4IP 1.5 in a Red Hat 7.3 Linux machine. These steps were designed to work with Apache HTTP Server version 1.3.26, Jakarta-Tomcat 4.0.4, and mod_jk.so. For the Tomcat installation, the recommended JDK to use is Sun JDK 1.3.1_04.

The user must be logged on as root to install and run NV4IP on Linux.

Note: These installation instructions cover the installation of NV4IP on the above listed components only. Though it is possible to get NV4IP to run correctly using other versions of Apache and Tomcat, the installation for other versions are not covered in this appendix.

This appendix covers two methods to install NV4IP 1.5 on your Linux machine. You could either utilize the setup script included with NV4IP 1.5, or you may wish to install all the components manually. If you already have Apache and Jakarta Tomcat up and running correctly, then it is recommended that you manually install NV4IP. If you currently do not have either Apache or Tomcat setup, then it is recommended that you use the automatic setup script.

Automatic Installation

Step 1: Copy setup.tar

Copy the file setup.tar from the /linux directory on the NV4IP 1.5 installation CD. Extract the tar file ***tar –xvf setup.tar***. Three files should be extracted from the tar file, setup.sh, nvip_mod_jk.conf and nvip_workers.properties.

Step 2: Run setup.sh

Run the setup.sh file ***./setup.sh*** from the command line. This shell script will install Apache 1.3.26, Jakarta-Tomcat 4.0.4 and NV4IP 1.5 on your Linux system. You will be prompted to enter your local server's IP address along with the location where your JDK is installed.

By default, Apache Web Server will be installed in your /usr/local/apache directory. If you wish to change this, modify the APACHE_HOME variable in the setup.sh file.

By default Jakarta Tomcat will be installed in your /usr/local/jakarta-tomcat directory. If you wish to change this, modify the TOMCAT_HOME variable in the setup.sh file.

Step 3: Set environment variables

After the setup script completes, set the following environment variables (assuming bash shell used). **Note – These are default locations.**

```
export APACHE_HOME=/usr/local/apache

export TOMCAT_HOME=/usr/local/jakarta-tomcat

export JAVA_HOME=/usr/local/jdk1.3.1_04

export PATH=$PATH:$JAVA_HOME/bin
```

Step 4: Starting the servers

To start the NV4IP server, first start the Tomcat server and then the Apache Web Server (in that order). You must be logged on as root to start both servers.

To start your Tomcat server, cd into your TOMCAT_HOME/bin directory and run the ***startup.sh*** script. To shutdown your Tomcat server, execute the ***shutdown.sh*** script.

To start your Apache Web server, cd into your APACHE_HOME/bin directory and run the command ***apachectl start.*** To shutdown your Apache web server, execute the command ***apachectl stop.***

Manual Installation

Step 1: Copy the NV4IP files from the installation CD

Next you need to copy the NV4IP files from the installation CD onto the Linux machine. Copy the file **nvip.war** into **$TOMCAT_HOME/webapps.** Copy the directory **htdocs/nvip** into **$APACHE_HOME/htdocs.** Lastly copy the files **pja.jar** and **pjatools.jar** into the **/usr/local/pja_2.4** directory (you may need to create this directory).

Step 2: Create the nvip_mod_jk.conf file

The nvip_mod_jk.conf serves two purposes. First, it tells Apache to load the mod_jk.so module. Second, it establishes the root context mounts for Tomcat. It is recommended that you place the following file in the $TOMCAT/conf/jk directory:

```
#nvip_mod_jk.conf

LoadModule jk_module libexec/mod_jk.so


<IfModule mod_jk.c>

JkWorkersFile /usr/local/jakarta-tomcat/conf/jk/workers.properties
```

```
JkLogFile logs/jk.log
JkMount /*.jsp ajp13
JkMount /servlet/* ajp13
JkMount /examples/* ajp13
JkMount /nvip/jsp/* ajp13
JkMount /nvip/servlet/* ajp13
JkMount /nvip/graphimages/* ajp13
</IfModule>
```

Step 3: Create nvip_workers.properties file

The nvip_workers.properties file defines the characteristic of the mod_jk plugin. It is recommended that you place the following file in the $TOMCAT/conf/jk directory.

```
#nvip_workers.properties
ps=\
worker.list=ajp12, ajp13
# Defs
worker.ajp13.port=8009
worker.ajp13.host=137.72.43.33          #insert your server IP
worker.ajp13.type=ajp13
```

Step 4: Edit httpd.conf file

Append the following line at the end of the $APACHE_HOME/conf/httpd.conf file.

```
Include /usr/local/jakarta-tomcat/conf/jk/nvip_mod_jk.conf
```

This will instruct the Apache HTTP server to include the nvip_mod_jk.conf configuration file at startup time.

Step 5: Edit startup.sh file

Add the following two statements at the top of the $TOMCAT_HOME/bin/startup.sh file. (As a line each for a total of two additional lines.)

```
export JAVA_OPTS="-Xbootclasspath/a:$TOMCAT_HOME/lib/pja.jar -
Djava.awt.fonts=/usr/share/fonts/default/TrueType -
Duser.home=$JAVA_HOME/jre"
```

```
export
CLASSPATH="/usr/local/pja_2.4/pja.jar:/usr/local/pja_2.4/pjatools.jar:$CL
ASSPATH"
```

Step 6: Start Tomcat Server

Start up your Tomcat server. Allow a couple seconds for the .war file to be expanded before continuing. You must be logged on as root to start the Tomcat server.

Step 7: Start Apache Server

Start up your Apache server. You must be logged on as root to start the Apache server.

Checking Your Environment Setup

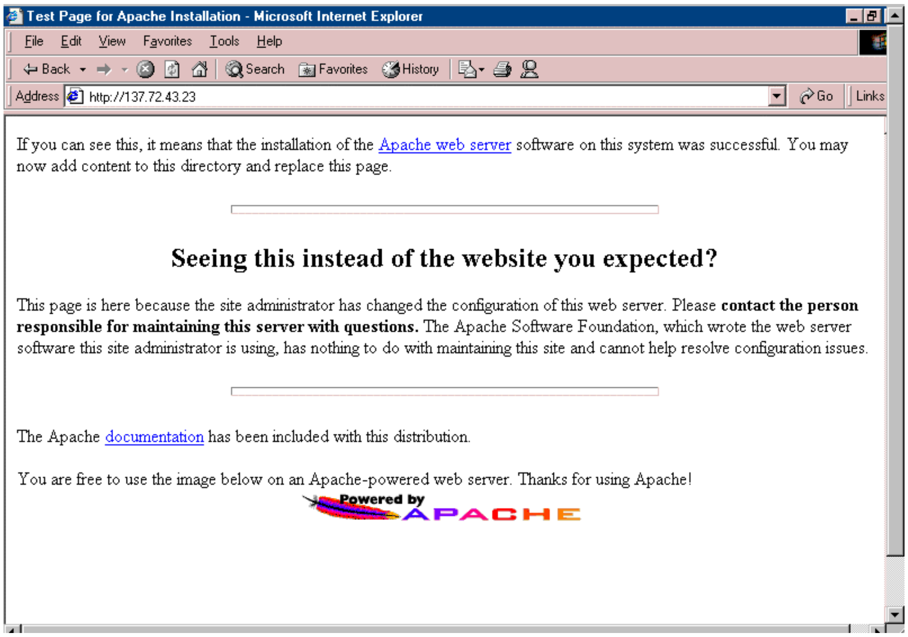
If you encounter any problems during your setup, please go through the following steps to verify that your environment is setup to support NV4IP 1.5. Your environment is set up correctly if all of the following statements are true:

Apache HTTP Server 1.3.26 is installed and running.

Verify that the Apache HTTP Server is installed correctly by entering the following address in a browser window:

http://servername

If the server has been installed correctly, the following screen appears:



If you can see this, it means that the installation of the Apache web server software on this system was successful. You may now add content to this directory and replace this page.

Seeing this instead of the website you expected?

This page is here because the site administrator has changed the configuration of this web server. Please **contact the person responsible for maintaining this server with questions.** The Apache Software Foundation, which wrote the web server software this site administrator is using, has nothing to do with maintaining this site and cannot help resolve configuration issues.

The Apache documentation has been included with this distribution.

You are free to use the image below on an Apache-powered web server. Thanks for using Apache!

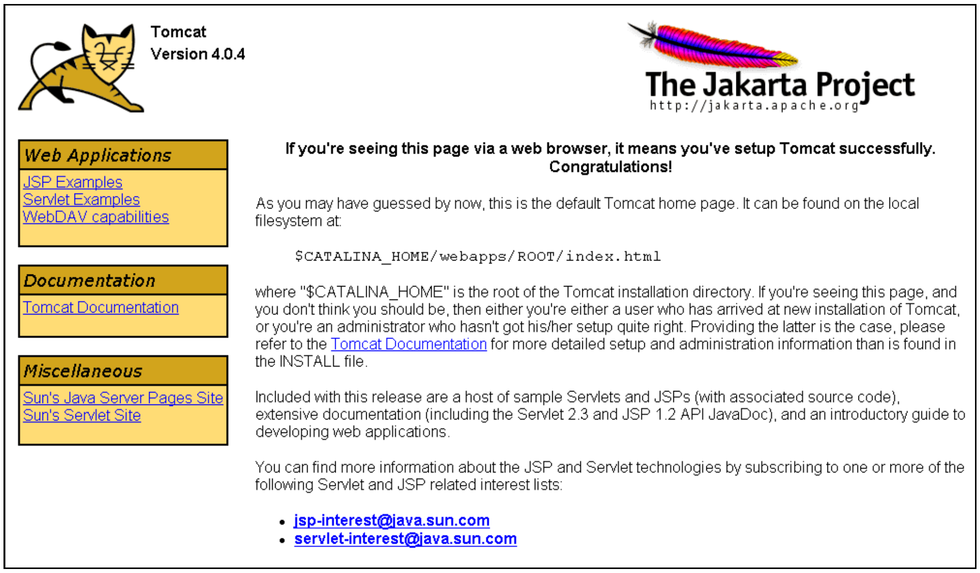
If you don't see this window, that means your Apache HTTP Server installation is faulty. Please correct the problem before moving on.

Jakarta Tomcat 4.0.4 is installed and running.

Verify that the Jakarta Tomcat is installed correctly by entering the following address in a browser window:

http://servername:8080

If the server has been installed correctly, the following screen appears:



If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

```
$CATALINA_HOME/webapps/ROOT/index.html
```

where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Documentation for more detailed setup and administration information than is found in the INSTALL file.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.3 and JSP 1.2 API JavaDoc), and an introductory guide to developing web applications.

You can find more information about the JSP and Servlet technologies by subscribing to one or more of the following Servlet and JSP related interest lists:

- **jsp-interest@java.sun.com**
- **servlet-interest@java.sun.com**

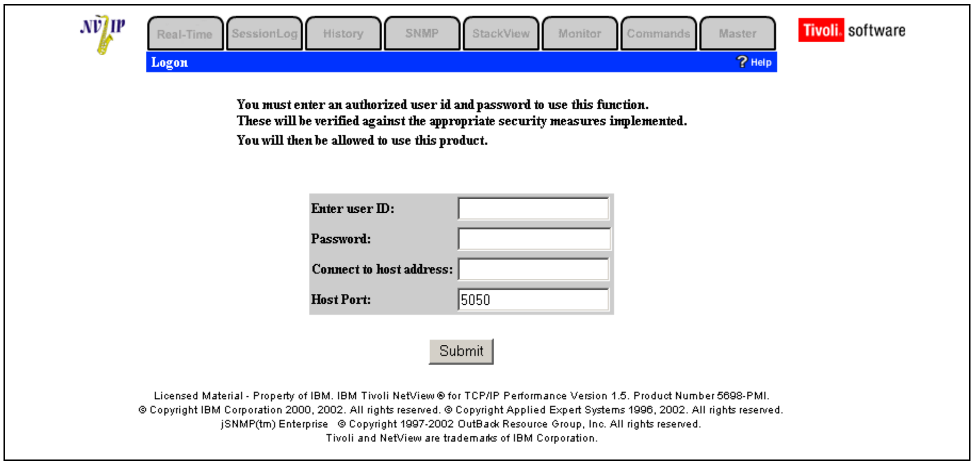
Verify that Servlet and JSP support is working by clicking on the links **JSP Examples** and **Servlet Examples** and running the sample pages listed. If any of these sample pages do not work, please check your Jakarta Tomcat installation.

If you don't see this window, that means your Jakarta Tomcat installation is faulty. Please correct the problem before moving on.

After verifying that your environment is correct. Verify that the NV4IP server is installed correctly by entering the following address in a browser window.

http://servername/nvip/jsp/logon.jsp

If the server has been installed correctly, the NV4IP logon page should appear.

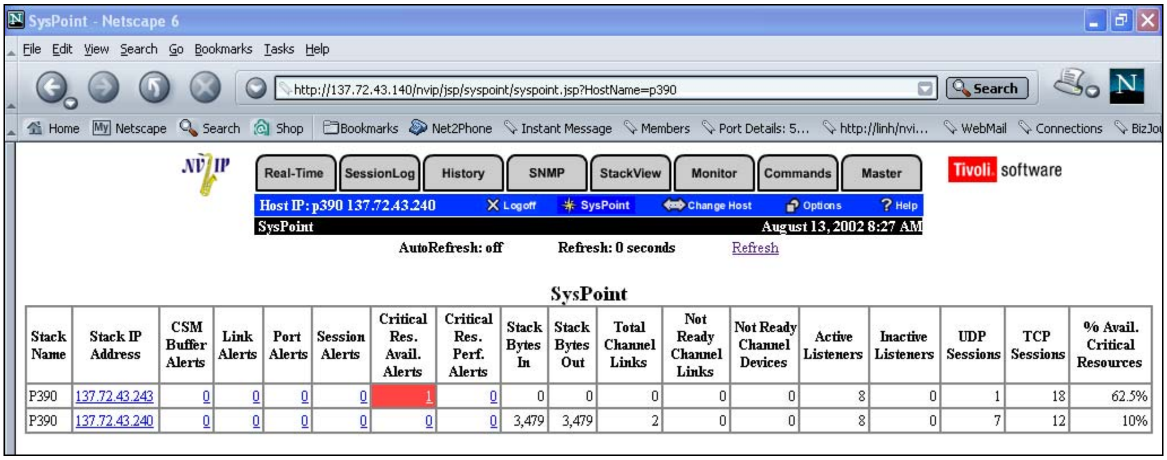


You must enter an authorized user id and password to use this function.
These will be verified against the appropriate security measures implemented.
You will then be allowed to use this product.

Enter user ID:	
Password:	
Connect to host address:	
Host Port:	5050

Licensed Material - Property of IBM. IBM Tivoli NetView® for TCP/IP Performance Version 1.5. Product Number 5698-PMI.
© Copyright IBM Corporation 2000, 2002. All rights reserved. © Copyright Applied Expert Systems 1996, 2002. All rights reserved.
jSNMP(tm) Enterprise © Copyright 1997-2002 OutBack Resource Group, Inc. All rights reserved.
Tivoli and NetView are trademarks of IBM Corporation.

After logging on, you should see the Syspoint screen:



http://137.72.43.140/nvip/jsp/syspoint/syspoint.jsp?HostName=p390

Host IP: p390 137.72.43.240

SysPoint August 13, 2002 8:27 AM

AutoRefresh: off Refresh: 0 seconds

SysPoint

Stack Name	Stack IP Address	CSM Buffer Alerts	Link Alerts	Port Alerts	Session Alerts	Critical Res. Avail. Alerts	Critical Res. Perf. Alerts	Stack Bytes In	Stack Bytes Out	Total Channel Links	Not Ready Channel Links	Not Ready Channel Devices	Active Listeners	Inactive Listeners	UDP Sessions	TCP Sessions	% Avail. Critical Resources
P390	137.72.43.243	0	0	0	0	1	0	0	0	0	0	0	8	0	1	18	62.5%
P390	137.72.43.240	0	0	0	0	0	0	3,479	3,479	2	0	0	8	0	7	12	10%

If you see this screen, that means your NV4IP installation is correct and running.

APPENDIX C – WEBSPHERE INSTALLATION

These are the steps to install NV4IP 1.5 on WebSphere 4.0.1. Where appropriate, comments are made relative to WebSphere 3.5 environment. NV4IP 1.5 is supported to run in the plugin mode.

The tasks involved in installing NV4IP 1.5 on WebSphere include the following:

1. Copy nvip.war file to host HFS file system.
2. Deploy nvip.war file using wartowebapp.sh.
3. Customization
    a. httpd.conf
    b. was.conf
    c. nvip.webapp
4. Recycle Web Server.

Copy war file to host HFS file system

NV4IP packages its Java Servlets, JSPs and other static files into a .war file named nvip.war. FTP the nvip.war file to host HFS file system in **binary**. For example, you may want to put it under /tmp directory.

Run wartowebapp.sh

WebSphere provides a tool called wartowebapp.sh to help deploy the .war file.

Wartowebapp.sh is located in the WebSphere binary directory (the default name/path is /usr/lpp/WebSphere/WebServerPlugIn/bin/wartowebapp.sh)[3]. To invoke the tool, you can simply issue wartowebapp.sh from that directory.

Follow the prompt and provide the information requested. Examples of the prompts include:

Prompts	Suggestion
TEMP_DIRECTORY	Take default
WAR_FILENAME	*e.g. /tmp/nvip.war*
VIRTUAL_HOST_NAME	Take default
WEBAPP_NAME	Take default

---

[3] For WAS 3.5, the default path may look like: /usr/lpp/WebSphere/AppServer/bin/wartowebapp.sh.

Prompts	Suggestion
WEBAPP_DESTINATION	*e.g. /usr/lpp*
WEBAPP_AUTO_RELOAD_INTERVAL	Take default
WEBAPP_PATH	*e.g. /nvip*
WAS_HOME	Take default
LOCAL_FILE_ENCODING	Take default

At the end of its execution, you should receive a "BUILD SUCCESSFUL" message. You may review the deployment result by viewing the newly created directories (as specified in WEBAPP_DESTINATION.)

Make sure to check that all newly deployed directories/files have the proper access authorization. You may want to do a chmod 755 * to all.

Customization

was.conf

The output of the wastowebapp.sh includes a file, was.conf.updates, which contains the necessary directives to deploy NV4IP as a web application. The file resides at the WEBAPP_DESTINATION specified.

The updates are to be copied to the was.conf file, which will be referenced by the Web Server Configuration file httpd.conf (described below). You may want to make a copy of the existing was.conf file before making the changes.

Append the contents of was.conf.updates to the end of your copy of was.conf.

Append the following three lines to the beginning of your copy of was.conf, replacing [WEB-APP DESTINATION] and [WEB-APP NAME] with what was entered above for wartowebapp.sh. In addition, replace [JAVA_HOME] with the same path specified for the JAVA_HOME environmental variable.

```
appserver.java.extraparm=-Xbootclasspath/a:[WEB-APP DESTINATION]/[WEB-APP NAME]/servlets/pja.jar

appserver.java.extraparm=-Djava.awt.fonts=[JAVA_HOME]/lib/fonts

appserver.java.extraparm=-Duser.home=[JAVA_HOME]
```

httpd.conf

It is assumed that IBM HTTP Web Server has been configured and is running prior to installation of NV4IP.

Add or update the following directives to the httpd.conf[4] configuration file to provide HTTP server with the entry point for Application Server's PlugIn initialization, request processing and termination.

Verify that the WebSphere Application Server configuration file (was.conf) specified on the ServerInit statement contains the directives needed for NV4IP (described in previous section).

You may want to make a copy of the existing httpd.conf file before making the updates.

ServerInit /usr/lpp/WebSphere/WebServerPlugIn/bin/was400plugin.so:init_exit /usr/lpp/WebSphere,*[was.conf configuration file]*
ServerTerm /usr/lpp/WebSphere/WebServerPlugIn/bin/was400plugin.so:term_exit[5]

Note: while the above two statements may appear to spread across multiple lines, they ought to remain as single lines in the configuration file. Check if statement was400plugin.so:init_exit has already been coded. If so, just update it.

Add a Service statement to pass all NV4IP URL requests to WebSphere Application Server.

Service /nvip/* /usr/lpp/WebSphere/WebServerPlugIn/bin/was400plugin.so:service_exit[6]

For description of these configuration directives, refer to HTTP Server Planning, Installing, and Using.

nvip.webapp

The nvip.webapp file created by the wartowebapp.sh utility resides in the servlets directory. For example, if WEBAPP_DESTINATION is /usr/lpp, then you will find it in /usr/lpp/nvip/servlets.

This file needs to be modified in order for WebSphere to serve out the NV4IP Java servlets correctly. Add the following five lines toward the beginning of the nvip.webapp generated by wartowebapp.sh utility.

```
<servlet>
  <name>InvokerServlet</name>
```

---

[4] On WAS 3.5, this file may be named as: httpd.was35.conf.

[5] Of course, on WAS 3.5, the plugin is called was350plugin.so…etc. These statements may look like:

```
ServerInit /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:init_exit /usr/lpp/W
EbSphere,[was.conf file]
ServerTerm /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:term_exit
```

[6] On WAS 3.5, you should have was350plugin.so instead.

```
  <code>com.ibm.servlet.engine.webapp.InvokerServlet</code>
  <servlet-path>/servlet/*</servlet-path>
</servlet>
```

httpd.envvars

On WAS 3.5, add the following to the CLASSPATH environmental variable setting in httpd.envvars, where [WEB-APP DESTINATION] and [WEB-APP NAME] are the same values entered for wartowebapp.sh above :

> **:[WEB-APP DESTINATION]/[WEB-APP NAME]/servlets/pja.jar:[WEB-APP DESTINATION]/[WEB-APP NAME]pjatools.jar**

Recycle Web Server

To make these changes effective, restart HTTP Web Server. After that, you may access NV4IP from the browser via:

> *http://your.server.name/nvip/jsp/logon.jsp.*

APPENDIX D – NV4IP SMF RECORDS

The default SMF record type for NV4IP is 251.

Performance SMF Record Layout

Byte	Length	Format	Description
0-17			Standard SMF header without subtypes
18-18	1	Binary	Record identifier (=X'01') **Bit** **Description** 0-2 Version compatibility flag: 000x xxxx - NV4IP V1.1 compatible 3-7 Record subtype: xxx0 0001 - Performance Record xxx0 0010 - Workload Record
19-22	4	Binary	IP address being monitored
23-24	2	Binary	Size (in bytes) of the test packet sent
25-26	2	Binary	Size (in bytes) of the test packet received
27-28	2	Binary	Round trip time (msec)

Workload SMF Record Layout

Byte	Length	Format	Description
0-17			Standard SMF header without subtypes
18-18	1	Binary	Record identifier (=X'02') **Bit** **Description** 0-2 Version compatibility flag: 000x xxxx – NV4IP V1 3-7 Record subtype: xxx0 0001 - Performance Record xxx0 0010 - Workload Record
19-26	8	EBCDIC	Application name
27-30	4	Binary	Bytes sent (delta value) by the application on the connection
31-34	4	Binary	Bytes received (delta value) by the application on the connection
35-42	8	EBCDIC	Local port (internal application name or port number)
43-46	4	Binary	IP address of the remote socket (client)
47-48	2	Binary	Port number of the remote socket (client)

APPENDIX E - SAMPLE JCL

The appendices provided here include sample JCLs and listings that you may find helpful.

AESTCPIP JCL

```
//AESTCPIP PROC DEBUG=NO,                             <=== VERIFY
//*--------------------------------------------------------------------*
//*  LIBRARY SPECIFICATION                                             *
//*--------------------------------------------------------------------*
//       AEDLINK=??????????????,                      <=== SPECIFY
//       CFGHILVL=?????????????,                      <=== SPECIFY
//       HILEVEL=??????????????,                      <=== SPECIFY
//       TCPDLIB=?????????????????????,               <=== SPECIFY
//       VSMHILVL=?????????????,                      <=== SPECIFY
//*--------------------------------------------------------------------*
//*  PARAMETER SPECIFICATION                                           *
//*--------------------------------------------------------------------*
//       AUTOMON=YES,                                 <=== VERIFY
//       CMDPROC=AESTCMDS,                            <=== VERIFY
//       HOSTPORT=5050,                               <=== VERIFY
//       NETSPROC=AESTNETS,                           <=== VERIFY
//       NINT=90,                                     <=== VERIFY
//       REFRESH=15,                                  <=== VERIFY
//       SMFRECID=251,                                <=== VERIFY
//       SMFSYSID=????,                               <=== SPECIFY
//       SOUT=*,                                      <=== VERIFY
//       R=210,                                       <=== VERIFY
//       TIMEOUT=5,                                   <=== VERIFY
//       CONF=CONF00                                  <=== VERIFY
//**********************************************************************
//*                                                                    *
//*  IBM TIVOLI NETVIEW (R) FOR TCP/IP PERFORMANCE (NV4IP)             *
//*  MAIN MONITOR                                                      *
//*                                                                    *
//*  DEBUG    - YES ³ NO                                               *
//*                                                                    *
//*             TURNS ON (OR OFF) DEBUGGING FOR NV4IP.                 *
//*                                                                    *
//*             DEFAULT IS NO.                                         *
//*                                                                    *
//*====================================================================*
//*  LIBRARY SPECIFICAITON                                             *
//*====================================================================*
//*                                                                    *
//*  AEDLINK  -                                                        *
//*             SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE TARGET       *
//*             LOAD LIBRARY SAEDLINK.                                 *
//*                                                                    *
//*             IF YOU DID NOT RENAME THE LOAD LIBRARY, THEN SPECIFY  *
//*             THE SAME VALUE AS HILEVEL.                             *
//*                                                                    *
//*  CFGHILVL -                                                        *
//*             SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE TARGET       *
//*             LIBRARY SAEDCONF FOR THIS SYSTEM.                      *
//*                                                                    *
//*             IF YOU ARE MONITORING ONLY ONE SYSTEM, THEN SPECIFY   *
//*             THE SAME VALUE AS HILEVEL.                            *
//*                                                                   *
//*  HILEVEL  -                                                       *
//*             SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE TARGET      *
//*             LIBRARIES.                                            *
//*                                                                   *
//*             FOR EXAMPLE, IF NV4IP'S CLIST LIBRARY WAS             *
//*             UNLOADED TO SYS2.PROD.AESTCP.SAEDCLIB, THEN SPECIFY   *
//*             'SYS2.PROD.AESTCP'.                                   *
//*                                                                   *
//*  TCPDLIB  -                                                       *
//*             SPECIFIES THE TCPIP DATA CONFIGURATION FILE FOR THE   *
//*             TCP/IP STACK THAT IS BEING MONITORED.                 *
//*             THIS DATA SET WILL BE ALLOCATED TO A //SYSTCPD DD.    *
//*                                                                   *
//*             IT SHOULD BE THE SAME DATA SET AS THE ONE THAT IS     *
//*             SPECIFIED IN THE //SYSTCPD DD STATEMENT IN THE TCP/IP *
//*             PROCEDURE.                                            *
//*                                                                   *
//*             *NOTE*                                                *
//*             IF YOU WISH TO SPECIFY THE HFS FILE /etc/resolv.conf  *
//*             FOR //SYSTCPD, PLEASE COMMENT OUT THIS STATEMENT AND  *
//*             SPECIFY //SYSTCPD AS FOLLOWS:                         *
//*                                                                   *
//*             //SYSTCPD DD PATH='/etc/resolv.conf',PATHOPTS=ORDONLY *
//*                                                                   *
//*  VSMHILVL -                                                       *
//*             SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE VSAM        *
//*             CLUSTERS FOR THIS SYSTEM.                             *
//*                                                                   *
//*===================================================================*
//*  PARAMETER SPECIFICATION                                          *
//*===================================================================*
//*                                                                   *
//*  AUTOMON  - YES ³ NO                                              *
//*                                                                   *
//*             SPECIFIES WHETHER TO START MONITORING THE CRITICAL    *
//*             RESOURCES THAT WERE LAST MONITORED BY NV4IP.          *
//*                                                                   *
//*             DEFAULT IS YES.                                       *
//*                                                                   *
//*  CMDPROC  -                                                       *
//*             SPECIFIES THE STARTED TASK NAME FOR THE REMOTE        *
//*             COMMAND PROCESSOR.  (THIS STARTED TASK WILL BE        *
//*             AUTOMATICALLY STARTED BY NV4IP.)                      *
//*                                                                   *
//*             DEFAULT IS AESTCMDS.                                  *
//*                                                                   *
//*  HOSTPORT - 5000 TO 65534                                         *
//*                                                                   *
//*             SPECIFIES A PORT NUMBER FOR NV4IP.                    *
//*             A PORT NUMBER UNIQUELY IDENTIFIES THIS APPLICATION TO *
//*             THE TCP/IP STACK.  PLEASE MAKE SURE THAT NO OTHER     *
//*             APPLICATION IS USING THE SAME PORT NUMBER.            *
//*                                                                   *
//*             DEFAULT IS 5050.                                      *
//*                                                                   *
//*  NINT     - NNNN                                                  *
//*                                                                   *
//*             SPECIFIES THE NETWORK WORKLOAD COLLECTOR MONITORING   *
//*            INTERVAL (IN SECONDS).                           *
//*                                                             *
//*            DEFAULT IS 90, WHICH MEANS THAT TCP/IP APPLICATION    *
//*            WORKLOAD WILL BE COLLECTED EVERY 60 SECONDS, AND     *
//*            THAT WORKLOAD RECORDS WILL BE WRITTEN TO SMF EVERY    *
//*            90 SECONDS.                                      *
//*                                                             *
//*  NETSPROC -                                                 *
//*            SPECIFIES THE STARTED TASK NAME FOR THE TCP/IP      *
//*            WORKLOAD COLLECTOR.  IF THIS IS NOT SPECIFIED, THEN   *
//*            NO TCP/IP APPLICATION WORKLOAD WILL BE COLLECTED.    *
//*            (THIS STARTED TASK WILL BE AUTOMATICALLY STARTED BY   *
//*            NV4IP.)                                          *
//*                                                             *
//*            DEFAULT IS AESTNETS.                             *
//*                                                             *
//*  REFRESH  - NN                                              *
//*                                                             *
//*            SPECIFIES HOW OFTEN (IN MINUTES) THE DATA SAMPLING    *
//*            COUNTERS ARE CLEARED.  THIS IS ALSO THE REPORTING     *
//*            INTERVAL FOR ALERTS.                             *
//*                                                             *
//*            DEFAULT IS 15.                                   *
//*                                                             *
//*  SMFRECID - 128 TO 255                                      *
//*                                                             *
//*            SPECIFIES THE SMF RECORD TYPE FOR THE SMF RECORDS     *
//*            WRITTEN BY NV4IP.                                *
//*                                                             *
//*            DEFAULT IS 251.                                  *
//*                                                             *
//*  SMFSYSID - CCCC                                            *
//*                                                             *
//*            SPECIFIES THE SYSTEM IDENTIFICATION FOR SMF RECORDS.  *
//*            THIS SHOULD BE THE SAME AS THE SID PARAMETER THAT     *
//*            IS IN SYS1.PARMLIB(SMFPRMXX).                    *
//*                                                             *
//*  SOUT     -                                                 *
//*            SPECIFIES THE SYSOUT CLASS FOR SESSION LOGS AND      *
//*            DIAGNOSTIC OUTPUT.                               *
//*                                                             *
//*            DEFAULT IS '*'.                                  *
//*                                                             *
//*  R        -                                                 *
//*            SPECIFIES THE RELEASE LEVEL OF OS/390.  E.G., SPECIFY *
//*            R=28 FOR OS/390 V2R8, R=210 FOR OS/390 V2R10,        *
//*            R=211 FOR Z/OS V1R1, R=212 FOR Z/OS V1R2, ETC.       *
//*                                                             *
//*            DEFAULT IS 210.                                  *
//*                                                             *
//*  TIMEOUT  -                                                 *
//*            SPECIFIES THE TIME OUT VALUE (IN SECONDS) FOR THE     *
//*            PERFORMANCE TEST.                                *
//*                                                             *
//*            DEFAULT IS 5, WHICH MEANS THAT IF THE TEST RESPONSE   *
//*            DID NOT COME BACK AFTER 5 SECONDS, THEN THE CRITICAL  *
//*            RESOURCE THAT IS BEING MONITORED IS CONSIDERED TO BE  *
//*            DOWN, OR THAT ITS IP ADDRESS IS NOT VALID.          *
//*                                                             *
//*  CONF     -                                                 *
//*            SPECIFIES THE MONITOR'S CONFIGURATION OPTIONS        *
//*             MEMBER IN SAEDSLIB.                                   *
//*                                                                   *
//*             DEFAULT IS CONF00.                                    *
//*                                                                   *
//*********************************************************************
//*                                                                   *
//*  *NOTE*     IF YOU ARE MONITORING MORE THAN ONE SYSTEM, YOU MUST  *
//*             USE A UNIQUE CFGHILVL AND VSMHILVL VALUES FOR EACH    *
//*             SYSTEM.                                               *
//*                                                                   *
//*  *NOTE*     NV4IP MAY GENERATE A LOT OF OUPPUT FOR FTP            *
//*             SERVER LOG AND TCP/IP SESSION LOGS.  THE LOGS ARE     *
//*             WRITTEN TO THE FOLLOWING DD NAMES:                    *
//*                                                                   *
//*               AESFTPLG - FTP SERVER LOG                           *
//*               AESSALOG - API SESSION LOG                          *
//*               AESSFLOG - FTP SESSION LOG                          *
//*               AESSLLOG - TELNET SESSION LOG                       *
//*                                                                   *
//*             YOU MAY USE THE "SEGMENT" PARAMETER TO ALLOW PART     *
//*             OF THE OUTPUT TO BE PRINTED (OR HELD IN JES2'S OUTPUT *
//*             QUEUE) WHILE NV4IP IS RUNNING.                        *
//*             DEFAULT SEGMENT IS 60.                                *
//*                                                                   *
//*********************************************************************
//*                                                                   *
//* LICENSED MATERIALS - PROPERTY OF IBM                              *
//* 5698-NTP                                                          *
//* (C) COPYRIGHT IBM CORPORATION 2000, 2002.  ALL RIGHTS RESERVED.   *
//* (C) COPYRIGHT APPLIED EXPERT SYSTEMS 1996, 2002.  ALL RIGHTS      *
//*     RESERVED.                                                     *
//*                                                                   *
//* US GOVERNMENT USERS RESTRICTED RIGHTS - USE, DUPLICATION OR       *
//* DISCLOSURE RESTRICTED BY GSA ADP SCHEDULE CONTRACT WITH IBM CORP. *
//*                                                                   *
//*********************************************************************
//AEST001 EXEC PGM=AEST001,REGION=0K,TIME=1440,
// PARM=('=P=&HOSTPORT =S=&SMFRECID =I=&SMFSYSID =T=&NINT =M=&AUTOMON
//              =O=&TIMEOUT =D=&DEBUG =R=&REFRESH =N=&NETSPROC =V=&R
//              =C=&CMDPROC')
//STEPLIB  DD DISP=SHR,
// DSN=&AEDLINK..SAEDLINK
//SYSTCPD  DD DISP=SHR,
// DSN=&TCPDLIB
//SYSOUT   DD SYSOUT=&SOUT
//SYSPRINT DD SYSOUT=&SOUT,DCB=(RECFM=FBA,LRECL=133,BLKSIZE=133)
//SYSTERM  DD SYSOUT=&SOUT
//STGRPT   DD SYSOUT=&SOUT
//AESTHOST DD DISP=SHR,
// DSN=&CFGHILVL..SAEDCONF(HOSTS)
//AESTCONF DD DISP=SHR,
// DSN=&CFGHILVL..SAEDCONF(SERVERS)
//AESTAMON DD DISP=SHR,
// DSN=&CFGHILVL..SAEDCONF(AUTOMON)
//AESTUSR1 DD DISP=SHR,
// DSN=&CFGHILVL..SAEDCONF(USER1)
//AESTUSR2 DD DISP=SHR,
// DSN=&CFGHILVL..SAEDCONF(USER2)
//AESTUSR3 DD DISP=SHR,
// DSN=&CFGHILVL..SAEDCONF(USER3)
//AESTHOIP DD DISP=SHR,
// DSN=&CFGHILVL..SAEDCONF(HOMEIP)
//AESTOPT1 DD DISP=SHR,
// DSN=&CFGHILVL..SAEDOPT1
//AESTOPT2 DD DISP=SHR,
// DSN=&CFGHILVL..SAEDOPT2
//AESTVSM0 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM0
//AESTVSM1 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM1
//AESTVSM2 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM2
//AESTVSM3 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM3
//AESTVSM4 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM4
//AESTVS4A DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM4.PATH
//AESTVSM5 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM5
//AESTCMDF DD DISP=SHR,
// DSN=&CFGHILVL..SAEDCMDS
//AESTPARM DD DISP=SHR,
// DSN=&HILEVEL..SAEDSLIB(&CONF)
//AESFTPLG DD SYSOUT=&SOUT,SEGMENT=60,
// DCB=(RECFM=FBA,LRECL=133,BLKSIZE=133)
//AESSALOG DD SYSOUT=&SOUT,SEGMENT=60,
// DCB=(RECFM=FBA,LRECL=133,BLKSIZE=133)
//AESSFLOG DD SYSOUT=&SOUT,SEGMENT=60,
// DCB=(RECFM=FBA,LRECL=133,BLKSIZE=133)
//AESSTLOG DD SYSOUT=&SOUT,SEGMENT=60,
// DCB=(RECFM=FBA,LRECL=133,BLKSIZE=133)
```

AESTNETS JCL

```
//AESTNETS PROC CTCV=,                                  <=== DO NOT SPECIFY
//       AEDLINK=????????????????,                      <=== SPECIFY
//       HILEVEL=????????????????,                      <=== SPECIFY
//       VSMHILVL=????????????????,                     <=== SPECIFY
//       DUNIT=SYSDA,                                   <=== VERIFY
//       SOUT=*,                                        <=== VERIFY
//       TCPDLIB=??????????????????,                    <=== SPECIFY
//       TCPXLBIN=?????????????????                     <=== SPECIFY
//*******************************************************************
//*                                                                 *
//*  IBM TIVOLI NETVIEW (R) FOR TCP/IP PERFORMANCE (NV4IP)          *
//*  NETWORK WORKLOAD COLLECTOR                                     *
//*                                                                 *
//*  *NOTE* THIS STARTED TASK IS STARTED BY THE MAIN MONITOR        *
//*         ADDRESS SPACE (DEFAULT NAME: AESTCPIP).  DO NOT START   *
//*         THIS ADDRESS SPACE BY ITSELF.                           *
//*                                                                 *
//*                                                                 *
//*  AEDLINK  -                                                     *
//*             SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE TARGET    *
//*             LOAD LIBRARY SAEDLINK.                              *
//*                                                                 *
//*             IF YOU DID NOT RENAME THE LOAD LIBRARY, THEN SPECIFY *
//*             THE SAME VALUE AS HILEVEL.                          *
//*                                                                 *
//*  HILEVEL  -                                                     *
//*             SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE TARGET    *
//*             LIBRARIES.                                          *
//*                                                                 *
//*             E.G., IF NV4IP'S CLIST LIBRARY WAS UNLOADED         *
//*             TO SYS2.AESTCP.SAEDCLIB, THEN SPECIFY 'SYS2.AESTCP'. *
//*                                                                 *
//*  VSMHILVL -                                                     *
//*             SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE VSAM      *
//*             CLUSTERS FOR THIS SYSTEM.                           *
//*                                                                 *
//*  DUNIT    -                                                     *
//*             SPECIFIES THE DASD UNIT FOR WORK FILE ALLOCATION.   *
//*             DEFAULT IS SYSDA.                                   *
//*                                                                 *
//*             *NOTE* A WORK FILE WILL BE ALLOCATED ON THIS DASD   *
//*                    UNIT.  THE WORK FILE MUST NOT BE ALLOCATED ON *
//*                    ANY UNIT WHERE IT MAY BE DELETED OR ARCHIVED  *
//*                    BY THE SYSTEM DURING EXECUTION OF THIS PROC.  *
//*                                                                 *
//*  SOUT     -                                                     *
//*             SPECIFIES THE SYSOUT CLASS FOR DIAGNOSTIC OUTPUT.   *
//*             DEFAULT IS '*'.                                     *
//*                                                                 *
//*  TCPDLIB  -                                                     *
//*             SPECIFIES THE TCPIP.DATA OF THE TCP/IP STACK BEING  *
//*             MONITORED.  THIS DATA SET WILL BE ALLOCATED TO A    *
//*             //SYSTCPD DD STATEMENT.                             *
//*                                                                 *
//*             IT SHOULD BE THE SAME DATA SET AS THE ONE THAT IS   *
//*             SPECIFIED IN THE //SYSTCPD DD STATEMENT IN THE TCP/IP *
//*             PROCEDURE.                                          *
//*                                                                 *
//*  TCPXLBIN -                                                     *
//*             SPECIFIES THE TCPIP TRANSLATE TABLE DATA SET        *
//*             (HILVL.STANDARD.TCPXLBIN).  THE NETSTAT COMMAND WILL  *
//*             DYNAMICALLY ALLOCATE THIS DATA SET EVERY TIME IT IS   *
//*             INVOKED.  PRE-ALLOCATING THIS DATA SET WILL ELIMINATE *
//*             THE OVERHEAD OF THESE DYNAMIC ALLOCATIONS, AS WELL AS *
//*             RELATED JOB LOG MESSAGES.                           *
//*                                                                 *
//*******************************************************************
//*                                                                 *
//* LICENSED MATERIALS - PROPERTY OF IBM                            *
//* 5698-NTP                                                        *
//* (C) COPYRIGHT IBM CORPORATION 2000, 2002.  ALL RIGHTS RESERVED.   *
//* (C) COPYRIGHT APPLIED EXPERT SYSTEMS 1996, 2002.  ALL RIGHTS      *
//*     RESERVED.                                                   *
//*                                                                 *
//* US GOVERNMENT USERS RESTRICTED RIGHTS - USE, DUPLICATION OR       *
//* DISCLOSURE RESTRICTED BY GSA ADP SCHEDULE CONTRACT WITH IBM CORP. *
//*                                                                 *
//*******************************************************************
//AEST044 EXEC PGM=IKJEFT01,REGION=0K,TIME=1440,
// PARM=('AEST044 =CTCV=&CTCV')
//STEPLIB  DD DISP=SHR,
// DSN=&AEDLINK..SAEDLINK
//SYSEXEC DD DISP=SHR,
// DSN=&HILEVEL..SAEDCLIB
//SYSTCPD  DD DISP=SHR,
// DSN=&TCPDLIB
//SYSPRINT DD DSN=&TCPPRINT,UNIT=&DUNIT,
//            SPACE=(TRK,(40,20)),DISP=(,DELETE),
//            DCB=(RECFM=VBA,LRECL=137,BLKSIZE=6160)
//AESTHOST DD DUMMY
//SYSOUT   DD SYSOUT=&SOUT
//SYSTERM  DD SYSOUT=&SOUT
//SYSTSPRT DD SYSOUT=&SOUT
//SYSTSIN  DD DUMMY
//AESTVSM2 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM2
//AESTVSM3 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM3
//SYS0002  DD DISP=SHR,
// DSN=&TCPXLBIN
```

AESTCMDS JCL

```
//AESTCMDS PROC CTCV=,                             <=== DO NOT SPECIFY
//       AEDLINK=?????????????????,                <=== SPECIFY
//       HILEVEL=?????????????????,                <=== SPECIFY
//       CFGHILVL=????????????????,                <=== SPECIFY
//       SOUT=*,                                   <=== VERIFY
//       TCPDLIB=????????????????????,             <=== SPECIFY
//       TCPXLBIN=????????????????????             <=== SPECIFY
//*********************************************************************
//*                                                                   *
//*  IBM TIVOLI NETVIEW (R) FOR TCP/IP PERFORMANCE (NV4IP)            *
//*  REMOTE COMMAND PROCESSOR                                         *
//*                                                                   *
//*  *NOTE* THIS STARTED TASK IS STARTED BY THE MAIN MONITOR          *
//*         ADDRESS SPACE (DEFAULT NAME: AESTCPIP).  DO NOT START     *
//*         THIS ADDRESS SPACE BY ITSELF.                             *
//*                                                                   *
//*                                                                   *
//*  AEDLINK  -                                                       *
//*             SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE TARGET      *
//*             LOAD LIBRARY SAEDLINK.                                *
//*                                                                   *
//*             IF YOU DID NOT RENAME THE LOAD LIBRARY, THEN SPECIFY  *
//*             THE SAME VALUE AS HILEVEL.                            *
//*                                                                   *
//*  HILEVEL  -                                                       *
//*             SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE TARGET      *
//*             LIBRARIES.                                            *
//*                                                                   *
//*             E.G., IF NV4IP'S CLIST LIBRARY WAS                    *
//*             UNLOADED TO SYS2.AESTCP.SAEDCLIB, THEN SPECIFY        *
//*             'SYS2.AESTCP'.                                        *
//*                                                                   *
//*  CFGHILVL -                                                       *
//*             SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE TARGET      *
//*             LIBRARY SAEDCMDS.                                     *
//*                                                                   *
//*             IF YOU ARE MONITORING ONLY ONE SYSTEM, THEN SPECIFY   *
//*             THE SAME VALUE AS HILEVEL IN THE AESTCPIP PROC.       *
//*                                                                   *
//*  SOUT     -                                                       *
//*             SPECIFIES THE SYSOUT CLASS FOR DIAGNOSTIC OUTPUT.     *
//*             DEFAULT IS '*'.                                       *
//*                                                                   *
//*  TCPDLIB  -                                                       *
//*             SPECIFIES THE TCPIP.DATA OF THE TCP/IP STACK BEING    *
//*             MONITORED.  THIS DATA SET WILL BE ALLOCATED TO A      *
//*             //SYSTCPD DD STATEMENT.                               *
//*                                                                   *
//*             IT SHOULD BE THE SAME DATA SET AS THE ONE THAT IS     *
//*             SPECIFIED IN THE //SYSTCPD DD STATEMENT IN THE TCP/IP *
//*             PROCEDURE.                                            *
//*                                                                   *
//*  TCPXLBIN -                                                       *
//*             SPECIFIES THE TCPIP TRANSLATE TABLE DATA SET          *
//*             (HILVL.STANDARD.TCPXLBIN).  THE NETSTAT COMMAND WILL  *
//*             DYNAMICALLY ALLOCATE THIS DATA SET EVERY TIME IT IS   *
//*             INVOKED.  PRE-ALLOCATING THIS DATA SET WILL ELIMINATE *
//*             THE OVERHEAD OF THESE DYNAMIC ALLOCATIONS, AS WELL AS *
//*             RELATED JOB LOG MESSAGES.                             *
//*                                                                   *
//*********************************************************************
//*                                                                   *
//*  *NOTE*     IF YOU ARE MONITORING MORE THAN ONE SYSTEM, YOU MUST  *
//*             ALLOCATE A UNIQUE CFGHILVL.SAEDCMDS FOR EACH SYSTEM   *
//*                                                                   *
//*             THIS DATA SET IS ALLOCATED TO THE DDNAME OF SYSPRINT  *
//*             IN THIS PROC.  IT IS ACCESSED BY BOTH THIS PROC AND   *
//*             THE AESTCPIP PROC.  YOU MUST MODIFY BOTH PROCS SO     *
//*             THAT THEY SPECIFY THE SAME CFGHILVL.                  *
//*                                                                   *
//*********************************************************************
//*                                                                   *
//* LICENSED MATERIALS - PROPERTY OF IBM                              *
//* 5698-NTP                                                          *
//* (C) COPYRIGHT IBM CORPORATION 2000, 2002.  ALL RIGHTS RESERVED.   *
//* (C) COPYRIGHT APPLIED EXPERT SYSTEMS 1996, 2002.  ALL RIGHTS      *
//*     RESERVED.                                                     *
//*                                                                   *
//* US GOVERNMENT USERS RESTRICTED RIGHTS - USE, DUPLICATION OR       *
//* DISCLOSURE RESTRICTED BY GSA ADP SCHEDULE CONTRACT WITH IBM CORP. *
//*                                                                   *
//*********************************************************************
//AEST049 EXEC PGM=IKJEFT01,REGION=0K,TIME=1440,
// PARM=('AEST049 =CTCV=&CTCV')
//STEPLIB DD DISP=SHR,
// DSN=&AEDLINK..SAEDLINK
//SYSEXEC DD DISP=SHR,
// DSN=&HILEVEL..SAEDCLIB
//SYSTCPD  DD DISP=SHR,
// DSN=&TCPDLIB
//SYSPRINT DD DISP=SHR,
// DSN=&CFGHILVL..SAEDCMDS
//SYSOUT   DD SYSOUT=&SOUT
//SYSTERM  DD SYSOUT=&SOUT
//SYSTSPRT DD SYSOUT=&SOUT
//SYSTSIN  DD DUMMY
//SYS0002  DD DISP=SHR,
// DSN=&TCPXLBIN
```

AESTINIV JCL

```
// JOB
//**********************************************************************
//*                                                                    *
//* IBM TIVOLI NETVIEW (R) FOR TCP/IP PERFORMANCE (NV4IP)              *
//*                                                                    *
//* SAMPLE JCL TO ALLOCATE AND INITIALIZE THE FOLLOWING VSAM           *
//* DATABASES:                                                         *
//*            SAEDVSM0                                                *
//*            SAEDVSM1                                                *
//*            SAEDVSM2                                                *
//*            SAEDVSM3                                                *
//*            SAEDVSM4                                                *
//*            SAEDVSM5                                                *
//*                                                                    *
//* AEDLINK  - SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE TARGET        *
//*            LOAD LIBRARY SAEDLINK.                                  *
//*                                                                    *
//* VSMHILVL - SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE DATABASES     *
//*            IN THE JCL                                              *
//*                                                                    *
//* hilvlvsm - SPECIFIES THE HIGH-LEVEL QUALIFIER OF THE DATABASES     *
//*            IN THE IDCAMS CONTROL STATEMENTS                        *
//*                                                                    *
//* volser   - VOLUME SERIAL OF THE DATABASES                          *
//*                                                                    *
//* SOUT     - SYSOUT CLASS.  DEFAULT=*                                *
//*                                                                    *
//* RGNSIZE  - REGION SIZE.   DEFAULT=4096K                            *
//*                                                                    *
//* *NOTE*     IF YOU ARE MONITORING MORE THAN ONE SYSTEM, YOU SHOULD *
//*            USE A UNIQUE VALUE OF VSMHILVL TO ALLOCATE ONE SET OF   *
//*            VSAM DATABASES PER SYSTEM.                              *
//*                                                                    *
//**********************************************************************
//*                                                                    *
//* LICENSED MATERIALS - PROPERTY OF IBM                               *
//* 5698-NTP                                                           *
//* (C) COPYRIGHT IBM CORPORATION 2000, 2002.  ALL RIGHTS RESERVED.    *
//* (C) COPYRIGHT APPLIED EXPERT SYSTEMS 1996, 2002.  ALL RIGHTS       *
//*     RESERVED.                                                      *
//*                                                                    *
//* US GOVERNMENT USERS RESTRICTED RIGHTS - USE, DUPLICATION OR        *
//* DISCLOSURE RESTRICTED BY GSA ADP SCHEDULE CONTRACT WITH IBM CORP.  *
//*                                                                    *
//**********************************************************************
//AESTINIV PROC AEDLINK=?????????????????,           <== SPECIFY
//             VSMHILVL=?????????????????,           <== SPECIFY
//             SOUT=*,                               <== VERIFY
//             RGNSIZE=4096K                         <== VERIFY
//*
//*--------------------------------------------------------------------
//* ALLOCATE ALL VSAM DATABASES
//*--------------------------------------------------------------------
//ALLOCV  EXEC PGM=IDCAMS,REGION=&RGNSIZE
//SYSPRINT DD SYSOUT=&SOUT
//SYSIN    DD DUMMY
```

```
//*-------------------------------------------------------------------
//* INITIALIZE SAEDVSM0
//*-------------------------------------------------------------------
//INIT0   EXEC PGM=AEST065,COND=(0,NE),REGION=&RGNSIZE
//STEPLIB  DD DISP=SHR,
// DSN=&AEDLINK..SAEDLINK
//AESTVSM0 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM0
//SYSPRINT DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//SYSTERM  DD SYSOUT=*
//*-------------------------------------------------------------------
//* INITIALIZE SAEDVSM1 AND SAEDVSM2
//*-------------------------------------------------------------------
//INIT12  EXEC PGM=AEST052,REGION=&RGNSIZE
//STEPLIB  DD DISP=SHR,
// DSN=&AEDLINK..SAEDLINK
//AESTVSM1 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM1
//AESTVSM2 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM2
//SYSPRINT DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//SYSTERM  DD SYSOUT=*
//*-------------------------------------------------------------------
//* INITIALIZE SAEDVSM3
//*-------------------------------------------------------------------
//INIT3   EXEC PGM=AEST062,REGION=&RGNSIZE
//STEPLIB  DD DISP=SHR,
// DSN=&AEDLINK..SAEDLINK
//AESTVSM3 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM3
//SYSPRINT DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//SYSTERM  DD SYSOUT=*
//*-------------------------------------------------------------------
//* INITIALIZE SAEDVSM4
//*-------------------------------------------------------------------
//INIT4   EXEC PGM=AEST064,REGION=&RGNSIZE
//STEPLIB  DD DISP=SHR,
// DSN=&AEDLINK..SAEDLINK
//AESTVSM4 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM4
//SYSPRINT DD SYSOUT=&SOUT
//SYSOUT   DD SYSOUT=&SOUT
//SYSTERM  DD SYSOUT=&SOUT
//*-------------------------------------------------------------------
//* INITIALIZE SAEDVSM5
//*-------------------------------------------------------------------
//INIT5   EXEC PGM=AEST070,REGION=&RGNSIZE
//STEPLIB  DD DISP=SHR,
// DSN=&AEDLINK..SAEDLINK
//AESTVSM5 DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM5
//SYSPRINT DD SYSOUT=&SOUT
//SYSOUT   DD SYSOUT=&SOUT
//SYSTERM  DD SYSOUT=&SOUT
//*-------------------------------------------------------------------
//* BUILD ALTERNATE INDEX FOR SAEDVSM4
//*-------------------------------------------------------------------
//BLDAIX  EXEC PGM=IDCAMS,REGION=&RGNSIZE
```

```
//BASEDD DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM4
//AIXDD  DD DISP=SHR,
// DSN=&VSMHILVL..SAEDVSM4.AIX
//SYSPRINT DD SYSOUT=&SOUT
//SYSIN    DD DUMMY
// PEND
// EXEC AESTINIV
//ALLOCV.SYSIN DD *

   DELETE -
     (hilvlvsm.SAEDVSM0)                  -
     PURGE CLUSTER

   DELETE -
     (hilvlvsm.SAEDVSM1)                  -
     PURGE CLUSTER

   DELETE -
     (hilvlvsm.SAEDVSM2)                  -
     PURGE CLUSTER

   DELETE -
     (hilvlvsm.SAEDVSM3)                  -
     PURGE CLUSTER

   DELETE -
     (hilvlvsm.SAEDVSM4)                  -
     PURGE CLUSTER

   DELETE -
     (hilvlvsm.SAEDVSM4.PATH)             -
     PURGE CLUSTER

   DELETE -
     (hilvlvsm.SAEDVSM5)                  -
     PURGE CLUSTER

   SET MAXCC = 0

   /* SAEDVSM0 */

   DEFINE CLUSTER -
          (NAME(hilvlvsm.SAEDVSM0) -
           VOLUMES(volser) -
           CYLINDERS(100 100) -
           INDEXED KEYS(32 0) -
           RECORDSIZE(1024 32760)) -
          DATA (NAME(hilvlvsm.SAEDVSM0.DATA)) -
          INDEX(NAME(hilvlvsm.SAEDVSM0.INDEX))

   /* SAEDVSM1 */

   DEFINE CLUSTER -
          (NAME(hilvlvsm.SAEDVSM1) -
           VOLUMES(volser) -
           CYLINDERS(100 100) -
           INDEXED KEYS(18 0) -
           SHAREOPTIONS(2,3)  -
           RECORDSIZE(26   42)) -
          DATA (NAME(hilvlvsm.SAEDVSM1.DATA)) -
```

```
       INDEX(NAME(hilvlvsm.SAEDVSM1.INDEX))

/* SAEDVSM2 */

DEFINE CLUSTER -
       (NAME(hilvlvsm.SAEDVSM2) -
        VOLUMES(volser) -
        CYLINDERS(100 100) -
        INDEXED KEYS(34 0) -
        SHAREOPTIONS(2,3)  -
        RECORDSIZE(42   66)) -
       DATA (NAME(hilvlvsm.SAEDVSM2.DATA)) -
       INDEX(NAME(hilvlvsm.SAEDVSM2.INDEX))

/* SAEDVSM3 */

DEFINE CLUSTER -
       (NAME(hilvlvsm.SAEDVSM3) -
        VOLUMES(volser) -
        CYLINDERS(100 100) -
        INDEXED KEYS(17 0) -
        SHAREOPTIONS(2,3)  -
        RECORDSIZE(132 164)) -
       DATA (NAME(hilvlvsm.SAEDVSM3.DATA)) -
       INDEX(NAME(hilvlvsm.SAEDVSM3.INDEX))

/* SAEDVSM4 */

DEFINE CLUSTER  -
  (NAME(hilvlvsm.SAEDVSM4)            -
   VOLUMES(volser) -
   INDEXED KEYS(25 0) RECORDSIZE(62 74) -
   SHAREOPTIONS(2,3)  -
   CYLINDERS(100 100) )    -
DATA  -
  (NAME(hilvlvsm.SAEDVSM4.DATA))       -
INDEX -
  (NAME(hilvlvsm.SAEDVSM4.INDEX))

/* SAEDVSM4.AIX */
IF MAXCC=0 THEN DO
    DELETE -
      (hilvlvsm.SAEDVSM4.AIX) -
      PURGE AIX
    SET MAXCC = 0

    DEFINE ALTERNATEINDEX -
        (NAME(hilvlvsm.SAEDVSM4.AIX) -
         RELATE(hilvlvsm.SAEDVSM4) -
         VOLUMES(volser) -
         KEYS(24 9) -
         SHAREOPTIONS(2,3)  -
         RECORDSIZE(518 2568) -
         KILOBYTES(1600 800) -
         UNIQUEKEY)
  END

/* SAEDVSM5 */

DEFINE CLUSTER -
       (NAME(hilvlvsm.SAEDVSM5) -
           VOLUMES(volser) -
           CYLINDERS(100 100) -
           INDEXED KEYS(21 0) -
           RECORDSIZE(556 600)) -
          DATA (NAME(hilvlvsm.SAEDVSM5.DATA)) -
          INDEX(NAME(hilvlvsm.SAEDVSM5.INDEX))
/*
//BLDAIX.SYSIN DD *
   BLDINDEX INFILE(BASEDD) OUTFILE(AIXDD)
   DEFINE PATH -
          (NAME(hilvlvsm.SAEDVSM4.PATH) -
           PATHENTRY(hilvlvsm.SAEDVSM4.AIX))
/*
```

APPENDIX F - SAMPLE FTP LOG LISTINGS

FTP Server Events (in AESFTPLG):

```
AES824I FTP OPEN CONNECTION,IP=137.72.43.11,PORT= 1079,TIME=18:00:17.52
 AES826I FTP CMD=USER    ,USER=        ,TIME=18:00:19.42,ARG=p390
 AES826I FTP CMD=PASS    ,USER=P390    ,TIME=18:00:20.42,ARG=
 AES825I FTP LOGIN,USER=P390    ,TIME=18:00:20.42
 AES826I FTP CMD=TYPE    ,USER=P390    ,TIME=18:00:21.96,ARG=A
 AES826I FTP CMD=CWD     ,USER=P390    ,TIME=18:00:25.11,ARG=..
 AES826I FTP CMD=CWD     ,USER=P390    ,TIME=18:00:30.00,ARG=aes.t30djc.c
 AES826I FTP CMD=PORT    ,USER=P390    ,TIME=18:00:35.23,ARG=137,72,43,11,4,56
 AES826I FTP CMD=RETR    ,USER=P390    ,TIME=18:00:35.29,ARG=aest085
 AES824I FTP OPEN CONNECTION,IP=137.72.43.33,PORT=50930,TIME=11:22:55.58
 AES826I FTP CMD=USER    ,USER=        ,TIME=11:22:59.51,ARG=p390b
 AES826I FTP CMD=PASS    ,USER=P390B   ,TIME=11:23:01.17,ARG=
 AES825I FTP LOGIN,USER=P390B   ,TIME=11:23:01.17
 AES826I FTP CMD=TYPE    ,USER=P390B   ,TIME=11:23:03.52,ARG=A
 AES826I FTP CMD=CWD     ,USER=P390B   ,TIME=11:23:10.67,ARG=..
 AES826I FTP CMD=CWD     ,USER=P390B   ,TIME=11:23:14.04,ARG=aes.t30djc.c
```

APPENDIX G - SAMPLE SMF LOG LISTINGS

API Events (in AESSALOG):

```
AES820I API:INIT,IP=137.72.43.11,PORT=23/1280,Job=TCPIP   ,ID=TCPIP   ,Time=14:27:06
AES820I API:INIT,IP=10.31.109.130,PORT=1031/23,Job=P390B   ,ID=P390B   ,Time=14:27:45
AES820I API:INIT,IP=137.72.43.11,PORT=21/1281,Job=TCPIP   ,ID=FTPD    ,Time=14:28:42
AES820I API:INIT,IP=137.72.43.11,PORT=20/1282,Job=FTPD5   ,ID=FTPD    ,Time=14:28:57
AES821I API:TERM,IP=10.31.109.130,PORT=1031/23,Job=P390B,ID=P390B
,BIn=6033,BOut=228,Time=14:29:22
AES820I API:INIT,IP=10.31.109.130,PORT=1032/21,Job=P390B   ,ID=P390B   ,Time=14:29:31
AES820I API:INIT,IP=10.31.109.130,PORT=1033/20,Job=TCPIP   ,ID=P390B   ,Time=14:29:55
AES821I API:TERM,IP=137.72.43.11,PORT=20/1282,Job=FTPD5   ,ID=FTPD
,BIn=0,BOut=18577,Time=14:30:01
AES821I API:TERM,IP=137.72.43.11,PORT=21/1281,Job=FTPD1   ,ID=FTPD
,BIn=91,BOut=402,Time=14:30:02
AES821I API:TERM,IP=137.72.43.11,PORT=23/1280,Job=TCPIP   ,ID=TCPIP
,BIn=1888,BOut=21419,Time=14:30:11
AES821I API:TERM,IP=137.72.43.11,PORT=23/1280,Job=TCPIP
,ID=,BIn=1888,BOut=21418,Time=14:30:11
AES821I API:TERM,IP=10.31.109.130,PORT=1033/20,Job=P390B   ,ID=P390B
,BIn=0,BOut=4674,Time=14:31:0
```

FTP Events (in AESSFLOG):
Three lines are displayed per server record, two lines are displayed per client record

```
AES801I FTPS:RETR,IP=137.72.43.11,PORT=21/1281,RC=250,User=P390C   ,Format= /S/A,ABND=
AES802I Start=14:28:57,End=14:28:57,Bytes=18577,Elapsed=0.060sec,Throughput=309.62KB/sec
AES803I DSN1=AES.T30DJC.C                          /AEST085 ,DSN2=               /
AES825I
FTPC:STOR,IP=10.31.109.130,PORT=1032/21,RC=250,User=P390B,RemoteUser=aesdjcl,Host=P390,For
mat=/S/A
AES826I Start=14:29:55,End=14:29:55,Bytes=4674,Elapsed=0.000sec,Throughput=0.00KB/sec
AES807I DSN=AES.T30DJC.ASM
AES801I FTPS:REN ,IP=137.72.43.11,PORT=21/1283,RC=250,User=P390    ,Format= /S/A,ABND=
AES802I Start=14:31:26,End=14:31:26,Bytes=0,Elapsed=0.000sec,Throughput=0.00KB/sec
AES803I DSN1=AESDJC1.MAIN.CNTL    /ZZZZZZZZ,DSN2=AESDJC1.MAIN.CNTL       /XXXXXXXX
```

Telnet Events (in AESSTLOG):
Two lines displayed per record

```
AES810I
TELS:LOGN,IP=137.72.43.11,PORT=23/1280,LU=SC0TCP02,APPL=A06TSO02,Dev=0008D619,Time=14:27:0
7
AES811I
TELS:LOGF,IP=137.72.43.11,PORT=23/1280,LU=SC0TCP02,APPL=A06TSO02,Dev=0008D619,BIn=114,BOut
=1419
AES812I Elapsed=00:00:07,Time=14:27:14
AES810I
TELS:LOGN,IP=137.72.43.11,PORT=23/1280,LU=SC0TCP02,APPL=A06TSO03,Dev=0008D619,Time=14:27:1
4
AES813I TELC:LGON,IP=10.31.109.130,PORT=1031/23,STC=P390B   ,NJE=P390    ,Time=14:27:45
AES813I TELC:LGOF,IP=10.31.109.130,PORT=1031/23,STC=P390B   ,NJE=P390    ,Time=14:29:22
AES811I
TELS:LOGF,IP=137.72.43.11,PORT=23/1280,LU=SC0TCP02,APPL=A06TSO03,Dev=0008D619,BIn=1758,BOu
t=19807
AES812I Elapsed=00:02:53,Time=14:30:07
AES810I
TELS:LOGN,IP=137.72.43.11,PORT=23/1280,LU=SC0TCP02,APPL=A06TSO02,Dev=0008D619,Time=14:30:0
8
AES811I
TELS:LOGF,IP=137.72.43.11,PORT=23/1280,LU=SC0TCP02,APPL=A06TSO02,Dev=0008D619,BIn=16,BOut=
193
```

INDEX