GC32-4689-01

IBM Tivoli NetView® for TCP/IP Performance BatchPR Utilities Reference Guide Version 1.5

Host-Based Reporting

Tivoli software

Fifth Edition (August, 2002)

This edition applies to the IBM Tivoli NetView Performance Monitor for TCP/IP BatchPR Utilities User Guide.

Trademarks

Read This First

Tivoli® NetView® Performance Monitor for TCP/IP (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.

BatchPR, a component of NV4IP, provides a Host Based option for the creation of batch performance reports.

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:

WHAT IS NV4IP?
provides a brief overview of the features, functions, and operation of the NV4IP product.

WHAT IS BATCHPR?
gives a brief description of the architecture, features, functions, and operation of each of the two BatchPR utilities.

USING BATCHPR FOR NETWORK ANALYSIS
provides a comprehensive description of the operation and functionality of the BatchPR for Network Analysis utility and its associated five reports, which consist of the System Level/Resource Performance/Resource Availability Summaries and the Resource Performance/Resource Availability Detail reports.

USING BATCHPR FOR WORKLOAD ANALYSIS
provides a comprehensive description of the operation and functionality of the BatchPR for Workload Analysis utility and its associated four reports, which consist of the Workload Summary, Workload Server/Client Application, and Workload Sessions reports.

(This page intentionally left blank.)

TABLE OF CONTENTS

Table of Figures

(This page intentionally left blank.)

What is NV4IP?

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
- real-time monitoring
- command submission to the mainframe host(s) as well as sending alerts to the operator console
- 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. Please see the *IBM Tivoli NetView for TCP/IP Performance Reference Guide* for more information.

NV4IP 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 utilities 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 servers, network printers, or end-user workstations. The data is written to SMF and also summarized in VSAM databases for historical reporting.

There are five reports included in the BatchPR for Network Performance utility and four in the BatchPR for Workload Performance utility. These reports are controlled with parameters specified in the Job control EXEC statement either in batch mode (JCL SUBMIT command) or interactively using ISPF.

For more information about the NV4IP product, please see the *IBM Tivoli NetView for TCP/IP Performance Reference Guide.*

What are the BatchPR Utilities?

Network performance and availability as well as server/client application workload are becoming an ever-increasing concern to enterprise businesses as the global nature of business today intensifies the focus on these important issues. The BatchPR for NV4IP utilities provide a TN3270-like mainframe reporting option for those who require it and helps IT organizations easily focus on such issues. The BatchPR reports are created by a batch program that network analysts and management can execute daily in order to better understand network performance as related to the major node(s) of an IBM Mainframe WAN.

What is the BatchPR for Network Analysis Utility?

The BatchPR for Network Analysis utility focuses on two aspects of network performance: response time and availability. This utility easily answers 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?

The BatchPR for Network Analysis utility helps IT organizations to address these issues in the following five reports:

- The **System Level Summary** report provides an overview of network availability and performance for the monitored critical resources.
- The **Resources Performance Summary** report provides information on network performance.
- The **Resource Availability Summary** report focuses on availability for the selected critical resources.
- The **Resource Performance Detail** report lists the performance details regarding each monitored critical resource.
- The **Resource Availability Detail** report provides availability details for each monitored critical resource.

What is the BatchPR for Workload Analysis Utility?

The use of high-end IBM servers operating on today's networks makes it imperative to understand how local host applications are serving clients and users. It can be useful to know how each server application has been running for an extended period of time. The BatchPR for Workload Analysis utility focuses on the byte counts associated with each session and who was using a specific service. This utility helps IT organizations easily address such issues in the following four reports:

- The **Batch/PR – Workload Summary** report provides an overview of the usage of the stack by TCP and UDP protocols. This report shows the overall throughput in Bytes In/Out and the maximum/average value in the extended period for both protocols. It also reports the server and client applications share of the data transfer volume as well as the number of sessions observed.
- The **Batch/PR – Workload Server Application** report provides details relative to the server applications running on the host. This report shows all ports a server application is using as well as the port's corresponding total, maximum, and average data transfer volumes.
- The **Batch/PR – Workload Client Application** report provides details relative to the Client applications running on the host. This report shows all ports a client application is using as well as the port's corresponding total, maximum, and average data transfer volumes.
- The **Batch/PR – Workload Sessions** report provides detailed information about each observed session. This report identifies the session by the local port and the foreign IP address/foreign port pair, and reports the session's corresponding total, maximum, and average data transfer volumes.

Using BatchPR for Network Analysis

BatchPR is executed through the submission of JCL or from the TSO command line of ispf.

To create a BatchPR report, complete the following steps:

1. Code the JCL for the reports you want to process. The job can be created by modifying the skeleton JCL provided with BatchPR or interactively through an ispf panel.
2. Submit your job for processing.
3. View the output or print hardcopy.

Overview

The BatchPR for Network Analysis utility produces five different reports with up to three specified work shifts in each report. Work shifts allow you to divide a day into one, two, or three shifts. The utility generates a report for each specified shift. The BatchPR for Network Analysis reports can be controlled with the parameters specified in the Job control EXEC statement either in batch mode (SUBMIT command) or interactively using the BatchPR Interactive Invocation Service.

SLS System Level Summary Report provides an overview of network availability and performance for monitored critical resources.

RPS Resources Performance Summary Report provides information on network performance per specified work shift.

RAS Resource Availability Summary Report focuses on availability for the monitored critical resources.

RPD Resource Performance Detail Report lists the performance details regarding each monitored critical resource per specified shift.

RAD Resource Availability Detail Report provides availability details for each monitored critical resource per specified shift.

Input and Output

The BatchPR for Network Performance utility uses the following data sources and statements as input:

- VSAM data set – SAEDVSM1
- Parameters specified in the Job Control EXEC statement
- A sequential file as defined in the AESTBPRM DD statement

Report output is sent to the AESRPT data set as specified in the JCL DD statement of your SYSOUT class. Up to five reports may be requested for each of three work shifts.

Specifying Parameters with Job Control Statements

The Batch PR for Network Performance utility allows you to specify information in the AESTBPRM DD data set in order to customize the report. The sample CONF file in the SAEDSLIB member BCONF00 provides self-explanatory details on the use of each statement. Please refer to the sample file for more information.

The statements are:

- EXEC
- STEPLIB DD
- AESTVSMDD
- AESTRPT DD
- AESTBPRM DD

Each statement is described below.

EXEC statement

The EXEC statement identifies the program to be executed and sets the limits of the data to be input and output. The reports to be produced are selected in the =RPT= parameter.

```
//TEST300 EXEC PGM=AESTBPR1,
// REGION=4096K,
// PARM=('=DATE=2001158 =SHFT=041520 =RPT=YYYYY =DBG=YES =I=NPM3')
//*
```

Figure 1. Job Control Statements for AESTBPR1

The parameters set in the EXEC statement are:

Parameter	Description
PGM=	Identify the utility program to be executed, AESTBPR1.
PARM=	Specify the steps the program should perform to get the requested data.
=DATE=	Specifies the Date to report in either Julian (yyyyddd) or Gregorian (mm/dd/yyyy) date format. For example, February 3, 2002 would display as 2002034 in Julian or 02/03/2002 in Gregorian date format.
=SHFT=	Default is 00, which treats the entire day as a single shift. Set the shifts to be reported on by indicating the starting hour of each shift in 24 hour format. For example, if you want to specify 3 shifts starting at 6 AM for the first shift, 2 PM for the second shift, and 10 PM for the third shift, set =SHFT= as follows:

Parameter	Description
	=SHFT=061422
=RPT=	Specifies which reports to produce or suppress. Indicate a Y for Yes or an N for No in its relative position in the sequential list. Each report type is assigned thefollowing number:
	1 SLS System Level Summary
	2 RPS Resource Performance Summary
	3 RAS Resource Availability Summary Report provides
	4 RPD Resource Performance Detail Report lists
	5 RAD Resource Availability Detail Report provides
	Example 1: YYNNN indicates you would like to produce the SLS (System Level Summary) and RPS (Resource Performance Summary) reports. Example 2: YNYNN produces SLS (System Level Summary) and RAS (Resource Availability Summary reports.
=I=	Specifies the SMFSYSID used in your installation. It is normally specified in SYS1.PARMLIB(SMFPRM00). For NV4IP, you can also specify it in the PROC SMFSYSID= statement. If you specify SMFSYSID in the PROC, the SMFSYID in SYS1.PARMLIB is ignored.
=DBG=	Default is NO. Specify YES to enable debugging. Debugging may be required when additional support information is needed.

STEPLIB DD Statement

STEPLIB DD statement identifies the NV4IP link library. This should be the same library dataset you use for running the NV4IP Monitor. The library can shared between the online Monitor and the BatchPR utility.

```
//STEPLIB DD DISP=SHR,DSN=hilvl.SAEDLINK
```

Figure 2. STEPLIB Statement for AESTBR01

AESTVSM1 DD Statement

The AESTVSM1 DD statement identifies the VSAM dataset that the Monitor uses to record the network-related information. Due to overhead considerations, it is recommended that the library be shared between the online Monitor and BatchPR. The VSAM SHAREOPTION must have been previously set to (2,3). Figure 3 shows the AESTVSM1 DD statement for AESTBR01.

```
//AESTVSM1 DD DISP=SHR,
//            DSN=AES.NPMTST13.SAEDVSM1
```

Figure 3. AESTVSM1 DD Statement for AESTBR01

AESTRPT DD Statement

The AESTRPT DD Statement identifies where the report output will be produced. Normally report output is specified to SYSOUT and queued to the printer for hardcopy output.

```
//AESTRPT DD SYSOUT=*
```

Figure 4. AESTVSM1 DD Statement for AESTBR01

AESTBPRM DD Statement

The AESTBPRM DD Statement identifies where batch configuration parameters are specified. See the sample member of BCONF00 for further details.

```
//AESTBPRM DD DISP=SHR,
//            DSN=AES.NPMTST13.SAEDSLIB(BCONF00)
```

Figure 5. AESTBPRM DD Statement

For the other required standard JCL specifications refer to the sample JCL file, AESTBR01, in the hilvl.SAEDJCL library. A complete sample job follows:

```
//AESDJCPR JOB (999),'DJC',CLASS=A,MSGCLASS=X,NOTIFY=P390
//*
//*
//TEST300 EXEC PGM=AESTBPR1,
// REGION=4096K,
// PARM=('=DATE=2002002 =SHFT=020612 =RPT=YYYNY
//              =DBG=N =I=NPM3')
//*
//*
//STEPLIB  DD DISP=SHR,DSN=AES.TSTNPM14.SAEDLINK
//AESTVSM1 DD DISP=SHR,
//            DSN=AES.NPMTST13.SAEDVSM1
//AESTBPRM DD DISP=SHR,
//            DSN=AES.TSTNPM14.SAEDSLIB(BCONF00)
//AESTRPT  DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//SYSTERM  DD SYSOUT=*
```

Figure 6. Sample AESTBR01 JCL

Using BatchPR Network Analysis Reports

Each of the five BatchPR for Network Analysis reports are described in the following sections:

- **SLS** – System Level Summary
- **RPS** – Resources Performance Summary Report
- **RAS** – Resource Availability Summary Report
- **RPD** – Resource Performance Detail Report
- **RAD** – Resource Availability Detail Report

SLS – System Level Summary

The System Level Summary report addresses two key issues concerning the health of a network: availability and performance. The NV4IP Monitor periodically checks the state of the network path between the Enterprise Server and the critical resources defined in the Master. This information is also kept in NV4IP's historical databases.

The SLS Report is divided into two areas of information:

- Availability
  - Network Availability Rating
  - Top 3 Critical Resources Reporting Unavailable Events
- Performance
  - Network Response Time Rating
  - Top 3 Critical Resources Exceeding RT Threshold

Summary information is given, relative to each shift, for the areas listed above. Critical resources to be monitored are defined in the Master on the PC workstation. If a device is not being monitored, its status is not included in the report. Thresholds for performance and availability are set in the Master on the PC workstation. For a complete description of thresholds and Critical Resource definitions, refer to the *IBM Tivoli NetView FOR TCP/IP Performance Reference Guide.*

Availability

The availability area of the System Level Summary Report is divided into two sections:

- **Network Availability Rating** provides a general overview of available devices during the monitored period.
- **Top 3 Critical Resources Reporting Unavailable Events** provides information on the top three critical resources reporting unavailability for the selected time period.

Use these results to fine tune the network monitoring scheme further and to establish service level criteria.

The Network Availability Rating section of the report identifies how many critical resources were monitored during the shift, the size of the sample space (how often and how many were monitored), the number of times the resources were found unavailable, and a Network Availability percentage.

```
NETWORK AVAILABILITY RATING

   Total # of Critical Resources Monitored:        16

   Total # of Observed Events:             4012

   Total # of Resources Unavailable Events        292

   Percentage of Network Availability:        92.722%
```

Figure 7. SLS Report - Network Availability Rating

The fields on the Network Availability Rating section of the SLS report are:

Total # of Critical Resources Monitored The total number of critical resources monitored during this shift as defined in the Master on the PC workstation. A critical resource may be a server, a printer, a workstation or any other network capable device.

Total # of Observed Events Total number of monitoring events that NV4IP Monitor logged for the selected Critical Resources during the specified shift(s). These events may or may not have generated an alert. An observed event is defined as one of the series of test PINGs issued by NV4IP to determine a critical resource's availability and performance.

Total # of Resources Unavailable Events Total number of Availability Alerts generated for monitored Critical Resources during the specified shift(s). A resource that was not defined and selected for monitoring in the Master is not included in this total.

Percentage of Network Availability Percentage of Network Availability = (Total # of Resources Unavailable Events)/(Total # of Observed Events)

The Top 3 Critical Resources Reporting Unavailable Events section of the SLS report provides information on the top three critical resources reporting unavailability for the selected time period. If a device has not been defined as a Critical Resource and selected for monitoring in the Master, it is not reflected in this report.

```
Top 3 Critical Resources Reporting Unavailable Events
 Resource IP Address  Events    # Unavailable     Percentage
 ------------------- -------- ------------------- -------------------
 137.72.43.244      991         85          8.577%
 137.72.43.21       260         81         31.154%
 137.72.43.141      371         65         17.520%
```

Figure 8. SLS Report - Top 3 Critical Resources Reporting Unavailable Events

The fields on the Top 3 Critical Resources Reporting Unavailable Events section of the SLS report are:

Resource IP Address IP address for the device defined as a Critical Resource in the Master.

Events Total number of monitoring events logged by the NV4IP Monitor for the selected Critical Resources. An event is defined as one of the series of test PINGs issued by NV4IP to determine a Critical Resources availability and performance.

 # Unavailable Total number of Availability Alerts observed by the Host Monitor for the selected Critical Resources

	Host Monitor for the selected Critical Resources.
Percentage	Percentage = (# Unavailable)/*(Events)

Performance

The performance area of the SLS Report provides a summary of how well an Enterprise Server is running. It identifies how often the Enterprise Server failed to communicate with a network resource within the Response Time Threshold defined in the Master on the PC Workstation. The report also provides a percentage showing the number of events exceeding the Response Time of the sample space for overall network performance during the specified work shift.

The performance area is divided into two sections:

- **Network Response Time Rating** provides an overview of network response time for monitored critical resources.
- **Top 3 Critical Resources Exceeding RT Threshold** provides information on the top three critical resources with the most Response Times exceeding the RT threshold for network resources.

```
NETWORK RESPONSE TIME RATING

      Total # of Critical Resources Monitored:        16

      Total # of Observed Events:                   4012

      Total # of Threshold Exceeding Events:         123

      Percentage of Network RT within Threshold       96.934%
```

Figure 9. SLS Report - Network Response Time Rating

The fields on the Network Response Time Rating section of the report are:

Total # of Critical Resources Monitored
The total number of Critical Resources monitored during the specified shift as defined in the Master on the PC workstation. A Critical Resource may be a server, a printer, a workstation, or any other network capable device.

Total # of Observed Events
Total number of monitoring events that NV4IP Monitor logged for the selected Critical Resources during the specified shift(s). These events may or may not have generated an alert. An observed event is defined as one of the series of test PINGs issued by NV4IP to determine a Critical Resource's availability and performance.

Total # of Threshold Exceeding Events
Total number of Performance Alerts generated for monitored Critical Resources during the specified shift(s).

Percentage of Network RT within Threshold
Percentage of Network RT within Threshold = 100%- (Total # of Threshold Exceeding Events)/(Total # of Observed Events)

The top 3 Critical Resources Exceeding RT Threshold area shows the top three resources with the most Response Times exceeding the threshold observed for network resources.

```
Top 3 Critical Resources Exceeding RT Threshold:
    Resource IP Addr   # Events   # Over Threshold      Percentage
    ------------------ ---------- ------------------- -------------------
    216.32.74.53        282          44        15.603%
    137.72.43.241       319          36        11.285%
    137.72.43.242       284          33        11.620%
```

Figure 10. SLS Report - Critical Resources Exceeding RT Threshold

The fields on the Critical Resources Exceeding RT Threshold section of the report are:

Resource IP Addr	IP address for the device defined as a Critical Resource in the Master.
# Events	Total number of monitoring events logged by the NV4IP Monitor for the selected Critical Resources. An event is defined as one of the series of test PINGs issued by NV4IP to determine a Critical Resource's availability and performance.
# Over Threshold	Total number of Performance Alerts observed by the Host Monitor for the selected Critical Resources. Response Time thresholds are set when the Critical Resource is defined in the Master on the PC workstation.
Percentage	Percentage=(# Over Threshold)/(# Events)

A sample of the entire report follows.

```
NV4IP Batch/PR (Batch/Performance Reporter)  Fri Dec 21 11:26:55 2001

 REPORT: BatchPRSLS

 Applied Expert Systems
     DATE: 2001.352
    SHIFT: 1
FROM Hour: 9
  TO Hour: 15

 NETWORK AVAILABILITY RATING
   Total # of Critical Resources Monitored:      16
   Total # of Observed Events:                 4012
   Total # of Resources Unavailable Events      292
   Percentage of Network Availability:           92.722%

 Top 3 Critical Resources Reporting Unavailable Events
  Resource IP Address      # Events    # Unavailable    Percentage
  ---------------------   ---------------- ----------------- -------------
  137.72.43.244              991            85           8.577%
  137.72.43.21               260            81          31.154%
  137.72.43.141              371            65          17.520%

 NETWORK RESPONSE TIME RATING

   Total # of Critical Resources Monitored:        16
   Total # of Observed Events:                   4012
   Total # of Threshold Exceeding Events:         123
   Percentage of Network RT within Threshold:       96.934%

 Top 3 Critical Resources Exceeding RT Threshold:
  Resource IP Address     # Events   # Over Threshold     Percentage
  -------------------    -------------  ------------------- ------------
  216.32.74.53              282             44           15.603%
  137.72.43.241             319             36           11.285%
  137.72.43.242             284             33           11.620%
```

Figure 11. SLS Report - Sample Output

RPS – Resource Performance Summary Report

The Resource Performance Summary Report focuses on network performance during a specific work shift period. This report provides a specific overview of the efficiency of a network. Thresholds for performance and availability are set in the Master on the PC workstation. Devices selected for reporting must be defined as critical resources, an Alert must be set for each defined device, and monitoring must then be started. Although a Performance Alert is initially specified in the Master, an Alert can be started later by specifying AUTOALERT=YES in CONFxx. For a complete description of thresholds and Critical Resource definitions, refer to the *"Performance Monitor For TCP/IP Installation Guide Or Reference Guide"*.

The RPS report provides summary information relative to each work shift in three sections:

- **Resource Performance Summary** provides an overview of the critical resources monitored in terms of response time alerts.

- **Top 5 Resources Exceeding RT Threshold (by events)** shows a maximum of five critical resources with the most events exceeding the threshold.
- **Top 5 Resources Exceeding RT Threshold (by percent)** shows a maximum of five critical resources with the highest percentage of events exceeding the threshold.

The NV4IP Monitor periodically checks the state of the network path between the Enterprise Server and the critical resources defined in the Master. NV4IP also keeps track of this information in its private databases.

```
RESOURCE PERFORMANCE SUMMARY
Total # of Critical Resources Monitored:          17
Total # of Events with RT Exceeding Threshold:       130
Total # of CRs with Performance Alerts            4
Percentage RT over Threshold:              1.368%
Percentage of Resources with RT over Threshold:     23.529%
```

Figure 12. RPS Report - Resource Performance Summary

The fields on the Resource Performance Summary section of the report are:

Total # of Critical Resources Monitored	The total number of critical resources monitored during this shift as defined in the Master on the PC workstation. A critical resource may be a server, a printer, a workstation or any other network capable device.
Total # of Events with RT Exceeding Threshold	Total number of events that the NV4IP Monitor observed during the selected period that exceeded the pre-defined threshold on monitored critical resources. Critical resources are defined and selected for monitoring in the Master on the PC workstation. The pre-defined alert threshold is set in the Master on the PC workstation.
Total # of CRs with Performance Alerts	Total number of monitored critical resources (CRs) that have experienced a Performance Alert as defined by the threshold. The threshold is set by creating a Performance and Availability Alert in the Master for the monitored critical resources. A critical resource may experience more than one performance event that causes an alert. For this reason the number of CRs may be equal to or less than the Total # of Events with RT Exceeding Threshold.
Percentage RT Over Threshold	Expressed as a percentage. Percentage RT Over Threshold = (Total # of Events with RT Exceeding Threshold)/ (Overall # Of Events).

Percentage of Resources with RT over the Threshold Expressed as a percentage. Pecentage of Resources with RT over the Threshold = (Total # of CRs with Performance Alerts)/(Total # of critical resources monitored).

The second section of the RPS Report shows up to five Critical Resources with the most events exceeding the threshold.

```
 Top 5 Resources Exceeding RT Threshold (by events)
    Resource IP Address   # Events   # Over Threshold      Percentage
    -------------------  ---------- ------------------- -------------------
    216.32.74.53               628                  44           7.006%
    137.72.43.241              781                  36           4.609%
    137.72.43.242              736                  33           4.484%
    137.72.43.112              643                  17           2.644%
```

Figure 13. RPS Report - Top 5 Resources Exceeding RT Threshold (by events)

The fields on the Top 5 Resources Exceeding RT Threshold (by events) section of the RPS report are:

Resource IP Addr IP address for the device defined as a Critical Resource in the Master.

 # Events Total number of monitoring events logged by the NPM/IP Monitor for the selected Critical Resources. An event is defined as one of the series of test PINGs issued by NPM/IP to determine a Critical Resources availability and performance.

 # Over Threshold Total number of Performance Alerts observed by the Host Monitor for the selected Critical Resources. Response Time thresholds are set when the Critical Resource is defined in the Master on the PC workstation.

Percentage Percentage=(# Over Threshold)/(# Events)

The third section of the RPS Report shows the top five critical resources with the highest percentage of events exceeding the threshold during the selected time period.

```
Top 5 Resources Exceeding RT Threshold (by percent)
   Resource IP Address  # Events   # Over Threshold      Percentage
   ------------------- ---------- ------------------- -------------------
   216.32.74.53        628         44        7.006%
   137.72.43.241        781         36        4.609%
   137.72.43.242        736         33        4.484%
   137.72.43.112        643         17        2.644%
```

Figure 14. RPS Report - Top 5 Resources Exceeding RT Threshold (by percent)

The fields on the Top 5 Resources Exceeding RT Threshold (by percent) section of the RPS report are:

Resource IP Addr	IP address for the device defined as a Critical Resource in the Master.
# Events	Total number of monitoring events logged by the NPM/IP Monitor for the selected Critical Resources. An event is defined as one of the series of test PINGs issued by NPM/IP to determine a Critical Resources availability and performance.
# Over Threshold	Total number of Performance Alerts observed by the Host Monitor for the selected Critical Resources. Response Time thresholds are set when the Critical Resource is defined in the Master on the PC workstation.
Percentage	Percentage=(# Over Threshold)/(# Events)

The figure below shows sample output of an RPS report.

```
NV4IP Batch/PR (Batch/Performance Reporter)          Fri Dec 21 11:26:55 2001

REPORT: BatchPRRPS
 Applied Expert Systems
      DATE: 2001.352
     SHIFT: 2
 FROM Hour: 15
   TO Hour: 20

 RESOURCE PERFORMANCE SUMMARY

 Total # of Critical Resources Monitored:          17
 Total # of Events with RT Exceeding Threshol     130
 Total # of CRs with Performance Alerts             4
 Percentage RT over Threshold:                      1.368%
 Percentage of Resources with RT over Threshold:   23.529%

 Top 5 Resources Exceeding RT Threshold (by events)
 Resource IP Address      # Events   # Over Threshold      Percentage
 -------------------   ------------------- ------------------- ------------------
--
 216.32.74.53              628           44                7.006%
 137.72.43.241             781           36                4.609%
 137.72.43.242             736           33                4.484%
 137.72.43.112             643           17                2.644%

 Top 5 Resources Exceeding RT Threshold (by percent)
 Resource IP Address       # Events    # Over Threshold      Percentage
 -------------------    ------------------ ------------------- -----------------
---
 216.32.74.53              628           44                7.006%
 137.72.43.241             781           36                4.609%
 137.72.43.242             736           33                4.484%
 137.72.43.112             643           17                2.644%
```

Figure 15. RPS Report – Sample Output

RAS – Resource Availability Summary Report

Resource Availability Summary Report focuses on availability. It provides an overview of network availability per specified work shift for the defined and monitored critical resources set in the Master. The devices selected for reporting must be defined as a critical resource, an Alert must set for the defined device, and monitoring must then be started. All actions are performed in the Master on the PC workstation. Although set initially by the Master, they may be automatically monitored for availability later by specifying AUTOMON=YES in the AESTCPIP Proc. The Availability Alert may be automatically started by specifying AUTOALERT=YES in CONFxx. For a complete description of thresholds and Critical Resource definitions, refer to the *IBM Tivoli NetView for TCP/IP Performance Reference Guide.*

The RAS report provides summary information relative to each work shift in three sections:

- **Resource Availability Summary** provides an overview of the Critical Resources monitored in terms of availability alerts.
- **Top 5 Resources Reporting Unavailable Events** shows a maximum of five critical resources with the most events exceeding the availability threshold.
- **Top 5 Resources Exceeding Unavailability Threshold (by percent)** shows the top five critical resources with the highest percentage of unavailable events during the specified work shift.

The NV4IP Monitor periodically checks the state of the network path between the Enterprise Server and the critical resources defined in the Master. NV4IP also keeps track of this information in its private databases.

```
RESOURCE AVAILABILITY SUMMARY
Total # of Critical Resources Monitored:         17
Total # of Unavailable Events Observed:         425
Total # of CRs with Unavailable Events            8
Percentage Network Unavailable:                   4.472%
Percentage Unavailable Resources:                47.059%
```

Figure 16. RAS Report - Resource Availability Summary

The fields on the Resource Availability Summary section of the report are:

Total # of Critical Resources Monitored The number of critical resources monitored during this shift as defined in the Master on the PC workstation. A Critical Resource may be a server, a printer, a workstation or any other network capable device.

Total # of Unavailable Events Observed Total number of events that the NPM/IP Monitor logged the Critical Resource as unavailable during the selected period. Critical resources are defined and selected for monitoring in the Master on the PC workstation. An observed event is defined as one of the series of test PINGs issued by NPM/IP to determine a Critical Resources availability. A device is considered unavailable when it cannot be reached by the Host Monitor.

Total # of CRs with Unavailable Events Total number of monitored Critical Resources (CRs) that have experienced an Availability Alert.

Percentage Network Unavailable Percentage Network Unavailable = (Total # of Unavailable Events)/(Total # of Events Observed)

Percentage Unavailable Resources Percentage Unavailable Resources=(Total # of CRs with Unavailable Events)/(Total # of Critical Resources Monitored)

The second section of the RAS Report shows up to five Critical Resources with the most events exceeding the availability threshold (most times unavailable).

```
Top 5 Resources Reporting Unavailable Events
    Resource IP Address   # Events    # Unavailable    Percentage
    ------------------- ----------- ------------------- ---------------
    137.72.43.141             676            115        17.012%
    137.72.43.244            3209             85         2.649%
    1.1.1.1                    84             83        98.810%
    137.72.43.21              413             81        19.613%
    137.72.43.107             429             29         6.760%
```

Figure 17. RAS Report - Top 5 Resources Reporting Unavailable Events

The fields on the Top 5 Resources Reporting Unavailable Events section of the report are:

Resource IP Addr IP address for the device defined as a Critical Resource in the Master.

 # Events Total number of monitoring events logged by the NPM/IP Monitor for the selected Critical Resources. An event is defined as one of the series of test PINGs issued by NPM/IP to determine a Critical Resources availability and performance.

 # Unavailable Total number of Availability Alerts observed by the Host Monitor for the selected Critical Resources.

Percentage Percentage=(# Unavailable)/*(Events)

The third section of the RAS Report shows the top five critical resources with the highest percentage of unavailable events during the specified work shift.

```
Top 5 Resources Exceeding Unavailability Threshold (by percent)
    Resource IP Address   # Events    # Unavailable    Percentage
    -------------------  -----------  ----------------- ---------------
    1.1.1.1                     84         83      98.810%
```

216.32.120.133	4	3	75.000%
137.72.43.21	413	81	19.613%
137.72.43.141	676	115	17.012%
137.72.43.28	334	28	8.383%

Figure 18. RAS Report - Top 5 Resources Exceeding Unavailability Threshold (by percent)

The fields on the Top 5 Resources Exceeding Unavailability Threshold section of the report are:

Resource IP Addr IP address for the device defined as a Critical Resource in the Master.

 # Events Total number of monitoring events logged by the NPM/IP Monitor for the selected Critical Resources. An event is defined as one of the series of test PINGs issued by NPM/IP to determine a Critical Resources availability and performance.

 # Unavailable Total number of Availability Alerts observed by the Host Monitor for the selected Critical Resources.

Percentage Percentage=(# Unavailable)/*(Events)

The figure below shows sample output of an RAS report.

```
NV4IP Batch/PR (Batch/Performance Reporter)          Fri Dec 21 11:26:55 2001
REPORT: BatchPRRAS

 Applied Expert Systems
      DATE: 2001.352
     SHIFT: 2
 FROM Hour: 15
   TO Hour: 20

 RESOURCE AVAILABILITY SUMMARY

 Total # of Critical Resources Monitored:          17
 Total # of Unavailable Events Observed:          425
 Total # of CRs with Unavailable Events             8
 Percentage Network Unavailable:                    4.472%
 Percentage Unavailable Resources:                 47.059%

 Top 5 Resources Reporting Unavailable Events
 Resource IP Address       # Events    # Unavailable      Percentage
 -------------------    ------------------ ------------------- -----------------
--
 137.72.43.141              676        115                17.012%
 137.72.43.244             3209         85                 2.649%
 1.1.1.1                     84         83                98.810%
 137.72.43.21               413         81                19.613%
 137.72.43.107              429         29                 6.760%

 Top 5 Resources Exceeding Unavailability Threshold (by percent)
 Resource IP Address       # Events    # Unavailable      Percentage
 -------------------    ------------------- ------------------- ----------------
---
 1.1.1.1                     84         83                98.810%
 216.32.120.133               4          3                75.000%
 137.72.43.21               413         81                19.613%
 137.72.43.141              676        115                17.012%
 137.72.43.28               334         28                 8.383%
```

Figure 19. RAS Report – Sample Output

RPD – Resource Performance Detail Report

The Resource Performance Detail Report provides the performance details regarding each critical resource defined in the Master and monitored per specified work shift. The NV4IP Monitor gathers the information through constant probing of the selected critical resources. By using up to four different packet sizes, NV4IP provides insights on how certain applications perform and their availability under differing workloads in their network environment.

The RPD Report describes the performance attributes of each packet size through tracking the average, minimum, and maximum response time, number of events where the response time is over the defined threshold, as well as the percentage of such events as part of the total observed events in the group.

```
NV4IP Batch/PR (Batch/Performance Reporter)       Mon Dec 31 09:31:08 2001

 REPORT: BatchPRRPD

 Applied Expert Systems
      DATE: 2001.352
     SHIFT: 2
 FROM Hour: 15
   TO Hour: 20


 Detail Resource Performance Report:

 Address     Packet   Pings  Avg RT  Min RT  Max RT   # PF Alert  % PF Alert
 ---------- --------  -----  ------- ------  ------   ----------  ----------
216.32.74.53   256      627    153      105    1660        44          7.006%
       Total:           628                                44          7.006%

137.72.43.241  256      229     32        8     481        12          5.240%
               512      185     26        9     185         7          3.784%
              1024      184     27       10     270         9          4.891%
              2048      183     32       14     354         8          4.372%
    Total:     781                                         36          4.609%

137.72.43.242  256      184     37       17     247        14          7.609%
               512      184     33       13     577         5          2.717%
              1024      184     32       15     138         5          2.717%
              2048      184     41       21     239         9          4.891%
    Total:     736                                         33          4.484%
```

Figure 20. RPD Report – Sample Output

The fields on the Detail Resource Performance Report are:

Address	IP Address for the selected Critical Resource.
Packet	Packet size sent to the selected Critical Resource to monitor performance and availability. This value is set when adding the Critical Resource in the Master. Available packet sizes are 256, 512, 1024, and 2048.
Pings	Number of Pings sent to the selected Critical Resource to monitor performance and availability. The Ping frequency is determined when adding the Critical Resource in the Master.
Avg RT	Average(Avg) response time in milliseconds the successful Ping took to reach that Critical Resource for the packet size shown.
Min RT	Minimum (Min) response timein milliseconds the successful Ping took to reach that Critical Resource for the packet size shown.
Max RT	Maximum(Max) response time in milliseconds the successful Ping took to reach that Critical Resource for the packet size shown.
# PFAlt	Number of Performance alerts received for this Critical Resource per packet type. Alerts are sent based upon the threshold level set in the Master.
% PF Alert	%PF Alert=(# PFAlt/Ping) * 100.

RAD – Resource Availability Detail Report

The Resource Availability Detail Report provides information on availability for each critical resource defined and monitored for the specified work shift. The NV4IP Monitor gathers the information through constant probing of the selected critical resources. By using up to four different packet sizes, NV4IP provides insights on how certain applications perform and their availability under differing workloads in their network environment.

The RAD Report describes the availability attributes of each packet size. It shows the sample size for each packet type, the number of unavailable events (AV Alerts), the availability percentage, and the percentage of availability alerts received per resource by packet size (% AV Alert = (AV Alerts per packet level / Total AV Alerts) * 100).

```
NV4IP BatchPR                                          Fri Mar 1 10:17:12 2002

 REPORT: BatchPRRAD



    Your Company
      DATE: 2001.352
     SHIFT: 2
 FROM Hour: 9
   TO Hour: 15

 Detail Resource Availability Report:

 Address            Packet      Pings     AV Alerts    % Avail.   % AV Alert
 --------------   ----------  ----------  ----------  ----------  ----------
 137.72.43.21          256          71           0     100.000%      0.000%
                       512          69           0     100.000%      0.000%
                      1024          69           0     100.000%      0.000%
                      2048           0          81       0.000%    100.000%
     Total:                        290          81                  27.931%
 137.72.43.141         256         111           1      99.107%      1.538%
                       512         111           0     100.000%      0.000%
                      1024         111           0     100.000%      0.000%
                      2048           0          64       0.000%     98.462%
     Total:                        398          65                  16.332%
 137.72.43.107         256          66          29      69.474%    100.000%
                       512          66           0     100.000%      0.000%
                      1024         132           0     100.000%      0.000%
     Total:                        293          29                   9.898%
 137.72.43.28          256          66          28      70.213%    100.000%
                       512          66           0     100.000%      0.000%
                      1024          66           0     100.000%      0.000%
     Total:            226          28                              12.389%
```

Figure 21. RAD Report – Sample Output

The fields on the Resource Availability Detail Report are:

Address	IP Address for the selected Critical Resource.
Packet	Packet size sent to the selected Critical Resource to monitor performance and availability. This value is set when adding the Critical Resource in the Master. Available packet sizes are 256, 512, 1024, and 2048.
Pings	Number of successful Pings sent to the selected Critical Resource to monitor performance and availability. The Ping frequency is determined when adding the Critical Resource in the Master.
AV Alerts	Count of availability alerts received for this Critical Resource per packet type during the period.
% Avail.	%Avail.=(Pings-AV Alerts)/Pings * 100)
% AV Alert	Percentage of availability alerts (device is unavailable) received per resource by packet size (% AV Alert = (AV Alerts per packet level / Pings) * 100). For Critical Resource 137.72.43.21 for packet size 2048, the % AV Alerts was 100%=81/81. The device was unreachable for all packet sizes of 2048.
Total Pings	Sum of all successful Pings, regardless of packet size, sent to the selected Critical Resource.
Total AV Alerts	Sum of all AV Alerts, regardless of packet size, for this Critical Resource.
Total % Avail.	Percentage this Critical Resource was available over the selected time period for all packet sizes. The formula is: Total % Avail. = (Total AV Alerts for all packet levels / Total Pings) * 100).

(This page intentionally left blank.)

Using BatchPR for Workload Analysis

The Batch PR for Workload Analysis utility reports the status of the local host, including information about the TCP/IP connections and their associated byte count information.

Overview

The BatchPR for Workload Analysis utility produces four different reports. These reports can be controlled by specifying parameters in the Job control EXEC statement either in batch mode (SUBMIT command), in the Control File, or interactively using ispf panels.

Workload Summary
This report provides an overview of the usage of the stack by TCP and UDP protocols. It shows the overall throughput in Bytes In/Out and the maximum/average value in the extended period for both protocols. It also reports the server and client applications share of the data transfer volume as well as the number of sessions observed.

Workload Server Application
This report provides details relative to the server applications running on the host. It shows all ports a server application is using as well as the port's corresponding total, maximum, and average data transfer volumes.

Workload Client Application
This report provides details relative to the Client applications running on the host. It shows all ports a client application is using as well as the port's corresponding total, maximum, and average data transfer volumes.

Workload Sessions Report
This report is a batch program that provides detailed information about each observed session. It identifies the session by the local port and the foreign IP address/foreign port pair, and reports the session's corresponding total, maximum, and average data transfer volumes.

Input and Output

The BatchPR for Workload Analysis utility uses the following data sources and statements as input:

1. VSAM data set – AESTVSM2 that is used by the online monitoring region. BatchPR for Workload Analysis can run concurrently with the online region.
2. Parameters specified in the Job Control EXEC statement.
3. Parameters specified in the Control File.

The Batch PR for Workload Analysis produces report output to the AESRPT data set as specified in the JCL DD statement.

Specifying Parameters with Job Control Statements

The BatchPR for Workload Analysis utility produces four reports as output. The utility is controlled by specifying parameters in either the Job Control statements or in the Control File.

EXEC Statement

The EXEC statement identifies the program to be executed and sets the limits of the data to be input and output. The reports to be produced are selected in the =RPT= parameter.

```
//TEST310 EXEC PGM=AESTBWL1,
// REGION=4096K,
// PARM=('=DATE=2/06/2002 =RPT=YYNY =DBG=NO =I=SYSZ
//         =TDATE=2/9/2002 =WDAY=NYYYYYN')
```

Figure 22. Job Control Statements for AESTBWL1

The parameters set in the EXEC statement are:

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>PGM=</td><td colspan="2">Identifies the utility program to be executed. To execute BatchPR for Workload Analysis, specify AESTBWL1.</td></tr>
<tr><td>PARM=</td><td colspan="2">Specifies the steps the program should perform to get the requested data.</td></tr>
<tr><td>=DATE=</td><td colspan="2">Specifies the Date to begin reporting in either Julian (yyyyddd) or Gregorian (mm/dd/yyyy) date format. For example, February 3, 2002 would display as 2002034 in Julian or 02/03/2002 in Gregorian date format.</td></tr>
<tr><td>=TDATE=</td><td colspan="2">Specifies the date to end reporting in either Julian (yyyyddd) or Gregorian (mm/dd/yyyy) date format. For example, February 3, 2002 would display as 2002034 in Julian or 02/03/2002 in Gregorian date format.</td></tr>
<tr><td>=WDAY=</td><td colspan="2">Specifies the days of the week (Sunday-Saturday) to include in the report. You must specify either Y or N for each day of the week. For example, to include Monday through Friday but no weekend days, specify NYYYYYN.</td></tr>
<tr><td rowspan="5">=RPT=</td><td colspan="2">Specifies which reports to produce or suppress. Indicate a Y for Yes or an N for No in its relative position in the sequential list. Each report is assigned the following number:</td></tr>
<tr><td>1</td><td>Workload Summary</td></tr>
<tr><td>2</td><td>Workload Server Application</td></tr>
<tr><td>3</td><td>Workload Client Application</td></tr>
<tr><td>4</td><td>Workload Sessions Report</td></tr>
</table>

Parameter	Description
	Example 1: YYNN indicates that you would like to produce report 1 and report 2 which are the Workload Summary and Workload Server Application reports. Example 2: YNYN produces the Workload Summary and the Workload Client Application reports.
=I=	Specifies the SMFSYSID used in your installation. It is normally specified in SYS1.PARMLIB(SMFPRM00). For NV4IP, you can also specify it in the PROC SMFSYSID= statement. If you specify SMFSYSID in the PROC, the SMFSYID in SYS1.PARMLIB is ignored.
=DBG=	Default is NO. Specify YES to enable debugging. Debugging may be required when additional support information is needed.

STEPLIB DD Statement

The STEPLIB DD statement identifies the SAEDLINK link library. This should be the same library dataset you use for running the NV4IP Monitor. The library can shared between the online Monitor and the BatchPR utility.

```
//STEPLIB DD DISP=SHR,DSN=hilvl.SAEDLINK
```

Figure 23. STEPLIB Statement for AESTBWL1

AESTVSM2 DD Statement

The AESTVSM2 DD statement identifies the VSAM dataset that the Monitor uses to record the workload-related information. The dataset can shared between the online Monitor and the BatchPR utility. The VSAM SHAREOPTION should have been previously set to (2,3).

```
//AESTVSM2  DD DISP=SHR,
//             DSN=AES.NPMTST13.SAEDVSM1
```

Figure 24. AESTVSM2 DD Statement for AESTBWL1

AESTRPT DD Statement

The AESTRPT DD Statement identifies where the report output will be produced. Normally report output is specified to SYSOUT and queued to the printer for hardcopy output.

```
//AESTRPT DD SYSOUT=*
```

Figure 25. AESTVSM2 DD Statement for AESTBWL1

AESTBPRM DD Statement

The AESTBPRM DD Statement identifies where batch configuration parameters are specified. See the sample member of BCONF00 for details.

```
//AESTBPRM DD DISP=SHR,
//            DSN=AES.NPMTST15.SAEDSLIB(BCONF00)
```

Figure 26. AESTBPRM DD Statement for AESTBWL1

Other standard JCL specifications also apply. For more details, see the sample JCL file AESTBWL1 in the *hilvl*.SAEDJCL library.

Interactive JCL submission

You will find a sample AESLIBDF in the SAEDCLIB library that enables interactive invocation of the batch job. For more details about Interactive BatchPR JCL Submission, refer to Appendix A. You may also use this facility to obtain JCL samples if desired.

Specifying Parameters with the Control File

The Batch PR for Workload Analysis utility allows you to specify information in the AESTBPRM DD data set in order to customize the report. The sample CONF file in the SAEDSLIB member BCONF00 provides self-explanatory details on the use of each statement. Please refer to the sample file for more information.

The statements included are:

- **COMPNAME** to specify installation-specific information.
- **SAP** to describe the server applications. For example, you may want to bundle both 23 and 1023 ports into a TELNET application.
- **CAP** to describe the client applications. For example, you may want to bundle both 23 and 1023 ports into a TELNET application.
- **EXCL** to specify a range of local ports you want to exclude.
- **EXCF** to specify a range of foreign IP addresses you want to exclude.

Using BatchPR Workload Analysis Reports

Each of the four BatchPR for Workload Analysis reports are described in the following sections:

- **Workload Summary**
- **Workload Server Application**
- **Workload Client Application**
- **Workload Sessions**

Workload Summary Report

The Workload Summary report provides summary level information about workloads that have been running on the monitored TCP/IP stack.

NV4IP provides capability for the Monitor to periodically check the applications running in the stack. Real-time and history workload reports provide various analyses of such data. Monitored workload data allows you to evaluate workloads running on the associated stack. It enables you to understand various performance aspects of specific applications.

The Workload Summary report provides an overview of applications over a period of time. You can use the DATE, TDATE and WDAY parameters to specify from or to dates, or specific days to include in the report. For example, you may want to identify if Fridays have a higher FTP workload than the rest of the days in the week.

```
Date From: 2/6/2002. To: 2/9/2002.
Days of week included: Monday Wednesday Friday
```

Figure 27. Workload Summary Report – Dates and Days Included

The Workload Summary report divides the workload into TCP and UDP sessions summaries so that you can assess, compare, and discover application usage of these protocols.

```
TCP Session Summary

 TCP Sessions     :        510
 TCP Total ByteOut:    9853981
     Max ByteOut  :    3485159
     Avg ByteOut  :      19321
 TCP Total ByteIn :    3202296
     Max ByteIn   :    2229102
     Avg ByteIn   :       6279

 UPD Session Summary

 UDP Sessions     :        988
 UDP Total ByteOut:     117861
     Max ByteOut  :        153
     Avg ByteOut  :        119
 UDP Total ByteIn :          0
     Max ByteIn   :          0
     Avg ByteIn   :          0
```

Figure 28. Workload Summary Report – TCP/UDP Session Summaries

The fields in the TCP/UDP Session Summaries section are:

TCP/UDP Sessions	The number of TCP/UDP sessions in the workload running on the stack during the specified time period.
TCP/UDP Total ByteOut	The total number of bytes sent out for the TCP/UDP session during the specified time period.
Max ByteOut	The highest number of bytes sent out per TCP/UDP session during the specified time period.
Avg ByteOut	The average number of bytes sent out per TCP/UDP session based on all intervals in the specified time period.
TCP/UDP Total ByteIn	The total number of bytes received for the TCP/UDP session during the specified time period.
Max ByteIn	The highest number of bytes received per TCP/UDP session during the specified time period.
Avg ByteIn	The average number of bytes received for the TCP/UDP session based on all intervals in the specified time period.

The Workload Summary report divides server applications running on the stack into server application groups. Using the SAP statement in the configuration file, you can identify the server applications to be analyzed.

```
Server Application Groups
    Name  # Ports  Sessions  Total BOut   BOut Max   BOut Avg  Total BIn   BIn Max   BIn Avg
  TELNET        2        17     9693810    3485159     570224    3155902   2229102    185641
     FTP        4        14       24520       5840       1751        901       131        64
    NVIP        1       472      113945      21176        241      29694       154        62
 DBMOVER        1         0           0          0          0          0         0         0
```

Figure 29. Workload Summary Report - Server Application Groups

The Workload Summary report divides client applications running on the stack into client application groups. Using the CAP statement in the configuration file, you can identify the client applications to be analyzed.

```
Client Application Groups
    Name  # Ports  Sessions  Total BOut   BOut Max   BOut Avg  Total BIn   BIn Max   BIn Avg
  TELNET        2         0           0          0          0          0         0         0
     FTP        4         2         228        143        114        797       430       398
```

Figure 30. Workload Summary Report – Client Application Groups

The fields in the Server/Client Application Groups sections are:

Name	The name of the server or client application.
# Ports	The number of ports used by the server or client application during the specified time period.
Sessions	The number of sessions reported for the server or client application during the specified time period.
Total BOut	The total number of bytes sent out during the specified time period
BOut Max	The highest number of bytes sent out per session during the specified time period.
BOut Avg	The average number of bytes sent out based on all intervals in the specified time period.
Total BIn	The total number of bytes received during the specified time period.
BIn Max	The highest number of bytes received per session during the specified time period.
BIn Avg	The average number of bytes received based on all intervals in the specified time period.

The following figure shows a sample output of a Workload Summary report:

```
Date: 2/12/2002
Report: Batch/PR Workload Summary Report

Applied Expert Systems
Date From: 2/6/2002. To: 2/9/2002.
Days of week included: Monday Wednesday Friday


TCP Session Summary

TCP Sessions     :        510
TCP Total ByteOut:    9853981
    Max ByteOut  :    3485159
    Avg ByteOut  :      19321
TCP Total ByteIn :    3202296
    Max ByteIn   :    2229102
    Avg ByteIn   :       6279

UPD Session Summary

UDP Sessions     :        988
UDP Total ByteOut:     117861
    Max ByteOut  :        153
    Avg ByteOut  :        119
UDP Total ByteIn :          0
    Max ByteIn   :          0
    Avg ByteIn   :          0

Server Application Groups
   Name  # Ports  Sessions  Total BOut   BOut Max   BOut Avg  Total BIn   BIn Max   BIn Avg
 TELNET        2        17     9693810    3485159     570224    3155902   2229102    185641
    FTP        4        14       24520       5840       1751        901       131        64
 TELNET        1       472      113945      21176        241      29694       154        62
DBMOVER        1         0           0          0          0          0         0         0

Client Application Groups
   Name  # Ports  Sessions  Total BOut   BOut Max   BOut Avg  Total BIn   BIn Max   BIn Avg
 TELNET        2         0           0          0          0          0         0         0
    FTP        4         2         228        143        114        797       430       398
```

Figure 31. Workload Summary Report – Sample Output

Workload Server Application Report

Resource Performance Summary Report focuses on the aspect of the Application Workloads associated with certain Server Applications. With this report, you may be able to understand what these Server Applications behave during the time period of interest. You will be able to tell the usage of these Server Applications, number of sessions, the BytesIn and BytesOut, average, max and total, as a whole or by the port.

The following figure shows a sample output of a Workload Server Application report:

```
Batch/PR Workload Server Application Summary                          Date: 2/12/2002
Report: WLServer

Applied Expert Systems
Date From: 2/6/2002. To: 2/9/2002.
Days of week included: Monday Wednesday Friday


Server Application Groups
   Name  # Ports  Sessions  Total BOut   BOut Max   BOut Avg  Total BIn   BIn Max   BIn Avg
 TELNET       23        17     9693810    3485159     570224    3155902   2229102    185641
 TELNET     1023         0           0          0          0          0         0         0
           Total        17     9693810    3485159     570224    3155902   2229102    185641
    FTP       20         4       19652       5840       4913          0         0         0
    FTP       21        10        4868        715        486        901       131        90
    FTP     1020         0           0          0          0          0         0         0
    FTP     1021         0           0          0          0          0         0         0
           Total        14       24520       5840       1751        901       131        64
  TELNET    5050       472      113945      21176        241      29694       154        62
           Total       472      113945      21176        241      29694       154        62
DBMOVER     6930         0           0          0          0          0         0         0
           Total         0           0          0          0          0         0         0
```

Figure 32. Workload Server Application Report – Sample Output

The fields in the Workload Server Application Report are:

Name	The name of the server application.
# Ports	The number of ports used by the application during the specified time period.
Sessions	The number of sessions reported for the application during the specified time period.
Total BOut	The total number of bytes sent out during the specified time period
BOut Max	The highest number of bytes sent out per session during the specified time period.
BOut Avg	The average number of bytes sent out based on all intervals in the specified time period.
Total BIn	The total number of bytes received during the specified time period.
BIn Max	The highest number of bytes received per session during the specified time period.
BIn Avg	The average number of bytes received based on all intervals in the specified time period.

Workload Client Application Report

The Workload Client Application report allows you to find out how the local host utilizes the services on the remote host. For example, applications may periodically transfer files to remote hosts via FTP. Using the Workload Client Application report, you can group the remote services together logically by their port numbers into an application group and then analyze how the local host uses these services.

The Workload Client Application report provides a summary for each Client Application Group as well as the usage by each remote server port.

```
1BatchWR                                                   Date: 2/12/2002
 Report: WLClient

 US Department of Defense
 Date From: 2/6/2002. To: 2/9/2002.
 Shift Start: 0.
       End : 0.

 Client Application Groups
    Name  # Ports  Sessions  Total BOut   BOut Max   BOut Avg  Total BIn   BIn Max   BIn Avg
  TELNET       23         0           0          0          0          0         0         0
  TELNET     1023         0           0          0          0          0         0         0
            Total         0           0          0          0          0         0         0
     FTP       20         0           0          0          0          0         0         0
     FTP       21         2         228        143        114        797       430       398
     FTP     1020         0           0          0          0          0         0         0
     FTP     1021         0           0          0          0          0         0         0
            Total         2         228        143        114        797       430       398
```

Figure 33. Workload Client Application Report – Sample Output

The fields in the Workload Client Application Report are:

Name	The name of the client application.
# Ports	The number of ports used by the application during the specified time period.
Sessions	The number of sessions reported for the application during the specified time period.
Total BOut	The total number of bytes sent out during the specified time period
BOut Max	The highest number of bytes sent out per session during the specified time period.
BOut Avg	The average number of bytes sent out based on all intervals in the specified time period.
Total BIn	The total number of bytes received during the specified time period.
BIn Max	The highest number of bytes received per session during the specified time period.
BIn Avg	The average number of bytes received based on all intervals in the specified time period.

Workload Sessions Report

The Workload Sessions report allows you to obtain a high-level view of each session's performance. A "session" describes the connection between a local port and the foreign IP/port combination. Using the Workload Sessions report, you can observe the duration of the session by the monitoring units used. You can also find out how much data, both incoming and outbound, has been used in the session in total, maximum, and average values. The Workload Sessions report allows you to determine the key clients of specific application servers, both remotely (using services on this host) and locally (using services on a remote host).

The Workload Sessions report identifies each session by the TCP/UDP application name it is using.

The following figure shows a sample output of the Workload Session report:

```
Batch/PR Workload Reporter                                        Date: 6/15/2002
Report: Workload Session Detail

Applied Expert Systems
Date From: 6/1/2002 To: 6/13/2002
Number of Sessions:    55


Workload Sessions Report
Name     T LPort Cnt FIP            FPort BOut Total  BOut Max BOut Avg  BIn Total  BIn Max BIn Avg
TCPIP    T 00023   9 137.72.43.120  4149      721228    251531    80136      15458     4152    1717 2002/154:12-2002/154:20
TCPIP    T 00023   2 137.72.43.38   4095       99718     74523    49859       1753     1349     876 2002/155: 1-2002/155: 2
TCPIP    T 00023   7 137.72.43.120  3035      631243    201613    90177      14648     3336    2092 2002/155:12-2002/155:18
FTPD1    T 00021   1 137.72.43.120  3014         837       837      837        121      121     121 2002/155:10-2002/155:10
FTPD1    T 00021   1 137.72.43.120  3145         837       837      837        121      121     121 2002/155:10-2002/155:10
NPMTCPIP T 05050   1 137.72.43.110  1897           0         0        0         46       46      46 2002/155:12-2002/155:12
FTPD1    T 00021   1 137.72.43.120  4269         843       843      843        118      118     118 2002/155:13-2002/155:13
TCPIP    T 00023   3 137.72.43.120  3039      159673    114999    53224       2574     1284     858 2002/155:18-2002/155:20
TCPIP    T 00023   2 137.72.43.38   4370       11439      5742     5719        422      274     211 2002/156:11-2002/156:12
P390     T 02654   1 137.72.43.38   4387       47880     47880    47880          0        0       0 2002/156: 8-2002/156: 8
FTPD1    T 00021   1 137.72.43.38   4371        8340      8340     8340       1166     1166    1166 2002/156: 8-2002/156: 8
TCPIP    T 00023   2 137.72.43.38   3225       15756     10012     7878        550      402     275 2002/156:16-2002/156:17
TCPIP    T 00023   1 137.72.43.38   3301       34221     34221    34221       1160     1160    1160 2002/156:13-2002/156:13
TCPIP    T 00023   1 137.72.43.38   3265       19086     19086    19086        641      641     641 2002/156:13-2002/156:13
TCPIP    T 00023   1 137.72.43.38   3079        8507      8507     8507        320      320     320 2002/156:18-2002/156:18
FTPD1    T 00021   1 137.72.43.38   3097        2210      2210     2210        297      297     297 2002/156:18-2002/156:18
TCPIP    T 00023   1 137.72.43.119  3192        8550      8550     8550        352      352     352 2002/157: 8-2002/157: 8
TCPIP    T 00023   4 137.72.43.119  3290      278648    133767    69662       9448     3702    2362 2002/157:13-2002/157:20
AESCYT2  T 03338   1 137.72.43.240    21         149       149      149        562      562     562 2002/157:10-2002/157:10
AESCYT2  T 03349   1 137.72.43.240    21          24        24       24        205      205     205 2002/157:10-2002/157:10
TCPIP    T 00023   1 137.72.43.38   4447       21761     21761    21761        539      539     539 2002/157:18-2002/157:18
TCPIP    T 00023   5 137.72.43.119  3211      240706    179401    48141       6333     4911    1266 2002/158:12-2002/158:17
NPMTCPIP T 05050   1 137.72.43.117  1299           0         0        0         78       78      78 2002/158: 9-2002/158: 9
FTPD1    T 00021   1 137.72.43.119  3334        1134      1134     1134        166      166     166 2002/158: 9-2002/158: 9
NPMTCPIP T 05050   1 137.72.43.117  1266           0         0        0        112      112     112 2002/158: 9-2002/158: 9
NPMTCPIP T 05050   1 137.72.43.117  1298          74        74       74         78       78      78 2002/158: 9-2002/158: 9
NPMTCPIP T 05050   1 137.72.43.117  1383           0         0        0         78       78      78 2002/158:10-2002/158:10
FTPD1    T 00021   1 137.72.43.119  3655         911       911      911        121      121     121 2002/158:13-2002/158:13
FTPD1    T 00021   1 137.72.43.119  3601        1469      1469     1469        200      200     200 2002/158:13-2002/158:13
```

Figure 34. Workload Sessions Report – Sample Output

The fields in the Workload Sessions Report are:

Name	Session identifier by TCP/UDP application name.
T	Type of protocol (TCP/UDP).
LPort	The local port from which the connection was made.
Cnt	The number of observed sessions during the specified time period.
FIP	The foreign IP address to which the connection was made.
FPort	The foreign port to which the connection was made.
BOut Total	The total number of bytes sent out for observed sessions during the specified time period
BOut Max	The highest number of bytes sent out per session during the specified time period.
BOut Avg	The average number of bytes sent out for observed sessions based on all intervals in the specified time period.
Total BIn	The total number of bytes received for observed sessions during the specified time period.
BIn Max	The highest number of bytes received per session during the specified time period.
BIn Avg	The average number of bytes received for observed sessions based on all intervals in the specified time period.
Duration	The specified time period the session was observed in Julian format. For example, if you specified a time period from February 3, 2002 at 12 noon till February 3, 2002 at 8 pm, the time period would display as 2002/034:12 – 2002/034:20.

(This page intentionally left blank.)

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.

<table>
<tr><td colspan="2">CUSTOMER ID:</td><td></td></tr>
<tr><td colspan="2">CUSTOMER NAME:</td><td></td></tr>
<tr><td colspan="3">PROBLEM DESCRIPTION:</td></tr>
<tr><td colspan="3">ERROR CODE / MESSAGES: (or SYSTEM ABEND CODE)</td></tr>
<tr><td colspan="3">ERROR MODULES TRACEBACK (if presented)</td></tr>
<tr><td colspan="2">TIVOLI
VERSION/RELEASE LEVELS:</td><td></td></tr>
<tr><td colspan="3">SYSTEM INFORMATION VERSION/RELEASE LEVELS:</td></tr>
<tr><td>Host
OS/390</td><td>Browser:
Netscape
Internet Explorer</td><td>Web Server:
Operating System:
Server software:</td></tr>
</table>

(This page intentionally left blank.)

Appendix A: Starting BatchPR with the JCL Submission Utility

Although batch jobs are frequently scheduled to run on a regular basis with the aid of an automation service using the skeleton JCLs provided with NV4IP, the BatchPR Interactive JCL Submission Utility can also be used for both BatchPR for Network Performance/BatchPR for Workload Analysis utilities.

Configuring

You must first configure the BatchPR Interactive JCL Submission Utility before you can use it. Perform the following steps:

1. Make a copy of the AESLIBDF member in SAEDCLIB and save it with a different name. For example, save it as "RUNBPR".
2. Edit the RUNBPR member by supplying a high-level qualifier for the library and save it.
3. It is recommended that you put the edited RUNBPR member into a dataset on the SYSPROC/SYSEXEC search chain.

Invoking

To invoke the BatchPR JCL Submittions Utility using the RUNBPR member, perform the following steps:

1. Do one of the following:
   - If RUNBPR is on the SYSPROC/SYSEXEC search chain, enter:

     ```
     TSO RUNBPR
     ```

   - If RUNBPR is not on the SYSPROC/SYSEXEC search chain, follow the TSO/ISPF convention:

     ```
     TSO EXEC {FULLLIBRARYNAME}(RUNBPR)
     ```

(This page intentionally left blank.)

Index