GC32-0761-02

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

Tivoli software

Fifth Edition (August, 2002)

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

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 as FTP, SMTP, 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 a knowledge of the MVS TCP/IP transaction environment.

How to Use This Book

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

WHAT IS NV4IP?

This introductory section gives a brief description of NV4IP's architecture, features, functions, requirements, and operation.

GETTING STARTED – A QUICK TOUR

Getting Started offers a guide to quickly familiarize yourself with the product's features and functions.

USING NV4IP

Using NV4IP provides basic information on using NV4IP, including user access, starting/stopping the application, online help, changing hosts, and report formats.

SETTING UP THE MASTER

Setting Up the Master provides information about logging on, security information, and defining critical resources.

SYSPOINT HOME PAGE

Syspoint Home Page provides detailed information about SysPoint, the prmary entry point into the NV4IP multi-Host Monitoring application. The SysPoint Home Page provides an overview of network activity for Operations, Systems, and Network staff.

ALERTS

Alerts provides comprehensive information on how to view Alerts data in both the Alert Summary and the Alert Detail Report screens for the six types of Alerts displayed in the SysPoint screen: CSM Buffer, Link, Port, Session, Critical Resource Availability, and Critical Resource Performance.

LINKVIEW

LinkView provides comprehensive information on how to use the LinkView feature to monitor channel processors in real time for TCP/IP and how to access the Thru24 for IP Link report to view throughput information for channel-attached devices in *near time*.

CONNECT EXPERT

Connect Expert provides detailed information on how to use the Connect Expert feature and its Port Workload/UDP reports to monitor sockets and session connectivity for TCP and UDP (non-EE) in real time. This section also explains how to access the Enterprise Extender (EE) Expert report from Connect Expert to view the current EE UDP workload by EE assigned ports.

STACKVIEW

StackView explains how to view CPU usage for address spaces associated with a selected TCP/IP address space, trend graphs for a particular address space, and comparison graphs of all address spaces at any point in time.

REAL-TIME REPORTS

Real-Time Reports explains how to obtain reports about real-time network response time between enterprise hosts and any other TCP/IP connection, real-time workload information for the enterprise TCP/IP hosts, and workload/network performance trending in real time. This section also explains how to access the Enterprise Extender (EE) Expert Report, which provides real-time network data for the current UDP workload by EE assigned ports.

REAL-TIME MONITORING

Real-Time Monitoring provides information on using the Performance, Telnet, and LinkView monitors to determine response time and availability of servers, routers, desktops, links, channel-attached processors, and Telnet sessions as they occur per IP device.

SESSIONLOG EXPERT

Session Log Expert focuses on how to view *near time* or current time FTP, Telnet, and API sessions.

SNMP MIB BROWSER

SNMP MIB Browser provides information about using the SNMP Browser, which provides a list of the public and private MIBs available in NV4IP and allows you to view the MIBS and any related information. This section explains how to track logical gateway activities and monitor both TN3270 and TN3270E server configuration setups and real-time operational status. It also provides information on obtaining reports for processor utilization, physical PCI bus utilization, and ethernet port diagnostics through OSA Express.

HISTORY REPORTS

History Reports provides information on obtaining sample-based trending and historical reports for TCP/IP through reporting on workload, usage, and response time. This section also provides information on obtaining interval-based throughput summaries of IP to channel links and Enterprise Extender's assigned UDP ports. It also covers the use of session-based reporting on FTP clients/servers, Telnet clients/servers, and API socket-based applications through their respective Expert functions.

COMMANDS

Commands concentrates on how to submit commands in order to monitor hop-to-hop response time, diagnose network problems, display shared storage, OSPF and RIP configuration and state information, and view all route table configurations or obtain information about a particular route. Available commands include Netstat, TraceRoute, RTPS Route Study, Ping, D NET,APING, VTAM, Storage, OSPF, RIP, Route Table, and OMVS USS (UNIX System Services). Master and Operations Manager users have full command authority. Performance Manager users are authorized to issue display commands only.

APPENDICES

The appendices provide information on TCP Connect States, FTP Replies, Sample Member BCONF00, and Report/Graph options.

(This page intentionally left blank.)

TABLE OF CONTENTS

(This page intentionally left blank.)

LIST OF FIGURES

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 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.

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 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, 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 JCL. The reports focus on two aspects of the network performance: response time and availability. 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?

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

NV4IP Server Components

NV4IP provides a browser-based user interface, which is provided on the installation CD. A NV4IP user has immediate access to the health of their network for their business enterprise through SysPoint, the primary entry point to the application.

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

The browser is the display platform and runs on any operating system platform that supports Netscape Navigator 6.2 or 7.0 or Microsoft Internet Explorer 5.5 or 6.0. 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 Master application determines who gets monitored and how frequently. It is recommended that one Master application be set up per installation. The Master performs all configuration and administrative tasks. It is 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 granularities: 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 Home Page Introduction

The SysPoint Home Page is the primary entry point into the NV4IP multi-Host Monitoring application. To access SysPoint, you must first logon to the Host running the Monitor. Once Logon is achieved, information from all host(s) running an MVS TCP/IP address space on a Monitor is retrieved. You must have at least one Host Monitor specified to be able to access data. The SysPoint Home Page displays the Stack Name and IP address for each active Host with its associated Alerts, workload for that stack, channel links status, and connection data for Listeners and Sessions. It also displays the Stack Name and IP address of any inactive Hosts (if you have added multiple Hosts).

Alerts Overview

The SysPoint Home Page provides both summary and detail data on Alerts by clicking in any Alert column. Current Alerts display 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 displays Alerts regarding the most recent occurrence, the last occurrence, and Alerts that have occurred since midnight; the second displays relevant data for the selected Alert. Alerts for Critical Resource Availability and Performance are set in the Master on the PC Workstation. All other Alerts are set on the Host in the CONF00 member.

LinkView Overview

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 Overview

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.

NV4IP Modules

NV4IP has these modules:

- Master
- Performance Manager
- Operations Manager

Master Module Overview

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 parameters for your network (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
- View Performance/Availability Alerting

Performance Manager Module Overview

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:

<table>
<tr><th colspan="2">Real-Time Tab</th></tr>
<tr><td><b>Real-Time</b></td><td>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.</td></tr>
<tr><th colspan="2">History Tab</th></tr>
<tr><td><b>Base History Reports</b></td><td>Provides workload, peak/valley, and response time reports for performance and workload historical data.</td></tr>
<tr><td><b>Thru99 EE History</b></td><td>Allows you to view interval-based throughput summaries of EE UDP data by port.</td></tr>
<tr><td><b>Thru99 Link History</b></td><td>Allows you to view interval-based throughput summaries of UDP IP data by port.</td></tr>
<tr><td><b>API Expert</b></td><td>Provides both global and detailed views of API activity. Reports are available in two catagories: address (activity based) and application based.</td></tr>
<tr><td><b>FTP Performance Expert</b></td><td>Provides both global and detailed views of FTP activity. Reports are address based, data set based, and failure based.</td></tr>
<tr><td><b>Telnet Expert</b></td><td>Provides both global and detailed views of Telnet activity. Reports are available in two catagories: address (activity based) and application based.</td></tr>
<tr><td><b>VTAM Buffer Pool Reports</b></td><td>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</td></tr>
<tr><td><b>CSM Buffer Pool Reports</b></td><td>Provides both global and detailed views of Communications Storage Manager (CSM) buffer pool activity. Reports are available in two categories: usage and Alerts.</td></tr>
</table>

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 Module Overview

Within NV4IP, there is a grouping of functions that are operational management in nature. This group is called 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: WebShpere 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.

(This page intentionally left blank.)

Customer 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	**Browser**:	**Web Server:**
OS/390	**Netscape** Internet Explorer	Name and model

(This page intentionally left blank.)

Getting Started

This guide assumes the following steps have been successfully completed:

1. Host Monitor is installed and operational.
2. Java servlets are installed and running on a Web server.
3. User ID and password have been entered correctly. The user ID and password you enter are determined by the security options selected during installation. If the RACF security option is being used, enter your existing user ID and password. If the NV4IP security option is in use, the default user ID and password are:

   User ID: TCPIP
   Password: TCPIP

If these steps have not been completed, do not proceed any further. Please contact Tivoli's 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 install the product and become fully operational. Customer Support will assist you with problem resolution, information on product enhancements, and tips/techniques for the most effective use of the product.

Operating Environments

Depending on the operating environment, the steps you take may be different. This guide is only a suggested approach to acquainting yourself with the product's features and functions. Start with the first step that applies to your working environment and continue from there. Skip those steps that do not apply to your setup. Once you have completed this guide, continue with the appropriate tasks for monitoring and tuning your TCP/IP network. If you need assistance in this area, please contact Tivoli. Technical and customer support is available for both on-line and on-site, in-depth consultations.

How to Begin

You may want to run through the various product functions, first on a test system with a light workload, then on a production system. To do this, complete the following operations for each system:

1. See the overall system health of your network by reviewing performance and tracking the status of any Alerts from SysPoint (all users).
2. View EE UDP workload data as well as UDP (non EE) and active TCP Listeners and Sessions in real time with the Connect Expert (all users).
3. Use StackView to monitor CPU Usage (Master/Operations Manager users).
4. Execute Commands (Master/Operations Manager users).
5. Run Real-Time Reports (all users).

6. Perform Real-Time Monitoring (Master/Operations Manager users).
7. Show SNMP MIB Browser capability (Master/Operations Manager users).
8. Show SNMP MIB Browser for CISCO CIP or IBM 2216 (Master/Operations Manager users).
9. Run the History Reports (Master/Performance Manager users).
10. View SessionLog data (Master/Performance Manager users).

For each function, see the associated section. Once the product has been moved to a production system (to obtain more data), other factors to consider include the following:

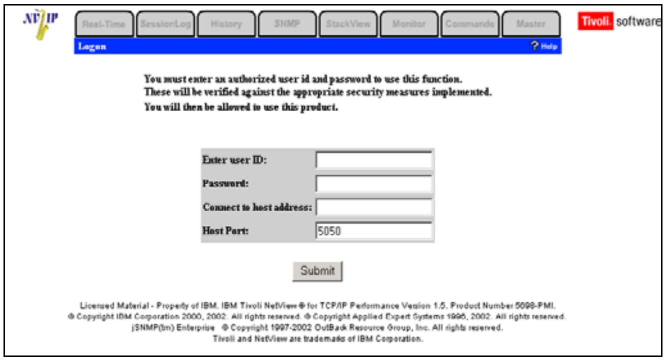
- Which critical resources to monitor in a production mode
- How much data to keep in the VSAM files for long-term trending and capacity planning

Logging on to NV4IP

To begin using NV4IP you must first log on. You need access to a supported browser, such as Internet Explorer or Netscape Navigator (see Product Requirements Section), and the IP address or name of the server on which the NV4IP Java servlets are running. The Monitor on the host must be running to collect the data for analysis.

To start NV4IP, complete the following steps:

1. Launch your browser.
2. Enter the server identifier for the server on which NV4IP is running in the address box. You must use either the IP address or server name, depending upon the information entered in the configuration file during installation. For example, enter http://{ip_address/server name}/nvip/jsp/logon.jsp. The login page appears.



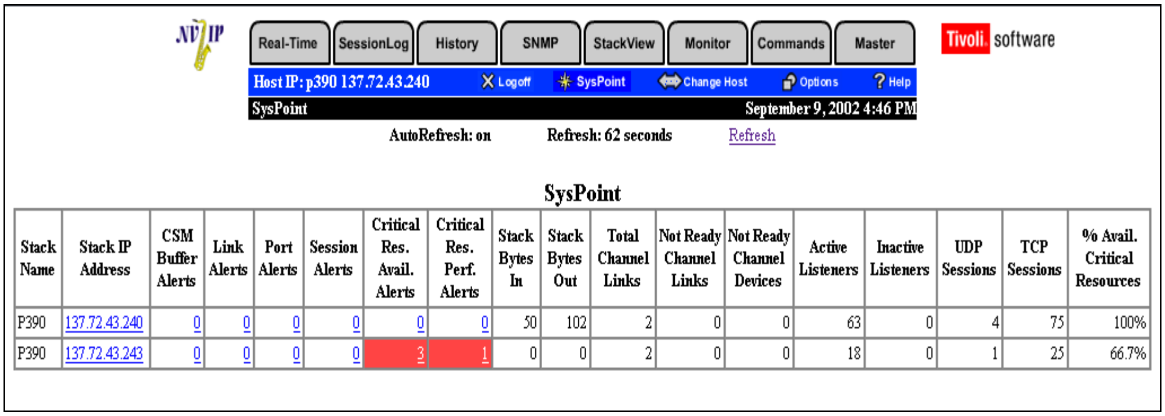
You must enter an authorized user id and password to use this function.
These will be verified against the appropriate security measures implemented.
You will then be allowed to use this product.

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.

3. Enter your existing user ID and password, if using an SAF security package, or the NV4IP defaults if running the NV4IP security option.
4. Enter the IP address for the host.
5. Enter the designation for the host port. The default is 5050.

6. Click Submit. The SysPoint Home Page appears.



Host IP: p390 137.72.43.240

SysPoint September 9, 2002 4:46 PM

AutoRefresh: on Refresh: 62 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	137.72.43.240	0	0	0	0	0	0	50	102	2	0	0	63	0	4	75	100%
P390	137.72.43.243	0	0	0	0	3	1	0	0	2	0	0	18	0	1	25	66.7%

The navigation tabs that appear on the top of each screen vary depending upon the level of access authorized by your User ID. SysPoint serves as the NV4IP home page. To return to this page at any time, simply click the SysPoint button in the menu bar under the tabs at the top of the screen.

The complete listing of tabs is shown below:

Navigation Tabs	Functions
Real-Time	Select from a variety of Real Time Reports, in graphic and tabular format, for response time, applications, clients, and workload in terms of bytes transferred and sessions.
SessionLog	View "near time" or current time sessions for the FTP, Telnet and API events.
History	View customizable History Reports, in tabular or graphical format, including: application usage per session, bytes sent and received by application, top clients by bytes, network response time, global and detailed views of FTP transactions by activity, data set, or failures. Also view interval-based throughput summaries for EE and IP UDP data, API or Telnet historical activity, and critical shared storage functions: VTAM buffer pool and CSM.
Thru99 EE History	Interval-based throughput summaries for Enterprise Extender (UDP-based) data traffic by port.
Thru99 Link History	Interval-based throughput summaries for TCP/IP data traffic to/from IP channel links.
SNMP	Shows public and private MIB information in tabular and graphic formats, including the following: IP, ICMP, UDP, TCP, Interface, CISCO CIP, and OSA Express. Reports are available for processor utilization, physical PCI bus utilization, and Ethernet port diagnostics.
StackView	Evaluate CPU usage of your TCP/IP address spaces and any socket-attached application address spaces that are currently running.
Monitor	Access Real-Time Monitoring for response time, availability, Telnet, and channel devices.
Commands	Enter a variety of commands (depending upon user authorization) to diagnose problems and control network activity while within NV4IP. Commands are available in the following categories: Route Display, Route Diagnostic (for IP, EE, and HPR), USS (UNIX System Services), D OMVS, and Communication Server.
Master	Add critical resources to be monitored. Set monitoring parameters, such as frequency and packet size. Check the status and parameters of monitored devices or hosts.

SysPoint Home Page Introduction

SysPoint is the primary entry point into the NV4IP multi-Host Monitoring application. SysPoint displays the Stack Name and IP address for each active Host with its associated Alerts, workload for that stack, channel links status, and connection data for Listeners and Sessions. If you added multiple Hosts and any of them are currently inactive, the Stack Name and IP address for each display with a message that the Host is inactive. The data is displayed in a table for quick reference and provides the ability to drill down by clicking in a cell when further information is needed.

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

From the SysPoint Home Page, you may:

1. View Alerts, both in a Summary showing all Alerts for the current, last, and since midnight time periods and in detail for a selected Alert.
2. View application activity and the connectivity of all your TCP/IP or UDP (non-EE) sessions as well as EE UDP workload in real time through the Connect Expert.
3. View all channel-attached processors and links associated with the TCP/IP stack in real time or access the Thru24 IP Summary/Detail reports for near-time IP throughput information through LinkView (Master and Operations Manager users only).

To drill down from the SysPoint Home Page, complete the following steps:

1. For Alerts, place the mouse cursor in the cell for the corresponding Alert and click. A drop-down menu appears from which either the All Alert Summary or Detail Report for the particular Alert type may be viewed.
2. For Connect Expert and/or LinkView, click the Stack IP Address, then click either Show Connect Expert or Show LinkView from the drop-down menu. LinkView will not display in the drop-down menu if you do not have user authorization to access it.

Connect Expert Introduction

The Connect Expert feature monitors current workload for Enterprise Extender (EE) UDP by port as well as your sockets and the connectivity to all your sessions for UDP (non-EE) and TCP/IP in real time. Zoom in to view details about workload, port, or application by clicking the appropriate hyperlink from each table. Click the EE link in the Enterprise Extender Expert table to open the Enterprise Extender Expert, which provides data for current EE UDP workload by EE assigned port. Click the UDP link in the UDP (non-EE) Sessions table to open the UDP report, which provides UDP (non-EE) workload for non-EE UDP applications. Click the Name or Port link from the TCP Sessions table to open the Port Workload/Port Details reports, in which you can perform functions (depending upon user authorization) such as TraceRoute, Drop, or Ping.

There are two tables related to TCP/IP data: Listeners and TCP Sessions. The Listeners table shows active Listener sessions. A Listener session allows remote ports to connect to the TCP/IP application on the mainframe. The TCP Sessions table shows the active application and the ports on which they are active. Not all applications require Listener sessions. If you do not have a Listener session for a particular application, there may be a problem. Verify your application's design with your System Administrator.

The Enterprise Extender Expert accessed from the EE link in the Enterprise Extender Expert table shows application name, port number, number of bytes in/out, percentage of bytes in/out relative to total bytes being received and sent, and throughput of bytes in/out per second. The report also provides access to the Thru24 Summary and Detail Reports as well as to the D NET,RTPS and D NET,APING commands. See *Enterprise Extender Expert* for more information.

The UDP report accessed from the UDP link in the UDP Sessions (non EE) table shows application name, port number, number of bytes in/out, percentage of bytes in/out relative to total bytes being received and sent, and throughput of bytes in/out per second.

The Port Workload/Port Details reports accessed from the Name or Port links in the TCP Sessions table shows the number of bytes sent/received, the number of sessions, and the number of sessions in a status other than established by port for each application. From the detailed display, you can issue commands (depending upon user authorization) such as TraceRoute, Drop, or Ping by clicking the appropriate hyperlink.

To use the Connect Expert function:

1. Do either of the following to access the Connect Expert screen:
   - From SysPoint, click the Stack IP Address of the Host whose port/application or session activity you wish to view and then click Show Connect Expert.
   - From the Real-Time tab, click Connect Expert from the Workload list.

   a. Do one or more of the following:

      i) Click the EE hyperlink in the Enterprise Extender Expert table to open the Enterprise Extender Expert. The Enterprise Extender Expert provides information about current EE UDP workload for all assigned EE ports in real time.

      ii) Click the UDP hyperlink in the UDP Sessions (non-EE) table to open the UDP report. The UDP report provides detailed session information by Application Name and Port, including the total amount of bytes coming in or going out and the throughput of bytes coming in or going out per second. The UDP report also provides percentage comparisons between the total bytes coming in/going out to the percentage of bytes actually received/sent out.

      iii) Click the Name or Port hyperlink in the TCP Sessions table to open the Port Workload or Port Details report. The Port Workload report provides detailed session information by port and allows you to issue TraceRte or Ping commands. The Port Details report provides detailed session information by application and allows you to issue Drop, TraceRte, and Ping commands.

You can also access the Client Details report by clicking the Foreign IP Address link in the Port Details report to view comprehensive detail information by Foreign IP Address as well as to issue Drop, TraceRte, and Ping commands.

Note: You can also access the Client Details report from the Client Workload report accessed in the Real-Time tab.

iv) To familiarize yourself with the Port Workload/Port Details reports, do the following tasks:

- Click a Name hyperlink in the TCP Sessions table to open the Port Workload report.
- From the Port Workload screen click the View Route hyperlink in the Route Information column to issue a TraceRte command. The Trace Route results display in the TraceRoute screen. When you are finished viewing the results, click the browser Back arrow or the "x" Close Box to return to the Port Workload screen.
- From the Port Workload screen click a Port or IP Address hyperlink to open the Port Details report and view further details. The Port Details report can also be accessed by clicking the Port hyperlink in the TCP Sessions table.
- From the Port Details screen click the Do Ping hyperlink in the Response Time column to ping a device for availability. The Ping results display in the Ping screen. When you are finished viewing the results, click your browser Back arrow or the "x" Close Box to return to the Port Details screen.
- From the Port Details screen click the Drop hyperlink in the Terminate column to drop a session (if required).
- From the Port Details screen click the Foreign IP Address hyperlink to open the Client Details report.
- View the detailed Sessions Report and then click the Route hyperlink in the Route column to perform a Trace Route for the Foreign IP Address. When you are finished viewing the results in the TraceRoute screen, click your browser Back arrow or the "x" Close Box to return to the Port Details screen.
- From the Port Details screen, click your browser Back arrow to return to the previous screen, or click the Connect Expert hyperlink at the top of the report to return to the Connect Expert main screen.
- Click a different Name or Port hyperlink in the TCP Sessions table to view detail information and issue commands in the Port Workload/Port Details/Client Details reports.

2. To exit Connect Expert, do one of the following:

- Click the SysPoint button to return to the SysPoint Home Page.
- Click one of the tabs in the menu bar to monitor other kinds of network information.

StackView Introduction

After working with Connect Expert, proceed to StackView (Master and Operations Manager users only). Use StackView to monitor CPU Usage. It shows the CPU usage of your TCP/IP address spaces and any socket-attached application address spaces that are currently running. To run StackView, complete the following steps:

1. Select the StackView navigation tab from the top of the screen.
2. Make sure that you have set at least one address space at the Host Monitor to be automatically monitored. The TCPMON=(name of address space) parameter is set for the NV4IP started task in high-level.SAEDSLIB(CONF00). Up to eight (8) address spaces can be predefined.

   The initial screen comes up with a table. The column on the left lists address spaces being monitored. The second column lists the port on which that address space has active sessions. The following parameters may be monitored from this page: TCB time, SRB Time, EXCP's, Real Frames storage utilization, HiperSpace time, I/O interrupt processing time, and dispatching priority.

Commands Introduction

Access to the Commands function and the Commands available to you depend upon your user authorization. The Commands function allows the submission of TCP/IP commands on the MVS host selected. These commands allow you to diagnose problems and control activity.

Access the Commands screen by clicking on the Commands tab. With full user authorization, you can execute commands in the following categories:

- **Route Display Commands**
  OSPF and **RIP** to specify dynamic routing protocols and **Route Table** to view Route Table configuration. These commands are implemented with the **OMPRoute** program application.
- **Route Diagnostic Commands**
  (IP): Ping to determine if a resource is available and **TraceRoute** to view TCP/IP route and segment status.
  (EE/HPR): D NET,APING to test network connectivity of EE links or APPN-based endpoints and **D NET,RTPS** to perform a VTAM-based RTP (Rapid Transport Protocol) Route Test across the HPR or RTPS pipe from an EE connection to a specific RTP endpoint.
- **USS Commands**
  D OMVS to display and diagnose OMVS-based settings and associated processes.
- **Communication Server Commands**
  Netstat to check the link, foreign port, client, or socket-attached application status, **VTAM** to display, inactivate, activate, or modify a resource in VTAM, and **Storage** to display shared storage, such as CSM or VTAM buffer pools.

Display Route

The **OSPF** and **RIP** commands used with the OMPROUTE program application provide an alternative to static TCP/IP gateway definitions by implementing dynamic routing protocols. The MVS host running with OMPROUTE becomes an active OSPF or RIP router, or both in a TCP/IP network. Either or both of these routing protocols can be used to dynamically maintain the host routing table. The **Route Table** command allows you to view the Route Table configuration.

The following is an example of issuing an OSPF command:

1. Select DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,ALL.
2. Click Submit. The response to the command appears on the next screen.

Route Diagnostic

Route Diagnostic covers these topics:

- Ping
- TraceRoute
- D NET, APING
- D NET, RTPS

PING

PING is used to diagnose network problems dealing with availability and response time. The PING command sends an echo request to a foreign node to determine if the computer is accessible. When the response to the PING command is received, the elapsed time is displayed. The time does not include the time spent communicating between the user and the TCP/IP address space. There are three PING command formats available: use defaults, change defaults and loopback.

The following is an example using the PING – Use Defaults command format:

1. From the Commands main screen, click the PING hyperlink.
2. Select PING - Use Defaults.
3. Enter the IP address of the host/device to be PINGed in the Name/IP address field. The default Ping parameters send one 64-byte packet with a timeout factor of 10 seconds.
4. Click Submit. The response to the command appears on the next screen.

TraceRoute Command

The TraceRte command sends UDP requests with varying Time to Live values (TTL). It waits for the routers between the local and remote hosts to send TTL exceeded messages. Use it to monitor response time from hop-to-hop and to diagnose network problems.

The following is an example of using the Trace Route – Change Defaults command format:

1. From the Commands main screen, click the Trace Route hyperlink.
2. Select Trace Route - Change Defaults from the drop-down menu.
3. Enter the IP address of the host/device to be tested.
4. Modify the values you wish to change.

   The fields affect the size, number, and timeout limits used to test the availability of the selected device.
5. Click Submit.

D NET,APING

D NET,APING performs a VTAM-based Advanced Peer to Peer Networking (APPN) Ping test from the originating host to the remote host. The D NET,APING command is the VTAM-based equivalent of the TCP/IP Ping command. D NET,APING is used to diagnose APPN availability and response time issues for a specific APPN Transmission Group (TG) that may be defined between two APPN endpoints, or to test network connectivity of Enterprise Extender links.

The following is an example of issuing the D NET,APING command under the Expert-Assist Interface:

1. From the Commands main screen, click the D NET,APING hyperlink. The D NET,APING Command screen displays.
2. From the D NET,APING menu, select either APING – Use Defaults or APING – Change Parameters.
3. Enter the CP or Resource Name. This is a required field.
4. Do one of the following:
   - For **APING – Use Defaults** click the Submit button.
   - For **APING – Change Defaults** change the default values in the appropriate fields and click the Submit button.

   The APING Results screen appears.

D NET,RTPS

The D NET,RTPS Route Test provides the ability to quickly perform a VTAM-based RTP (Rapid Transport Protocol) Route Test across the 'HPR or RTPS pipe' for any Enterprise Extender (EE) connection to a specific RTP endpoint. In most EE environments this endpoint will usually be the same destination as the previously defined VTAM Cross Domain (CDRM) and associated Control Point (CP). The new RTP data transport, however, uses UDP and IP between both endpoints instead of SNA.

The following is an example of issuing the D NET,RTPS Route Test under the Expert-Assist Interface:

1. From the Commands main screen, click the D Net,RTPS hyperlink. The RTPS Command screen displays.
2. From the menu in the RTPS Command screen, select either RTPS Pipe Information or HPR Route Test.
3. Do one of the following:
   - For **RTPS Pipe Information** proceed to Step 4.
   - For **HPR Route Test** enter a Rapid Transport Protocol PU Name (required) in the field provided and proceed to Step 4.
4. Click the Submit button. The RTPS Route Results screen appears.

USS

The system uses USS (UNIX System Services) command D OMVS.

D OMVS

The D OMVS command is a UNIX System Services command used to display and diagnose current OMVS-based settings and associated processes. After you specify the desired display option and the required parameters, submit the command through the target TCP/IP for the MVS host to which you are connected. The D OMVS command is sent directly to MVS to be issued. To view detailed information and explanations for each D OMVS Command, please refer to the IBM MVS System Commands for the appropriate z/OS release.

The following is an example of issuing the D OMVS command under the Expert-Assist Interface:

1. From the Commands main screen, click the D OMVS hyperlink. The D OMVS Command screen appears.
2. From the D OMVS menu, select one of the D OMVS commands. Some D OMVS commands require additional parameters.
3. Click Submit to issue the command. The D OMVS Results screen appears.

Communication Server

Commuication Server uses these commands:

- Netstat
- VTAM
- Standalone command options
- Storage

Netstat

The Netstat command is used to diagnose network problems and control network activity. Access Netstat commands by clicking on the Command tab, clicking the Netstat Submit button, and then selecting the desired command from the Netstat drop-down menu. For most of these commands, simply click the Submit button to view the report. Some commands require you to provide additional information in the fields before clicking the Submit button.

The following is an example of issuing the Netstat command under the Expert-Assist Interface:

1. From the Commands main screen, click the Netstat hyperlink.
2. From the Netstat menu, select one of the Netstat commands. Additional data may be required for certain commands.
3. Click Submit to proceed. The NETSTAT output screen appears. Some additional fields may be required for specific commands.

Note: You can also access Netstat commands by clicking the Gateways button in the LinkView screen. See the LinkView section for more information.

VTAM

VTAM commands may be submitted to diagnose network problems for resources. You may execute Display (D Net), Vary Active (V Net,Act), Vary Inactive (V Net,Inact), or Modify (F Net) commands.

The following is an example using the assisted VTAM command **Display (D Net)**:

1. From the Commands main screen, click the VTAM hyperlink.
2. Select D NET - Display resource from the list of available VTAM commands.
3. Enter the nodename of the device to be displayed in the Nodename field.
4. Click Submit. The response to the command appears on the next screen.

Standalone Command Option

You may also enter commands by explicitly typing in the command yourself. This is the standalone command option. All commands must be prefaced by the actual command name ("D NET", "V NET", or "F NET"). To use the standalone command option, simply enter the command in the space provided and press Submit. The response to the command is shown on the following screen.

Note: You can also access VTAM commands by clicking the VTAM TRLE button in the LinkView screen. See the LinkView section for more information.

Storage

Commands that may be submitted to display shared storage, such as CSM or VTAM buffer pools, include D NET, CSM,OWNERID=All (display CSM usage for all owners), D NET,CSM (display CSM allocations/max used), and D NET,BFRUSE (display VTAM buffer pools).

The following is an example using the storage command **D NET,CSM – Display resource**:

1. From the Commands main screen, click the Storage hyperlink.
2. Select D NET,CSM – Display resource.
3. Click Submit. The response to the command appears on the next screen.

Real-Time Introduction

The Real-Time Reports provide data on current activity that has not yet been placed in the VSAM history files.

The Real-Time reports are divided into three sections:

Workload

Connect Expert
Details Selected Port/Address
Top Application Sessions Graph
Top Application Bytes Graph
Selected Application Session Graph
Selected Application Bytes Graph
Client Workload Report

Performance

Network Health Graph
Response Time Report
Selected Response Time Graph

Enterprise Extender

Enterprise Extender Expert Report

1. Do either of the following to access the Connect Expert Main Page:
   - From the Real-Time Reports screen, click the Connect Expert hyperlink under Workload.
   - From the SysPoint screen, click a Stack IP address and then click Show Connect Expert from the drop-down menu.
     Connect Expert displays the applications and ports currently running, providing a solid basis for learning about application and resource usage in your operating environment.

   Note: In OS/390 V2.5 and above, TCP/IP may show as the name for Telnet.

   a. Do either of the following:
      - If there are no applications running, start some sessions (for example, use TN3270)
      - If there are more than one or two applications running, view the graph function by selecting Top Applications Bytes Graph from the Workload reports list. This report shows the number of bytes and updates continuously.

   b. Select Client Workload from the Workload reports list. Client Workload shows the number of bytes per client coming in and going out using TCP/IP.

Note: In OS/390 V2.5 and above, 127.0.0.1 is the loopback address. The Value Unknown address is assigned to high address values such as 255.255.255.255. These addresses are either UDP traffic or traffic for which the product could not identify an assigned address.

Monitor

The Real-Time Monitor function provides on-line, real-time data regarding your operating environment for devices and applications using the MVS TCP/IP address space. Critical resources must be defined in order to monitor current, on-going activity for availability and performance.

On the initial selection of Performance and Availability Monitoring, start monitoring for no more than 20 resources. This allows you to see how the function works and provides quick update screens. In production mode, if people are monitoring many resources, the PC will most likely be in the Operations Center with Alerts being forwarded to the console.

Before You Begin Real-Time

Before you access the Real-Time monitoring functions, please refer to the following overview:

1. Confirm that critical resources are defined by using the View Resource Definitions function (Master user). If none are defined, use the Add Resource Definitions in the Master module to set up the devices for monitoring.
2. Start monitoring for five to six critical resources. Use the Start Monitoring function in the Master tab to first select the devices to be monitored and then to set Start Monitoring.

   After Start Monitoring has been set, events that occur on the PC are irrelevant. The Host performs the monitoring for Performance and Availability. There are other functions that require the PC to be active, but for the Performance and Availability Monitoring function, the PC may either be turned off or used for another task.

Using the Monitor

To use the Monitor, perform the following steps:

1. Click on the Monitor tab
2. Click the Performance and Availability Monitor hyperlink under Critical Resource Monitors.
   a. View the ratings for the resource(s):
   - a **raining cloud** signifies that the resource is unavailable.
   - a **sun obscured by clouds** signifies that the resource may have exceeded the response time threshold or be experiencing packet loss.
   - a **bright shining sun** signifies that all is well.

   b. Access the Telnet Monitor by clicking the Back button on your browser to return to the Monitor tab main menu and then click the Telnet hyperlink under Telnet Monitor. The Telnet Monitor displays data for Telnet server sessions that are currently active.

   Begin with 200 or fewer sessions. On a production system with many thousands of sessions, use a filter to limit the number of sessions viewed. If all sessions are selected this function can take a lot of time to yield data results.

SNMP MIB Browser Capability

NV4IP reports on the public MIBs and certain private MIBs. Access SNMP MIB Browser by selecting the SNMP tab from any panel. To begin, look at one or two routers in your network. For this function, you need the address of a router and its community name. The product is shipped with the default community name of "public". This name is case-sensitive and must be lower-case. Private MIBs generally have a different community name. If your installation has changed the community name, change the Community Name value to set it to the correct name for your installation.

1. Once you have access to the router MIBs, data displays in the screen and you can view various MIBs by changing the MIB type.
   a. Look at the ICMP MIB to see any errors. Select the checkbox to view changes. This displays current activity. The MIB variables display data from the time the router was brought up, so it is difficult to see exactly when the errors occurred.
   b. Look at the Interfaces MIB. This shows all the interfaces and any activity. When a problem in response time or availability is shown, it is used to determine if an interface may be down, causing congestion or rerouting.
   c. Look at the IP MIB. From this screen, the routing table within the router may be seen.

SNMP MIB Browser for CISCO CIP

If you are using routers with the Cisco Systems CIP card in your network, you may wish to look at some of the private MIBs. For this function, you need the address of a router and its community name. The product is shipped with the default community name of PUBLIC. For private MIBs, this is generally *not* the correct community name. Locate the community name for the router. Contact your system or network administrator for the correct name.

1. Once you have selected the correct community name for the router and have access to the router's MIBs, data will appear on the screen. You may look at some of the other MIB types.
2. Start with the CISCO CIP MIB. This shows the global parameters for the CIP such as total memory, free memory, CPU usage, etc.
3. You may then elect to view more detail by clicking on a selected row. This shows the channels on the CIP.
4. If you are using TN3270 server on the CISCO CIP, view the TN3270 server MIB from the main menu panel. You may then navigate from the server level to the PU and LU levels.

History

The following section will walk you through four of the many History reports available in order to acquaint you with NV4IP. The reports covered here are as follows:

- Client Usage Details report
- Top FTP Users (All Sessions) report
- Total FTP Bytes report
- Response Time for Network report

This is a very rich source of data and you can spend many days exploring and investigating this area. To begin, complete the following steps:

1. Click on the History tab.
2. Click the Base History hyperlink under Workload and Performance. This is the historical version of the real-time report viewed earlier.
    - You can use the Client Usage Details report to see specific usage information for any selected IP address.
    - Use the report to determine which IP addresses to monitor. The clients who appear as top users during real-time monitoring may be good candidates. In production mode, it is recommended that top clients from the historical reports be used.
3. Return to the History tab and click the FTP Performance Expert hyperlink under Expert Reports to view and work with the FTP Performance Expert. If FTP data has been loaded, you may want to look at some of the reports found in FTP Expert. Start with the Top FTP Users (All Sessions) report. If you have done FTPs from the PC to the host, select Include FTP Server when asked what data to view. Otherwise select Include FTP Client. If you do not know, try selecting the server first.
4. Total FTP Bytes - This report shows any large file/data transfers that have occurred for the selected time period. For example, this report may be used to view FTPs that exceed one gigabyte.
    - When asked for minimum bytes, enter a large number if you have data; otherwise, enter a small one just to view how the report works.
    - There are over 20 other reports which analyze FTP performance including Top Data Sets, which allows you to see the most heavily used data sets. This information can assist in optimizing placement of these data sets. Top Failing Addresses shows who is sending failing jobs and what they are.
5. Return to the History tab and click the Base History hyperlink and then select the Response Time for Network report. This report shows how peaks vs. average loads are handled in your network. Often, networks may handle normal traffic well but fail in their handling of bursts or large volumes. By viewing this report, you get a sense of how bad the peaks are. You should have the necessary data for this report if you completed the steps for using the Monitor. To determine a pattern, start with 256 byte packets to determine:
    - What is the average?

- What is the maximum?

  In good networks, sometimes the maximum is 10 times the average. In poorer performing networks, the multiplier may be substantially greater. There have been cases where the maximum has been up to 200 times the average.

SessionLog

The SessionLog Expert allows viewing of "near time" or current time sessions, that is, sessions that are either currently active or have recently happened. The definition of "recently" is determined by the installation and is set in the parameters for the FTP or SMF exits. SessionLog requires that the FTP and SMF exits have been previously installed on the host.

SessionLog divides data into four logs under two categories: FTP and Telnet/API.

FTP	
FTP SMF Log	Provides details on completed FTPs.
FTP Error Log	Subset of the FTP SMF Log that provides detail on FTP errors.
FTP Server Activity Log	Shows commands entered for completed and in-progress FTPs.
Telnet and API	
TELNET SMF Log	Shows the details on Telnet sessions that are completed or are still active. Logon and logoff events are captured.
API SMF Log	Details API sessions that are completed or still active by capturing the initiation and termination events. It includes all socket-attached applications.

To view session logs for FTP, Telnet, or API, complete the following steps:

1. Click on the SessionLog tab.
2. Select the log to view by clicking its hyperlink.
3. If desired, enter selection criteria within the given fields to filter the resulting data. If no filtering is desired, leave all fields blank.
4. Click the Submit button.

Logoff

To logoff from any page, simply click on the Logoff icon in the menu bar below the main navigation tabs. You are returned to the Logon page.

Summary

This introductory tour provides a cross-section of the functions and features available in NV4IP. Please explore other areas according to your operating environment interests and needs. Good luck in successfully monitoring and tuning your TCP/IP network.

This page intentionally left blank.

Using NV4IP

NV4IP views TCP/IP network performance from the enterprise level to the remote user connection. The information that NV4IP gathers reduces the types of software and number of monitoring efforts previously required to try to get a handle on the TCP/IP transaction environment. NV4IP gathers sufficient data to meet all of your reporting requirements and further, provides a data repository facility in SMF data format for your customized reporting needs.

Performance indicators for both workload and response time are reported by time, by application, or by host. Performance Manager uses both historical and real-time reports to provide a complete and accurate picture of network performance. The historical reports integrate the data collected so that problem histories, managerial reporting, and trending can be done from the same database. The real-time reports are used to gather data for monitoring the network in the daily work environment. Real-time monitoring facilities are provided for response time and availability per device; Telnet server sessions, and channel processors. Real-time monitoring facilities are provided for response time and availability per device; Telnet server sessions, and channel processors. These reports are available immediately after the Host Monitor is started.

SysPoint is the primary entry point into the NV4IP multi-Host Monitoring application. SysPoint's main screen provides an overview of network activity for Operations, Systems, and Network staff. The data is displayed in a table for quick reference and provides the ability to drill down by clicking in a cell when further information is needed. SysPoint provides information on Alerts, stack workload, channel activity, and traffic for connections. From SysPoint, LinkView, Connect Expert, or Alerts may be accessed for further information and analysis.

LinkView provides real-time Channel Processor Monitoring. 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. LinkView shows all the channel-attached processors and links associated with your TCP/IP address space on one screen. At a glance, see any device that is unavailable or has exceeded the queue threshold. The LinkView screen also provides access to the Thru24 IP Summary/Detail reports, which provide near-time IP throughput information for channel-attached devices.

Connect Expert allows you to view EE UDP workload for assigned ports or monitor sockets and the connectivity to all your sessions for UDP (non-EE) and TCP. You can access the Enterprise Expert report from the EE hyperlink in the EE table to investigate EE UDP data further, or find out more about UDP (non-EE) session connectivity by accessing the UDP report from the UDP hyperlink in the UDP Sessions table. You can also zoom in to any port/application or session to view details using the Port Workload/Port Details reports accessed from the Name or Port hyperlinks in the TCP Sessions table. From the Port Workload/Port Details reports, you can execute a TraceRoute command to analyze routes, a Drop command to terminate a session, or Ping a device to determine its availability (only Master or Operations Manager users can issue these commands).

SysPoint provides both summary and detail data on Alerts by clicking in any Alert column. Current Alerts display 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 main screen. The Detail data consists of two charts: one shows Alerts regarding the most recent occurrence, the last occurrence, and Alerts that have occurred since midnight; the second chart displays relevant data about the selected Alert. Alerts for Critical Resource Availability and Performance are set in the Master on the PC Workstation. All other Alerts are set on the Host in the CONF00 member.

The SessionLog Expert allows viewing of *near time* or current time sessions, that is, sessions that are either currently live or have recently happened. The definition of *recently* is determined by the installation and is set in the parameters for the FTP or SMF exits. The records for these sessions are held in memory by the monitor executing on the MVS host. The data for the logs comes from exits provided by SMF. For further information on the determination of how many such records to hold, please refer to the Installation Manual.

Other key features include StackView and SNMP MIB Browser. StackView provides CPU usage information for the address spaces associated with TCP/IP (TCP/IP, SNALK, FTP server, and so forth), as well as for any address space associated with a socket-attached application.

SNMP exchanges network information through messages known as PDU (protocol data units). From a high-level perspective, the PDU is seen as an object containing variables consisting of both titles and values. SNMP uses five types of PDUs to monitor a network: two deal with setting terminal data, two deal with reading terminal data, and one, the trap, is used for monitoring network events such as start-ups and shut-downs.

Using the Product

NV4IP helps network operations staff, network support analysts, and system programmers monitor and support the mission-critical TCP/IP based applications. By providing historical data and trending patterns through workload, usage, and response time reports, NV4IP makes SNA and TCP/IP network integration manageable. In order to use NV4IP on multiple browsers, the following steps must be taken:

1. The Monitor must be installed and activated on the MVS host and NV4IP Java servlets must be installed on the Web servers.
2. A User ID and password must be set up for each user by the Master administrative function if NV4IP security is being used. RACF security access is determined on the Host. Individual users have access to the application via their TCP/IP Intranet. The individual user only has access to those applications set up for his/her User ID by either the Master workstation user or the Host Security Administrator.
3. For History Reports modules and some Real-Time Monitoring modules, the host Monitors and critical resources to be monitored must be defined and Alerts must be set by the Master function.

Security Authorizations and User IDs

Each site sets up as many Master and secondary administrative workstations as the site requires. The Master provides default parameters for the frequency and packet sizes settings. Since the Master performs configuration for NV4IP and parameters which may impact the network, access to the Master should be controlled.

The level of security used by NV4IP is determined by the option set in the CONFxxx member of the SAEDSLIB data set during installation. An installation may choose to use either the security authorization provided by NV4IP 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). The available options and their operation are described below:

Security Option	Description
0	NV4IP security authorization. User access depends upon the User ID and password. A Master has access to all modules, an Operations Manager to OM and shared modules, and a Performance Manager to PM and shared modules.
1	SAF User ID and password authorization. A verified user has full access to the Master, Performance Manager, and Operations Manager.
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:

Group name	Description
AESMSTR	Full access to the Master, Performance Manager, and Operations Manager functions.
AESPM	Access to the Performance Manager functions and shared modules. A Performance Manager does not have command authority for Expert Commands.
AESOM1	Access to the Operations Manager functions and the shared modules, with informational command authority for Expert Commands.
AESOM2	Access to the Operations Manager functions and the shared modules, with full command authority for Expert Commands.

Note: For instructions on adding, deleting, or viewing User IDs and passwords, see *Using the Master to Configure the Monitor*.

NV4IP : Security=0

Each PC-based application has a separate User ID and password. You may choose between Master, Operations Manager or Performance Manager User IDs. A Master User ID is able to use any installed NV4IP application modules. An Operations User ID may use any installed Operations Manager modules as well as the shared Manager User ID modules. A Performance Manager ID may use any installed Performance Manager modules as well as the shared Manager User ID modules.

User IDs are saved and validated on the Host. Tivoli supplies one start-up User ID and password for the application. Only Security=0 authorizes adding, deleting, or viewing User IDs.

SAF Security: SECURITY=1

If security is set to the SECURITY=1 option, the User ID and password must be set up by the SAF security administrator on the Host. If the NV4IP user already has an SAF User ID and password, such as for TSO, no further steps are required.

When the user accesses NV4IP, he/she will logon with their SAF User ID. User IDs and passwords are validated by the SAF security application on the Host. Under these circumstances, no User IDs need to be created within the NV4IP application. The User has full access to the Master, Operations Manager, and Performance Manager modules.

SAF Security: SECURITY=2

If security is set to utilize SECURITY=2, the administrator of the security package must authorize the existing User IDs, such as TSO, by connecting them with the appropriate group in the SAF application. These groups are: AESMSTR, AESPM, AESOM1, and AESOM2 as described earlier. A user may be connected to more than one group.

When accessing NV4IP, the user will logon with his/her SAF User ID. User IDs and passwords are validated by the SAF security application on the Host. The User has access to the applications authorized by his/her group membership. Under these circumstances, no User IDs need be created within the NV4IP application.

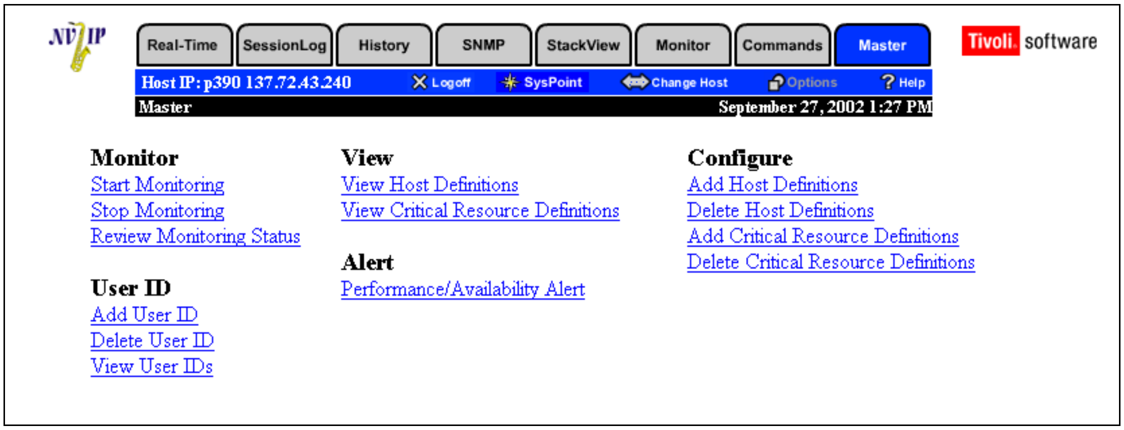


Figure 1. Master User Tab

Note: Access to the User ID function is only available to Master users.

Using SysPoint

SysPoint is the primary entry point into the NV4IP multi-Host Monitoring application. To access SysPoint, you must first logon to the Host running the Monitor. Once Logon is achieved, information from all host(s) running an MVS TCP/IP address space with a Monitor is retrieved. SysPoint displays the Stack Name and IP address for each active Host with its associated Alerts, throughput for that stack, channel links status, and connection data for Listeners and Sessions. If you have added multiple Hosts and any of them are currently inactive, the Stack Name and IP address for each displays with a message that the Host is inactive.

To view further information about the system overview data, select a cell to drill down to investigate Alerts, access LinkView to monitor Channel Processors in real- or near-time, or use Connect Expert to view UDP (EE and non-EE) workload/session connectivity or monitor sockets and connectivity for all socket-attached applications in real time. All three functions are accessed from SysPoint's main screen.

Note: You must specify one Host Monitor the first time you use NV4IP. Use the Add Host Definitions function in the Master module to do this. If there is not at least one Host Monitor specified, you will receive an error message when you attempt to access data from a Host.

Using the Navigation Tabs

After viewing overall network health, move through the product's other major functions by clicking on the navigation tabs at the top of each screen. The tabs you see or are able to access vary depending upon the level of access permitted by your User ID. If you need to use a function that is inaccessible, contact your system administrator. The complete listing of navigation tabs is:

Real-Time	Includes graphs and tabular reports for response time, applications, ports, clients, Connect Expert, workload in terms of bytes transferred and sessions, and workload/throughput data for all assigned EE ports .
SessionLog	Allows viewing of "near time" or current time sessions for the FTP, Telnet and API SMF exits. The progress of an FTP session may also be viewed via the FTP server exits.
History	Includes graphs and tabular reports for sample-based workload and response time, interval-based throughput summaries for Enterprise Extender (UDP-based) data traffic by port and UDP IP to IP/channel link data (tabular only), the API, FTP, and Telnet Experts, CSM usage and alerts (tabular only), VTAM usage and trends for buffer pools, and session-based TraceRoute results (tabular only).
SNMP	An MIB browser and real-time charting function designed to view critical SNMP information in any SNMP capable device. Public MIBs such as

	ICMP, UDP, TCP, IP, Interface as well as CISCO CIP or OSA Express private MIBs may be displayed.
StackView	Shows the CPU usage of your TCP/IP address spaces and any socket-attached application address spaces that are currently running.
Monitor	Allows monitoring for response time, availability, Telnet, and channel devices.
Commands	Allows user-assisted network management command entry. Access to commands depends upon user authorization. Expert assistance is available for commands in the following categories: **Route Display** (OSPF, RIP, and Route Table), **Route Diagnostic** (IP: TraceRoute and PING; EE/HPR: D NET,APING and D NET,RTPS), **USS** (D OMVS), and **Communication Server** (Netstat, VTAM, and Storage).
Master	Used to start/stop monitoring and alerting, view alerts/host/resource definitions, check the status and parameters of monitored devices/applications, add/delete host definitions and add/delete User IDs (with Master authorization).

Menu Bar

The Menu Bar is located immediately below the Navigation Tabs. The buttons located on the Menu Bar may change according to the function you are using. If all of the buttons are available, they provide the functions detailed below:

SysPoint	Return to SysPoint for an overview of the TCP/IP network for all active/inactive Hosts.
Logoff	Logoff the current user ID and return to the main logon page (logon.jsp). The application will be unusable until a valid user ID and password are entered again.
Change Host	Changes the processing host. The processing host is the TCP/IP stack to which commands and requests are routed.
Options	Options is available for specific functions and contains parameters related to the function being performed. For example, you may change the graph type, graph colors, or your workstation's refresh rate using the Options button. See the Appendix D for more information.
Help	Opens a secondary window containing NV4IP online help.

Using Help

On-line Help is available from any screen. Simply click on the Help button in the menu bar below the main navigation tabs. To exit the Help function, click on the Close box on the right hand side of the screen.

Creating a Report

NV4IP provides three types of reports: Real-Time, SessionLog, and History. These reports are available in both tabular and graphical format.

The Real-Time Reports tab provides tabular and graphical reports for data that has not yet been merged into the historical files. Reports are provided for response time, applications, clients, and their workload per bytes transferred and sessions. The Real-Time reports include the Enterprise Extender Expert, which displays workload and throughput data for all EE assigned ports. The Enterprise Extender Expert report also provides access to the Thru24 EE Summary/Detail reports, which provide near-time EE throughput information.

SessionLog provides reports for the FTP server activity/error logs and FTP, Telnet, and API SMF logs in *near real time*. The FTP SMF log displays data for completed FTPs. Information shown includes return code, data set name, data set type, local or remote user ID, and bytes transferred. The FTP Server log displays data for FTPs that are still in progress and completed FTPs. Information shown includes the commands typed in for each FTP during the progress of the session. The Telnet SMF log displays data for Telnet client or Telnet server sessions that are completed or still executing. The API SMF log displays data for socket API sessions that are completed or still executing. Data shown includes application name, foreign port, record type and bytes transferred.

From the Base History reports under Workload and Performance in the History tab, the Workload Reports collect and report information by applications, sessions, bytes sent and received, and top clients. The Base History/Usage Reports show the absolute usage per interval chosen for applications or clients. For an application the report indicates which clients (addresses) were using that application or, for a client, the report indicates which applications the client was using. Data can be viewed in different time slices: month, week, day, or hour. The Base History/Response Time Reports show the times per packet sent for the addresses that are being monitored and for the entire network. The Thru99 EE History and Thru99 Link History reports under Workload and Performance are throughput summaries for Enterprise Extender UDP data by port and UDP IP to IP/channel link data. The Expert Reports category in the History tab provides access to reports for API applications and Telnet as well as the FTP Performance Expert Reports, which provide global network views as well as detailed views of FTP activity by: address, data set, and failures. Reports are also available in the Buffer section for CSM History and VTAM Buffers. The TraceRoute section provides access to the TraceRoute History report, which shows session-based results of the TraceRte command for any defined critical resources which have exceeded their performance threshold parameters.

Starting Reports

Once the steps for using the product have been completed, start viewing Reports by completing the following steps:

1. Enter: http://{server name}/nvip/jsp/logon.jsp where *server name* is the DNS name or IP address where the Java servlets are installed.

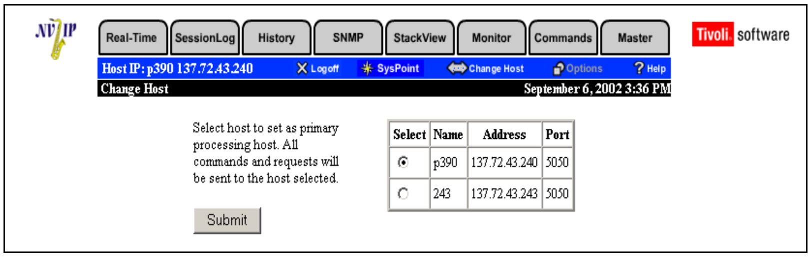
2. Logon on using the appropriate User ID and password for your facility. All fields must be completed. If you are using a security package such as RACF, the User ID must be authorized via that interface.
3. Change Hosts, if desired. While information is always gathered for all hosts, you may only view this information or direct commands to one Host at a time.
4. Select Real-Time, SessionLog, or History by clicking on the corresponding navigation tab at the top of the page.
5. Set any desired options and click the Get Log or Submit button to open the report.

***Note**:* The reporting functions in History and Real-Time are always available via the Real-Time or History tabs. The SessionLog reports require that SMF exits be installed.

Changing Hosts

NV4IP shows reports based on the primary host. The primary host is the TCP/IP stack associated with the IP address used in the Logon page. If you wish to monitor resources associated with a different Host, you must execute a Change Host request. After executing the Change Host command, you are prompted to logon to the system whose resources you wish to monitor. To do this, complete the following steps:

1. Click on the Change Host icon located in the task bar directly below the Commands tab. The Change Host screen appears.



Host IP: p390 137.72.43.240

Change Host September 6, 2002 3:36 PM

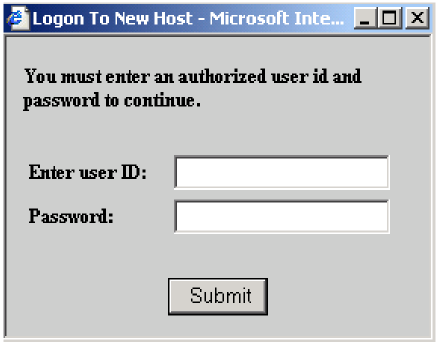
Select host to set as primary processing host. All commands and requests will be sent to the host selected.

Select	Name	Address	Port
●	p390	137.72.43.240	5050
○	243	137.72.43.243	5050

Figure 2. Change Host

2. Use the table on the right to determine which Host you wish to monitor. Select the Host name from the list provided, then click Change Host.(If the desired Host name is not listed, you will need to go to the Master and Add a Host Definition.)

3. You are prompted to enter a user ID and password, which should already have been created for the new host to which you want to change. Enter the required information, then click Submit.



You must enter an authorized user id and password to continue.

Enter user ID:

Password:

Figure 3. Change Host Authorization

4. The following message appears: Host changed to (selected IP address).

5. To continue, please select another function or click the button at the bottom of the page to return to the previous function. Using the browser's back button will interfere with the proper completion of the Change Host Function.

Exiting/Logging Off

To exit a module, complete the step below appropriate to your next task:

- To exit NV4IP entirely, logoff from any page by clicking on the Logoff icon in the menu bar below the main navigation tabs. You are returned to Logon page.
- To return to the SysPoint Home Page, click on the SysPoint button in the menu bar below the main navigation tabs.
- To work on other modules to which you have access, if any, click on the appropriate tab for the desired function.

Setting Up NV4IP

The Master is used to determine who gets monitored and how the host Monitor gathers that data. Each company must determine which critical resources to monitor and whether or how to set Alerts for various parameters. These functions are performed by the Master.

Using the Master to Configure the Monitor

The Monitor collects workload statistics on the TCP/IP MVS transaction environment. It collects workload data on such factors as the number of clients, applications, and network traffic. In addition, the Monitors perform customized traffic tests, set up through the Master, to selected addresses in your network to obtain response time information once monitoring is set up and activated. Up to 1,200 critical resources are monitored by each Host Monitor. Critical resource is used here as a generic term that refers to a host, a client, a server, or any other remote device.

Once you have logged on and entered the User IDs, you are ready to configure the Host Monitors and the critical resources (devices) to be monitored. When the set up is complete, you can begin such tasks as viewing the TCP/IP transaction environment or performing real-time monitoring.

The Master module is used to manage and configure parameters for probing and monitoring network devices. It also controls user access to the application under NV4IP security options as well as for monitoring (addresses, frequencies, and packet sizes for the tests used to collect response time data for the monitored servers).

The following steps are an overview of what you need to do to use the Master to configure the Monitor. These steps will be covered in more detail in later sections:

1. Set up the MVS TCP/IP addresses.
    - Viewing Host Definitions
    - Adding a Host Definition
2. Set up the User IDs and Passwords for each MVS TCP/IP Host environment if NV4IP security is being utilized. (If you are using an SAF security package, the system programmer and SAF Administrator must have set it up during installation.)
3. Set up the Critical Resource Definitions.
    - Viewing Resource Definitions
    - Adding a Resource Definition
4. Start/Stop Monitoring
5. Review the Monitoring Status
6. Set up the MVS Alerts
7. Start/Stop Alerts

Once the Monitor is running on the Host, you are ready to view your workload and response time data or monitor real-time performance/availability and perform command submission to control the MVS mainframe Monitor. ***For workload monitoring, you do not need to take any action from the Master.***

Setting up the MVS TCP/IP Addresses

NV4IP is a browser and Host product. The browser can communicate with multiple Host Monitors. In order to establish initial communication, the browser must know about one Host Monitor. From this Host *seed,* the browser downloads the information about other Host Monitors known to that Host seed monitor.

Note: You must specify one Host Monitor the first time you use NV4IP. Use the Add Host Definitions function in the Master module to do this. If there is not at least one Host Monitor specified, you will receive an error message when you attempt to access data from a Host.

After logging on, click on the Master tab from the navigation tabs at the top of the screen. The Master main screen appears.

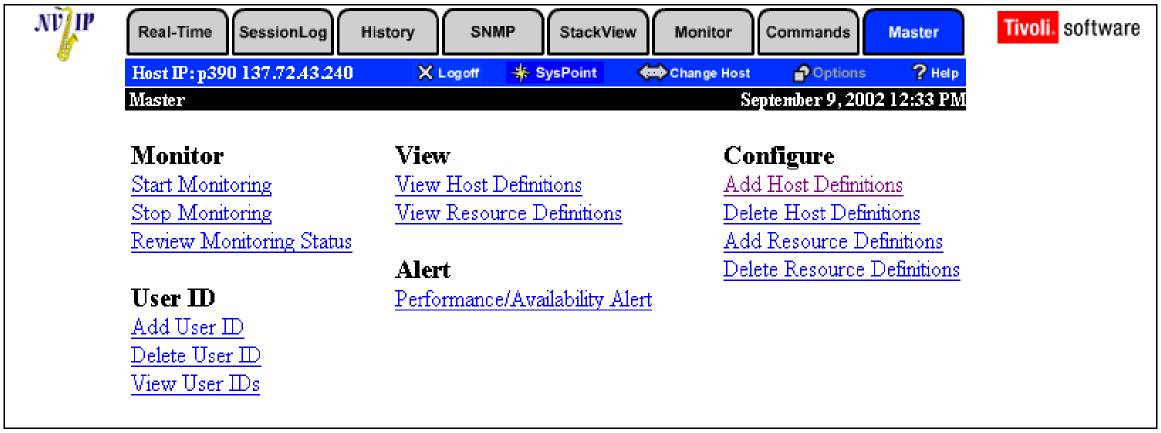


Figure 4. Master Main Screen

The command options available from the Master Selections screen are:

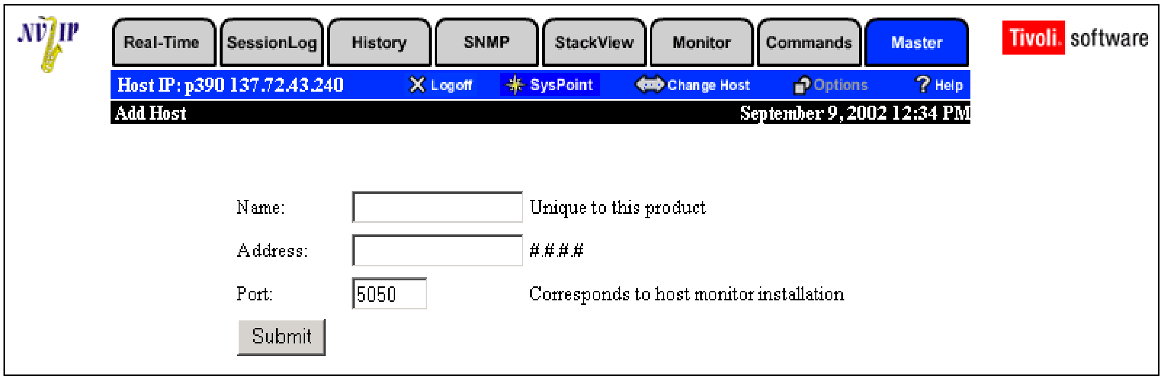
Monitor	Turn monitoring on/off. Verify that the Host Monitor is operating. Review which resources are currently being monitored.
View	Review all critical resource and MVS TCP/IP definitions.
Configure	Add and delete MVS TCP/IP addresses and their corresponding critical resources.
UserID	This option is only available if the Security Authorization set at the Host is NV4IP (Security=0). Add, delete, and view local User IDs and Passwords for NV4IP. These are not RACF User IDs, but particular to this application.
Alert	View MVS performance and availability alerts.

Adding a Host

You must define one Host Monitor for the browser to be able to establish initial communication and download information about other Host Monitors from that initial Host.

To add a Host:

1. Click Add Host Definitions from the Master Selections screen. The Add Host screen appears.



Host IP: p390 137.72.43.240

Add Host

September 9, 2002 12:34 PM

Name: Unique to this product

Address: #.#.#.#

Port: 5050 Corresponds to host monitor installation

Figure 5. Add Host Definitions

The following fields are displayed on the Add Host Definitions screen:

Name	One to sixteen character name for this host Monitor. This name is used internally by NV4IP only.
Address	Enter the Internet Protocol address for this host Monitor. This is the IP address of the MVS TCP/IP on which the Monitor is running.
Port Number	Default=5050. Numerical value, 0 through 65535, assigned to the port as an identifier. This number must match the HOSTPORT parameter that is specified in the MONITOR'S STC PROC. The default name for the STC PROC is AESTCPIP.

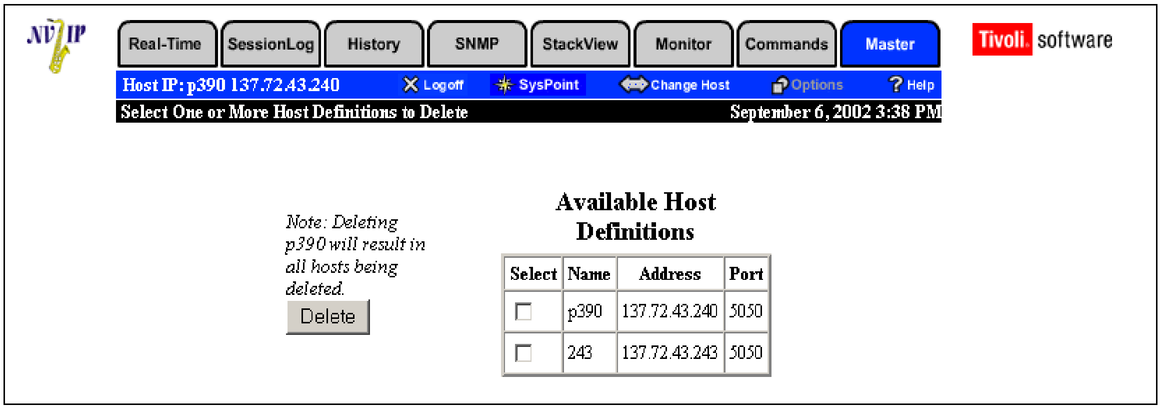
2. For each device to be monitored, complete the required fields and click Submit. The following message appears: Host definition added successfully.
3. Click on the Master tab to return to the Master Selections screen.

Deleting a Host

You must have at least one Host Monitor defined to be able to access data from one or more Hosts, so be sure to either keep one of your currently defined Hosts or to define a new one if you have to delete all of them.

To delete a Host:

1. Click Delete Host Definitions from the Master Selections screen. The Delete Host screen appears.



Host IP: p390 137.72.43.240

Select One or More Host Definitions to Delete

September 6, 2002 3:38 PM

Note: Deleting p390 will result in all hosts being deleted.

Available Host Definitions

Select	Name	Address	Port
☐	p390	137.72.43.240	5050
☐	243	137.72.43.243	5050

Figure 6. Delete Host Definitions

The following fields are displayed on the Delete Host Definitions screen:

Name	One to sixteen character name for this host Monitor. This name is used internally by NV4IP only.
Address	This is the IP address of the MVS TCP/IP on which the Monitor is running.
Port Number	Default=5050. Numerical value, 0 through 65535, assigned to the port as an identifier. This number matches the HOSTPORT parameter that is specified in the MONITOR'S STC PROC. The default name for the STC PROC is AESTCPIP.

2. From the table, select the host(s) to be deleted, then click Delete Host(s). The following message appears: *Resource definition deleted successfully*.
3. Click on the Master tab to return to the Master Selections screen.

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

Setting Up the User IDs and Passwords

User IDs and passwords are setup through the Master only if you are using NV4IP security. You may add, delete, or view User IDs in the Master. Users who do not have the Master on their workstations must have a Master administrator set up their User ID and password.

When the NV4IP application is installed, one default password is supplied with the application software in order to get you started. The User IDs and Passwords set up by the Master administrator are not RACF User IDs. They are verified only by the NV4IP

Monitor as valid for this application. If RACF security is being used, the system programmer must set them up during installation.

If you are using NV4IP's security, the following section provides information on:

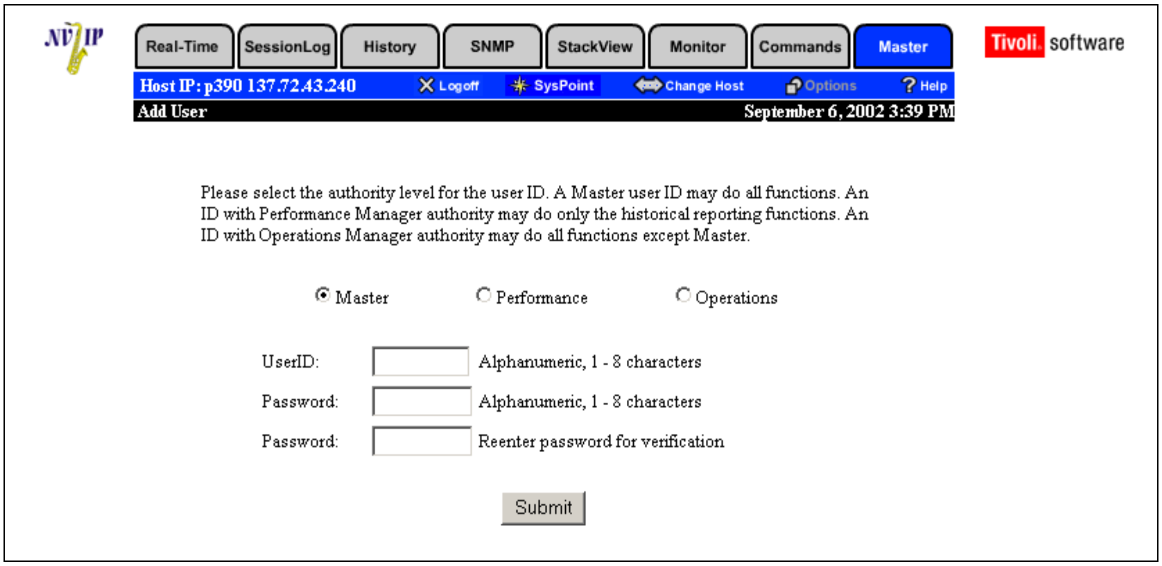
- Adding a User ID
- Deleting a User ID
- Viewing User IDs

For more detailed security information, see *Security Authorizations and User IDs.*

Adding a User ID

To add a User ID, complete the following steps:

1. Select Add User ID from the Master Selections screen. The Add User ID screen appears.



Host IP: p390 137.72.43.240

Add User

September 6, 2002 3:39 PM

Please select the authority level for the user ID. A Master user ID may do all functions. An ID with Performance Manager authority may do only the historical reporting functions. An ID with Operations Manager authority may do all functions except Master.

● Master ○ Performance ○ Operations

UserID: Alphanumeric, 1 - 8 characters
Password: Alphanumeric, 1 - 8 characters
Password: Reenter password for verification

Submit

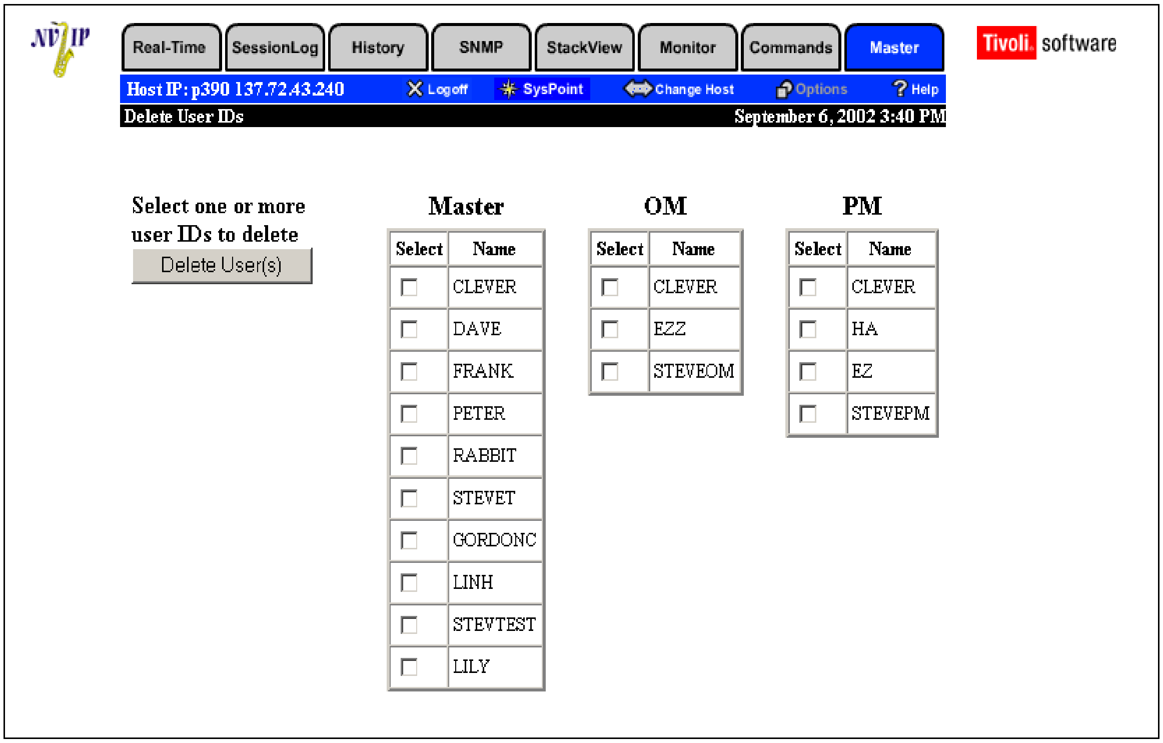
Figure 7. Add a User ID

2. Enter the level of authority: Master, Operations Manager, or Performance Manager.
3. Enter User ID, password, and password verification.
4. Click Submit.
5. The following message appears: *User ID/password added successfully.*
6. Click on the Master tab to return to the Master Selections screen.

Deleting a User ID

To delete a User ID, complete the following steps:

1. Select Delete User ID from the Master Selections screen. The Delete User ID screen appears.



Host IP: p390 137.72.43.240

Delete User IDs

September 6, 2002 3:40 PM

Select one or more user IDs to delete

Master

Select	Name
☐	CLEVER
☐	DAVE
☐	FRANK
☐	PETER
☐	RABBIT
☐	STEVET
☐	GORDONC
☐	LINH
☐	STEVTEST
☐	LILY

OM

Select	Name
☐	CLEVER
☐	EZZ
☐	STEVEOM

PM

Select	Name
☐	CLEVER
☐	HA
☐	EZ
☐	STEVEPM

Figure 8. Delete a User ID

2. Enter a check in the box next to the User IDs from the selected authority levels, you wish to delete.

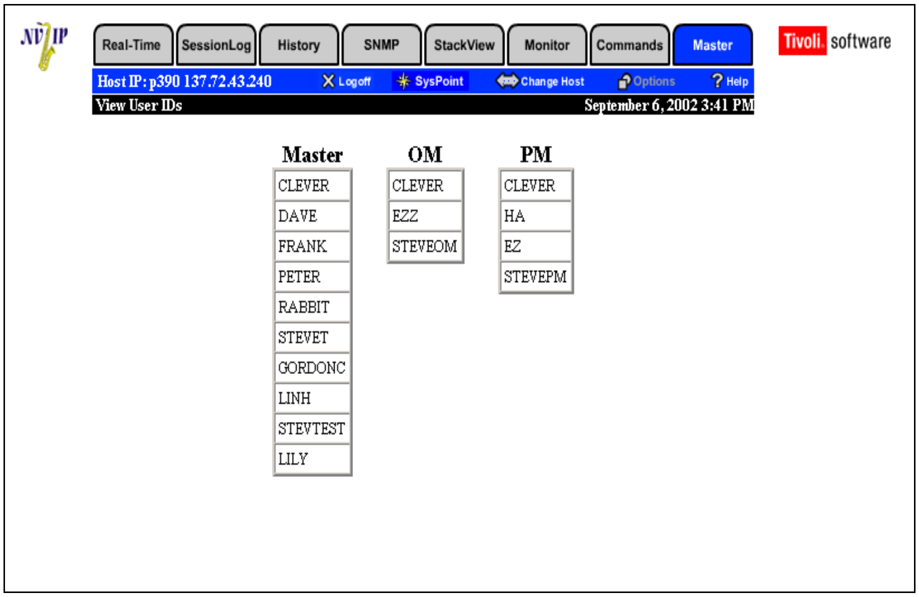
   The following message appears: *User ID/password deleted successfully.*

3. Click on the Master tab to return to the Master Selections screen.

Viewing User IDs

User IDs may be added, viewed, and deleted from the Master application. To view the list of current User IDs and passwords, complete the following steps:

1. Click View User IDs from the Master Selections screen. The list of current users is displayed.



Host IP: p390 137.72.43.240

View User IDs September 6, 2002 3:41 PM

Master	OM	PM
CLEVER	CLEVER	CLEVER
DAVE	EZZ	HA
FRANK	STEVEOM	EZ
PETER		STEVEPM
RABBIT		
STEVET		
GORDONC		
LINH		
STEVTEST		
LILY		

Figure 9. View User IDs

2. Click on the Master tab to return to the Master Selections screen.

Setting up the Critical Resource Definitions

Each Host Monitor tracks up to 1200 critical resources for response time and availability monitoring. As each critical resource is set up, you must determine the interval or frequency at which it is monitored and the packet sizes to be sent for simulating traffic patterns. How these factors are set up is dependent upon network load, peak hours of operation, and the reasons for which you are gathering data. Defaults are provided for both the frequency and packet size. However, these may change based upon your objectives, such as matching particular applications to the devices they use or testing for fragmentation on the network. In addition, you may wish to set Alerts for certain critical resources depending upon the reasons for gathering data.

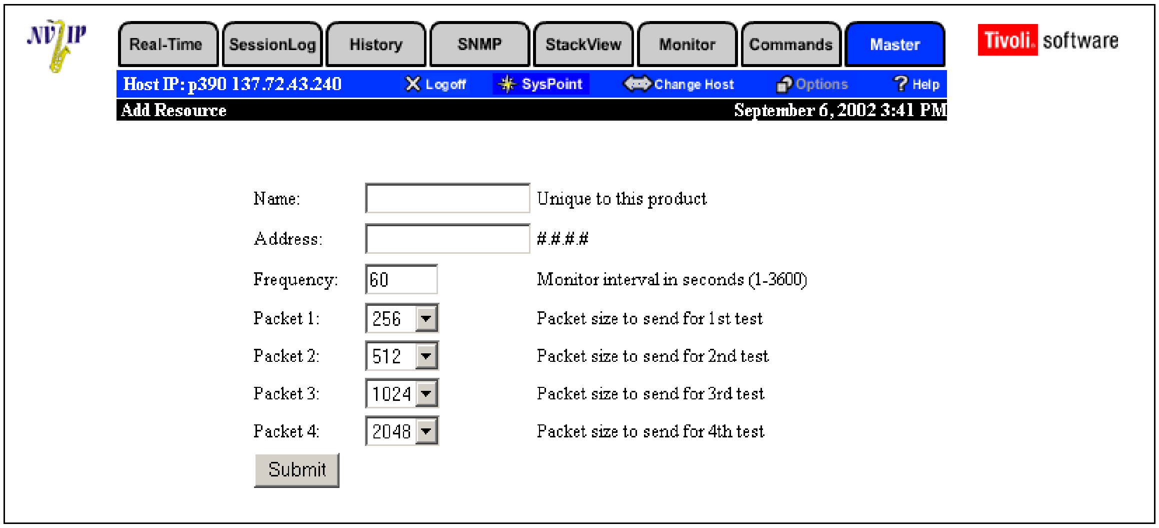
Performance data, real-time and historical, may be accessed without configuring any Critical Resources. Real-Time Graphs and Reports provide information on the top ten clients and current workload as long as the Host Monitor is running.

Add Resource Definitions

To add devices to be monitored, complete the following steps:

1. Click Add Resource Definitions under Configure in the Master tab.

   The Add Resource Definitions screen appears.



Host IP: p390 137.72.43.240

Add Resource September 6, 2002 3:41 PM

Name:		Unique to this product
Address:		#.#.#.#
Frequency:	60	Monitor interval in seconds (1-3600)
Packet 1:	256	Packet size to send for 1st test
Packet 2:	512	Packet size to send for 2nd test
Packet 3:	1024	Packet size to send for 3rd test
Packet 4:	2048	Packet size to send for 4th test

Figure 10. Add Resource Definitions

The following fields are displayed on the Add Resource Definitions screen:

Name	One to sixteen character name for this critical resource. This name is used only internally by NV4IP.
Address	The IP address for this critical resource.
Frequency	The period of time between monitoring tests. Always consider the load on the network in terms of all the critical resources to be set up and how many, at any one time, you wish to actually monitor when setting the timing interval.
Packets #1 - 4	The number of bytes sent in each monitoring packet. The default packet sizes may be modified as required for your operating environment.

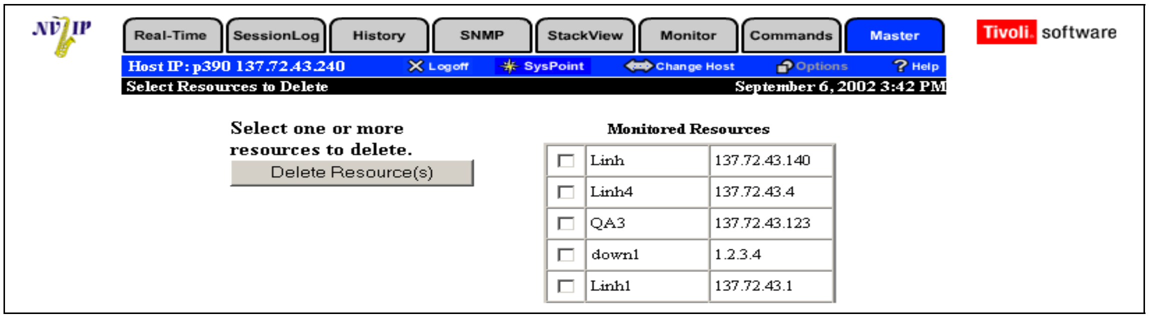
2. Enter the required information for each field for each device to be monitored.
3. Click Submit. The following message appears: Resource definition added successfully.
4. Click on the Master tab to return to the Master Selections screen.

Delete Critical Resource Definitions

To delete devices to be monitored, complete the following steps:

1. Click Delete Resource Definitions from the Configure group in the Master tab.

   The Select Resource to Delete screen appears.



Host IP: p390 137.72.43.240

Select Resources to Delete

September 6, 2002 3:42 PM

Select one or more resources to delete.

Monitored Resources

☐	Linh	137.72.43.140
☐	Linh4	137.72.43.4
☐	QA3	137.72.43.123
☐	down1	1.2.3.4
☐	Linh1	137.72.43.1

Figure 11. Select Resources to Delete

The following fields are displayed on the Delete Resource Definitions screen:

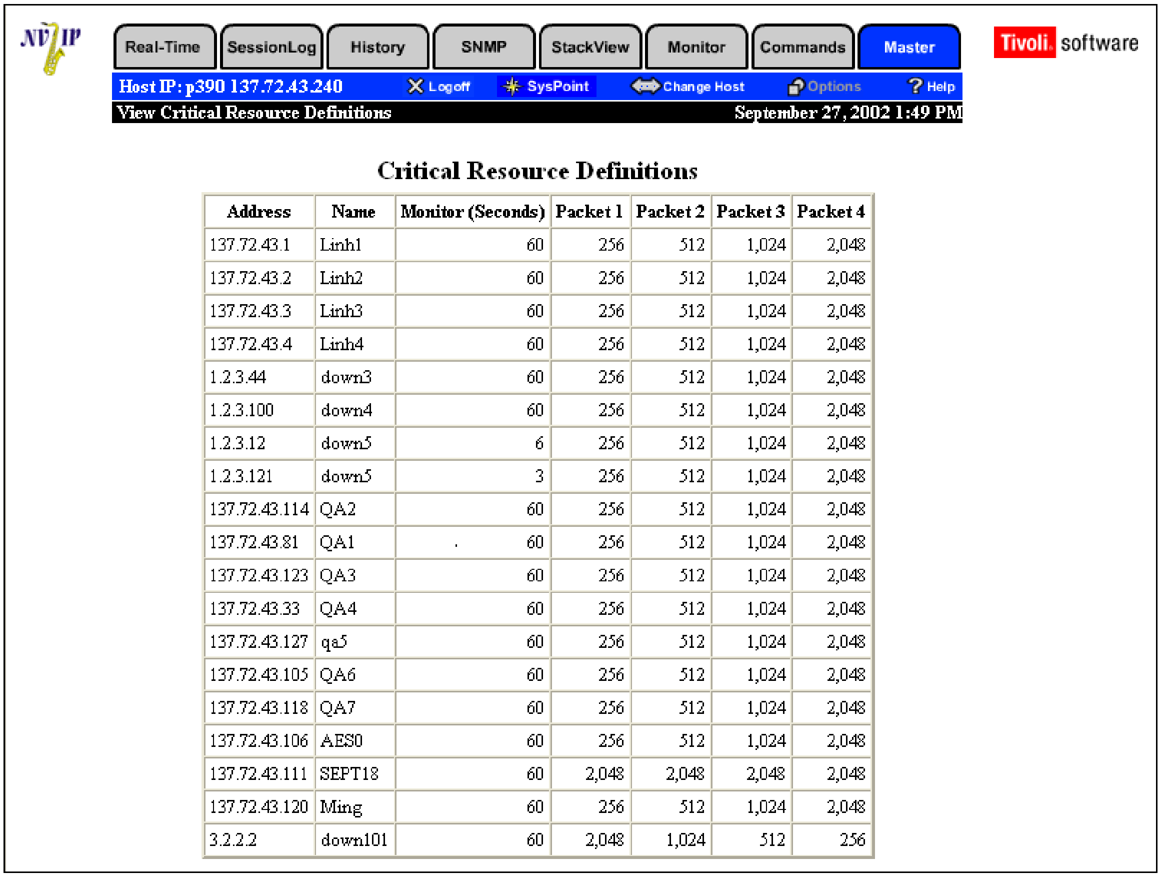
Name	One to sixteen character name for this critical resource. This name is used only internally by NV4IP.
Address	The IP address for this critical resource.

2. From the Monitored or Unmonitored Resources table, check the boxes to the left of the address(es) you wish to delete.
3. Click Delete Resource(s). The following message appears: Resource definition deleted successfully.
4. Click on the Master tab to return to the Master Selections screen.

View Critical Resource Definitions

To view which devices are available to be monitored, complete the following steps:

1. Click View Resource Definitions from the View group in the Master tab.
   The View Critical Resource Definitions screen appears.



Host IP: p390 137.72.43.240

View Critical Resource Definitions September 27, 2002 1:49 PM

Critical Resource Definitions

Address	Name	Monitor (Seconds)	Packet 1	Packet 2	Packet 3	Packet 4
137.72.43.1	Linh1	60	256	512	1,024	2,048
137.72.43.2	Linh2	60	256	512	1,024	2,048
137.72.43.3	Linh3	60	256	512	1,024	2,048
137.72.43.4	Linh4	60	256	512	1,024	2,048
1.2.3.44	down3	60	256	512	1,024	2,048
1.2.3.100	down4	60	256	512	1,024	2,048
1.2.3.12	down5	6	256	512	1,024	2,048
1.2.3.121	down5	3	256	512	1,024	2,048
137.72.43.114	QA2	60	256	512	1,024	2,048
137.72.43.81	QA1	60	256	512	1,024	2,048
137.72.43.123	QA3	60	256	512	1,024	2,048
137.72.43.33	QA4	60	256	512	1,024	2,048
137.72.43.127	qa5	60	256	512	1,024	2,048
137.72.43.105	QA6	60	256	512	1,024	2,048
137.72.43.118	QA7	60	256	512	1,024	2,048
137.72.43.106	AES0	60	256	512	1,024	2,048
137.72.43.111	SEPT18	60	2,048	2,048	2,048	2,048
137.72.43.120	Ming	60	256	512	1,024	2,048
3.2.2.2	down101	60	2,048	1,024	512	256

Figure 12. View Critical Resource Definitions

The following fields are displayed on the View Critical Resource Definitions screen:

Name	One to sixteen character name for this critical resource. This name is used only internally by NV4IP.
Address	The IP address for this critical resource.
Monitor(Seconds)	The period of time between monitoring tests (frequency).
Packets #1 - 4	The number of bytes sent in each monitoring packet.

2. Click on the Master tab to return to the Master Selections screen.

Start/Stop Monitoring

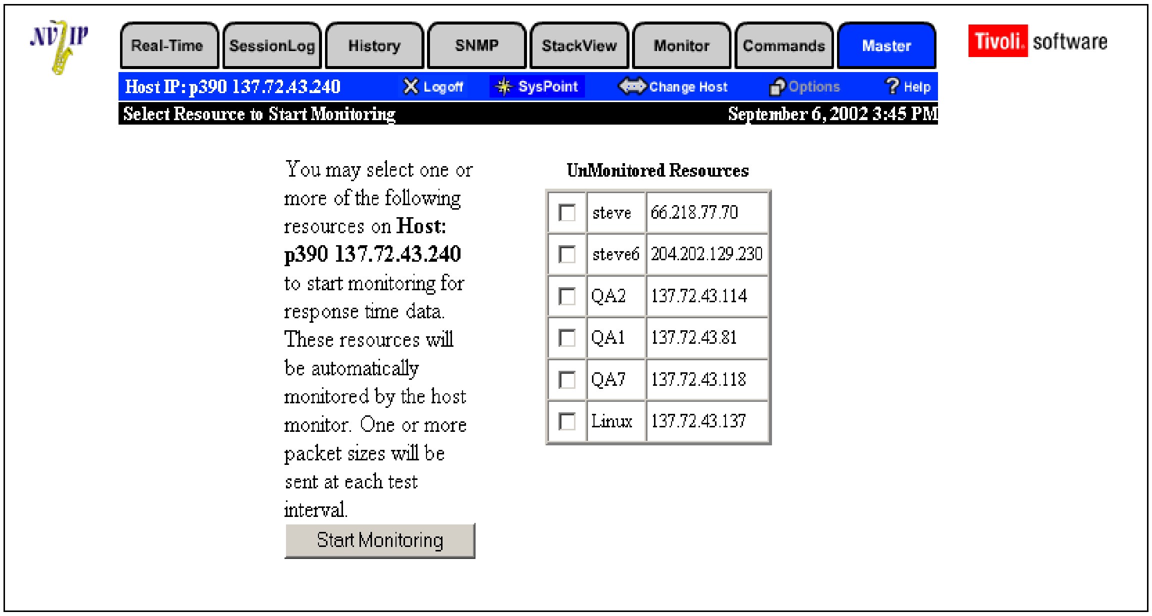
Once the parameters for the TCP/IP components of the network have been set up and NV4IP is active on the Host, you are ready to monitor the network. It may be that only workload data is collected for a period of time until a feel for the network load has been determined. Workload monitoring does not require the Master to execute a Start Monitoring Command. The information collected is written to the NV4IP SMF record type (default: 251) and may be reviewed in the Real-Time Graphs/Reports module. The record contains the IP address of the resource, the packet sizes sent/received, and the round trip response time measured in milliseconds.

Real-time response time monitoring of your network requires that the Master workstation execute a Start Monitoring command. Once monitoring has been turned on, four packets of the size and for the frequency determined by you are sent to the critical resources defined for each Host Monitor. The Start Monitor command need only be done once at the Master for each Host being monitored. SysPoint provides an overview of all Hosts being monitored, and multiple hosts may be monitored simultaneously. Once you select a Stack for further study, only one host can be viewed at a time, so you will need to change Hosts in order to view all results. If you specify AUTOMON=YES in the AESTCPIP PROC, each time the Host Monitor is restarted, it automatically collects performance data for the critical resources that were last being monitored.

Access Real-Time Monitoring to interrogate mission critical application service levels and identify potential performance bottlenecks.

To begin monitoring, complete the following steps:

1. Click Start Monitoring from the Master Selections screen. The Select Resources to Start Monitoring screen appears.



Host IP: p390 137.72.43.240

Select Resource to Start Monitoring

September 6, 2002 3:45 PM

You may select one or more of the following resources on **Host: p390 137.72.43.240** to start monitoring for response time data. These resources will be automatically monitored by the host monitor. One or more packet sizes will be sent at each test interval.

UnMonitored Resources

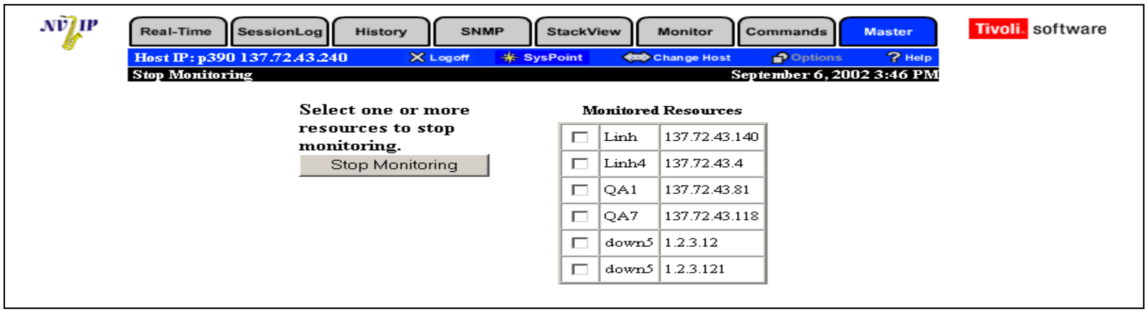
☐	steve	66.218.77.70
☐	steve6	204.202.129.230
☐	QA2	137.72.43.114
☐	QA1	137.72.43.81
☐	QA7	137.72.43.118
☐	Linux	137.72.43.137

Figure 13. Start Monitoring

2. From the table, select the resource(s) you wish to start monitoring by placing a checkmark in the Select column.
3. Click Start Monitoring. The following message appears: *Monitoring started successfully for the resources selected.*
4. Click on the Master tab to return to the Master Selections screen or, to start monitoring on another host, click the Change Host icon in the menu bar.

To stop monitoring, complete the following steps:

1. Click Stop Monitoring from the Master Selections screen. The Stop Monitoring screen appears. (If you are monitoring multiple hosts, you may need to use the Change Host option to access those resources you wish to stop monitoring.)



Host IP: p390 137.72.43.240

Stop Monitoring September 6, 2002 3:46 PM

Select one or more resources to stop monitoring.

Stop Monitoring

Monitored Resources

☐	Linh	137.72.43.140
☐	Linh4	137.72.43.4
☐	QA1	137.72.43.81
☐	QA7	137.72.43.118
☐	down5	1.2.3.12
☐	down5	1.2.3.121

Figure 14. Stop Monitoring

2. From the table, select those resource(s) you wish to stop monitoring.
3. Click Stop Monitoring. The following message appears: *Monitoring stopped*. It may take up to 15 seconds for all activity to stop completely.
4. Click on the Master tab to return to the Master Selections screen.

Setting Up the MVS Alerts

Next you need to determine if any Alerts should be sent directly to the MVS system operators console when certain conditions occur. There are two types of Alerts that may be sent to the MVS operator's console: performance (response time) and availability. Each Alert is started, stopped, or viewed from the Master Start/Stop MVS Alerting pull-down menu. Following is a brief description of each Alert:

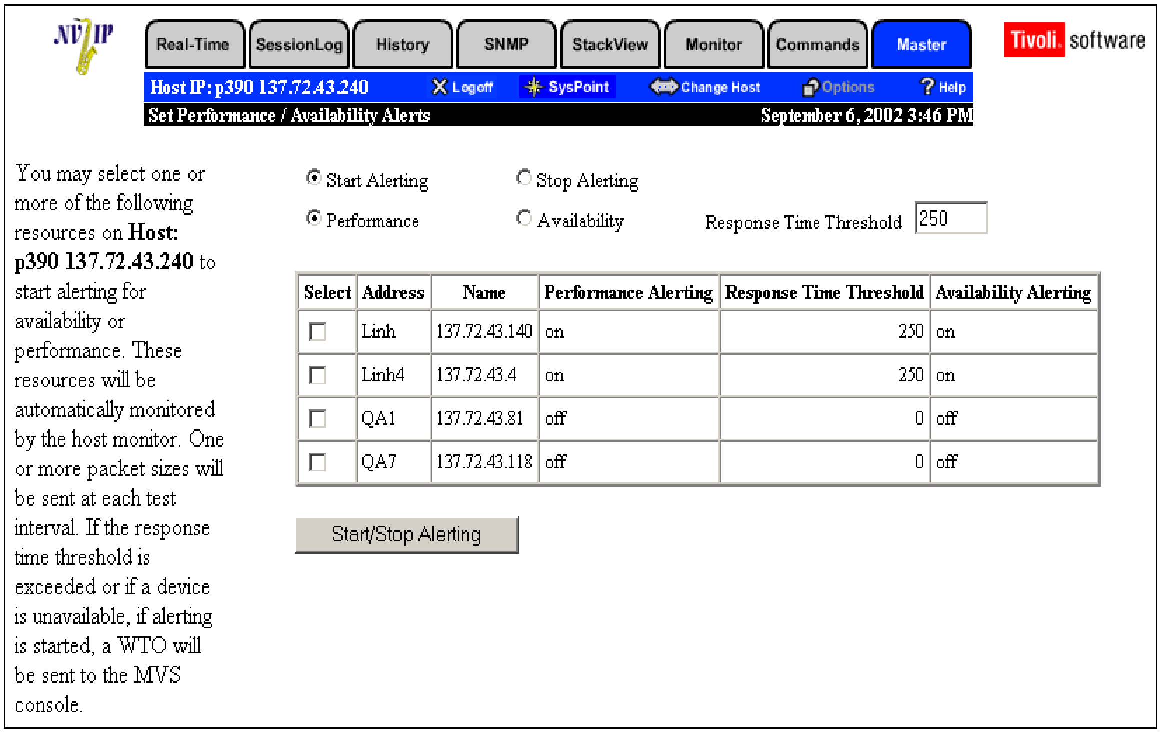
Availability	An Alert to the MVS console may be sent if the address is not communicating with the host.
Performance	The response time threshold is for the customized test sent to collect response time data by the host Monitor.

Setting Availability Alerts immediately informs the Operations staff when a critical resource or other device is not responding. The IP address and the time are given for the non-responding device. Alerting may be set per address through the Master. Alerting occurs if the customized test sent to collect response time data by the host Monitor does not reach its destination.

With Performance Alerts, an Alert may be sent to the MVS console if the response time threshold is exceeded for a device. The response time threshold set is for the customized test sent to collect response time data by the host Monitor. A different threshold may be set per address.

To set the Alerts, complete the following steps:

1. Click Performance/ Availability Alert from the Master tab. The Set Performance/Availability Alerts screen appears.



Set Performance / Availability Alerts September 6, 2002 3:46 PM

You may select one or more of the following resources on **Host: p390 137.72.43.240** to start alerting for availability or performance. These resources will be automatically monitored by the host monitor. One or more packet sizes will be sent at each test interval. If the response time threshold is exceeded or if a device is unavailable, if alerting is started, a WTO will be sent to the MVS console.

● Start Alerting ○ Stop Alerting

● Performance ○ Availability Response Time Threshold 250

Select	Address	Name	Performance Alerting	Response Time Threshold	Availability Alerting
☐	Linh	137.72.43.140	on	250	on
☐	Linh4	137.72.43.4	on	250	on
☐	QA1	137.72.43.81	off	0	off
☐	QA7	137.72.43.118	off	0	off

Start/Stop Alerting

Figure 15. Set Performance / Availability Alerts

2. Select Start Alerting and Performance <u>*or*</u> Availability, enter a response time threshold.

3. From the table, select the address(es) for which you wish to set Alerts.

4. Click Start/Stop Monitoring. The following message appears: *Action successfully completed: Alert Start for* (*Performance/ Availability*).

5. Click on the Master tab to return to the Master Selections screen.

Alerts for one Alert, then repeat the process for the other.

When an Alert is triggered, the following MVS console message is displayed:

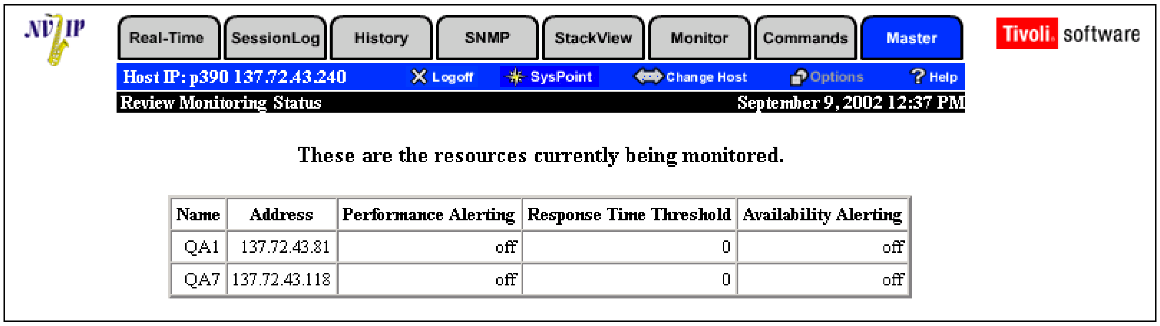
Availability Alert	AES902W IP=[IP Address] NOT RESPONDING TIME=[HH:MM:SS]
Performance Alert	AES901W IP=[IP Address] PK=[Packet Size] RT=[Response Time] TH=[Threshold] TIME=[HH:MM:SS] where PK=packet size in bytes, RT=response time in milliseconds, TH=threshold in milliseconds.

Reviewing Monitoring Status

After you have set up the Host Monitors and determined what critical resources are to be monitored, you may wish to review the configuration. If your environment changes or you find an error after reviewing the options you've set up, return to the Master Selections screen menu to make any necessary changes.

To view which devices are currently being monitored, complete the following steps:

1. Click Review Monitoring Status from the Master tab. The Review Monitoring Status screen appears.



Host IP: p390 137.72.43.240

Review Monitoring Status September 9, 2002 12:37 PM

These are the resources currently being monitored.

Name	Address	Performance Alerting	Response Time Threshold	Availability Alerting
QA1	137.72.43.81	off	0	off
QA7	137.72.43.118	off	0	off

Figure 16. Review Monitoring Status

The fields on the Review Monitoring Status screen are:

Address	The IP address for this Host Monitor (the MVS TCP/IP) on which the Monitor is running.
Name	One to sixteen character name for each device listed. These names are used only internally by NV4IP.
Performance Alerting	Indicates whether a response time or performance Alert has been set for each critical resource listed.
Response Time Threshold	Indicates the target set for an Alert threshold, if any, on each critical resource listed.
Availability Alerting	Indicates whether an availability Alert has been set for each critical resource listed.

2. Click on the Master tab to return to the Master Selections screen.

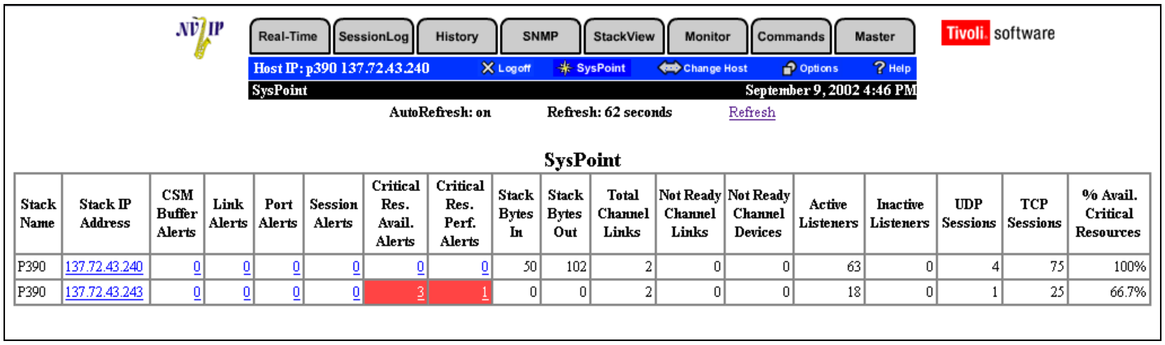
SysPoint Home Page

The SysPoint Home Page is the primary entry point into the NV4IP multi-Host Monitoring application. To access the SysPoint Home Page, you must first logon to the Host running the Monitor. Once Logon is achieved, information from all hosts running an MVS TCP/IP address space with a Monitor is retrieved. The SysPoint Home Page displays the Stack Name and IP address for each active Host with its associated Alerts, throughput for that stack, channel links status, and connection data for Listeners and Sessions. If you have added multiple Hosts and any of them are currently inactive, the Stack Name and IP address for each display with a message that the Host is inactive.

Note: You must have defined one Host Monitor the first time you use NV4IP in order to be able to access Host data.

SysPoint Screen

The SysPoint screen provides an overview of network activity for Operations, Systems, and Network staff. The data is displayed in a table for quick reference and provides the ability to drill down by clicking in a cell when further information is needed. The SysPoint screen provides information on Hosts, Alerts, stack workload, channel activity, and traffic for connections.



Host IP: p390 137.72.43.240

SysPoint September 9, 2002 4:46 PM

AutoRefresh: on Refresh: 62 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	137.72.43.240	0	0	0	0	0	0	50	102	2	0	0	63	0	4	75	100%
P390	137.72.43.243	0	0	0	0	3	1	0	0	2	0	0	18	0	1	25	66.7%

Figure 17. SysPoint

The fields on the SysPoint screen are:

Stack Name	Host name of the TCP/IP stack as defined in the TCPIP.DATA dataset.
Stack IP Address	IP address of the selected host.
CSM Buffer Alerts	There are two types of Buffer Alerts: • Low Availability • High Usage
Link Alerts	Total count of Alerts sent during the current time period for channel links found in a Not Ready state for the channel device or link and/or for exceeding the queue size.

Port Alerts	Total count of Alerts sent during the current time period for unavailable ports.
Session Alerts	Total count of Alerts sent during the current time period for applications/sessions that have exceeded the threshold values for throughput, data size, and/or hung sessions.
Crit. Res. Avail. Alerts	Total count of Alerts sent during the current time period for Critical Resources that were unreachable (Ping command timed out).
Crit. Res. Perf. Alerts	Total count of Alerts sent during the current time period for Critical Resources that exceeded the value set for acceptable response time when the device was defined in the Master.
Stack Bytes In	Total number of bytes received by this connection since the last sampling interval.
Stack Bytes Out	Total number of bytes sent by this connection since last sampling interval.
Total Channel Links	Count of all the channel-attached processors and links associated with the selected TCP/IP address space for the current time period.
Not Ready Channel Links	Count of those channel links showing a status of Not Ready.
Not Ready Channel Device s	Count of those channel processors showing a status of other than Ready. These states could be any of the following conditions: Starting, Sent SETUP request, Enabling, Connecting, Connecting2, Negotiating, Deactivating or Not Ready.
Active Listeners	A Listener session is established and application transactions are occurring between the remote port and the TCP/IP application. The Listeners group contains ports and applications which have at least one "Listener" session. A Listener session allows remote ports to connect to the TCP/IP application on the mainframe.
InActive Listeners	A Listener session is established but no activity is present.
UDP Sessions	Total number of User Datagram Protocol instances since last sampling interval.
TCP Sessions	Total number of Transfer Control Protocol instances since last sampling interval.
% Avail. Critical Resources	Percentage=((All monitored Critical Resources-Unavailable Critical Resources)/All monitored Critical Resource) * 100%

Further analysis can be done using the SysPoint's drill-down features: Alerts, LinkView, and Connect Expert. Each feature is briefly described below:

Alerts	When an Alert occurs for a stack during the current interval, the Alert shows in red. The SysPoint screen provides a count per Alert for the listed activities and a drill-down capability for Alerts. SysPoint provides both Summary and Detail Reports by Alert Type to assist in the analysis of related network problems. To obtain further information about a particular Alert, simply place your cursor in the appropriate cell and click. Refer to *Viewing Alerts* on page 66 for further information.
LinkView	To obtain further information on channel link activity in real time or near-time IP throughput information on channel-attached devices, use LinkView. 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. The LinkView screen also provides access to the Thru24 Summary/Detail reports which show near-time IP throughput data for channel-attached devices. LinkView is accessed from the SysPoint screen by clicking on a Stack IP Address and then clicking Show LinkView from the drop-down menu.
Connect Expert	Connect Expert allows you to view UDP (EE and non-EE) workload/session connectivity information as well as monitor sockets and the connectivity to all your sessions in real time. You can also view further UDP details (EE and non-EE) by accessing the Enterprise Extender Expert or UDP report, or zoom in to any port/application or session to view TCP/IP details using the Port Workload/Port Details reports. Connect Expert is accessed from the SysPoint screen by clicking on a Stack IP Address and then clicking Show Connect Expert from the drop-down menu.

Data Sources

Since SysPoint provides an overview of your network's availability and performance, the data it displays is affected by:

- Sampling intervals set on the Host for collecting the different network data elements
- Reporting interval set on the Host
- Refresh interval set on the individual workstation

- Thresholds set for service levels to generate the various Alerts
- Critical resources defined and monitored

The data sources for each area of the SysPoint display are described below:

Fields	**Data Source**
CSM Buffer Alerts, **Link Alerts,** **Port Alerts,** **Session Alerts,** **Critical Res. Perf. Alerts**	The Alerts in the SysPoint screen are reported on the basis of the reporting interval set by the REFRESH parameter in the AESTCPIP Proc. This value provides the basis for the Current, Last, and Since Midnight values shown in the Alert Summary and Detail Reports.
	The thresholds for the Alerts are set in the CONFxx member of SAEDSLIB. An Alert is received when a threshold is exceeded. Alerts for Performance and Availability may also be set on the Master workstation as well as the Host.
Stack Bytes In, **Stack Bytes Out**	The bytes in and bytes out values displayed are the deltas between the current and last sampling periods. The sampling interval is determined by the NINT parameter in the AESTCPIP Proc.
Total Channel Links, **Not Ready Channel Links,** **Not Ready Channel Devices**	The link information displayed consists of a total count and its sub-parts: Not-Ready-Channel Links and Not Ready Channel Devices. The information is gathered through the DEVLINKMON statement in the CONFxx member. The DEVLINKMON statement is used to set the monitoring frequencies and the queue size threshold. If the threshold is exceeded, an Alert is sent to the Operators Console.
Active Listeners, **InActive Listeners,** **UDP Sessions,** **TCP Sessions**	Data is obtained from the Network Statistics Collector. The sampling interval is through the NINT parameter in AESTCPIP.
% Avail. Critical Resources	Data is obtained through the monitoring of the Critical Resources.
	Critical Resources are defined in the Master on the PC workstation. Monitoring must be started by executing a Start Monitoring command for all selected Critical Resources.

Setting the Reporting and Refresh Intervals

The way information is displayed on the workstation is affected by the refresh interval. There are three refresh intervals that determine how data is collected by the host, how often the host counters are cleared, and what is displayed for the real-time data reports on the workstation.

In setting the refresh interval for the workstation, one must determine at what intervals the data has been collected and the counters cleared at the host. For example, if the refresh interval at the host is set at 6 minutes, then the response time average, maximum, and minimum counters are cleared every 6 minutes. During this time, the monitoring frequency is set for 30 seconds; therefore every 30 seconds new data is added to the running averages.

The refresh interval at the workstation may be set to 1 minute, providing new data at the workstation every minute. Since the test interval is set at 30 seconds, there are two new test results added into the running averages at every new display at the workstation.

Sampling Intervals for Monitoring on the Host

The sampling interval at which the Host Monitor collects data for each type of Alert is set in CONFxx. The threshold that generates an Alert when it is exceeded is also set at the Host.

The interval at which the Host Monitor collects application and client workload data is set using the monitoring frequency panel for each client or IP address that is monitored via the Master as Critical Resources are defined on the PC workstation. The default interval for application and client workload is 60 seconds (NINT parameter in AESTCPIP Proc).

The Refresh interval (Reporting interval) for clearing the counters at the host is set as a parameter to the Host Monitor startup job. New workload data may be added during this interval. The current default is set to 15 minutes in the REFRESH parameter in AESTCPIP Proc. Excluding availability and performance, all other data collection intervals and their thresholds are set on the Host in the CONFxx member.

Data	Data Collection Interval
CSM Buffer Pool Monitoring	Minimum interval is 60 seconds. There is no maximum interval. Parameter is set by the CSMINTERVAL statement in CONFxx member.
Link	Default is 600 seconds. Minimum value is 60 seconds. Parameter set by the DEVLINKMON statement
Port	Default is 600 seconds. Minimum value is 60 seconds Parameter set by the TCPPORTMONINTERVAL statement
Session	There is no default. Specify I=<interval> for each APPLMON statement.
Critical Resource Availability Alerts	Default is 60 seconds. Set when the Critical Resource is defined using the Master or by using the SERVDEF Modify command.
Critical Resource	Default is 60 seconds. Set when the Critical Resource is

Data	Data Collection Interval
Performance Alerts	defined using the Master or by using the SERVDEF Modify command.

Sampling Intervals (Refresh) on the Workstation

To display meaningful data at the browser, the frequency with which the workstation accesses the host must be a numerical value greater than the intervals set at the host. If the refresh intervals are not set correctly, duplicate information is displayed until the host interval values are reached and the counters cleared. To verify that the workstation values are valid, check with your systems administrator for the host refresh interval parameters.

The refresh interval at the workstation controls how often the wnrkstation accesses the host to update the screen display. The workstation interval may be set at any time the real-time graphical display is used. AutoRefresh, Refresh Interval, and Refresh are used to control the timing.

AutoRefresh	Automatically refreshes the screen with new data from the Host by the Refresh Interval set at the workstation without any user action required.
Refresh Interval	Determines the AutoRefresh Interval for new data being displayed on the workstation screen (hours:minutes:seconds). To change the AutoRefresh Interval, double-click on the current AutoRefresh value, then enter the desired numerical value. The new timer interval begins with the next Refresh. Avoid setting a local interval value less than the Host Monitor interval value.
Refresh	If AutoRefresh is not set, the user must execute the Refresh command manually to periodically update the data displayed on the workstation.

Since the reporting and refresh intervals for a particular workstation may be different than the monitoring interval set on the Host, it is important to set the workstation Refresh Interval to a value that is as large as the largest of the Host sampling intervals set for reporting data and/or Alerts. Otherwise, the most current interval can potentially be missed if the REFRESH parameter in AESTCPIP is less than the sampling intervals.

Setting Thresholds

Alerts are generated when a value set for a particular network element is exceeded. Notification of the "error condition" may be sent directly to the Operator's Console. The threshold values are set on the Host for all thresholds except Availability and Performance. Each data element and its threshold are listed below:

Data	**Threshold**
CSM Buffer Pool Monitoring	No Defaults. Set thresholds for the following Alerts: – ECSA threshold: maximum KB of ECSA buffer space to be used. – DSP threshold: maximum KB of DSP buffer space to be used – % Free threshold: minimum percent free for any CSM buffer area. Parameter set by CSMALERT in CONFxx member.
Link	Queuesize threshold: Number of outbound packets for this link which are queued and waiting for ARP resolution. Parameter set by DEVLINKMON in CONFxx member.
Port	No threshold defined. Port is either available or unavailable.
Session	No defaults. Set three thresholds for each application: – Throughput threshold: Minimum bytes/second that the application must perform. – Size threshold: Maximum data size in bytes that the application is allowed to transfer. – Application Hung: No threshold. If no activity between two samples, the application is considered hung and an Alert is sent. Specified in the APPLMON statement.
Critical Resource Availability Alerts	No threshold. Device is available or not available.
Critical Resource Performance Alerts	Thresholds are set in the Master. Each Critical Resource can have its own performance threshold for response time.

Defining Critical Resources

The PC workstation sets the definitions for the Critical Resources to be monitored and may also set the Availability and Performance Alerts. The intervals set on the PC workstation determine the rate at which the data displayed at the workstation is updated with the latest information obtained by the Host.

What Can You Do From the SysPoint Home Page?

The SysPoint Home Page serves as the nerve center for reporting information on network performance and availability. From the SysPoint Home Page you can:

- view Alert Summaries and Detail.
- access LinkView to monitor channel-attached processors and their links in real time or to open the Thru24 IP Detail/Summary reports to view near-time IP throughput information on channel-attached devices.
- access Connect Expert to view UDP (EE and non-EE) workload/session connectivity information or to monitor socket-attached applications and view the connectivity to all sessions in real time.

Viewing Alerts – quick look

From the SysPoint Home Page you can view both summary and detail data on Alerts. Current Alerts are displayed in red. View Alerts data by clicking in any Alert column.

The Summary Alert Report provides data for all Alerts displayed on the SysPoint Home Page. The Detail Report is context-sensitive and provides data for a selected Alert on the SysPoint Home Page.

The Detail data consists of two charts: one provides Total counts for the most recent occurrence, the last occurrence, and any Alerts that have occurred since midnight; the second chart displays detail data about the selected Alert time period.

Alerts for Critical Resource Availability and Performance are set in the Master on the PC Workstation. All other Alerts are set on the Host in the CONF00 member.

LinkView – quick look

LinkView provides real-time Channel Processor Monitoring. The LinkView report displays all the channel-attached processors and links associated with your TCP/IP address space on one screen. At a glance, you can see any device that is unavailable or that has exceeded the queue threshold. 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.

The LinkView screen also provides access through the Link Name hyperlink to the Thru24 IP Summary/Detail reports, which show near-time IP throughput information on channel-attached devices. LinkView is accessible to authorized Manager and Operations Manager users only.

Connect Expert – quick look

Connect Expert allows you to view EE UDP workload for assigned ports and non-EE UDP session connectivity information or to monitor your sockets and the connectivity to all your sessions in real time.

You can view further EE UDP information by accessing the Enterprise Extender Expert report from the EE table, or more detail on non-EE UDP connectivity by opening the UDP report from the UDP Sessions (non-EE) table.

You can view TCP/IP data about Listeners/Sessions, or zoom in to any port, application, or session to view TCP/IP details, such as the number of bytes sent/received, the number of sessions, and the number of sessions in a status other than established by port for each application. From the Port Workload/Port Details screens accessed from the TCP Sessions table, you can perform functions such as Trace Route, Drop, or Ping (authorized Master and Operations Manager users only). The application may be Telnet, e-mail, or any other socket-attached OLTP application using the selected TCP/IP address space.

(This page intentionally left blank.)

Alerts

The Alerts in the SysPoint screen are reported on the basis of the sampling interval set by the REFRESH parameter in the AESTCPIP Proc. This value provides the basis for the Current, Last, and Since Midnight values shown in the Alert Summary and Detail Reports.

The thresholds for the Alerts are set in the CONFxx member of SAEDSLIB. An Alert is received when a threshold is exceeded. Alerts for Performance and Availability may also be set on the Master workstation as well as the Host. SysPoint provides information at a glance for the following Alerts:

CSM Buffer Alerts	There are two types of Buffer Alerts: – Low Availability – High Usage
Link Alerts	Total count of Alerts sent during the current time period for channel links found in a Not Ready state for the channel device/link and for exceeding the queue size.
Port Alerts	Total count of Alerts sent during the current time period for unavailable ports.
Session Alerts	Total count of Alerts sent during the current time period for applications/sessions that have exceeded the threshold values for throughput, data size, and/or hung sessions.
Crit. Res. Avail. Alerts	Total count of Alerts sent during the current time period for Critical Resources that were unreachable (Ping command timed out).
Crit. Res. Perf. Alerts	Total count of Alerts sent during the current time period for Critical Resources that exceeded the value set for acceptable response time when the device was defined in the Master.

Current Alerts display in red on the SysPoint screen. Both a Summary and an Alert Detail report are available by clicking in any Alert column and then clicking the type of report you would like to view from the table.

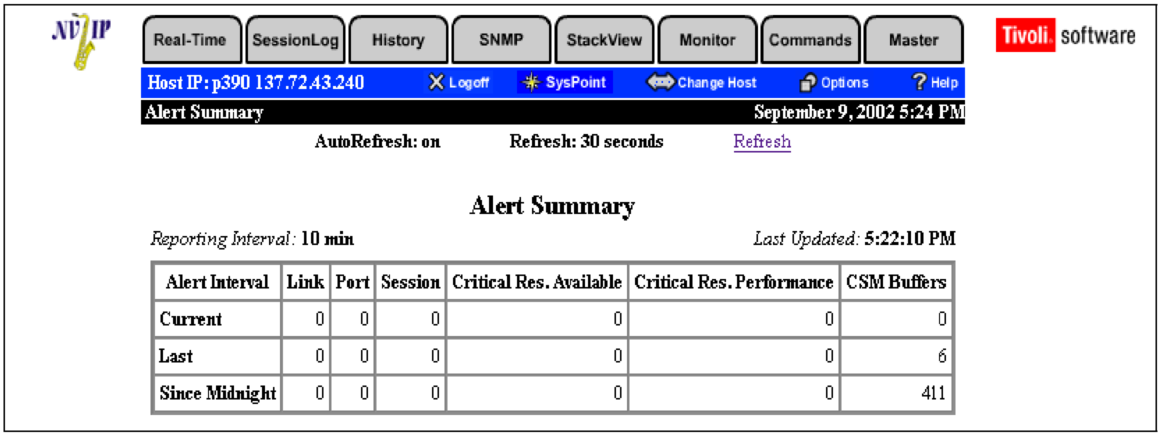
The Summary Alert Report provides current interval data, last occurrence, and since midnight for all Alerts on the SysPoint screen. The Detail report is context-sensitive and provides data from the Alert selected on the SysPoint screen. The Detail data consists of two charts: the left chart displays Alerts regarding the most recent occurrence, the last occurrence, and Alerts that have occurred since midnight; the right chart displays relevant data about the selected Alert.

To access further information about Alerts, perform the following steps:

1. From the SysPoint screen, select an Alert by placing the cursor over the value in the Alert cell.
2. Click once to view the drop-down list.
3. Click either Summary Report or Alert Detail to select the report type.
4. The correlating screen appears.

Alert Summary

The Alerts Summary Report provides information on all six Alerts shown on the SysPoint screen. For each Alert, the number of Alerts received per type and time period is listed in one table. The REFRESH parameter in the AESTCPIP Proc determines the duration of the Current and Last time periods. The Reporting Interval determines when the data that has been collected is written to the database. The AutoRefresh and Refresh options affect the frequency with which the information is updated on the individual's workstation display.



Host IP: p390 137.72.43.240

Alert Summary September 9, 2002 5:24 PM

AutoRefresh: on Refresh: 30 seconds

Alert Summary

Reporting Interval: 10 min *Last Updated:* 5:22:10 PM

Alert Interval	Link	Port	Session	Critical Res. Available	Critical Res. Performance	CSM Buffers
Current	0	0	0	0	0	0
Last	0	0	0	0	0	6
Since Midnight	0	0	0	0	0	411

Figure 18. Alerts Summary Report

The fields on the Alert Summary table are:

Reporting Interval	The interval, in minutes, at which new data is obtained from the Host.
Last Updated	Time in hh:mm:ss that the data display on the screen was last refreshed.
Alert Interval	The SysPoint screen displays the Current Interval results for all Alerts. The Alerts Summary report shows the number of Alerts that occurred during the following three time periods for all Alerts:

Current	The number of Alerts observed in the current ongoing interval.
Last	The number of Alerts observed in the previous interval.
Since Midnight	The number of Alerts observed since midnight today, given that the Host Monitor has not been reset. This includes all Alerts from the Current and Last intervals as well.

Alert Detail

The Alert Details tables vary by Alert type. The left portion of the screen provides hyperlinks to data per reporting interval for the selected Alert. Reporting intervals are Current, Last, and Since Midnight. The right portion of the screen provides detailed information about the Alerts that have been generated during the selected interval.

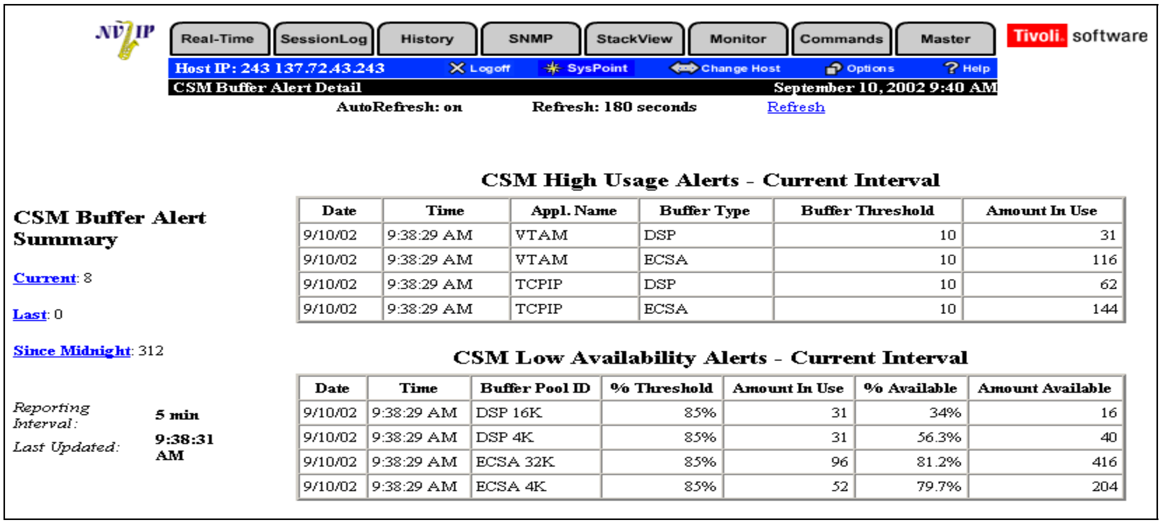
Alerts are generated when a value set for a particular network element is exceeded. Notification of the "error condition" may be sent directly to the Operator's Console. The values are set on the Host for all thresholds except Availability and Performance. Each data element and its threshold are listed below.

Data	**Threshold**
CSM Buffer Pool	No Defaults. Set thresholds for the following Alerts: – ECSA threshold: Maximum KB of ECSA buffer space to be used. – DSP threshold: Maximum KB of DSP buffer space to be used – % Free threshold: Minimum percent free for any CSM buffer area. Parameter set by CSMALERT in CONFxx member.
Link	Queuesize threshold: Number of outbound packets for this link that are queued and waiting for ARP resolution. Parameter set by DEVLINKMON in CONFxx member.
Port	No threshold defined. Port is either available or unavailable.
Session	No defaults. Set three thresholds for each application: – Throughput threshold: Minimum bytes/second that the application must perform. – Size threshold: Maximum data size in bytes that the application is allowed to transfer. – Application Hung: No threshold. If no activity between two samples, the application is considered hung and an Alert is sent. Specified in the APPLMON statement.
Critical Resource Availability Alerts	No threshold. Device is available or not available.
Critical Resource Performance Alerts	Thresholds are set in the Master. Each Critical Resource can have its own performance threshold for response time.

CSM Buffer Pool Alerts

The CSM Buffer Pool Alert provides both Summary and Detail Information for Buffer Alerts. The left portion of the screen provides hyperlinks to CSM Buffer Alert reports received for the following reporting intervals: Current, Last, and Since Midnight. The Current reporting interval is displayed first. To access the Last or Since Midnight intervals, click the hyperlink. This data is refreshed based on the Reporting Interval shown at the bottom of the Alert Summary Table.

The right portion of the screen provides detailed information about the Alert that has been generated. In this case, information on high usage and low availability of the buffers is reported.



Host IP: 243 137.72.43.243

CSM Buffer Alert Detail

September 10, 2002 9:40 AM

AutoRefresh: on

Refresh: 180 seconds

CSM Buffer Alert Summary

Current: 8

Last: 0

Since Midnight: 312

Reporting Interval: **5 min**

Last Updated: **9:38:31 AM**

CSM High Usage Alerts - Current Interval

Date	Time	Appl. Name	Buffer Type	Buffer Threshold	Amount In Use
9/10/02	9:38:29 AM	VTAM	DSP	10	31
9/10/02	9:38:29 AM	VTAM	ECSA	10	116
9/10/02	9:38:29 AM	TCPIP	DSP	10	62
9/10/02	9:38:29 AM	TCPIP	ECSA	10	144

CSM Low Availability Alerts - Current Interval

Date	Time	Buffer Pool ID	% Threshold	Amount In Use	% Available	Amount Available
9/10/02	9:38:29 AM	DSP 16K	85%	31	34%	16
9/10/02	9:38:29 AM	DSP 4K	85%	31	56.3%	40
9/10/02	9:38:29 AM	ECSA 32K	85%	96	81.2%	416
9/10/02	9:38:29 AM	ECSA 4K	85%	52	79.7%	204

Figure 19. CSM Buffer Alert Detail Report

The fields on the Buffer Alerts table for usage are:

Date	Day the Alert occurred, written in the format: mm/dd/yyyy.
Time	Time of day when the Alert occurred, written in the format: hh:mm:ss.
Appl. Name	Name of application that exceeded the threshold.
Buffer Type	Type of CSM buffer the application was using.
Buffer Threshold	The maximum amount (KB) allowed to be used.
Amount In Use	The actual amount (KB) being used by the application.

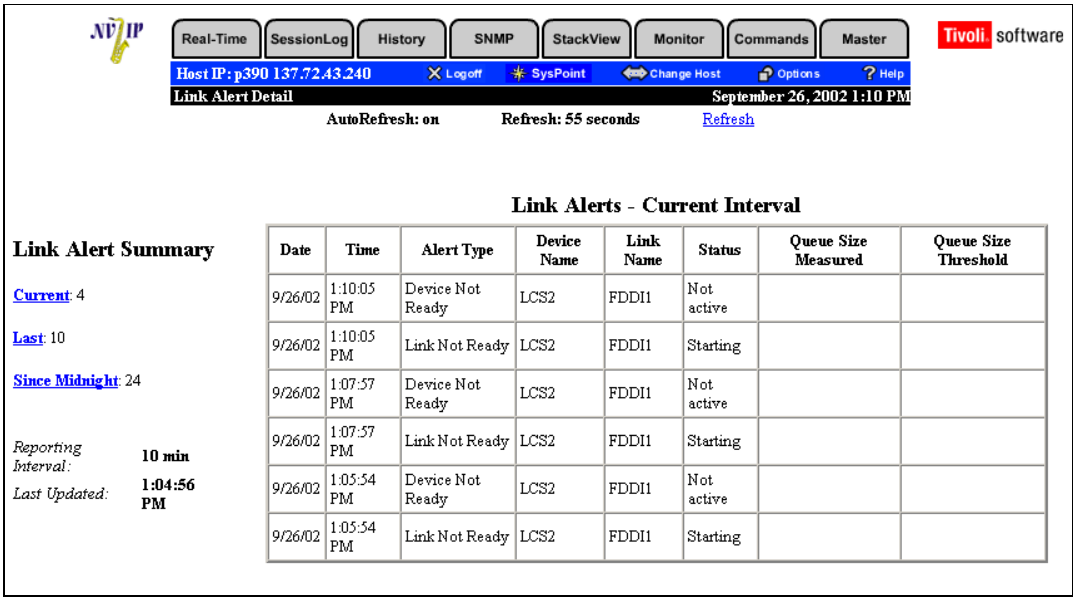
The fields on the Buffer Pool Alerts table for low availability are:

Date	Day the Alert occurred, written in the format: mm/dd/yyyy.
Time	Time of day when the Alert occurred, written in the format: hh:mm:ss.
Buffer Pool ID	Type of CSM Buffer Pool; e.g. 4K, 16K, etc.
Threshold	The minimum percent free for any CSM Buffer Pool.
Amount In Use	The actual amount in use (KB).
% Available	Percent available in the specified CSM Buffer Pool.
Amount Available	Amount available (KB) in the specified CSM Buffer Pool.

Link Alert Detail

The Link Alert Detail report provides both Summary and Detail Information for the links on channel-attached devices. The left portion of the screen provides hyperlinks to Link Alert reports received for the following reporting intervals: Current, Last, and Since Midnight. The Current reporting interval is displayed first. To access the Last or Since Midnight intervals, click the hyperlink. This data is refreshed based on the Reporting Interval shown at the bottom left portion of the Link Alert Summary screen.

The right portion of the screen provides detailed information about the Alert that has been generated. Alerts are generated when the number of outbound packets for this link that are queued and waiting for ARP resolution exceed the threshold. The type of Alert generated may be either for the link or for the device.



Host IP: p390 137.72.43.240

Link Alert Detail September 26, 2002 1:10 PM

AutoRefresh: on Refresh: 55 seconds

Link Alert Summary

Current: 4

Last: 10

Since Midnight: 24

Reporting Interval: **10 min**

Last Updated: **1:04:56 PM**

Link Alerts - Current Interval

Date	Time	Alert Type	Device Name	Link Name	Status	Queue Size Measured	Queue Size Threshold
9/26/02	1:10:05 PM	Device Not Ready	LCS2	FDDI1	Not active		
9/26/02	1:10:05 PM	Link Not Ready	LCS2	FDDI1	Starting		
9/26/02	1:07:57 PM	Device Not Ready	LCS2	FDDI1	Not active		
9/26/02	1:07:57 PM	Link Not Ready	LCS2	FDDI1	Starting		
9/26/02	1:05:54 PM	Device Not Ready	LCS2	FDDI1	Not active		
9/26/02	1:05:54 PM	Link Not Ready	LCS2	FDDI1	Starting		

Figure 20. Link Alert Detail Report

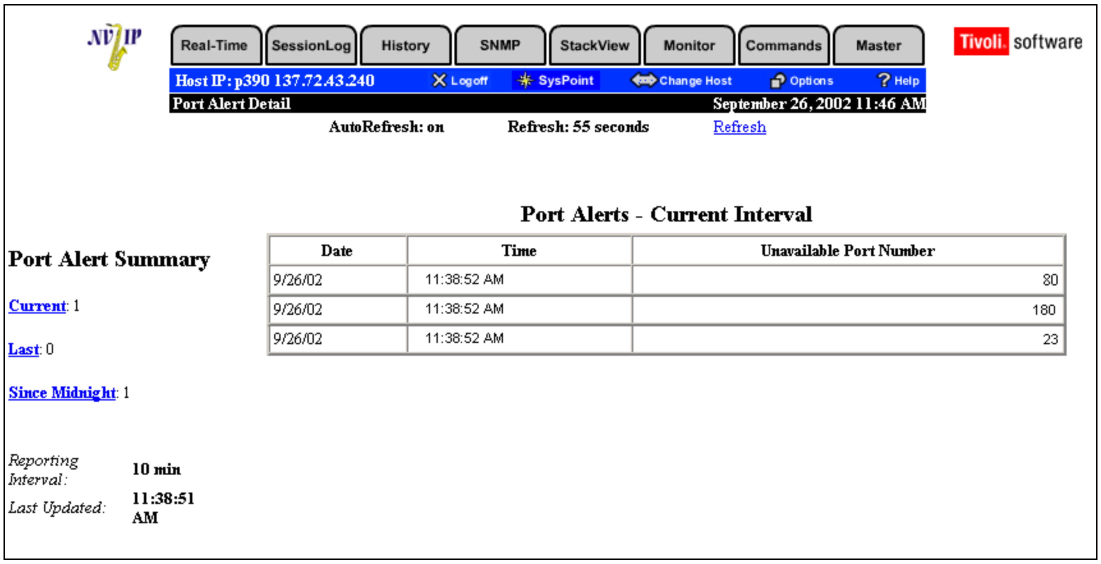
The fields on the Link Alert Detail Report are:

Date	Day the Alert occurred, written in the format: mm/dd/yyyy.
Time	Time of day when the Alert occurred, written in the format: hh:mm:ss.
Alert Type	One of the following types: link not ready, device not ready, or queue size exceeded threshold.
Device Name	Name assigned to this Device.
Link Name	Uniquely assigned link name.
Status	Device status (for "device not ready").
Queue Size Measured	The measurement of the size of outbound packets for this link that are queued and waiting for ARP resolution.
Queue Size Threshold	The threshold size set for the number of outbound packets for this link that are queued and waiting for ARP resolution.

Port Alert Detail

The Port Alert Detail report provides both Summary and Detail Information for ports. The left portion of the screen provides hyperlinks to Port Alert reports received for the following reporting intervals: Current, Last, and Since Midnight. The Current reporting interval is displayed first. To access the Last or Since Midnight intervals, click the hyperlink. This data is refreshed based on the Reporting Interval shown at the bottom left portion of the Alert Summary Table.

The right portion of the screen provides detailed information about the Alert that has been generated. Alerts are generated based on availability. No threshold is set because the port is either available or unavailable.



Host IP: p390 137.72.43.240

Port Alert Detail September 26, 2002 11:46 AM

AutoRefresh: on Refresh: 55 seconds Refresh

Port Alerts - Current Interval

Date	Time	Unavailable Port Number
9/26/02	11:38:52 AM	80
9/26/02	11:38:52 AM	180
9/26/02	11:38:52 AM	23

Port Alert Summary

Current: 1

Last: 0

Since Midnight: 1

Reporting Interval: 10 min

Last Updated: 11:38:51 AM

Figure 21. Port Alert Detail

The fields on the Port Alert Detail Report are:

Date	Day the Alert occurred, written in the format: mm/dd/yyyy.
Time	Time of day when the Alert occurred, written in the format: hh:mm:ss.
Unavailable Port Number	The port that could not be reached, generating an Alert. The Port Number is a numerical value, 0 through 65535, assigned to the port as an identifier.

Session Alert Detail

The Session Alert Detail report provides both Summary and Detail Information for all socket-attached applications. The left portion of the screen provides hyperlinks to Session Alert reports received for the following reporting intervals: Current, Last, and Since Midnight. The Current reporting interval is displayed first. To access the Last or Since Midnight intervals, click the hyperlink. This data is refreshed based on the Reporting Interval shown at the bottom of the Alert Summary Table.

The right portion of the screen provides detailed information about the Alert that has been generated. Session Alerts are generated based on the application's session exceeding one of three Session thresholds set in the APPLMON statement:

- Throughput threshold: Minimum bytes per second that the application must process.
- Size threshold: Maximum data size in bytes that the application is allowed to transfer.
- Application Hung: No threshold. If there is no activity between two samples, the application is considered hung and an Alert is sent.

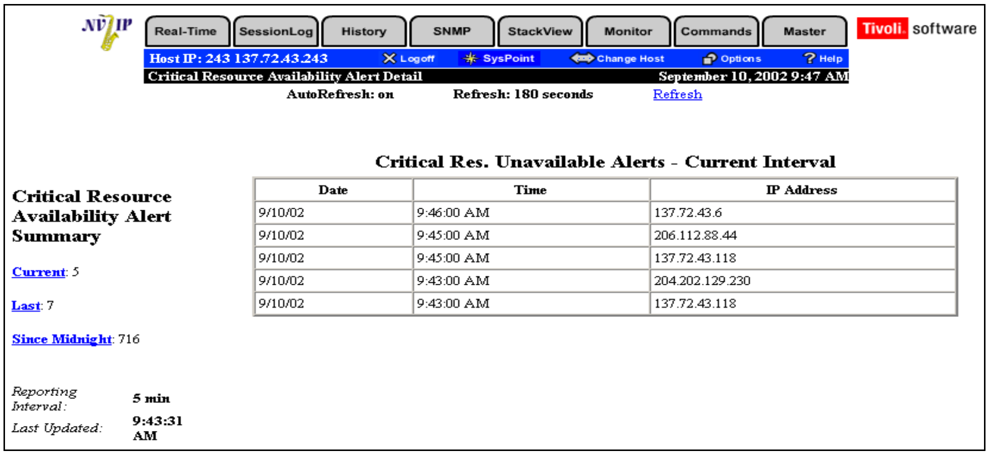
The fields on the Session Alert Detail panel are:

Date	Day the Alert occurred, written in the format: mm/dd/yyyy.
Time	Time of day when the Alert occurred, written in the format: hh:mm:ss.
Port Number	Numerical value, 0 through 65535, assigned to the port as an identifier. Each application uses a particular port.
Appl. Name	Name of application that exceeded the threshold.
Client IP Address	IP address of Client using the application that exceeded the threshold.
Throughput Measured	Throughput (bytes/second).
Throughput Threshold	Minimum bytes/second that the application must perform.
Data Size Measured	Total bytes transferred.
Data Size Threshold	Maximum data size in bytes that the application is allowed to transfer.

Critical Resource Availability Alert

The Critical Resource Availability Alert Detail report provides both Summary and Detail Information for critical resources defined in the Master. The left portion of the screen provides hyperlinks to Availability Alert reports received for the following reporting intervals: Current, Last, and Since Midnight. The Current reporting interval is displayed first. To access the Last or Since Midnight intervals, click on the hyperlink. This data is refreshed based on the Reporting Interval shown at the bottom of the Alert Summary Table.

The right portion of the screen provides detailed information about the Alert that has been generated. Alerts are generated based on availability. A device is considered unavailable when the Ping command times out. No threshold is set because the critical resource is either available or unavailable.



Host IP: 243 137.72.43.243

Critical Resource Availability Alert Detail September 10, 2002 9:47 AM

AutoRefresh: on Refresh: 180 seconds

Critical Res. Unavailable Alerts - Current Interval

Date	Time	IP Address
9/10/02	9:46:00 AM	137.72.43.6
9/10/02	9:45:00 AM	206.112.88.44
9/10/02	9:45:00 AM	137.72.43.118
9/10/02	9:43:00 AM	204.202.129.230
9/10/02	9:43:00 AM	137.72.43.118

Critical Resource Availability Alert Summary

Current: 5

Last: 7

Since Midnight: 716

Reporting Interval: **5 min**

Last Updated: **9:43:31 AM**

Figure 22. Critical Resource Availability Alert

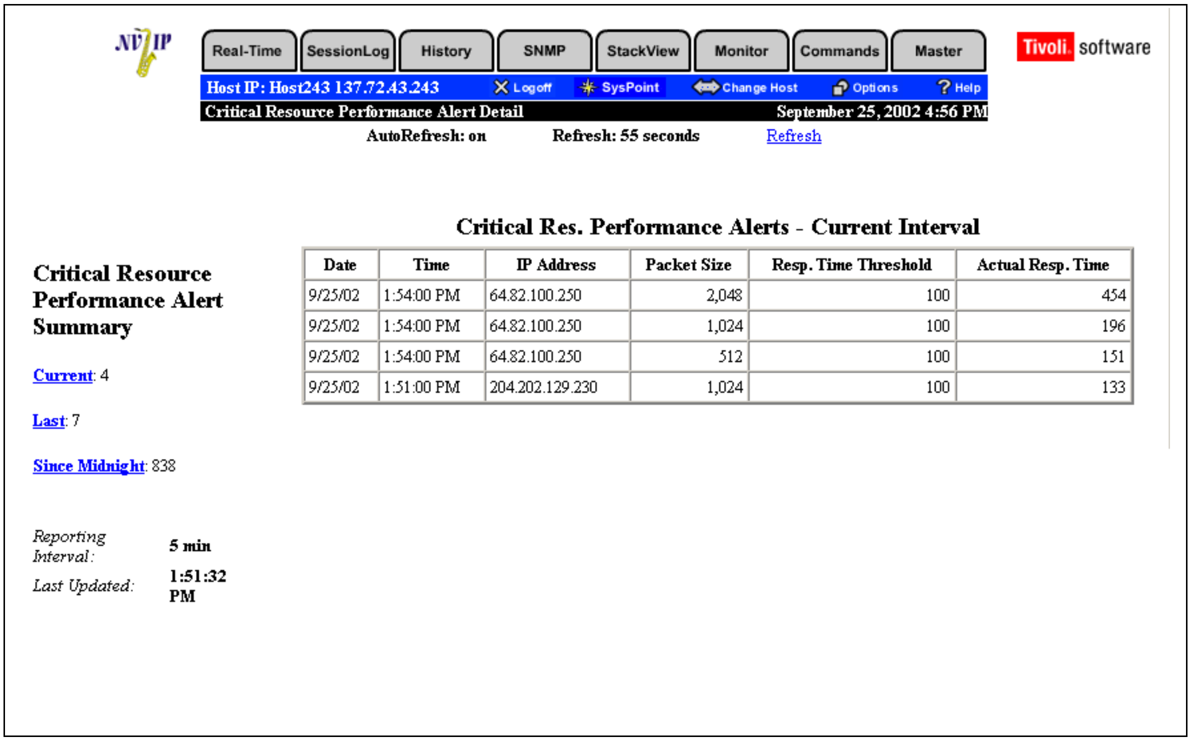
The fields on the Critical Resource Availability Detail panel are:

Date	Day the Alert occurred, written in the format: mm/dd/yyyy.
Time	Time of day when the Alert occurred, written in the format: hh:mm:ss.
IP Address	Internet Protocol address for the monitored critical resource that had an availability Alert.

Critical Resource Performance Alert

The Critical Resource Performance Alert Detail report provides both Summary and Detail Information for critical resources defined in the Master. The left portion of the screen provides hyperlinks to Performance Alert reports received for the following reporting intervals: Current, Previous, and Since Midnight. The Current reporting interval is displayed by default. To access the Last or Since Midnight intervals, click their hyperlinks. The data is refreshed based on the Reporting Interval shown at the bottom of the Alert Summary Table.

The right portion of the screen provides detailed information about the Alert that has been generated. Performance Alerts are generated based on Critical Resources that exceeded the value set for acceptable response time when the device was defined in the Master. Test packet sizes and their thresholds are set in the Master when the resource is defined.



Host IP: Host243 137.72.43.243

Critical Resource Performance Alert Detail September 25, 2002 4:56 PM

AutoRefresh: on Refresh: 55 seconds Refresh

Critical Resource Performance Alert Summary

Current: 4

Last: 7

Since Midnight: 838

Reporting Interval: 5 min

Last Updated: 1:51:32 PM

Critical Res. Performance Alerts - Current Interval

Date	Time	IP Address	Packet Size	Resp. Time Threshold	Actual Resp. Time
9/25/02	1:54:00 PM	64.82.100.250	2,048	100	454
9/25/02	1:54:00 PM	64.82.100.250	1,024	100	196
9/25/02	1:54:00 PM	64.82.100.250	512	100	151
9/25/02	1:51:00 PM	204.202.129.230	1,024	100	133

Figure 23. Critical Resources Performance Alerts

The fields on the Critical Resource Performance Alert Detail panel are:

Date	Day the Alert occurred, written in the format: mm/dd/yyyy.
Time	Time of day when the Alert occurred, written in the format: hh:mm:ss.
IP Address	Internet Protocol address for the monitored critical resource that had a performance Alert.
Packet Size	Size of packets (256, 512, 1024, 2048 bytes) used for measuring response time.
Resp. Time Threshold	The value set for acceptable roundtrip response time between the Host and the critical resource (ms).
Actual Resp. Time	The actual roundtrip response time between the Host and the critical resource (ms).

This page intentionally left blank.

LinkView

LinkView provides real-time Channel Processor Monitoring. The LinkView screen 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, and router cards such as the CISCO CIP card.

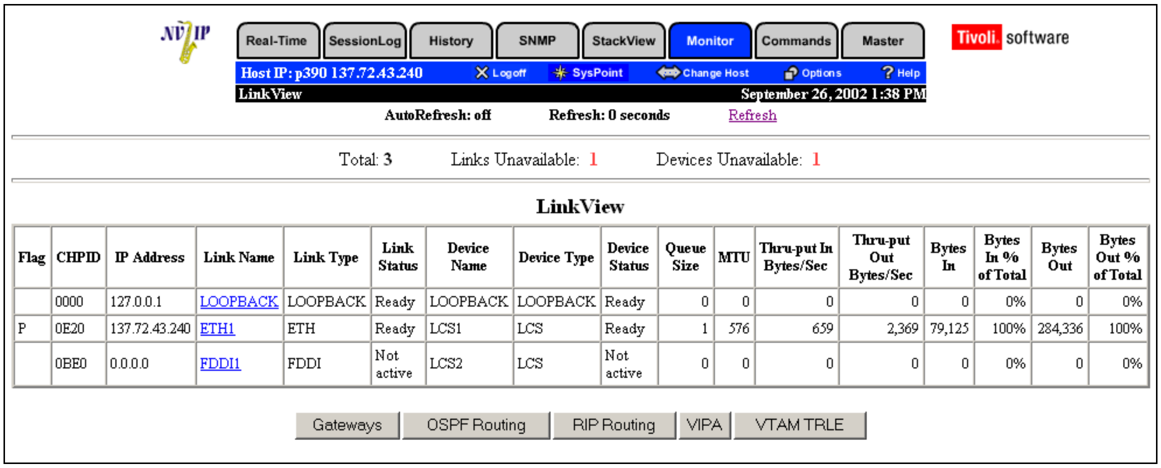
LinkView also provides access through the Link Name hyperlink in the table to the interval-based Thru24 IP Summary/Detail reports, which provide near-time IP throughput information on channel-attached devices.

Note: LinkView is accessible to Master and Operations Manager users only.

Using LinkView

LinkView is accessed from the SysPoint screen by clicking on a Stack IP Address hyperlink for the desired stack and then clicking Show LinkView from the drop-down menu. You can also access LinkView by clicking on the Monitor tab and then clicking the LinkView hyperlink under Critical Resource Monitors. LinkView is only accessible to Master or Operations Manager users.

The LinkView screen shows link and device information for each channel-attached processor associated with the selected TCP/IP address space. LinkView provides a synopsis of the Total physical links available, the Links Unavailable, and the Devices Unavailable. Detail information is provided by Channel Processor ID in the chart below. Click a Link Name hyperlink to open the Thru24 IP Summary or Detail report to view near-time IP throughput information for channel-attached devices. The Thru24 IP Summary report provides a comprehensive overview and the Detail report provides detail by interval (Current, Last, or Since Midnight). Context-sensitive commands can be executed (with full command user authorization) by clicking the buttons at the bottom of the screen to access command menus for: Gateways, OMPRoute OSPF Routing, OMPRoute RIP Routing, VIPA, or the VTAM Table.



Host IP: p390 137.72.43.240

LinkView September 26, 2002 1:38 PM

AutoRefresh: off Refresh: 0 seconds Refresh

Total: 3 Links Unavailable: 1 Devices Unavailable: 1

LinkView

Flag	CHPID	IP Address	Link Name	Link Type	Link Status	Device Name	Device Type	Device Status	Queue Size	MTU	Thru-put In Bytes/Sec	Thru-put Out Bytes/Sec	Bytes In	Bytes In % of Total	Bytes Out	Bytes Out % of Total
	0000	127.0.0.1	LOOPBACK	LOOPBACK	Ready	LOOPBACK	LOOPBACK	Ready	0	0	0	0	0	0%	0	0%
P	0E20	137.72.43.240	ETH1	ETH	Ready	LCS1	LCS	Ready	1	576	659	2,369	79,125	100%	284,336	100%
	0BE0	0.0.0.0	FDDI1	FDDI	Not active	LCS2	LCS	Not active	0	0	0	0	0	0%	0	0%

Figure 24. LinkView

The fields on LinkView for channel device monitoring are:

Flag	Blank	No flag
	I	Primary interface
	P	IP address was created as a result of this TCP/IP being identified as a target stack for this address from a Sysplex distributing stack.
CHPID	Channel Processor ID.	
IP Address	IP address of the link.	
Link Name	Uniquely assigned link name. Hyperlink to the Thru24 IP Summary or Detail report, which provides near-time IP throughput information for the selected link.	
Link Type	Category of network interface link associated with a device. For example, Ethernet.	
Link Status	Link status is either Not active or Ready.	
Device Name	Name assigned to this device	
Device Type	Category of device (e.g. CLAW)	
Device Status	Valid states for the device's status may be: • Starting • Sent SETUP Request • Enabling • Connecting	

	• Connecting2 • Negotiating • Ready • Deactivating • Not active
Queue Size	Number of outbound packets for this link which are queued and waiting for ARP resolution.
MTU	Link Maximum Transmission Unit. Example: 576.
Thru-put In Bytes/Sec	Data transfer rate in (Bytes/Second).
Thru-put Out Bytes/Sec	Data transfer rate out (Bytes/Second).
Bytes In	Number of bytes received in the current time period. This is a delta value. The interval is defined in the DEVLINKMON statement. The default is 600 seconds.
Bytes In % of Total	Bytes In % of Total=Bytes In for One Link /(Total Bytes In for All Links). Percentage based upon a comparison between the Bytes In for one Link and the total Bytes In for all Links. This is a delta value. The interval is defined in the DEVLINKMON statement. The default is 600 seconds.
Bytes Out	Bytes transferred for this channel device.
Bytes Out % of Total	Bytes Out % of Total=Bytes Out for One Link /(Total Bytes Out for All Links). Percentage based upon a comparison between the Bytes Out for one Link and the total Bytes Out for all Links. This is a delta value. The interval is defined in the DEVLINKMON statement. The default is 600 seconds.

Note: Bytes in and Bytes Out are the delta values between consecutive samples. All other data members are the current values obtained from the latest sampling event.

The buttons on LinkView for channel device monitoring are:

Gateways	Click this button to enter Netstat Gateway commands.
OSPF Routing	Click this button to enter OMPRoute/OSPF commands.
RIP Routing	Click this button to enter OMPRoute/RIP commands.
VIPA	Click this button to enter Netstat VIPA commands.
VTAM TRLE	Click this button to enter VTAM TRLE commands. TRLEs define the connectivity characteristics of PUs that provide SNA/APPN or TCP/IP application traffic.

Device States Status

Valid states for the status of the channel processor are:

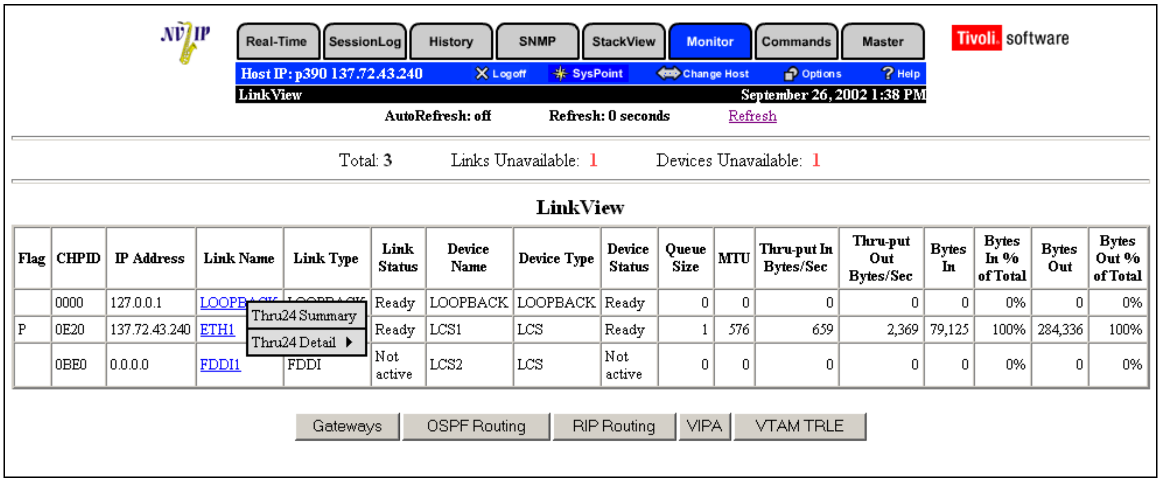
Starting	The operator has executed a START command to the device. TCP/IP has sent an Activation request to the data link control layer (DLC).
Sent Setup	DLC has acknowledged TCP/IP's Activation request. TCP/IP has requested that DLC perform the initial I/O sequence with the device.
Connecting	DLC has accepted the Initial Sequence request.
Connecting2	Control connection for a CLAW device has been established.
Negotiating	Initial I/O sequence with the device is complete. TCP/IP is performing additional link-layer initialization.
Ready	Initialization sequence with the device is complete. Device is ready for operation (use).
Sent Clear	Operator has executed a STOP command to the device. TCP/IP has sent a Deactivation request to the DLC.
Deactivated	DLC has performed the first stage of an orderly device deactivation.
Not Active	Device is unavailable. It has never been started or has been stopped.

Accessing the Thru24 IP Summary and Detail Reports

The Thru24 IP Summary and Detail reports provide near-time IP throughput information on links used by channel-attached devices. The reports are accessed from the Link Name hyperlink in the LinkView screen. The Thru24 IP Summary report shows the current workload and provides hyperlinks to the interval-based Thru24 IP Detail report. The Thru24 IP Detail report shows interval-based (Current, Last, and Since Midnight) data by Link Name, IP Address, and workload.

To access the Thru24 IP Summary report:

1. From the LinkView screen, click the Link Name of the link you want to view. A popup displays with the following options:
    - Thru24 Summary
    - Thru24 Detail



Host IP: p390 137.72.43.240

LinkView September 26, 2002 1:38 PM

AutoRefresh: off Refresh: 0 seconds Refresh

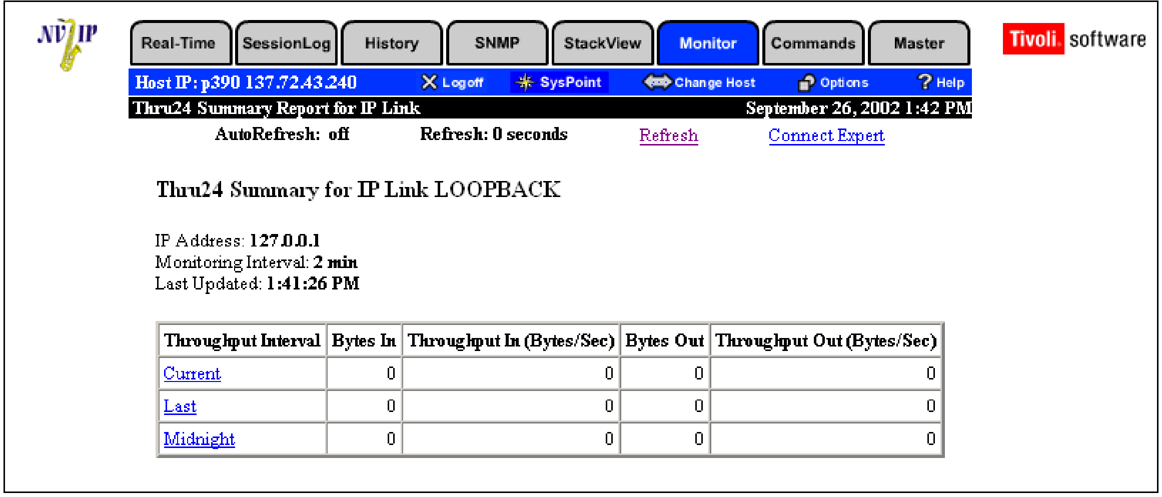
Total: 3 Links Unavailable: 1 Devices Unavailable: 1

LinkView

Flag	CHPID	IP Address	Link Name	Link Type	Link Status	Device Name	Device Type	Device Status	Queue Size	MTU	Thru-put In Bytes/Sec	Thru-put Out Bytes/Sec	Bytes In	Bytes In % of Total	Bytes Out	Bytes Out % of Total
	0000	127.0.0.1	LOOPB		Ready	LOOPBACK	LOOPBACK	Ready	0	0	0	0	0	0%	0	0%
P	0E20	137.72.43.240	ETH1		Ready	LCS1	LCS	Ready	1	576	659	2,369	79,125	100%	284,336	100%
	0BE0	0.0.0.0	FDDI1	FDDI	Not active	LCS2	LCS	Not active	0	0	0	0	0	0%	0	0%

Figure 25. Thru24 Summary/Thru24 Detail Options

2. Click Thru24 Summary. The Thru24 IP Summary report displays:



Host IP: p390 137.72.43.240

Thru24 Summary Report for IP Link September 26, 2002 1:42 PM

AutoRefresh: off Refresh: 0 seconds Refresh Connect Expert

Thru24 Summary for IP Link LOOPBACK

IP Address: 127.0.0.1
Monitoring Interval: 2 min
Last Updated: 1:41:26 PM

Throughput Interval	Bytes In	Throughput In (Bytes/Sec)	Bytes Out	Throughput Out (Bytes/Sec)
Current	0	0	0	0
Last	0	0	0	0
Midnight	0	0	0	0

Figure 26. Thru24 IP Summary Report

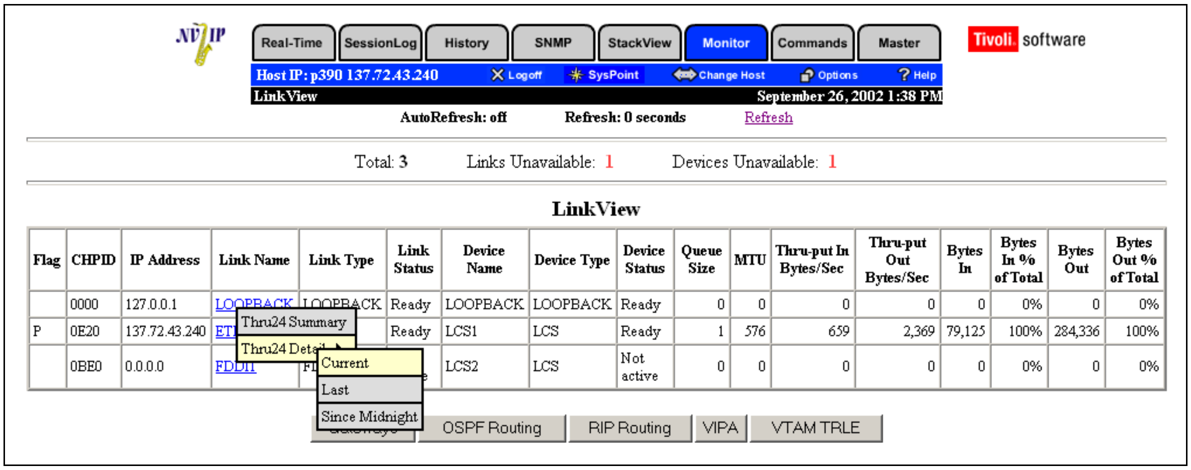
The fields on the Thru24 IP Summary report are:

Throughput Interval	Displays the intervals Current, Last, and Midnight. These fields are hyperlinks to the Thru24 IP Detail report for the selected interval.
Bytes In	The number of bytes coming in for the requested monitoring interval.

Throughput In Bytes/Sec	Data transfer rate for incoming bytes in bytes per second.
Bytes Out	The number of bytes transmitted out for the requested monitoring interval.
Throughput Out Bytes/Sec	Data transfer rate for outgoing bytes in bytes per second.

To access the Thru24 IP Detail report:

1. From the LinkView screen, click a Link Name hyperlink. A popup displays with the following options:
   - Thru24 Summary
   - Thru24 Detail
2. Click Thru24 Detail. A popup displays with the following options for the monitoring interval you want to view:
   - Current
   - Last
   - Since Midnight



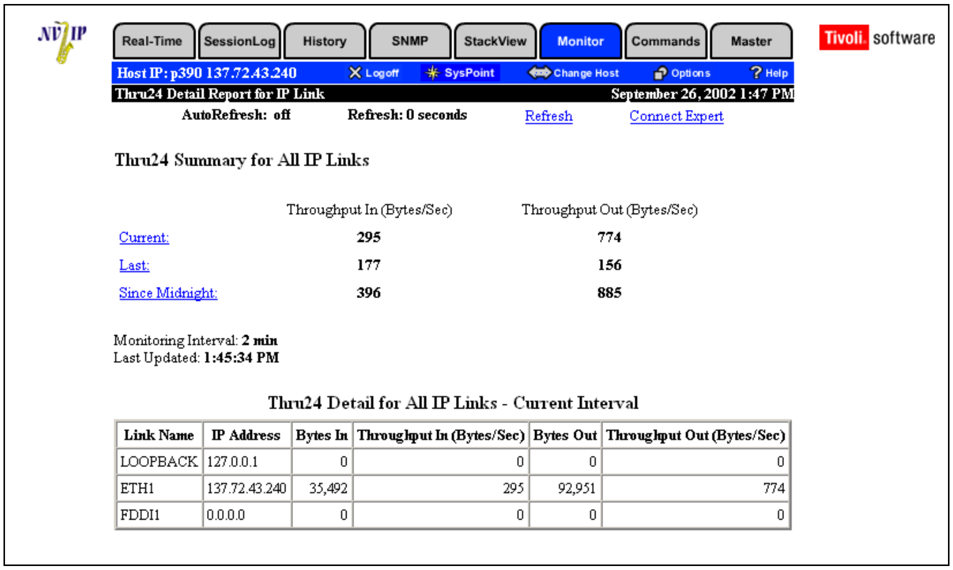
Total: 3 Links Unavailable: 1 Devices Unavailable: 1

LinkView

Flag	CHPID	IP Address	Link Name	Link Type	Link Status	Device Name	Device Type	Device Status	Queue Size	MTU	Thru-put In Bytes/Sec	Thru-put Out Bytes/Sec	Bytes In	Bytes In % of Total	Bytes Out	Bytes Out % of Total
	0000	127.0.0.1	LOOPBACK	LOOPBACK	Ready	LOOPBACK	LOOPBACK	Ready	0	0	0	0	0	0%	0	0%
P	0E20	137.72.43.240	ETI		Ready	LCS1	LCS	Ready	1	576	659	2,369	79,125	100%	284,336	100%
	0BE0	0.0.0.0	FDDII	FI		LCS2	LCS	Not active	0	0	0	0	0	0%	0	0%

Figure 27. Thru24 Detail Interval Selection

3. Click the desired interval. The Thru24 IP Detail report opens for the selected interval. In the following example, the Last Interval was selected:



Host IP: p390 137.72.43.240

Thru24 Detail Report for IP Link September 26, 2002 1:47 PM

AutoRefresh: off Refresh: 0 seconds Refresh Connect Expert

Thru24 Summary for All IP Links

	Throughput In (Bytes/Sec)	Throughput Out (Bytes/Sec)
Current:	295	774
Last:	177	156
Since Midnight:	396	885

Monitoring Interval: **2 min**
Last Updated: **1:45:34 PM**

Thru24 Detail for All IP Links - Current Interval

Link Name	IP Address	Bytes In	Throughput In (Bytes/Sec)	Bytes Out	Throughput Out (Bytes/Sec)
LOOPBACK	127.0.0.1	0	0	0	0
ETH1	137.72.43.240	35,492	295	92,951	774
FDDI1	0.0.0.0	0	0	0	0

Figure 28. Thru24 IP Detail report for Last Interval

Note: You can also access the Thru24 IP Detail report by clicking a Current, Last, or Since Midnight hyperlink from the Thru24 IP Summary report.

The fields in the Thru24 IP Detail report are:

Link Name	The selected Link Name.
IP Address	Internet Protocol address for device being monitored.
Bytes In	The number of bytes coming in for the requested monitoring interval.
Throughput In Bytes/Sec	Data transfer rate for incoming bytes in bytes per second.
Bytes Out	The number of bytes transmitted out for the requested monitoring interval.
Throughput Out Bytes/Sec	Data transfer rate for outgoing bytes in bytes per second.

Options Button

There are two Base Options available for LinkView. The AutoRefresh option sets data refresh to occur automatically at the current workstation at intervals set in Refresh Interval. Both options must be set for data to be automatically updated without user intervention.

AutoRefresh	Automatically refreshes the screen by the refresh interval without any user action required.
Refresh Interval	Determines the refresh interval for new data being displayed on the screen (minimum = 30 seconds, maximum =400 seconds). Avoid setting a local interval value less than the Host Monitor interval value.

This page intentionally left blank.

Connect Expert

The Connect Expert feature allows you to view real-time UDP data (EE workload for assigned ports and non-EE session connectivity) as well as monitor your sockets and the connectivity to all sessions running over TCP/IP in real time.

You can investigate further EE UDP data in the Enterprise Extender Expert report accessed from the EE link in the EE table. This report displays workload and throughput data for all EE assigned ports. The Enterprise Extender Expert report also provides access to the Thru24 EE Summary/Detail reports, which provide near-time EE throughput information, as well as the D NET,APING or RTP Route Test commands. You can view further UDP (non-EE) session connectivity data in the UDP report accessed from the UDP link in the UDP Sessions (non-EE) table. The UDP report shows workload and throughput information by UDP (non-EE) application name and port number.

From the Name or Port links in the TCP Sessions table, you can zoom in to any application/port or session to view details in the Port Workload/Port Details reports. The TCP Sessions table shows the number of bytes sent/received as well as a percentage comparison of the total bytes in/out to actual port usage, number of sessions, percentage of sessions attributable to the local port or application, number of sessions in a status other than established by port for each application, and the number of sessions in a Time-Wait or Closed status. From the Port Workload/Port Details reports, you can issue commands (depending upon your user authorization) such as Trace Route to analyze route data, Drop to terminate a session, or Ping to check device availability and response time. The number of bytes for the session indicates the amount since the session was started. The application may be Telnet, e-mail, or any other socket-attached OLTP application using the selected TCP/IP address space.

New data is gathered periodically at the Host according to the interval specified on the parameters to the started task. The data display at the workstation is automatically refreshed at the intervals set in Options. If you have not set Options, you can manually refresh the screen by clicking the Refresh button.

Connect Expert Main Page

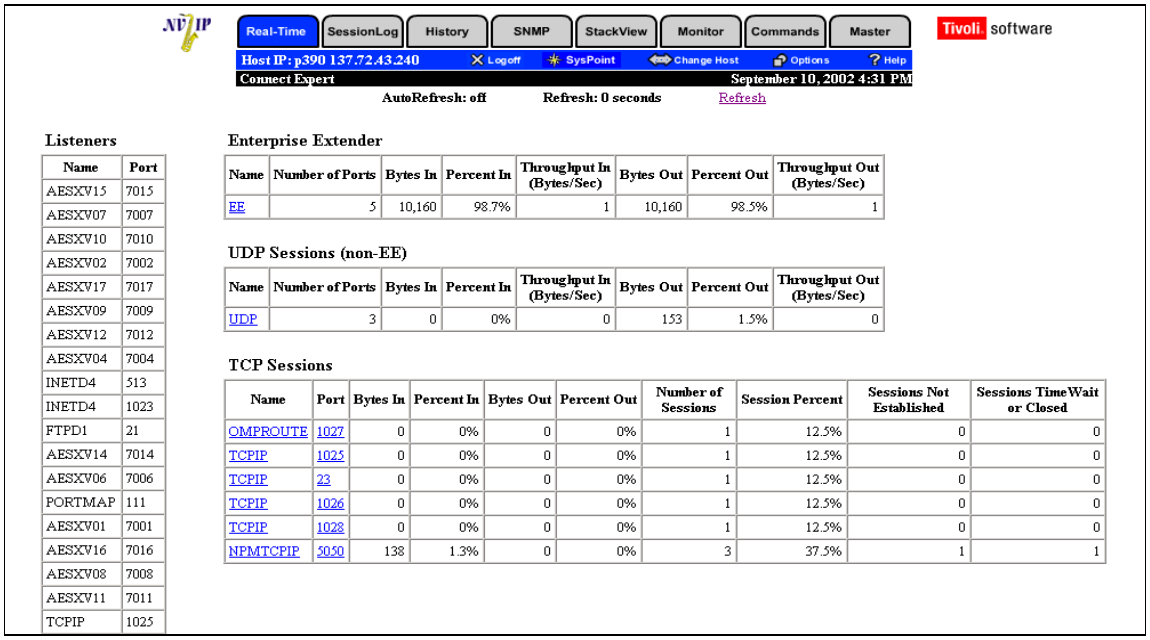
The Connect Expert screen is accessed by clicking a Stack IP Address hyperlink from the SysPoint screen and then clicking Show Connect Expert from the drop-down menu. You can also access Connect Expert by clicking its hyperlink under the Workload group in the Real-Time tab. If you are not logged on to the Host whose Stack IP Address you have selected to view, you are prompted for your User ID/Password and logged onto the selected Host after entering the requested information.

The Enterprise Extender Expert table at the top of the screen shows the current EE workload by port. The table shows the number of ports, bytes in/out, percent (of bytes) in/out actually being used by the port, and the throughput in bytes per second.

The UDP Sessions (non-EE) table shows the application name, port number, bytes in/out, percent (of bytes) in/out actually being used by the port, and the throughput in bytes per second.

Two sets of data are shown in the two tables at the bottom of the screen: Listeners and TCP Sessions. The Listeners set displays applications and ports that have at least one "Listener" session running. A Listener session allows remote ports to connect to the TCP/IP application on the mainframe. If you do not have a Listener session for a particular application that uses Listener sessions, it may be an indication of a network problem. For example, if you want to have Telnet (TN3270) sessions, there must be a Listener active on the well-known Port 23.

Note: Some applications do not use Listener sessions. Verify your application's design with your Systems Administrator.



Host IP: p390 137.72.43.240

Connect Expert September 10, 2002 4:31 PM

AutoRefresh: off Refresh: 0 seconds

Listeners

Name	Port
AESXV15	7015
AESXV07	7007
AESXV10	7010
AESXV02	7002
AESXV17	7017
AESXV09	7009
AESXV12	7012
AESXV04	7004
INETD4	513
INETD4	1023
FTPD1	21
AESXV14	7014
AESXV06	7006
PORTMAP	111
AESXV01	7001
AESXV16	7016
AESXV08	7008
AESXV11	7011
TCPIP	1025

Enterprise Extender

Name	Number of Ports	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
EE	5	10,160	98.7%	1	10,160	98.5%	1

UDP Sessions (non-EE)

Name	Number of Ports	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
UDP	3	0	0%	0	153	1.5%	0

TCP Sessions

Name	Port	Bytes In	Percent In	Bytes Out	Percent Out	Number of Sessions	Session Percent	Sessions Not Established	Sessions TimeWait or Closed
OMPROUTE	1027	0	0%	0	0%	1	12.5%	0	0
TCPIP	1025	0	0%	0	0%	1	12.5%	0	0
TCPIP	23	0	0%	0	0%	1	12.5%	0	0
TCPIP	1026	0	0%	0	0%	1	12.5%	0	0
TCPIP	1028	0	0%	0	0%	1	12.5%	0	0
NPMTCPIP	5050	138	1.3%	0	0%	3	37.5%	1	1

Figure 29. Connect Expert

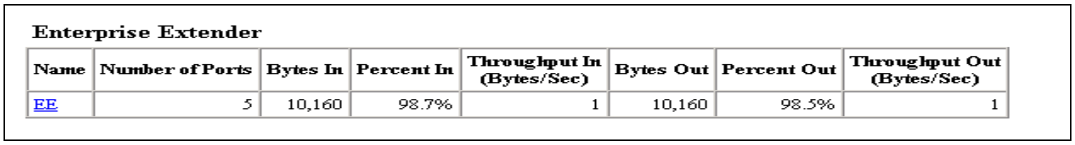
The fields in the Connect Expert tables are:

Enterprise Extender	
EE	The VTAM application name for Enterprise Extender on that system. Hyperlink to the Enterprise Extender Expert report to view details on the current EE UDP workload for each of the assigned EE ports. See *Real-Time Reports/Enterprise Extender Expert Report* for more information.
Number of Ports	The count of ports assigned to the EE application.
Bytes In	Number of bytes coming in to all assigned EE UDP ports.
Percent In	Percentage of bytes received relative to the total number of bytes coming in for all assigned EE UDP, UDP (non-EE), and TCP ports.
Throughput In Bytes/Sec	Data transfer rate inbound in bytes per second.
Bytes Out	Number of bytes transmitted out from all assigned EE UDP ports.
Percent Out	Percentage of bytes received outbound relative to the total number of bytes transmitted out for all assigned EE UDP, UDP (non-EE), and TCP ports.
Throughput Out Bytes/Sec	Data transfer rate outbound in bytes per second.
UDP Sessions (non-EE)	
UDP	Name of non-EE UDP application. Hyperlink to the UDP report.
Number of Ports	The count of ports currently in use by the UDP (non-EE) application.
Bytes In	Number of bytes coming in for all UDP (non-EE) sessions.
Percent In	Percentage of bytes received relative to the total number of bytes coming in for all assigned EE UDP, UDP (non-EE), and TCP ports.
Throughput In Bytes/Sec	Data transfer rate inbound in bytes per second.
Bytes Out	Number of bytes transmitted out for all UDP (non-EE) sessions.
Percent Out	Percentage of bytes received outbound relative to the total number of bytes transmitted out for all assigned EE UDP, UDP (non-EE), and TCP ports.
Throughput Out Bytes/Sec	Data transfer rate outbound in bytes per second.

Listeners	
Name	Application name. The applications listed in the Listeners Name fields have Listener sessions active on the ports noted.
Port	Local port number. An application may be active on more than one port. The ports listed in the Listeners Port fields have Listener sessions active on the ports noted.
TCP Sessions	
Name	Application name. Hyperlink to the Port Workload report to view details on the sessions for that application (all ports).
Port	Local port number. An application may be active on more than one port. Hyperlink to the Port Details report to view details on the sessions for that port.
Bytes In	Bytes in to TCP/IP on the mainframe since the session was started.
Percent In	Percentage of bytes received relative to the total number of bytes coming in for all assigned EE UDP, UDP (non-EE), and TCP ports.
Bytes Out	Bytes out to the remote IP address since the session was started.
Percent Out	Percentage of bytes received outbound relative to the total number of bytes transmitted out for all assigned EE UDP, UDP (non-EE), and TCP ports.
Number of Sessions	Total sessions.
Session Percent	The percentage of total sessions attributable to this local port or application.
Sessions Not Established	Total number of sessions in a status other than established by port. These sessions may need further investigation.
Sessions Time-Wait or Closed	Total number of sessions in a Time-Wait or Closed status. These sessions may need further investigation.

Accessing Enterprise Extender Expert

The Enterprise Extender Expert is accessed from the EE hyperlink in the Enterprise Extender table in Connect Expert:

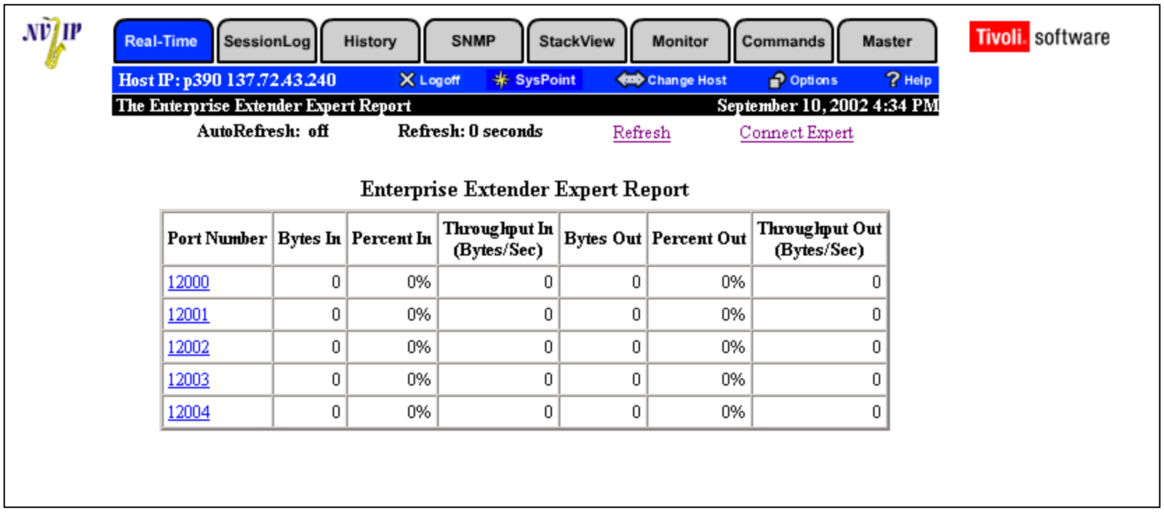


Enterprise Extender

Name	Number of Ports	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
EE	5	10,160	98.7%	1	10,160	98.5%	1

Figure 30. Enterprise Extender Table in Connect Expert

The Enterprise Extender Expert report provides real-time EE UDP workload data for EE assigned ports, as well as access to the Thru24 EE Summary/Detail reports and the D NET, APING or RTP Route Test commands.



Host IP: p390 137.72.43.240

The Enterprise Extender Expert Report September 10, 2002 4:34 PM

AutoRefresh: off Refresh: 0 seconds

Enterprise Extender Expert Report

Port Number	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
12000	0	0%	0	0	0%	0
12001	0	0%	0	0	0%	0
12002	0	0%	0	0	0%	0
12003	0	0%	0	0	0%	0
12004	0	0%	0	0	0%	0

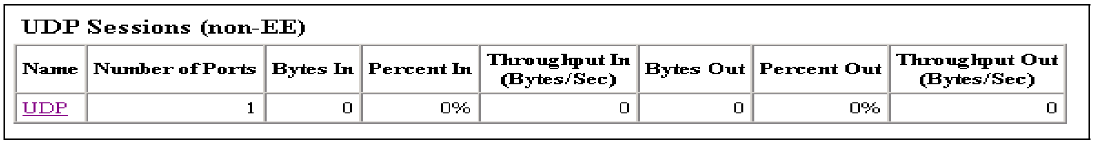
Figure 31. Accessing Enterprise Extender Expert from Connect Expert

See *Enterprise Extender Expert* for more information.

Note: You can also access the Enterprise Extender Expert from the Real-Time tab.

Accessing the UDP (non EE) Report

The UDP report shows current UDP (non-EE) workload and throughput information. The UDP report is accessed from the UDP hyperlink in the UDP Sessions (non-EE) table in Connect Expert.

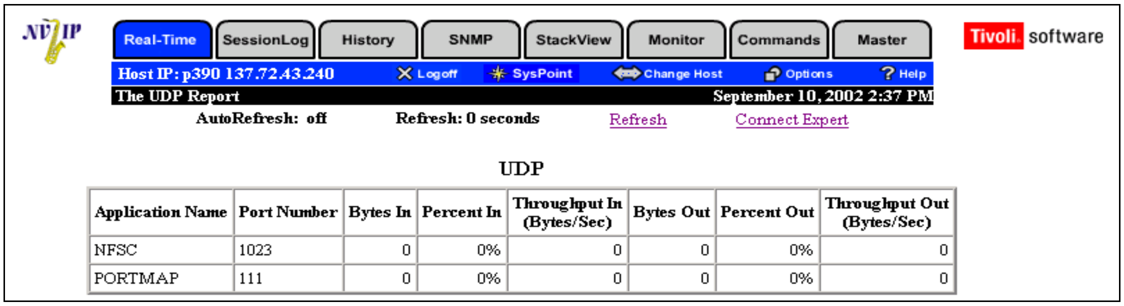


UDP Sessions (non-EE)

Name	Number of Ports	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
UDP	1	0	0%	0	0	0%	0

Figure 32. UDP Sessions (non-EE) Table in Connect Expert

The UDP report provides data by Application Name, Port Number, Bytes In/Out, Percent In/Out, and Throughput In/Out in bytes per second.



Host IP: p390 137.72.43.240

The UDP Report

September 10, 2002 2:37 PM

AutoRefresh: off

Refresh: 0 seconds

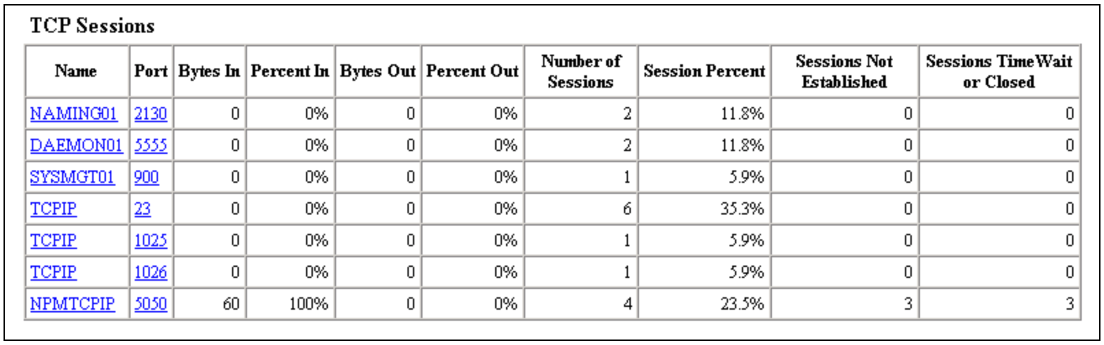
UDP

Application Name	Port Number	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
NFSC	1023	0	0%	0	0	0%	0
PORTMAP	111	0	0%	0	0	0%	0

Figure 33. UDP (non-EE) Report

Accessing the Port Workload Report

The Port Workload report is accessed from the Name hyperlink in the TCP Sessions table in Connect Expert. The report allows you to monitor the details of any application or socket and the connectivity to the sessions on the port(s) in real time. You can view further session details in the Port Details report by clicking the hyperlink for the selected Port in the TCP Sessions table. The data is refreshed periodically at the Host according to the interval specified on the parameters to the started task.



TCP Sessions

Name	Port	Bytes In	Percent In	Bytes Out	Percent Out	Number of Sessions	Session Percent	Sessions Not Established	Sessions TimeWait or Closed
NAMING01	2130	0	0%	0	0%	2	11.8%	0	0
DAEMON01	5555	0	0%	0	0%	2	11.8%	0	0
SYSMGT01	900	0	0%	0	0%	1	5.9%	0	0
TCPIP	23	0	0%	0	0%	6	35.3%	0	0
TCPIP	1025	0	0%	0	0%	1	5.9%	0	0
TCPIP	1026	0	0%	0	0%	1	5.9%	0	0
NPMTCPIP	5050	60	100%	0	0%	4	23.5%	3	3

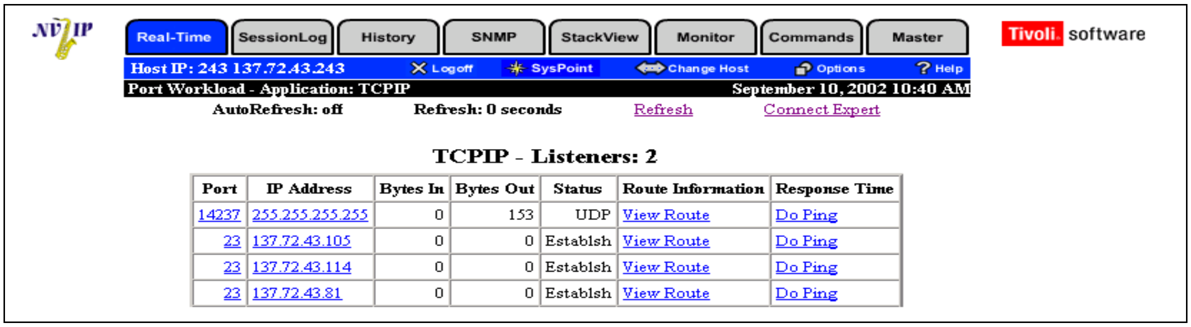
Figure 34. Accessing the Port Workload report from Connect Expert

The Port Workload report shows the number of bytes sent/received for each session and the status of the session. The Client Details report accessed from the IP Address hyperlink provides the connection ID, number of bytes sent/received, the status of the session, and many other critical parameters. You may obtain route details, information about a session drop, or view response time data by clicking the appropriate hyperlink.

Note: You can also access the Client Details report from the Client Workload report accessed in the Real-Time tab.

A note such as "Listeners: 1" next to the port and application name indicates the port has at least one "Listener" session. A Listener session allows remote ports to connect to the TCP/IP application on the mainframe. For example, if you want to have Telnet (TN3270) sessions, there must be a Listener active on Port 23 or the port assigned to Telnet sessions at your installation. For applications that do use Listeners there is no note of a Listener session.

Information regarding the workload on the local port for the selected session is displayed in the Port Workload report. Based on the status of the session as well as your user authorization, you can issue a TraceRoute command to verify the network path or a Ping command to check for availability and performance.



Host IP: 243 137.72.43.243

Port Workload - Application: TCPIP September 10, 2002 10:40 AM

AutoRefresh: off Refresh: 0 seconds Refresh Connect Expert

TCPIP - Listeners: 2

Port	IP Address	Bytes In	Bytes Out	Status	Route Information	Response Time
14237	255.255.255.255	0	153	UDP	View Route	Do Ping
23	137.72.43.105	0	0	Establsh	View Route	Do Ping
23	137.72.43.114	0	0	Establsh	View Route	Do Ping
23	137.72.43.81	0	0	Establsh	View Route	Do Ping

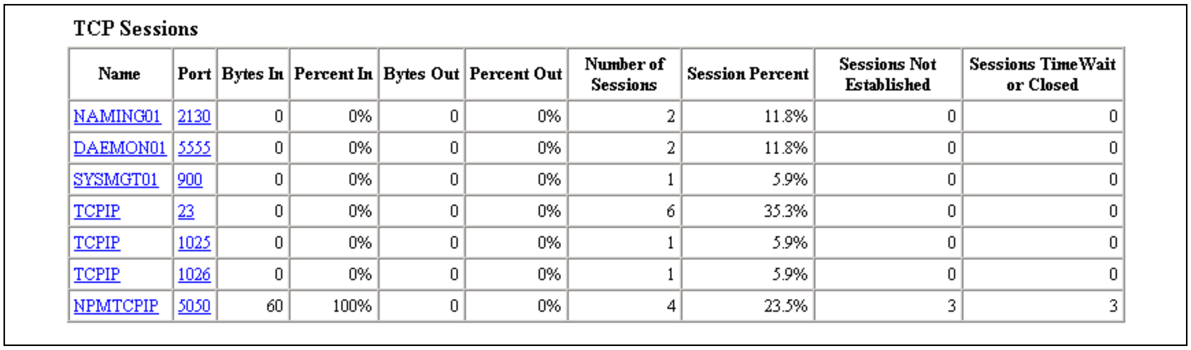
Figure 35. Port Workload Report

The fields on the Port Workload report are:

Port	Local port on mainframe TCP/IP. Hyperlink to the Port Details report to view details on all sessions for this IP address on this port.
IP Address	Remote IP address. Hyperlink to the Client Details reports to view details on all sessions for this IP address on all ports.
Bytes In	Bytes in to TCP/IP on the mainframe since the session was started.
Bytes Out	Bytes out to the remote IP address since the session was started.
Status	The state of this session. Valid states are: LISTEN, SYN-SENT, SYS-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK.
Route Information	Hyperlink to issue a TraceRte command to view the path or route this IP address is taking to the TCP/IP application on the mainframe.
Response Time	Hyperlink to issue a Ping command to check for availability and response time.

Accessing the Port Details Report

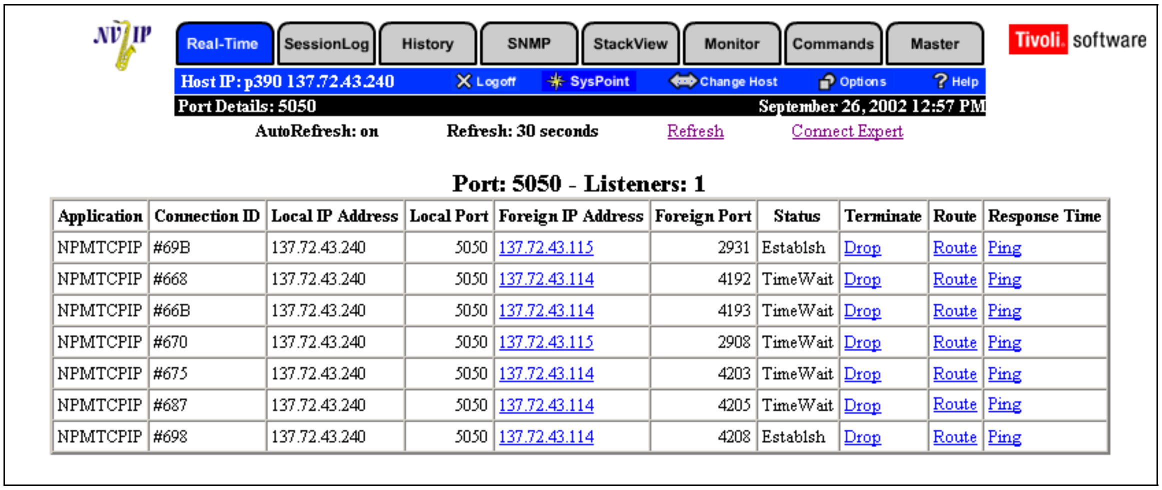
The Port Details report is accessed from the Port hyperlink in the TCP Sessions table in Connect Expert or from within the Port Workload report by clicking the Port hyperlink in the Port Workload table.



TCP Sessions

Name	Port	Bytes In	Percent In	Bytes Out	Percent Out	Number of Sessions	Session Percent	Sessions Not Established	Sessions TimeWait or Closed
NAMING01	2130	0	0%	0	0%	2	11.8%	0	0
DAEMON01	5555	0	0%	0	0%	2	11.8%	0	0
SYSMGT01	900	0	0%	0	0%	1	5.9%	0	0
TCPIP	23	0	0%	0	0%	6	35.3%	0	0
TCPIP	1025	0	0%	0	0%	1	5.9%	0	0
TCPIP	1026	0	0%	0	0%	1	5.9%	0	0
NPMTCPIP	5050	60	100%	0	0%	4	23.5%	3	3

Figure 36. Accessing the Port Details Report from TCP Sessions Table



Host IP: p390 137.72.43.240

Port Details: 5050 September 26, 2002 12:57 PM

AutoRefresh: on Refresh: 30 seconds

Port: 5050 - Listeners: 1

Application	Connection ID	Local IP Address	Local Port	Foreign IP Address	Foreign Port	Status	Terminate	Route	Response Time
NPMTCPIP	#69B	137.72.43.240	5050	137.72.43.115	2931	Establsh	Drop	Route	Ping
NPMTCPIP	#668	137.72.43.240	5050	137.72.43.114	4192	TimeWait	Drop	Route	Ping
NPMTCPIP	#66B	137.72.43.240	5050	137.72.43.114	4193	TimeWait	Drop	Route	Ping
NPMTCPIP	#670	137.72.43.240	5050	137.72.43.115	2908	TimeWait	Drop	Route	Ping
NPMTCPIP	#675	137.72.43.240	5050	137.72.43.114	4203	TimeWait	Drop	Route	Ping
NPMTCPIP	#687	137.72.43.240	5050	137.72.43.114	4205	TimeWait	Drop	Route	Ping
NPMTCPIP	#698	137.72.43.240	5050	137.72.43.114	4208	Establsh	Drop	Route	Ping

Figure 37. Port Details Report

Based on your user authorization, you can issue a TraceRoute command to verify the network path, a Drop command to terminate the session, or a Ping command to check network performance.

The fields on the Port Details report are:

Application	Application name assigned to this port.
Connection ID	Four position hexadecimal value assigned to this connection between the Host and the application.
Local IP Address	Local IP address on mainframe TCP/IP.

Local Port	Local port on mainframe TCP/IP.
Foreign IP Address Hyperlink	Remote IP address. Hyperlink to the Client Details report to view details on all sessions for this IP address on all ports.
Status	The status of this session. Valid states are: LISTEN, SYN-SENT, SYS-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK.
Terminate	Hyperlink to issue a Drop command to terminate the session.
Route Information	Hyperlink to issue a TraceRte command to view the path or route this IP address is taking to the TCP/IP application on the mainframe.
Response Time	Hyperlink to issue a PING command to check response time for the network from this IP address to the TCP/IP address space on the mainframe.

(This page intentionally left blank.)

StackView

StackView provides CPU usage information for the address spaces associated with TCP/IP (TCP/IP, SNALK, FTP server, and so forth), as well as for any address space associated with a socket-attached application. The data is shown numerically or pictorially. The numbers shown for CPU usage (TCB time, etc) are the total since the address space was initiated.

Address spaces may be predefined by a started task for the Host Monitor associated with each stack. These address spaces are automatically monitored when the host or stack is selected. The TCPMON=(nameofaddressspace) parameter is set for the Host Monitor started task in AESTCPIP.JCL(CONF00). Up to eight (8) address spaces can be predefined. You may also choose to see CPU times for all ports that have active TCP sessions. Either option may be selected from the Options panel.

Options

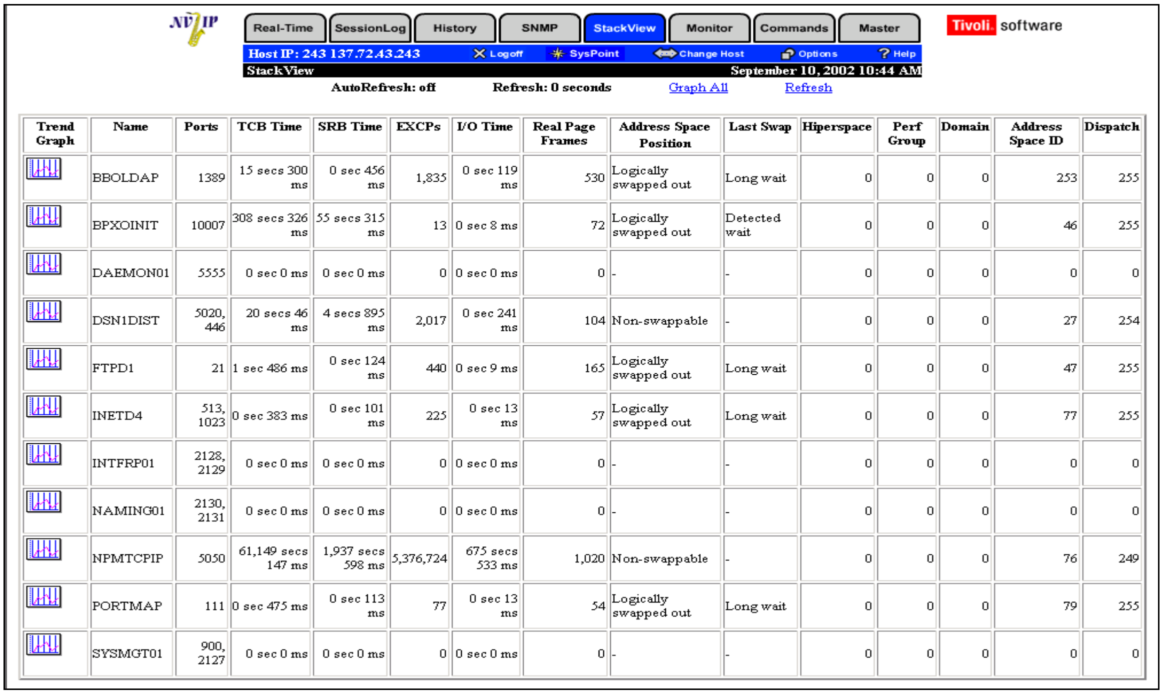
The default display shows all the address spaces associated with ports that are currently in use with a socket-attached application or associated with TCP/IP. The Base Options available affect the automatic refresh rate for displaying data at your workstation and limit the amount of information displayed by either the predefined address spaces or by all ports currently in use on the selected stack.

You may choose to see only the pre-defined values by selecting the 'predefined address spaces' option. The default is the CPU times for all ports that have active TCP sessions ('ports currently in use option).

To view the CPU usage for the address spaces associated with a selected TCP/IP address space, perform the following steps:

1. On the StackView panel, click the Options button.
2. In the Options panel, select predefined address spaces to monitor.
3. On the Base Options panel, place a checkmark in the AutoRefresh box to use the screen refresh interval set.
4. Enter a value for the Refresh Interval in seconds. The minimum refresh interval must be between 29 and 400 seconds. The refresh interval and AutoRefresh controls must be set to control the updating of data at the workstation. These values only affect viewing at your workstation and do not affect the Host Monitor's data collection rates. Avoid setting a local interval value less than the Host Monitor's data collection rate.
5. Click Done.

6. The options selected take effect the next time the StackView panel is refreshed.



Host IP: 243 137.72.43.243

StackView September 10, 2002 10:44 AM

AutoRefresh: off Refresh: 0 seconds

Trend Graph	Name	Ports	TCB Time	SRB Time	EXCPs	I/O Time	Real Page Frames	Address Space Position	Last Swap	Hiperspace	Perf Group	Domain	Address Space ID	Dispatch
	BBOLDAP	1389	15 secs 300 ms	0 sec 456 ms	1,835	0 sec 119 ms	530	Logically swapped out	Long wait	0	0	0	253	255
	BPXOINIT	10007	308 secs 326 ms	55 secs 315 ms	13	0 sec 8 ms	72	Logically swapped out	Detected wait	0	0	0	46	255
	DAEMON01	5555	0 sec 0 ms	0 sec 0 ms	0	0 sec 0 ms	0	-	-	0	0	0	0	0
	DSN1DIST	5020, 446	20 secs 46 ms	4 secs 895 ms	2,017	0 sec 241 ms	104	Non-swappable	-	0	0	0	27	254
	FTPD1	21	1 sec 486 ms	0 sec 124 ms	440	0 sec 9 ms	165	Logically swapped out	Long wait	0	0	0	47	255
	INETD4	513, 1023	0 sec 383 ms	0 sec 101 ms	225	0 sec 13 ms	57	Logically swapped out	Long wait	0	0	0	77	255
	INTFRP01	2128, 2129	0 sec 0 ms	0 sec 0 ms	0	0 sec 0 ms	0	-	-	0	0	0	0	0
	NAMING01	2130, 2131	0 sec 0 ms	0 sec 0 ms	0	0 sec 0 ms	0	-	-	0	0	0	0	0
	NPMTCPIP	5050	61,149 secs 147 ms	1,937 secs 598 ms	5,376,724	675 secs 533 ms	1,020	Non-swappable	-	0	0	0	76	249
	PORTMAP	111	0 sec 475 ms	0 sec 113 ms	77	0 sec 13 ms	54	Logically swapped out	Long wait	0	0	0	79	255
	SYSMGT01	900, 2127	0 sec 0 ms	0 sec 0 ms	0	0 sec 0 ms	0	-	-	0	0	0	0	0

Figure 38. StackView Report

The data shown when Reports has been selected on the main panel is:

Trend Graph	Clicking on the graph icon will chart the address space selected in real time. The graphs include: CPU time, I/O time, EXCPs and real frames.(See *Trend Graph for Address Space Selection* for more explanation.)
Name	Address space name.
Ports	The port(s) that this address space has active sessions on if using the appropriate option. This field will not show when using the show predefined address space option.
TCB Time	TCB CPU time in seconds:milliseconds from the time the address space was started
SRB Time	SRB CPU time in seconds:milliseconds from the time the address space was started.
EXCPs	Number of Execute channel program (I/O) from the time the address space was started.
I/O Time	I/O interrupt processing time from the time the address space was started.
Real Page Frames	Real storage utilization by the number of frames from the time the address space was started.

Address Space Position	Address space position may be swapped in, swapped out, non-swappable or in transition. Valid values are: **IN** In storage **OT** Swapped out and ready **LO** Logically swapped out **NS** Non-swappable **WM** Waiting for a resource: job is swapped in, is eligible for dispatching, and has accumulated no CPU time after some seconds **WL** Wait queue: long wait as a result of either WAIT TYPE=LONG or of STIMER >0.5 seconds **WT** Wait queue: terminal wait **WO** Wait queue: reasons other than WM, WL, or WT **DL** TSO user delayed by SRM to meet response time objective **PR** Privileged >> In the process of being swapped out of storage << In the process of being swapped into storage
Last Swap	Reason for last swap out associated with the address space. This field is blank if the address space position is NS, IN, or PR. Valid values are: **TI** Terminal input wait **TO** Terminal output wait **LW** Long wait **XS** Auxiliary storage shortage **RS** Central storage shortage **DW** Detected wait **RQ** Requested swap **NQ** Enqueue exchange **EX** Exchange based on recommendation value **US** Unilateral **TS** Transition swap **AW** APPC wait **IC** Improve central storage

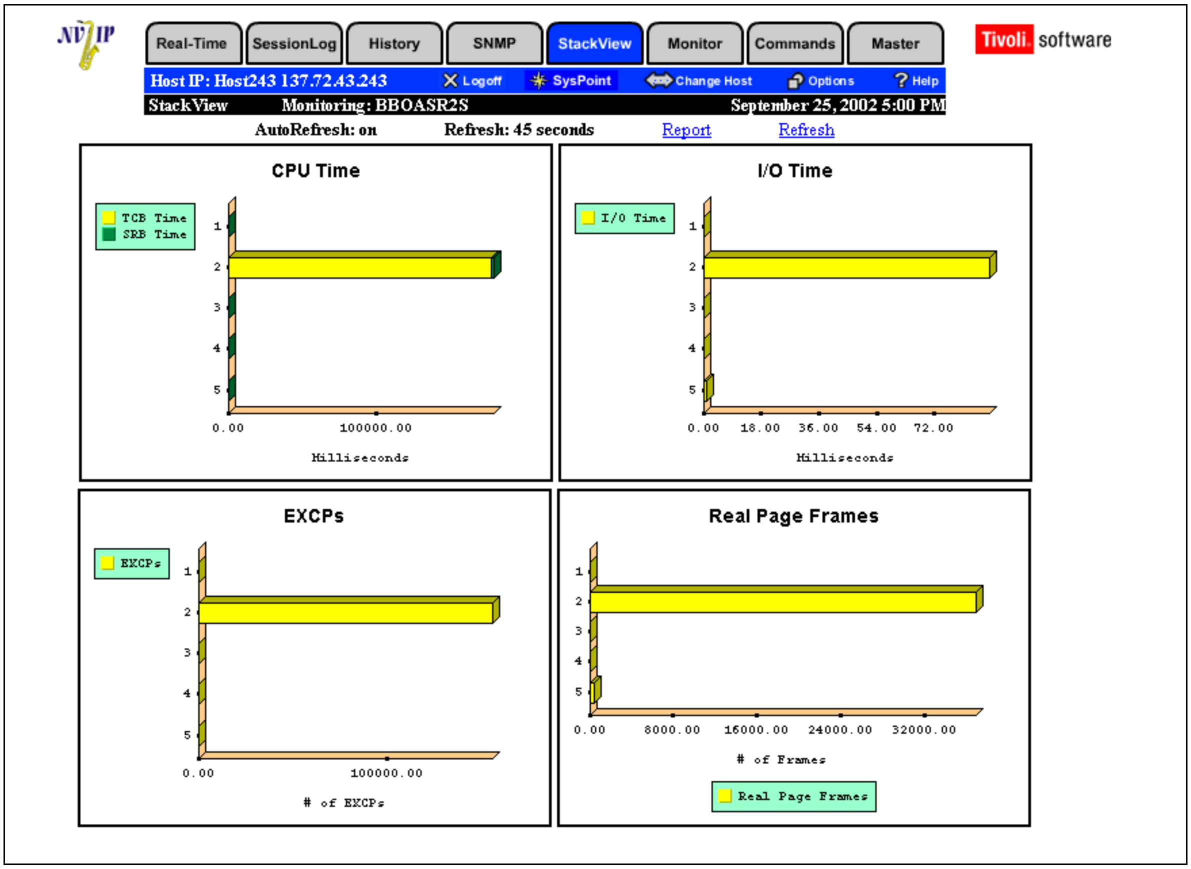
	IP Improve system paging rate **MR** Make room to swap in an out-too-long user
Hiperspace	Hiperspace processing time in seconds:milliseconds from the time the address space was started.
Perf Group	Performance Group number.
Domain	Domain number assigned to the address space. Defaults are domain 1 for ordinary address spaces and domain 0 for privileged address spaces.
Address Space ID	Address space identifier.
Dispatch	Address space dispatching priority.

Trend Graph for Address Space Selection

From the main StackView panel, you may choose to view trend graphs for a particular address space. The following information is graphed to show the usage of the address space over time.

- CPU Time which shows the TCB and SRB times
- I/O Time
- EXCP Count
- Real Page Frames

The graphs show the delta or change since the last sample. At times, the graph may show negative data for the Real Storage Frames Used graph. This means that more real storage frames were used in the current interval than in the previous one. This makes the delta or change negative.



Host IP: Host243 137.72.43.243

StackView Monitoring: BBOASR2S September 25, 2002 5:00 PM

AutoRefresh: on Refresh: 45 seconds

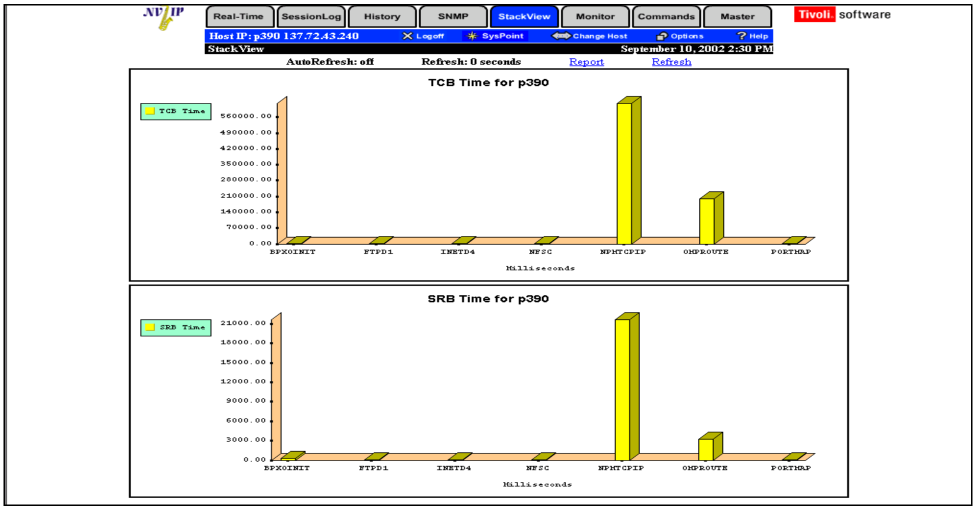
Figure 39. StackView – Trend Graph for Selected Address Space

Graph All Selection

The Graph All option provides a pictorial representation of the data displayed in the StackView report. The default display is the Report format. To change the display format, simply click on Graph All.

The information graphed is limited by the Base Option selection. Graphing All shows either the predefined address spaces or the ports currently in use as determined by the Base Option setting. The graphs provide the following information to allow comparisons of the selected address spaces at any given point in time.

- TCB Time
- SRB Time
- EXCP Count
- I/O Time
- Real Page Frames



Host IP: p390 137.72.43.240

StackView September 10, 2002 2:30 PM

AutoRefresh: off Refresh: 0 seconds

Figure 40. StackView – Graph All Selection with the Base Option of Ports Currently in Use

Graph Options - Introduction

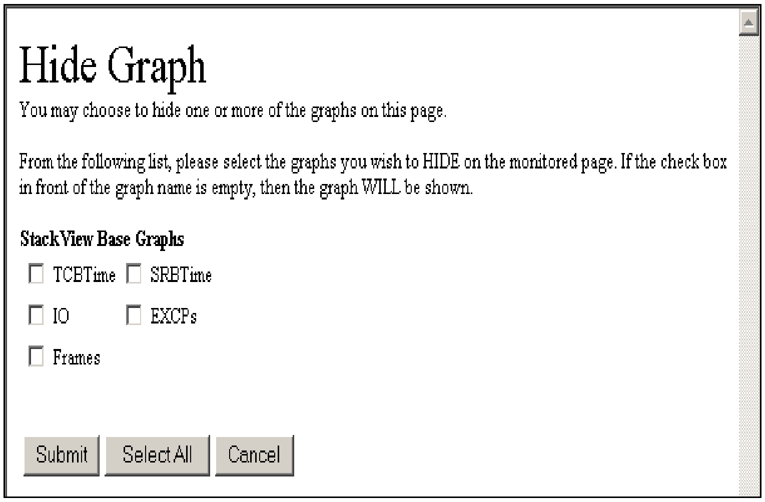
Two additional options are available when a StackView graph is displayed: Change Graph and Hide Graph Options.

Change Graph Option

Refer to appendices for information regarding changing the graph types, colors, titles, and format using the options button.

Hide Graph Option

When viewing StackView graphs, the Hide Graph option is available from the Option button. You may choose to view only selected graphs. The hide graph option is available for both the Graph All address spaces selection and the Trend Graph for Address space selection.



Hide Graph

You may choose to hide one or more of the graphs on this page.

From the following list, please select the graphs you wish to HIDE on the monitored page. If the check box in front of the graph name is empty, then the graph WILL be shown.

StackView Base Graphs

☐ TCBTime ☐ SRBTime

☐ IO ☐ EXCPs

☐ Frames

Figure 41. Hide Graph

(This page intentionally left blank.)

Real-Time

Real-Time Reports are available in both tabular and graphical format. The tabular format uses the table report elements that are common in most reporting environments. It allows for the quick and easy location of critical information. The graphical format provides the same information in a format suitable for presentations. Real-Time reports also includes the Enterprise Extender Expert, which is only available in tabular format and provides data on the current EE UDP workload by port. The graphical format (charts) provide information on the following:

- Real-time network response time between enterprise hosts and any other TCP/IP connection
- Real-time workload information for the enterprise TCP/IP hosts such as the number of sessions, total number of bytes transmitted since last monitoring interval, and average number of bytes transmitted
- Workload and network performance trending are provided in real time. The information can be summarized by time or by host.
- Enterprise Extender UDP information

On the following pages, both report formats are provided for each reporting function. Both formats may be printed via the browser functions.

Note: For information on report options, please refer to the appendices.

NV4IP views the TCP/IP network performance from the enterprise level to the remote user connection. Performance indicators are available for workload, usage, and response time. The Real-Time Reports are available for gathering and monitoring network data in the daily work environment. The Real-Time and History reports are available as soon as the Host Monitor has been active for a period of time. The SessionLog Expert allows viewing of *near time* or current time sessions, that is, sessions that are either currently live or have recently happened.

To view a Real-Time Report, perform the following steps:

1. From the Real-Time Reports window, click the Workload or Performance Report you wish to view:

Workload
Connect Expert
Details/Selected Port/Address
Top Applications Sessions
Top Applications Bytes
Selected Application Session
Selected Application Bytes
Client Workload

Performance
Network Health
Response Time
Selected Response Time

Enterprise Extender Expert
Enterprise Extender Expert Report

If you are prompted to enter or select additional information (such as entering an IP Address or selecting a resource), provide the information and click the appropriate button.

The Real-Time Report screen for your selection appears.

2. Enter AutoRefresh parameters for viewing the selected report if you would like data at your workstation to be automatically refreshed at specified intervals. You must set two Options to activate this feature at your workstation:
   - AutoRefresh rate
   - Refresh Interval (in seconds)
3. The report screen appears. Real-Time Reports provide three categories of reporting:

Workload	Shows the workload by sessions and bytes per application(s) creating the most demand on your system. Available reports are: – Connect Expert – Details Selected/Port/Address – Top Applications Sessions – Top Applications Bytes – Selected Application Session – Selected Application Bytes – Client Workload
Performance	Provides information on the average response times for a particular address and the network, as well as providing information in terms of overall network performance. – Network Health (Network) – Response Time – Selected Response Time (Resource)
Enterprise Extender Expert	Provides data on the current UDP EE workload by for each of the assigned EE ports.

Refresh Interval

The way information is displayed is affected by the refresh interval. There are three refresh intervals that determine how data is collected by the host, how often the host counters are cleared, and what is displayed for the real-time data reports on the workstation.

In setting the refresh interval for the workstation, one must determine at what intervals the data has been collected and the counters cleared at the host. For example, if the refresh interval at the host is set at 6 minutes, then the response time average, maximum, and minimum counters are cleared every 6 minutes. During this time, the monitoring frequency is set for 30 seconds; therefore every 30 seconds new data is added to the running averages. The refresh interval at the workstation may be set to 1 minute, providing new data at the workstation every minute. (See the Options Button section in the appendices for more information.) Since the test interval is set at 30 seconds, there are two new test results added into the running averages in every new display at the workstation.

To display meaningful data at the browser, the frequency with which the workstation accesses the host must be a numerical value greater than the intervals set at the host. If the refresh intervals are not set correctly, duplicate information is displayed until the host interval values are reached and the counters cleared. To verify that the workstation values are valid, check with NV4IP Technical Support for the host refresh interval parameters.

The interval at which the Host Monitor collects application and client workload data is set using the monitoring frequency panel for each client or IP address that is monitored. The default interval for application and client workload is 60 seconds. The refresh interval for clearing the counters at the host is set as a parameter to the Host Monitor startup job. New workload data may be added during this interval. The current default is every 60 seconds.

The refresh interval at the workstation controls how often the workstation accesses the host to update the screen display. The workstation interval may be set at any time the real-time graphical display is used.

Workload Reports

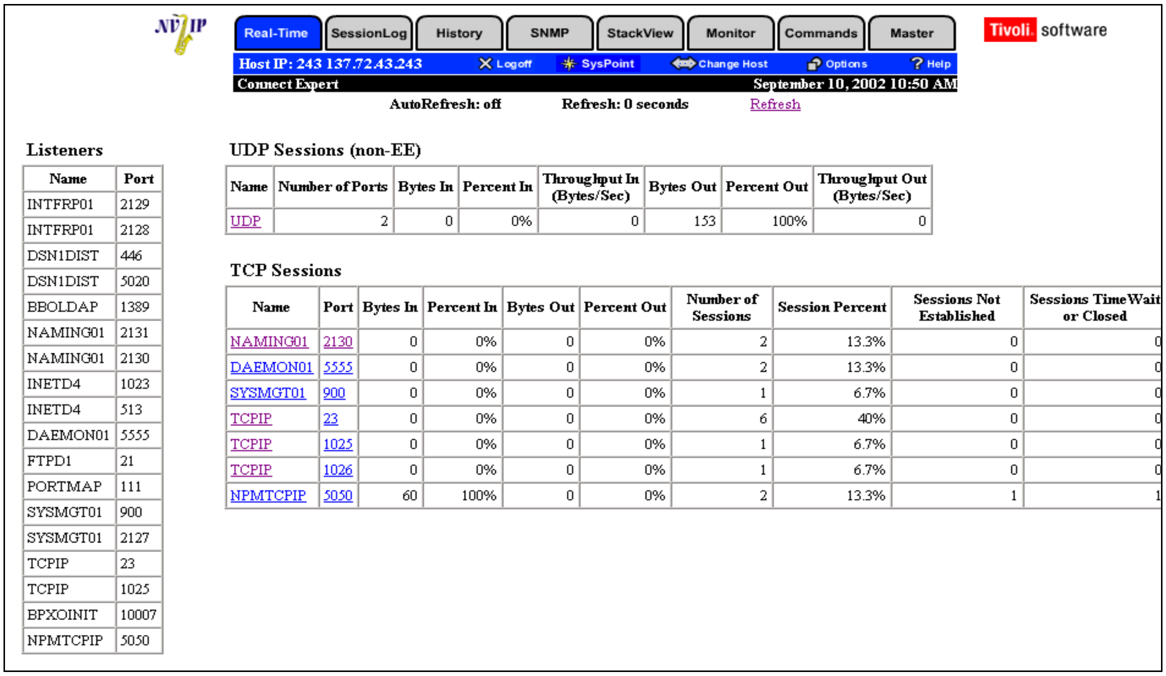
Each Workload Report provides online real-time information. Each report type is briefly described below:

Connect Expert	Monitors your sockets and the connectivity to all your sessions in real time. The Port Workload feature shows details about port/application or session.
Details Selected Port/Address	Monitors the details of any socket port and connectivity to all sessions in real time. Shows the number of bytes sent/received, the number of sessions, and the number of sessions in a status other than established by port for each port.
Top Applications Sessions Graph	Top n applications using the TCP/IP address space. Workload is reported in terms of sessions
Top Applications Bytes Graph	Top n applications using the TCP/IP address space (workload reported in terms of bytes transferred in/out since last monitoring interval)
Selected Application Sessions Graph	Trend graph in real time of any particular application in terms of sessions
Selected Application Bytes Graph	Trend graph in real time of any particular application in terms of bytes transferred in and out since last monitoring interval
Client Workload Report	The current clients with active sessions using the TCP/IP stack

Connect Expert Report

The Connect Expert report shows EE UDP workload by port as well as UDP (non EE) and TCP Session data.

You can access the Connect Expert screen by clicking Connect Expert from the Workload list of the Real-Time Reports screen or by clicking the Connect Expert link from the drop-down menu in SysPoint.



Host IP: 243 137.72.43.243

Connect Expert

September 10, 2002 10:50 AM

AutoRefresh: off

Refresh: 0 seconds

Listeners

Name	Port
INTFRP01	2129
INTFRP01	2128
DSN1DIST	446
DSN1DIST	5020
BBOLDAP	1389
NAMING01	2131
NAMING01	2130
INETD4	1023
INETD4	513
DAEMON01	5555
FTPD1	21
PORTMAP	111
SYSMGT01	900
SYSMGT01	2127
TCPIP	23
TCPIP	1025
BPXOINIT	10007
NPMTCPIP	5050

UDP Sessions (non-EE)

Name	Number of Ports	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
UDP	2	0	0%	0	153	100%	0

TCP Sessions

Name	Port	Bytes In	Percent In	Bytes Out	Percent Out	Number of Sessions	Session Percent	Sessions Not Established	Sessions TimeWait or Closed
NAMING01	2130	0	0%	0	0%	2	13.3%	0	0
DAEMON01	5555	0	0%	0	0%	2	13.3%	0	0
SYSMGT01	900	0	0%	0	0%	1	6.7%	0	0
TCPIP	23	0	0%	0	0%	6	40%	0	0
TCPIP	1025	0	0%	0	0%	1	6.7%	0	0
TCPIP	1026	0	0%	0	0%	1	6.7%	0	0
NPMTCPIP	5050	60	100%	0	0%	2	13.3%	1	1

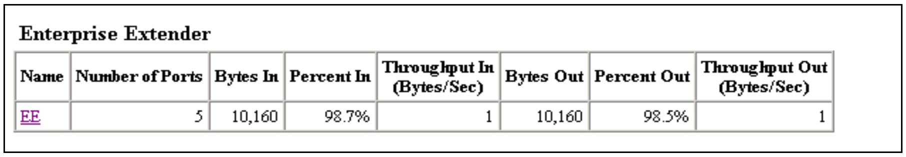
Figure 42. Connect Expert

You can view details about workload, application, or port by clicking the EE, UDP, or Port links from the Enterprise Extender, UDP Sessions (non EE), or TCP Sessions tables. Clicking the EE link in the Enterprise Extender Expert table opens the Enterprise Extender Expert, which provides data for current EE UDP workload by EE assigned port. Clicking the UDP link in the UDP Sessions (non EE) table opens the UDP report, which provides non-EE UDP workload for non-EE UDP applications. Clicking the Name or Port link from the TCP Sessions table opens the Port Workload/Port Details reports, in which you can perform functions (depending upon user authorization) such as Trace Route, Drop, or Ping. The byte count for the session indicates the number of bytes from the start of the session. The application may be Telnet, e-mail, or any other socket-attached OLTP application using the selected TCP/IP address space.

Enterprise Extender Expert Table

The Enterprise Extender Expert table shows the details of EE UDP activity for EE assigned ports in real time. It shows the Name, Number of Ports currently in use, total Bytes In/Out since last monitoring interval, Percent In/Out, and Throughput In/Out in Bytes per second. The Name in the table represents the Enterprise Extender application. The Percent In/Out is a percentage comparison between the in/outbound bytes and the actual port usage for all current EE activities.

The EE link in the Enterprise Extender Expert table opens the Enterprise Extender Expert, which provides data on current EE UDP workload by EE assigned ports.



Enterprise Extender

Name	Number of Ports	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
EE	5	10,160	98.7%	1	10,160	98.5%	1

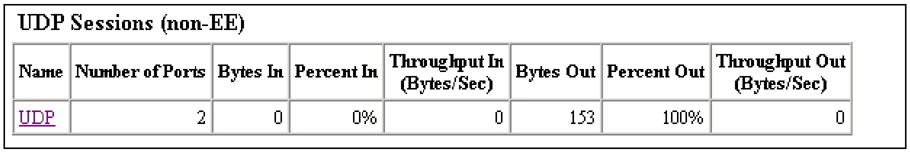
Figure 43. Enterprise Extender Table in Connect Expert

See *Enterprise Extender Expert* for more information.

UDP Sessions (non EE) Table

The UDP Sessions (non EE) table shows the details of UDP (non EE) activity in real time. It shows the Name, Number of Ports currently in use, total Bytes In/Out since last host monitoring interval, Percent In/Out, and Throughput In/Out in Bytes per second. The Name field in the table displays non-EE UDP applications. The Percent In/Out is a percentage comparison between the in/outbound bytes and the total number of all bytes coming in/going out for all current UDP activities.

The UDP report breaks the data down further by Application Name and Port Number. You can access this report by clicking the UDP link in the UDP Sessions (non EE) table in Connect Expert.



UDP Sessions (non-EE)

Name	Number of Ports	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
UDP	2	0	0%	0	153	100%	0

Figure 44. UDP Sessions (non EE) Table (in Connect Expert)

Details Selected Port/Address

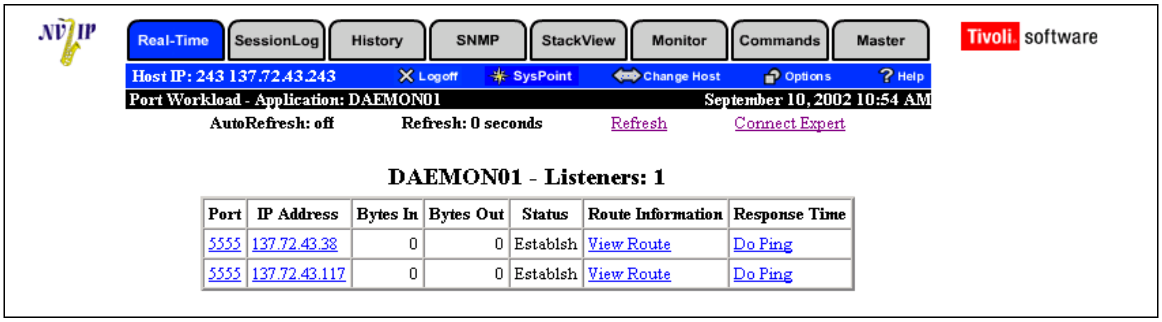
The Details Selected Port/Address reports consist of the Port Workload and Port Detail reports. The Port Workload report provides an overview of any application or socket and the connectivity to the sessions on the ports in real time. The Port Details report shows details of any socket port and connectivity to all sessions in real time.

Port Workload Report

The Port Workload report allows you to monitor the details of any application or socket and the connectivity to the sessions on the ports in real time. You can access the report and view details of any session by clicking the Details Selected Port/Address hyperlink in the Workload list of the Real-Time Report screen, or from the Name link in the Connect Expert TCP Sessions table. The report shows the number of bytes sent/received for each session and the status of the session. The data is refreshed periodically at the Host according to the interval specified on the parameters to the started task.

Information about the workload on the selected port is displayed in the Port Workload report. Based on the status of the session and your user authorization, you can issue a TraceRoute command to verify the network path, or a Ping command to check for availability and performance.

If the Session Name is selected, the following Port Workload report appears:



Host IP: 243 137.72.43.243

Port Workload - Application: DAEMON01 September 10, 2002 10:54 AM

AutoRefresh: off Refresh: 0 seconds

DAEMON01 - Listeners: 1

Port	IP Address	Bytes In	Bytes Out	Status	Route Information	Response Time
5555	137.72.43.38	0	0	Establsh	View Route	Do Ping
5555	137.72.43.117	0	0	Establsh	View Route	Do Ping

Figure 45. Port Workload Report (from Connect Expert)

The fields on the Port Workload report are:

Port	Local port on mainframe TCP/IP. Hyperlink to view details on all sessions for this IP address on this port.
IP Address	Remote IP address. Hyperlink to the Client Details report to view details on all sessions for this IP address on all ports.
Bytes In	Bytes in to TCP/IP on the mainframe since the session was started.
Bytes Out	Bytes out to the remote IP address since the session was started.

Status	The state of this session. Valid states are: LISTEN, SYN-SENT, SYS-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK.
Terminate	Hyperlink to issue a Drop command to terminate the session.
Route Information	Hyperlink to issue a TraceRte command to view the path or route this IP address is taking to the TCP/IP application on the mainframe.

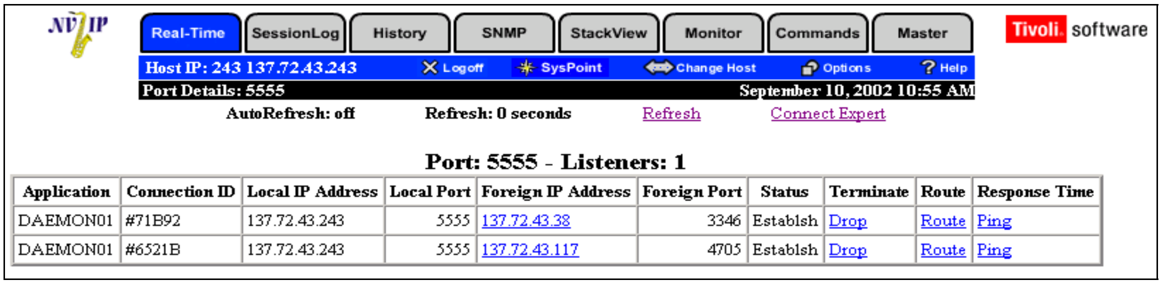
1. From the Workload list of the Real-Time Reports screen, click the Details Selected Port/Address hyperlink. You can also access the Port Workload report from the Name link in the Connect Expert TCP Sessions table. Complete the desired fields and click Submit. The report appears.
2. Do one of the following:
   - To enter another port number/address, click the Back button on the browser.
   - To return to the SysPoint Home Page, click SysPoint on the main menu bar.

Port Details Report

The Port Details report shows the details of any socket port and connectivity to all sessions in real time. It shows the number of bytes sent/received, the number of sessions, and the number of sessions in a status other than established by port for each port.

You can access this report by selecting Details Selected Port/Address in the Workload list of the Real-Time Reports screen. You can also access the Port Details report by clicking the Port link from the TCP Sessions table of Connect Expert.

The following screen appears:



Host IP: 243 137.72.43.243

Port Details: 5555

September 10, 2002 10:55 AM

AutoRefresh: off

Refresh: 0 seconds

Port: 5555 - Listeners: 1

Application	Connection ID	Local IP Address	Local Port	Foreign IP Address	Foreign Port	Status	Terminate	Route	Response Time
DAEMON01	#71B92	137.72.43.243	5555	137.72.43.38	3346	Establsh	Drop	Route	Ping
DAEMON01	#6521B	137.72.43.243	5555	137.72.43.117	4705	Establsh	Drop	Route	Ping

Figure 46. Port Details Report (from Connect Expert)

The fields for the Port Details report are:

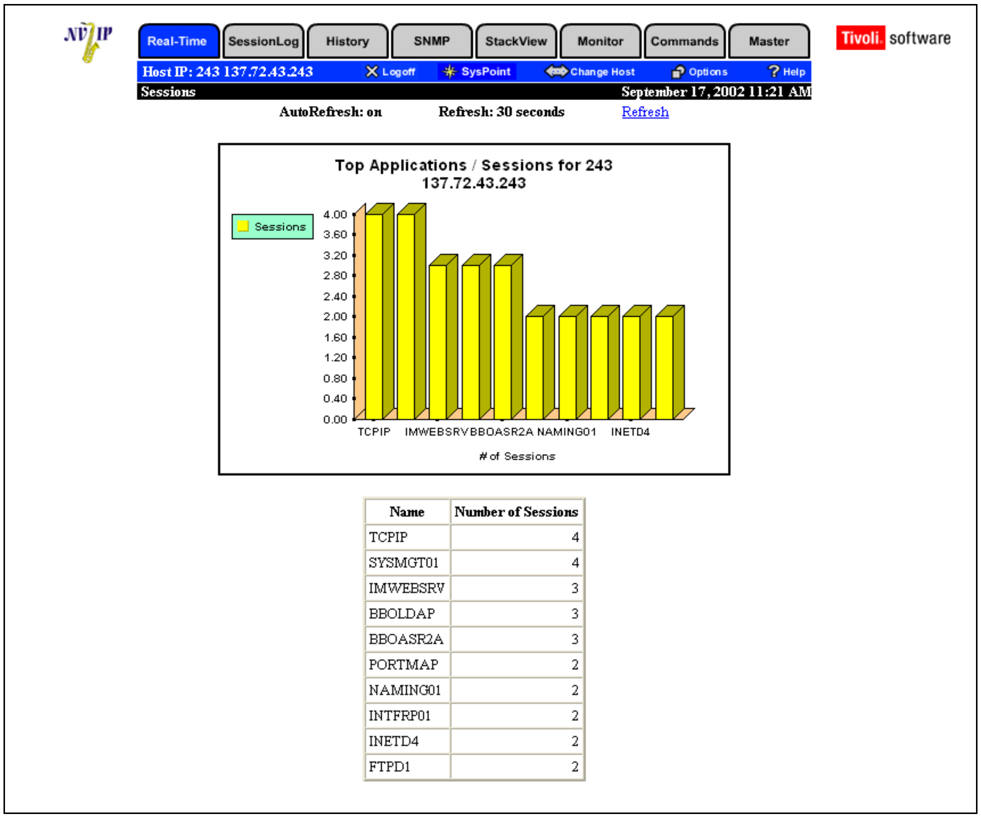
Application	Application name assigned to this Port/Address.
Connection ID	Four position hexadecimal value assigned to this connection between the Host and the application.
Local IP Address	Local IP address on mainframe TCP/IP.
Local Port	Local port on mainframe TCP/IP.

Foreign IP Address	Hyperlink to open detail screen about the Remote IP Address.
Foreign Port	Remote Port.
Status	The status of this session. Valid states are: LISTEN, SYN-SENT, SYS-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK.
Terminate	Hyperlink to execute a DROP command for the session. The DROP command terminates the session.
Route	Hyperlink to execute a TraceRte command. The TraceRte command displays the path or route this IP address is taking to the TCP/IP on the mainframe.
Response Time	Hyperlink to execute a PING command. The PING command determines the response time from this IP address to the TCP/IP address space on the mainframe.

3. From the Workload list of the Real-Time Reports screen click the Details Selected/Port Address hyperlink. You can also access the Port Details report from the Port link in the TCP Sessions table of Connect Expert. Complete the desired fields and click Submit. The report appears.
4. Do one of the following:
   - To enter another port number/address, click the Back button on the browser.
   - To return to the SysPoint Home Page, click SysPoint on the main menu bar.

Top Applications/Sessions Graph

The Top Applications/Sessions Graph displays the total number of sessions for the applications that are the heaviest users. The applications displayed are those currently using the TCP/IP address space.



Name	Number of Sessions
TCPIP	4
SYSMGT01	4
IMWEBSRV	3
BBOLDAP	3
BBOASR2A	3
PORTMAP	2
NAMING01	2
INTFRP01	2
INETD4	2
FTPD1	2

Figure 47. Top Applications/Sessions Graph

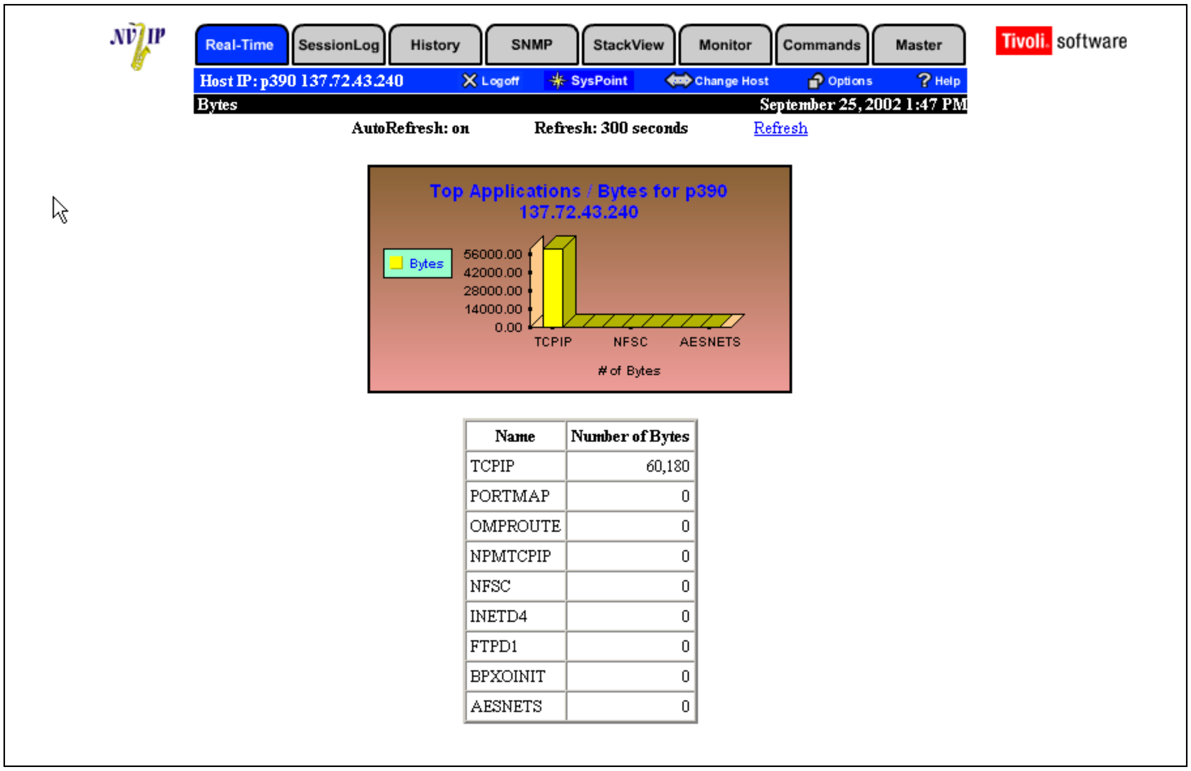
In the Top Applications/Sessions Graph, the number of sessions for your mission-critical applications are viewed as they change in real time. To monitor a particular application, use the Selected Applications/Sessions Graph.

The tabular report appears below the graphic report. The fields on this report are:

Name	Application or local port name.
Number of Sessions	Total active sessions.

Top Applications/Bytes Graph

The Top Applications/Bytes Graph provides the total number of bytes in and out since last host monitoring interval for the applications that are the heaviest users. The applications displayed are those currently using the TCP/IP address space.



Host IP: p390 137.72.43.240

Bytes September 25, 2002 1:47 PM

AutoRefresh: on Refresh: 300 seconds Refresh

Name	Number of Bytes
TCPIP	60,180
PORTMAP	0
OMPROUTE	0
NPMTCPIP	0
NFSC	0
INETD4	0
FTPD1	0
BPXOINIT	0
AESNETS	0

Figure 48. Top Applications/Bytes Graph

In a dynamic TCP/IP environment, FTP, Telnet, MVS-based Web applications, socket-attached OLTP applications, and/or other client/server applications may be executing. The Top Applications/Bytes Graph displays who is transmitting the most data over your network at the current time.

The tabular report appears below the graphic report. The fields on this report are:

Name	Application or local port name.
Number of Bytes	Sum of bytes sent and received.

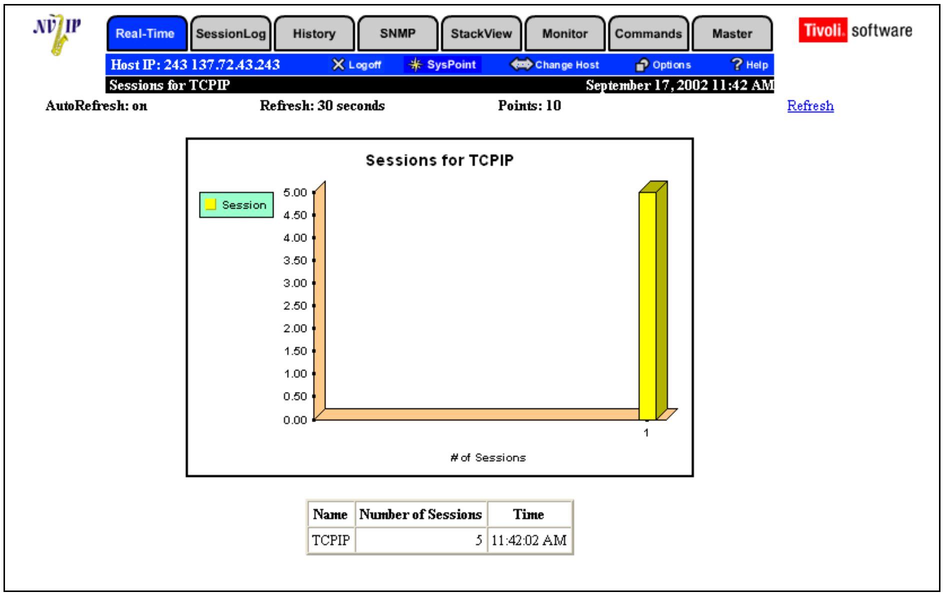
Selected Application/Session Graph

The Selected Application/Sessions Graph provides the total number of sessions for the selected application. The application displayed for selection is the one currently using the TCP/IP address space.

The Selected Application/Sessions report provides the ability to see spikes in activity. Network capacity needs to handle these infrequent events to provide continued user satisfaction.

To view this report, select the report(s) you wish to view from the table and click Do Graph.

The following screen appears:



Host IP: 243 137.72.43.243

Sessions for TCPIP September 17, 2002 11:42 AM

AutoRefresh: on Refresh: 30 seconds Points: 10

Name	Number of Sessions	Time
TCPIP	5	11:42:02 AM

Figure 49. Selected Application/Sessions

The tabular report appears below the graphic report. The fields on this report are:

Name	Application or local port name.
Number of Sessions	Total active sessions.
Time	Time the sample was taken.

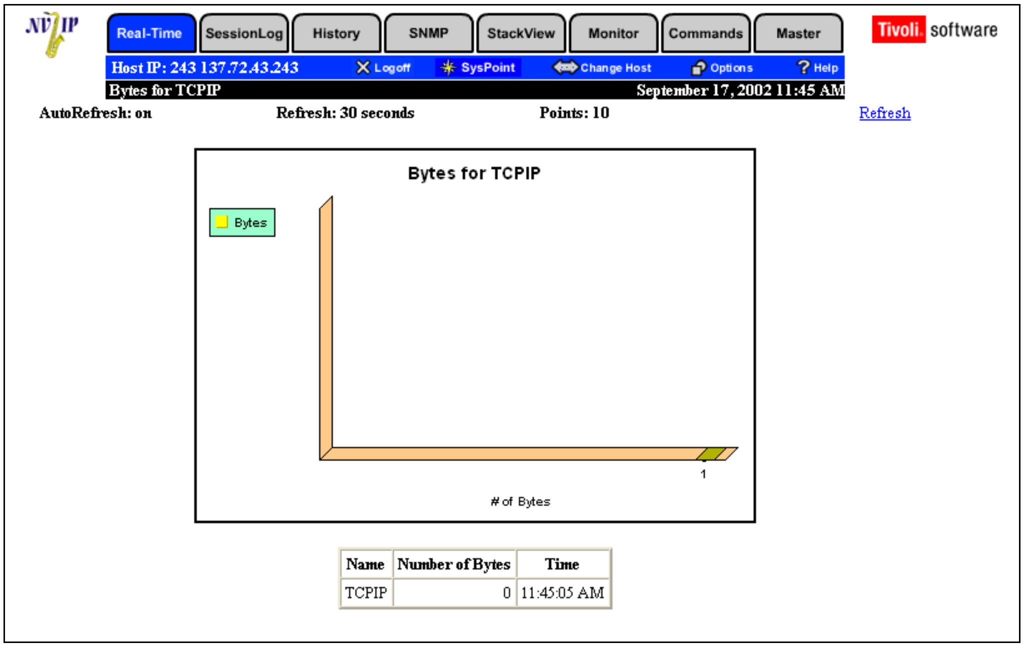
Selected Application/Bytes Graph

The Selected Application/Bytes Graph provides the total number of bytes in and out for the selected application. The applications displayed are those currently using the TCP/IP address space.

The Selected Application/Bytes Graph allows you to zoom in on the activity of any application. It is helpful in determining trends for the reallocation of resources and to head off potential performance problems.

To view this report, select the report(s) you wish to view from the table and click Do Graph.

The following screen appears:



Host IP: 243 137.72.43.243

Bytes for TCPIP

September 17, 2002 11:45 AM

AutoRefresh: on

Refresh: 30 seconds

Points: 10

Name	Number of Bytes	Time
TCPIP	0	11:45:05 AM

Figure 50. Selected Applications/Bytes Graph

The tabular report appears below the graphic report. The fields on this report are:

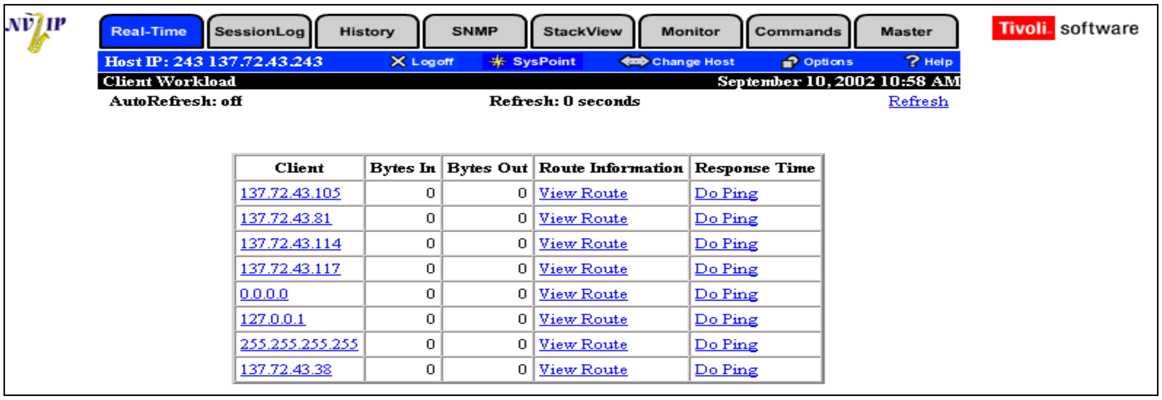
Name	Application or local port name.
Number of Bytes	Total number of bytes sent and received.
Time	Time the sample was taken.

Client Workload Report

The Client Workload Report provides information for clients (IP addresses) currently connected. Information is provided on the current clients using the TCP/IP address space and their workload in terms of bytes transferred in/out. When the report is displayed, you also have the option to obtain more detailed information (View Details, View Route) or submit a ping command (Do Ping) by clicking on the appropriate hyperlink for each.

This report shows the number of bytes sent and received since last host monitoring interval for up to 60,000 clients with at least one active session since the session was started. The application or local port may be Telnet, e-mail, or any other socket-attached application. The data is refreshed periodically at the host according to the interval specified on the parameters to the started task.

If you see an address with all high values (255.255.255.255), this is most likely an address that has had UDP traffic. It is not possible to get foreign addresses for UDP traffic from the TCP/IP stack, so all such traffic is attributed to the high values address. You may also see the loopback address: 127.0.0.1 in some traffic. This is the TCP/IP stack itself.



Host IP: 243 137.72.43.243

Client Workload September 10, 2002 10:58 AM

AutoRefresh: off

Refresh: 0 seconds

Client	Bytes In	Bytes Out	Route Information	Response Time
137.72.43.105	0	0	View Route	Do Ping
137.72.43.81	0	0	View Route	Do Ping
137.72.43.114	0	0	View Route	Do Ping
137.72.43.117	0	0	View Route	Do Ping
0.0.0.0	0	0	View Route	Do Ping
127.0.0.1	0	0	View Route	Do Ping
255.255.255.255	0	0	View Route	Do Ping
137.72.43.38	0	0	View Route	Do Ping

Figure 51. Client Workload Report

The Client Workload Report is available in tabular format only. The fields on this report are:

Client	Internet Protocol address for the selected client. Click on the IP address to see details, including the address, DNS name, and a session summary.
Bytes In	Total bytes received by MVS TCP/IP for this client for the specified interval.
Bytes Out	Total bytes sent by MVS TCP/IP for this client for the specified interval.
Route Information	Click View Route to obtain route information for that device.
Response Time	Click Do Ping to send a ping request and display the resulting response time and the number of successes so far.

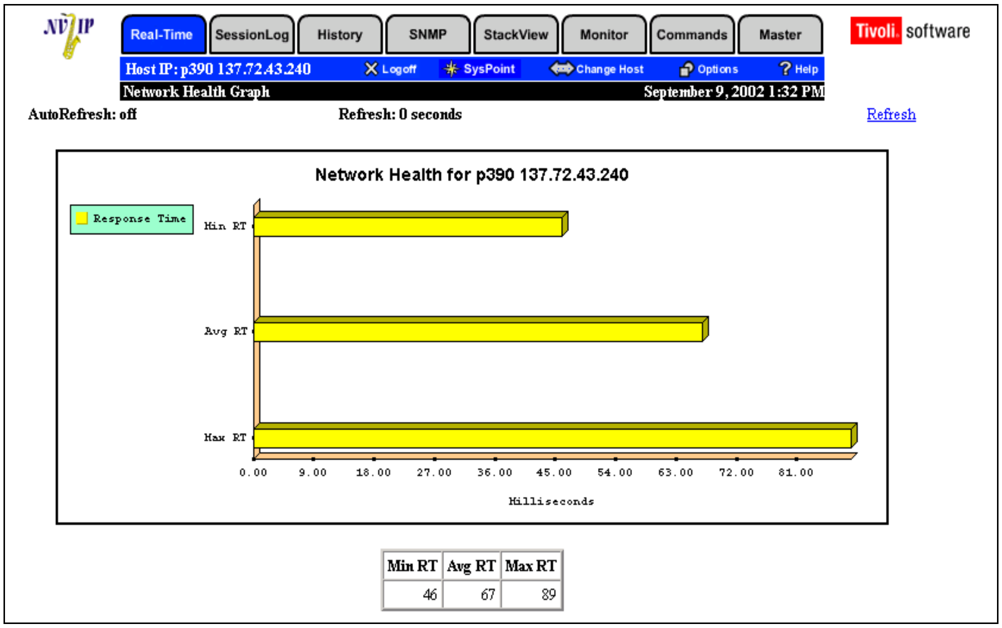
Performance Reports

The Performance reports are described on the following pages. Each report provides on-line real-time information. Each report type is briefly described below:

Network Health Graph	Graph of minimum, maximum, and average response time for all packets sent to/from all monitored clients.
Response Time Report	Tabular overview of packet size, minimum/average/ maximum response time and packet loss for all packets sent to/from a selected monitored client.
Response Time Graph	Graphical detail of average round trip response time for all packets sent to/from a selected monitored client.

Network Health Graph

The Network Health Graph is provided for clients (IP addresses) currently being monitored. These are the critical resources you have defined in the Master (1200 nodes per stack) and selected from the Start Monitoring command list of defined resources for this TCP/IP stack. The Network Health Graph provides the minimum, average, and maximum response times for all packets sent for all monitored clients for a selected host.



Host IP: p390 137.72.43.240

Network Health Graph

September 9, 2002 1:32 PM

AutoRefresh: off

Refresh: 0 seconds

Refresh

Min RT	Avg RT	Max RT
46	67	89

Figure 52. Network Health Graph

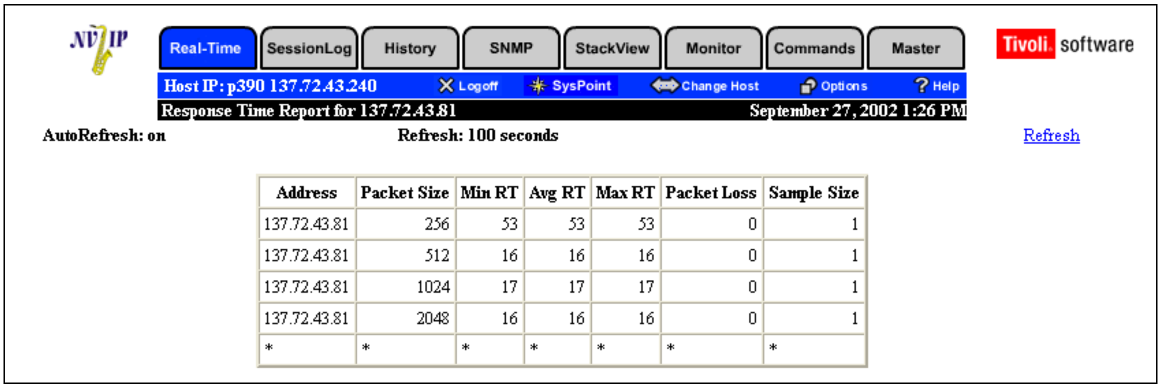
Use this real-time report to view global performance for the most critical resources in the network. By closely monitoring these critical resources, you can take appropriate action before the users notice a decline in performance. This allows you to maintain high service levels while avoiding performance problems that lead to real degradation.

The tabular report appears below the graphic report. The fields on this report are:

Minimum Response Time	Minimum response time for all packet sizes during the time interval indicated.
Average Response Time	Average response time for all packet sizes during the time interval indicated.
Maximum Response Time	Maximum response time for all packet sizes during the time interval indicated.

Response Time Report

The Response Time Report provides information in tabular format for a current selected client being monitored and its minimum, maximum, and average response times by packet size. The client is listed by IP address. Packet sizes for the test are set in the Master per IP address. To access the report, click the Selected Response Time Report hyperlink listed under Performance, select a resource, and then click the Do Report button. The following screen appears:



Host IP: p390 137.72.43.240

Response Time Report for 137.72.43.81 September 27, 2002 1:26 PM

AutoRefresh: on Refresh: 100 seconds

Address	Packet Size	Min RT	Avg RT	Max RT	Packet Loss	Sample Size
137.72.43.81	256	53	53	53	0	1
137.72.43.81	512	16	16	16	0	1
137.72.43.81	1024	17	17	17	0	1
137.72.43.81	2048	16	16	16	0	1
*	*	*	*	*	*	*

Figure 53. Response Time Report for Selected Resource

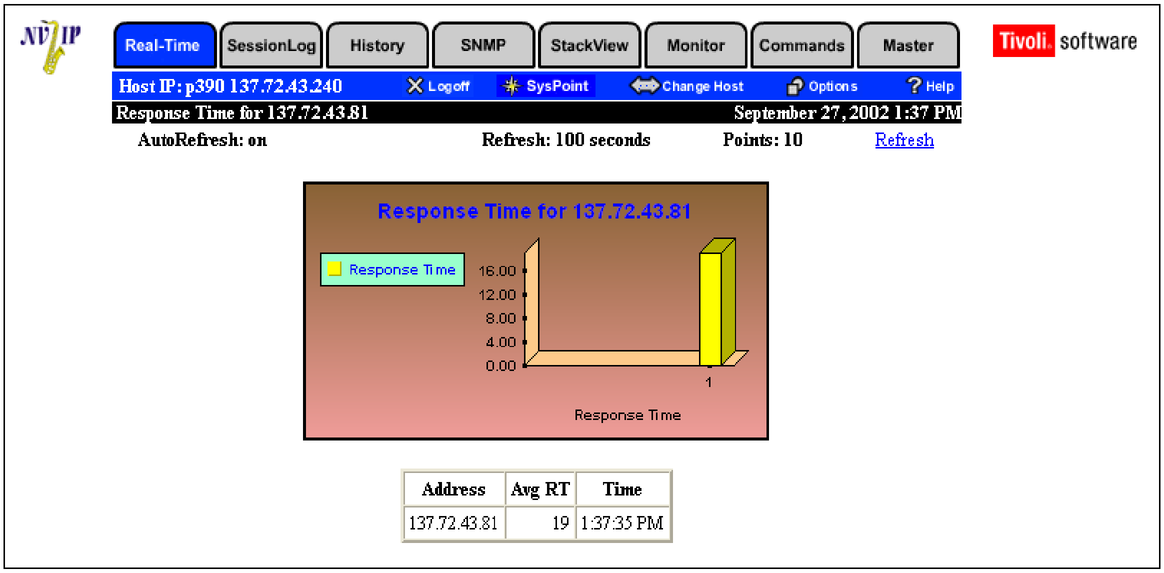
The fields on this report are:

Address	Remote IP address.
Packet Size	The packet size sent.
Min RT	Minimum response time for the packet sizes during the time interval indicated.
Average RT	Average response time for the packet sizes during the time interval indicated.
Maximum RT	Maximum response time for the packet sizes during the time interval indicated.
Packet Loss	Percent of packet loss for the packet sizes during the time interval indicated.
Sample Size	The number of samples during the time interval indicated.

To see further information for any current client, select a client by clicking on the IP Address hyperlink and then pressing the Select button. See Selected *Response Time Report* for more information.

Response Time Graph

The Response Time Graph provides information in graphical format for a current selected client and the average round trip response time of all packets sent for the selected client. The client address displays at the top of the graph. The packet response time is averaged based on the maximum response time for all the packets sent for that address in the time frame specified. To access the graph, click the Selected Response Time Graph hyperlink from under Performance, select a resource, and then click the Do Graph button.



Host IP: p390 137.72.43.240

Response Time for 137.72.43.81 September 27, 2002 1:37 PM

AutoRefresh: on Refresh: 100 seconds Points: 10

Address	Avg RT	Time
137.72.43.81	19	1:37:35 PM

Figure 54. Selected Response Time Graph for Selected Resource

Use the Response Time Graph to closely monitor a particular device that may be suspect. If a user reports a problem, you may be able to verify the network timings while the user recreates the problem.

A tabular report appears below the graph. The fields on this report are:

Address	Remote IP address.
Avg RT	Average response time for all packet sizes during the specified time period.
Time	The time of day.

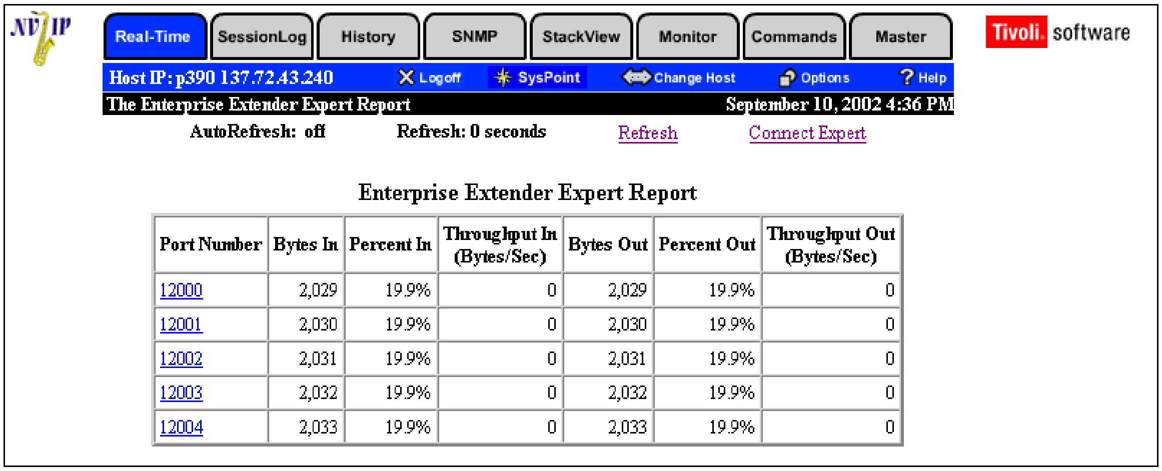
Enterprise Extender Expert

The Enterprise Extender Expert shows the EE UDP workload for each of the assigned EE ports in real time. By default, five port numbers are assigned: 12000-12004. Enterprise Extender Expert displays the number of total EE UDP bytes in/out, a percentage comparison between the in/outbound bytes and the actual port usage for all current EE activities, and the data transfer rate in bytes per second for the requested monitoring interval. The Port Number hyperlink in the report provides access to the interval-based Thru24 Summary and Detail reports as well as to the D NET,APING and D NET,RTPS Route commands.

Perform the following steps to access the Enterprise Extender Expert:

1. From the Real-Time Reports screen, click Enterprise Extender Expert. The Enterprise Extender Expert screen opens.

Note: You can also access the Enterprise Extender Expert report from Connect Expert by clicking the EE hyperlink in the Enterprise Extender Expert table.



Host IP: p390 137.72.43.240

The Enterprise Extender Expert Report September 10, 2002 4:36 PM

AutoRefresh: off Refresh: 0 seconds Refresh Connect Expert

Enterprise Extender Expert Report

Port Number	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
12000	2,029	19.9%	0	2,029	19.9%	0
12001	2,030	19.9%	0	2,030	19.9%	0
12002	2,031	19.9%	0	2,031	19.9%	0
12003	2,032	19.9%	0	2,032	19.9%	0
12004	2,033	19.9%	0	2,033	19.9%	0

Figure 55. Enterprise Extender Expert

The Enterprise Extender Expert is available only in tabular format. Each entry represents one of the ports assigned to the EE application.

The fields on the Enterprise Extender Expert tabular report are:

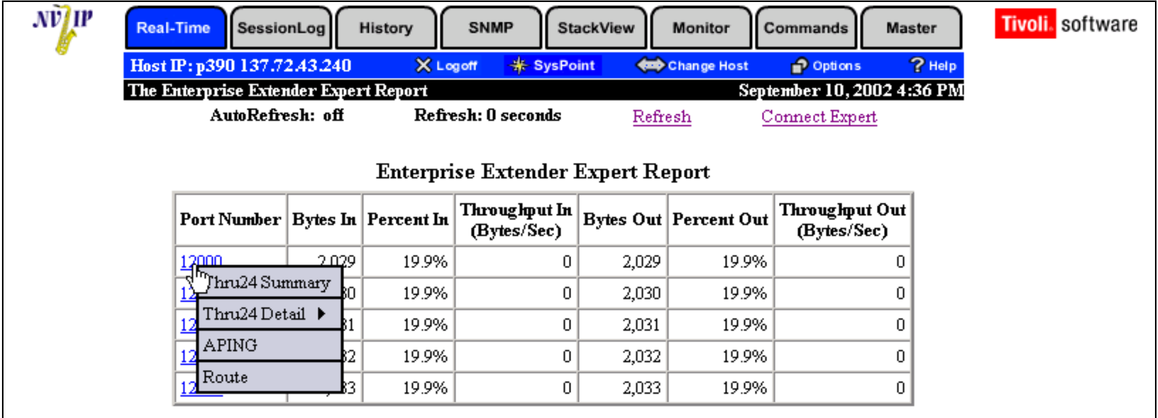
Port Number	The port number assigned to the VTAM application for Enterprise Extender. By default, the following five numbers are used:12000-12004. The Port Number is a hyperlink to the Thru24 for EE Detail and Summary reports as well as to the D NET,APING and D NET,RTPS commands.
Bytes In	The number of bytes sent in to the EE assigned port during the requested interval.
Percent In	The percentage of bytes currently being used by the EE assigned port in comparison to the total number of all bytes coming in.

Throughput In Bytes/Sec	Data transfer rate in bytes per second for bytes sent in to the EE assigned port during the requested interval.
Bytes Out	Number of bytes sent out to the VTAM application for Enterprise Extender during the requested interval.
Percent Out	Percentage of bytes received outbound by the VTAM application for Enterprise Extender compared to the total number of all bytes transmitted out.
Throughput Out Bytes/Sec	Data transfer rate in bytes per second for bytes sent out for the interval requested.

Accessing Thru 24 for EE or D NET,APING/D NET,RTPS

To access the interval-based Thru24 for EE reports or the D NET,APING/D NET,RTPS commands:

1. Click a Port Number hyperlink. A popup displays with Thru24 Summary, Thru24 Detail, APING, and RTP Route links:



Host IP: p390 137.72.43.240

The Enterprise Extender Expert Report September 10, 2002 4:36 PM

AutoRefresh: off Refresh: 0 seconds

Enterprise Extender Expert Report

Port Number	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
12000	2,029	19.9%	0	2,029	19.9%	0
12	30	19.9%	0	2,030	19.9%	0
12	31	19.9%	0	2,031	19.9%	0
12	32	19.9%	0	2,032	19.9%	0
12	33	19.9%	0	2,033	19.9%	0

Figure 56. EE Port Number popup

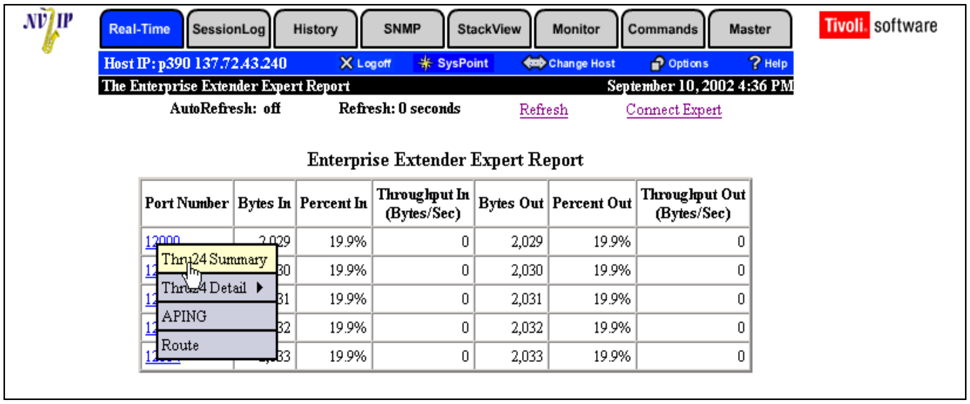
2. Do one of the following:
   - Click the Thru24 Summary link to view the Thru24 for EE Summary Report.
   - Click the Thru24 Detail link to view the Thru24 for EE Detail Report.
   - Click the APING link to open the APING Command screen. See *Commands:D NET,APING* for more information.
   - Click the Route link to open the RTPS Route Study Test Command screen. See *Commands:D NET,RTPS* for more information.

Accessing the Thru24 for EE Summary/Detail Reports

The Thru24 EE Summary and Detail reports provide near-time throughput information on EE assigned ports. The Thru24 EE Summary report shows current EE workload. It also provides a hyperlink to access the interval-based Thru24 EE Detail report. The Thru24 EE Detail report shows interval-based data for all EE assigned ports by application name, port number, TOS, Priority, and workload data.

To access the Thru24 EE Summary report:

1. From the Enterprise Extender Expert report screen, click a Port Number hyperlink. A popup appears displaying Thru24 Summary, Thru24 Detail, APING, and Route.



Host IP: p390 137.72.43.240

The Enterprise Extender Expert Report September 10, 2002 4:36 PM

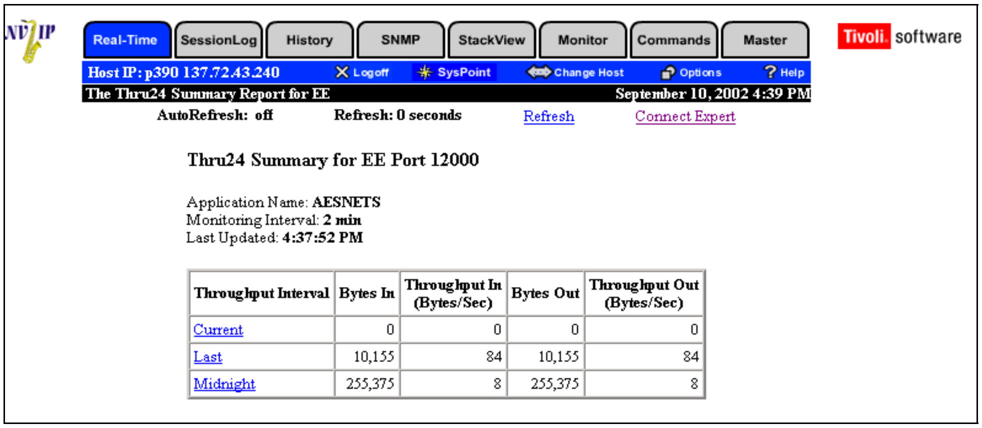
AutoRefresh: off Refresh: 0 seconds Refresh Connect Expert

Enterprise Extender Expert Report

Port Number	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
12000	2,029	19.9%	0	2,029	19.9%	0
12	30	19.9%	0	2,030	19.9%	0
12	31	19.9%	0	2,031	19.9%	0
12	32	19.9%	0	2,032	19.9%	0
12	33	19.9%	0	2,033	19.9%	0

Figure 57. Accessing the Thru24 EE Summary Report from Enterprise Extender Expert

2. Click Thru24 Summary. The Thru24 Summary report opens. In the following example, the user selected the Port Number "12002":



Host IP: p390 137.72.43.240

The Thru24 Summary Report for EE September 10, 2002 4:39 PM

AutoRefresh: off Refresh: 0 seconds Refresh Connect Expert

Thru24 Summary for EE Port 12000

Application Name: AESNETS
Monitoring Interval: 2 min
Last Updated: 4:37:52 PM

Throughput Interval	Bytes In	Throughput In (Bytes/Sec)	Bytes Out	Throughput Out (Bytes/Sec)
Current	0	0	0	0
Last	10,155	84	10,155	84
Midnight	255,375	8	255,375	8

Figure 58. Thru24 EE Summary Report for Port 12002

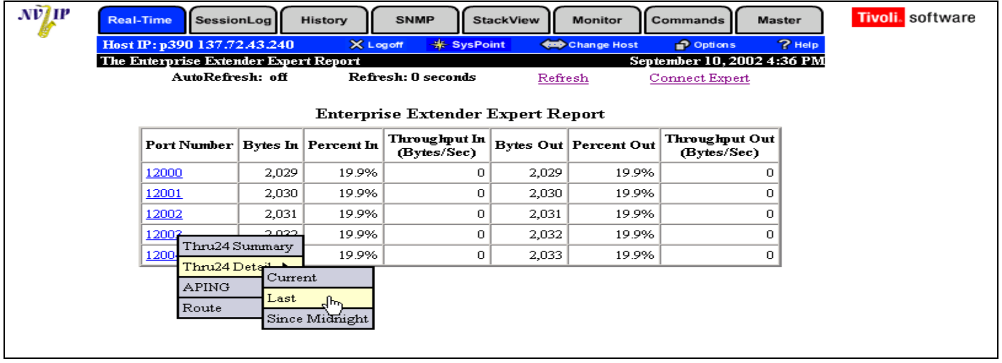
The fields in the Thru24 EE Summary report are:

Throughput Interval	Displays the intervals Current, Last, and Midnight. These fields are hyperlinks to the Thru24 EE Detail report for the selected interval.

Bytes In	The number of bytes coming in for the requested monitoring interval.
Throughput In Bytes/Sec	Data transfer rate for incoming bytes in bytes per second.
Bytes Out	The number of bytes transmitted out to the EE application for the requested monitoring interval.
Throughput Out Bytes/Sec	Data transfer rate for outgoing bytes in bytes per second.

To access the Thru24 EE Detail report:

1. From the Enterprise Extender Expert report screen, click a Port Number hyperlink. A popup displays with the following options:
   - Thru24 Summary
   - Thru24 Detail
   - APING
   - Route
2. Click Thru24 Detail. A popup displays with the following options for the monitoring interval you want to view:
   - Current
   - Last
   - Since Midnight



Host IP: p390 137.72.43.240

The Enterprise Extender Expert Report September 10, 2002 4:36 PM

AutoRefresh: off Refresh: 0 seconds

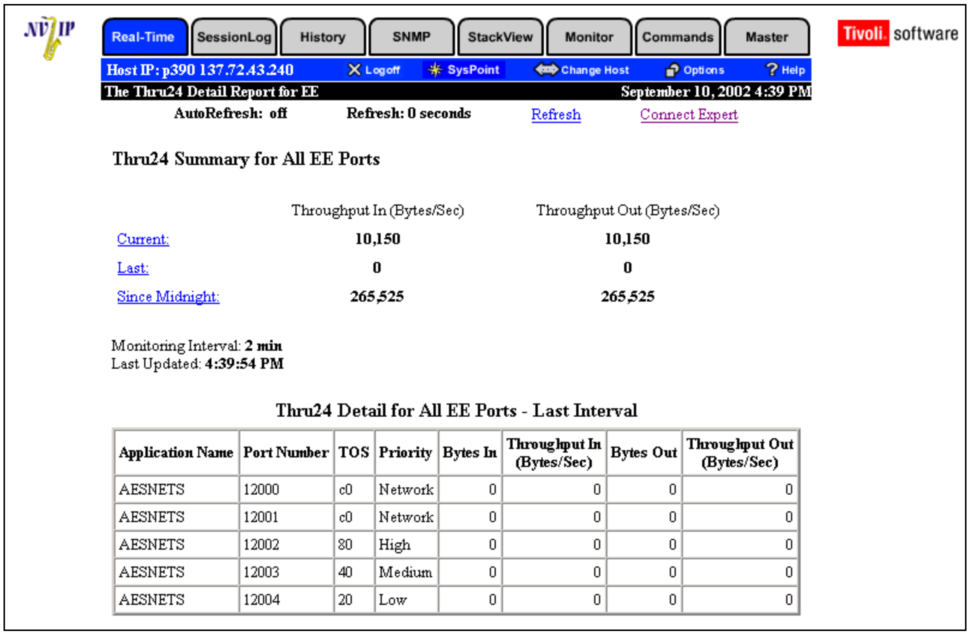
Enterprise Extender Expert Report

Port Number	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
12000	2,029	19.9%	0	2,029	19.9%	0
12001	2,030	19.9%	0	2,030	19.9%	0
12002	2,031	19.9%	0	2,031	19.9%	0
12003	2,032	19.9%	0	2,032	19.9%	0
1200		19.9%	0	2,033	19.9%	0

Figure 59. Accessing the Thru24 EE Detail Report from Enterprise Extender Expert

3. Click the desired interval. The Thru24 EE Detail report opens for the selected interval.

In the following example, the Last Interval was selected:



Host IP: p390 137.72.43.240

The Thru24 Detail Report for EE September 10, 2002 4:39 PM

AutoRefresh: off Refresh: 0 seconds

Thru24 Summary for All EE Ports

	Throughput In (Bytes/Sec)	Throughput Out (Bytes/Sec)
Current:	10,150	10,150
Last:	0	0
Since Midnight:	265,525	265,525

Monitoring Interval: **2 min**
Last Updated: **4:39:54 PM**

Thru24 Detail for All EE Ports - Last Interval

Application Name	Port Number	TOS	Priority	Bytes In	Throughput In (Bytes/Sec)	Bytes Out	Throughput Out (Bytes/Sec)
AESNETS	12000	c0	Network	0	0	0	0
AESNETS	12001	c0	Network	0	0	0	0
AESNETS	12002	80	High	0	0	0	0
AESNETS	12003	40	Medium	0	0	0	0
AESNETS	12004	20	Low	0	0	0	0

Figure 60. Thru24 EE Detail report for Last Interval

Note: You can also access the Thru24 EE Detail report by clicking a Current, Last, or Since Midnight hyperlink from the Thru24 EE Summary report.

The fields in the Thru24 EE Detail report are:

Application Name	The name of the EE application.
Port Number	The number of the assigned EE port. By default, a number between 12000-12004. Port 12000 is reserved for signaling data involved in establishing and maintaining an active EE connection.
TOS	TOS=Type of Service. The priority classification of the IP data being transported and associated port, referenced by the TOS priority level values.
Priority	There are four TOS priority level values specified for Enterprise Extender data transmission. Each TOS value is associated with an assigned EE port: • 20=LOW Priority → Port 12004 • 40=MEDIUM Priority → Port 12003 • 80=HIGH Priority → Port 12002 • C0=NETWORK → Port 12001 Port 1200 is also assigned a TOS value of "C0".

Bytes In	The number of bytes coming in for the requested monitoring interval.
Throughput In Bytes/Sec	The data transfer rate for incoming bytes in bytes per second.
Bytes Out	The number of bytes transmitted out to the EE application for the requested monitoring interval.
Throughput Out Bytes/Sec	Data transfer rate for outgoing bytes in bytes per second.

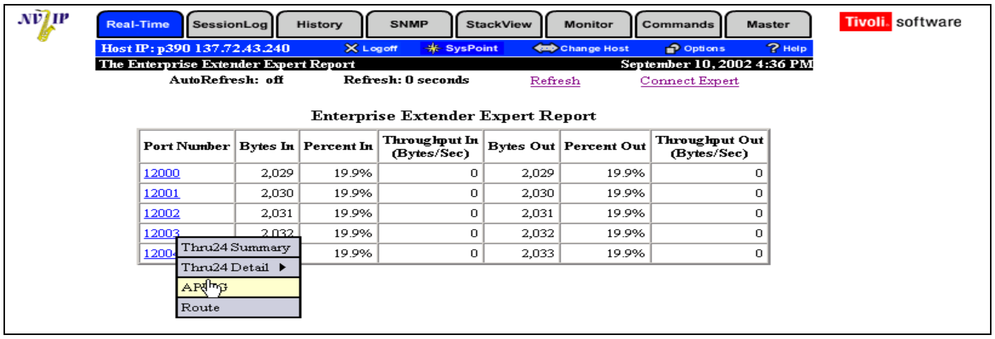
Click a different interval hyperlink in the Thru24 EE Detail report to refresh the screen and display data for that interval.

Accessing D NET,APING/D NET,RTPS Commands from EE

Access to D NET,APING and D NET,RTPS commands are provided using the Port Number hyperlink in the Enterprise Extender Expert. The D NET,APING command performs a VTAM-based Advanced Peer to Peer Networking (APPN) Ping test from the originating host to the remote host. The D NET,RTPS allows you to quickly perform a VTAM-based RTP (Rapid Transport Protocol) Route Test across the HPR pipe from any EE assigned port to a specific RTP endpoint. You can also access these commands directly from the Commands tab.

To access the D NET,APING or D NET,RTPS command:

1. From the Enterprise Extender Expert screen, click a Port Number hyperlink. A popup displays with the following options:
   - Thru24 Summary
   - Thru24 Detail (Current, Last, Since Midnight)
   - APING
   - Route



Host IP: p390 137.72.43.240

The Enterprise Extender Expert Report September 10, 2002 4:36 PM

AutoRefresh: off Refresh: 0 seconds

Enterprise Extender Expert Report

Port Number	Bytes In	Percent In	Throughput In (Bytes/Sec)	Bytes Out	Percent Out	Throughput Out (Bytes/Sec)
12000	2,029	19.9%	0	2,029	19.9%	0
12001	2,030	19.9%	0	2,030	19.9%	0
12002	2,031	19.9%	0	2,031	19.9%	0
12003	2,032	19.9%	0	2,032	19.9%	0
1200		19.9%	0	2,033	19.9%	0

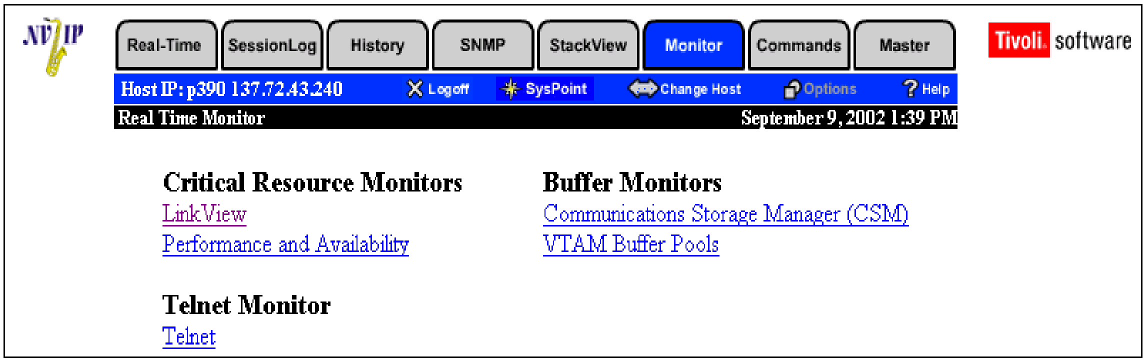
Figure 61. Accessing D NET,APING/D NET,RTPS Commands from Enterprise Extender Expert

Click APING or Route, depending upon which command you want to issue. The selected command screen appears. For more information about the D NET,APING or D NET,RTPS command, see *Commands/D NET,APING* or *Commands/D NET,RTPS*.

Real-Time Monitoring

Real-time monitoring facilities are provided for response time and availability per device; Telnet server sessions, and channel processors. To begin real-time monitoring, perform the following steps:

1. Click the Monitor tab from anywhere in the application. The Real-Time Monitoring screen opens:



Critical Resource Monitors
LinkView
Performance and Availability

Buffer Monitors
Communications Storage Manager (CSM)
VTAM Buffer Pools

Telnet Monitor
Telnet

Figure 62. Real-Time Monitor Screen

The Real-Time Monitoring functions are divided into three categories:

- **Critical Resource Monitors**
  - LinkView (Master/Operations Manager users only)
  - Performance and Availability
- **Buffer Monitors**
  - Communications Storage Manager (CSM)
  - VTAM Buffer Pools
- **Telnet Monitor**
  - Telnet

2. Click the the hyperlink of the function you would like to begin monitoring.
3. Enter the requested filters or options for the function if required.
4. Click the Submit button on the filter page if required.

Note: You can also access LinkView from the SysPoint Home page by clicking a Stack IP Address hyperlink and then clicking Show LinkView from the drop-down menu (Master and Operations Manager users only). Please see *SysPoint* for more information.

Critical Resource Monitors

Critical resource monitors include:

- Linkview
- Performance and Availability

LinkView Monitor

The LinkView feature provides the ability to monitor all links and channel-attached processors associated with your TCP/IP address space on one screen. The LinkView feature also provides access to the Thru24 for IP Link Summary/Detail reports, which provide current IP workload and throughput information. 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.

Performance and Availability Monitor

The Performance and Availability Monitor shows, at a glance, any device that is exceeding the response time threshold, experiencing packet loss, or is unavailable. The Performance Monitor provides response time and availability monitoring of servers, routers, or desktops on one screen.

Buffer Monitors

Buffer Monitors provide Real-Time monitoring of buffer status. Buffer Monitors include:

- Communications Storage Manager
- VTAM Buffer Pools

Communications Storage Manager (CSM) Buffer Pools

Communications Storage Manager (CSM) buffer pools are a critical storage resource shared between SNA and TCP/IP. The CSM History includes the following:

- CSM History Reports
- CSM Details Report
- CSM Address Space Alerts
- CSM Alerts for Buffer Pools

See *History Reports* for more information.

VTAM Buffer Pools

VTAM buffer pools are a critical storage resource shared between SNA and TCP/IP. The VTAM Buffer History reports provide both a global and a detailed view of this shared resource. The reports include:

- Usage for all buffer pools or a specific buffer pool
- Times in Expansion
- Detailed usage per Interval

Telnet Monitor

The Telnet Monitor provides the ability to monitor Telnet sessions for the selected Host on one screen. Information on Telnet sessions includes: IP address, SNA LU name, SNA application in use, and bytes transferred in/out. The Telnet Monitor displays up to 20,000 sessions. If there are no active sessions, an informational message displays *No Data Found*.

Using Critical Resource Monitors

Critical Resource Montiors include:

- LinkView
- Performance and Availability Monitor

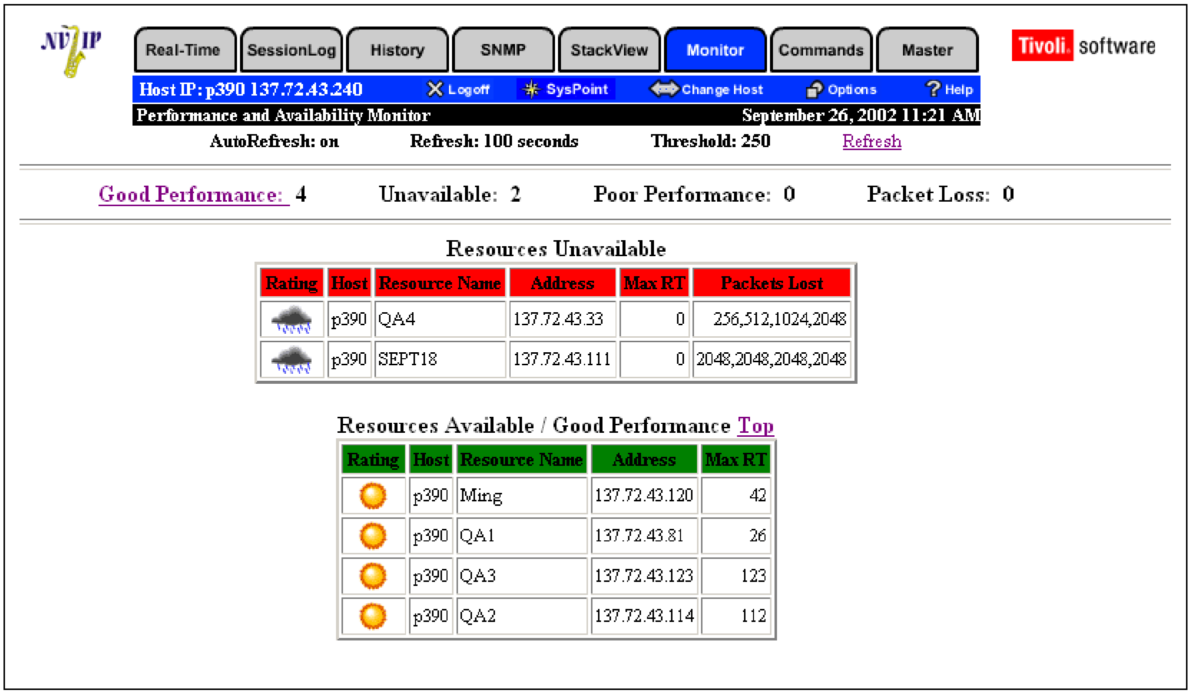
Using LinkView Mointor

LinkView shows all the channel-attached processors and links associated with your TCP/IP address space on one screen. LinkView also provides access to the interval-based Thru24 IP Summary/Detail reports, which provide near-time IP throughput information on channel-attached devices.

Using the Performance and Availability Monitor

The Performance and Availability Monitor shows, at a glance, the status of any monitored device (IP address) in the network. Devices are separated into four categories: unavailable devices, devices with packet loss, devices exceeding the response time limit, and devices without problems.

Each device is assigned a rating. The rating is a bright, shining sun if the device is available and no response time problems are found. If any device exceeds the response time limit, the rating is a sun with a few clouds on it. If a device is experiencing packet loss, the sun is shown with clouds threatening to rain. If a device is unavailable, the rating is clouds pouring down rain. For each monitored device, the specific response time or packet sizes lost may also be viewed.



Host IP: p390 137.72.43.240

Performance and Availability Monitor September 26, 2002 11:21 AM

AutoRefresh: on Refresh: 100 seconds Threshold: 250

Good Performance: 4 Unavailable: 2 Poor Performance: 0 Packet Loss: 0

Resources Unavailable

Rating	Host	Resource Name	Address	Max RT	Packets Lost
🌧	p390	QA4	137.72.43.33	0	256,512,1024,2048
🌧	p390	SEPT18	137.72.43.111	0	2048,2048,2048,2048

Resources Available / Good Performance

Rating	Host	Resource Name	Address	Max RT
☀	p390	Ming	137.72.43.120	42
☀	p390	QA1	137.72.43.81	26
☀	p390	QA3	137.72.43.123	123
☀	p390	QA2	137.72.43.114	112

Figure 63. Performance and Availability Monitor

Performance and Availability Main Panel

The real-time Performance and Availability Monitor shows, at a glance, any device that is exceeding the response time threshold, is experiencing packet loss, or is unavailable.

The following information is provided for each monitored device:

Rating	Device's assigned rating: • Available/no response time problems=shining sun • Device exceeds response time limit=sun with a few clouds • Device experiencing packet loss=sun with clouds threatening to rain • Device unavailable=clouds pouring down rain
Host	Name of MVS TCP/IP stack monitoring this resource.
Resource Name	Name assigned to this resource within this product.
Address	IP address of this resource.
Max RT	The maximum response time received for any packet sent to this resource by the Host Monitor. Up to four different packet sizes may be sent at the interval specified: 256, 512, 1024, and 2048.
Packets Lost	List of packet sizes that have been lost.

Starting the Performance and Availability Monitor

To use the real-time Performance and Availability Monitor, perform the following steps:

1. Click on the Monitor tab.
2. Click the Performance and Availability hyperlink from under Critical Resources Monitor.

   Use the Change Host option if a different Host is desired.
3. To stop viewing at any time and return to the SysPoint Home Page, click the SysPoint button on the main menu bar.

Using Buffer Monitors

Buffer Monitors provide Real-Time monitoring of buffer status. Buffer Monitors include:

- Communications Storage Manager
- VTAM Buffer Pools

Using Buffer Monitors covers:

- Using Communications Storage Manager (CSM)
- Using Telnet Monitor

Using Communications Storage Manager (CSM)

Click the Communications Storage Manager (CSM) hyperlink under Buffer Monitors to open the CSM History reports. The Communications Storage Manager (CSM) is a buffer pool resource shared between SNA and TCP/IP. Please see *History Reports* for more information.

Using VTAM Buffer Pools

Click the VTAM Buffer Pools hyperlink under Buffer Monitors to access the VTAM Buffer History reports. The VTAM Buffer Pools are a critical storage resource shared between SNA and TCP/IP. The VTAM Buffer History reports provide both a global and a detailed view of this shared resource. Please see *History Reports* for more information.

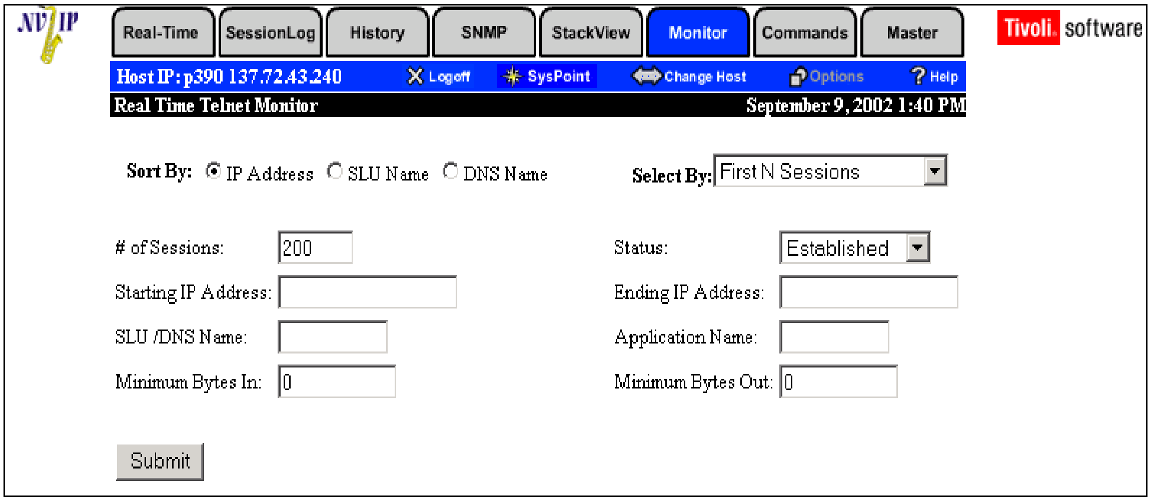
Telnet Monitoring SNA-IP Connections

The Real-Time Telnet Monitoring function provides the ability to monitor Telnet sessions for the selected Host on one screen. The main Telnet Monitor screen shows the total number of sessions along with IP address, SNA LU name, SNA application in use, and bytes in/out for a Telnet session. Telnet SNA-IP monitors and displays up to 20,000 sessions. If there are no active sessions, an informational message displays *No sessions for selected application.*

After clicking the Telnet hyperlink, the Telnet Expert Reports filter page appears. After you enter the desired filters in the Telnet SMF Log Filter screen and click the Submit button, the Telnet SMF Log main screen appears. You can move back and forth between the two screens to specify different filters and view different aspects of the report.

Telnet Expert Reports Filter Page

The Real-time Telnet Monitor filter screen allows you to set viewing options for filtering Telnet sessions. Access the filter screen by clicking the Telnet hyperlink under Telnet Monitor in the Monitor tab.



Host IP: p390 137.72.43.240

Real Time Telnet Monitor September 9, 2002 1:40 PM

Sort By: ● IP Address ○ SLU Name ○ DNS Name

Select By: First N Sessions

# of Sessions: 200

Status: Established

Starting IP Address:

Ending IP Address:

SLU /DNS Name:

Application Name:

Minimum Bytes In: 0

Minimum Bytes Out: 0

Figure 64. Real-Time Telnet Monitor - Filter Screen

To start Telnet monitoring, select the parameters that are to be operational for this monitoring session:

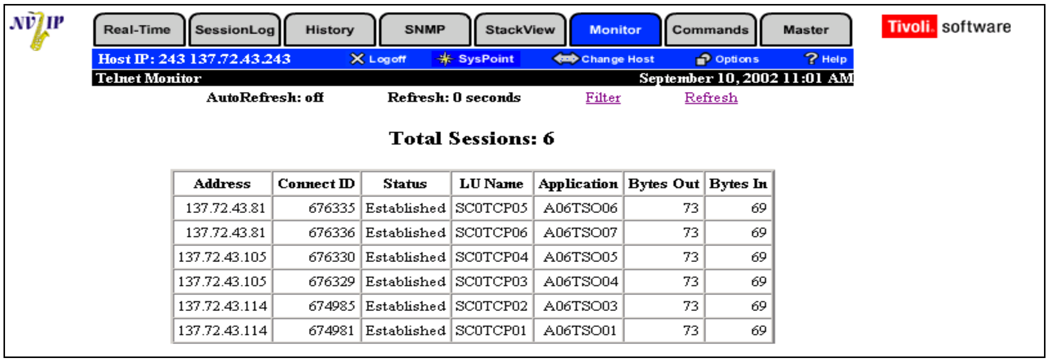
AutoRefresh	Automatically refreshes the screen by the refresh interval without any user action required.
Refresh Interval	Determines the refresh interval for new data being displayed on the screen. The minimum refresh interval is 30 seconds. The maximum is 400 seconds. Avoid setting a local interval value less than the Host Monitor interval value.
Sort By	You may choose to see the data sorted by IP Address, SLUName or DNSName.
Number of Sessions	If you choose to filter the data by number of sessions, this parameter must be entered.
Status	If you choose to filter the data by status (TCP connect state), then this parameter must be entered. You may choose to see all sessions which are in the following states: "Established", "Listen", "Syn-sent", "Syn-received", "Fin-wait-1", "Fin-wait-2", "Close-wait", "Closing", "Last-ack", "Time-wait", or "Closed".
Application Name	If you choose to filter the data by Host application name (SNA application name), this parameter must be entered.
SLU /DNS Name	If you choose to filter the data by SLU or DNS name, this parameter must be entered.
Starting IP	If you choose to filter the data by address range, this parameter

Address	must be entered.
Ending IP Address	If you choose to filter the data by address range, this parameter must be entered.
Minimum Bytes In	If you choose to filter the data by number of bytes in/out, this parameter must be entered.
Minimum Bytes Out	If you choose to filter the data by number of bytes in/out, this parameter must be entered.
Select By	You may choose to filter the data by a number of options. The available session viewing filters are:

Select first n Telnet sessions	Default = 200. Enter the number of sessions to be displayed.
Select ALL Telnet sessions	Displays all current sessions. If you are monitoring over 1000 sessions, NV4IP may take a considerable amount of time to process your request before displaying the status of all Telnet sessions.
Select by address or address range	Enter a single or a contiguous group of addresses to be monitored. Again, the number of sessions selected affects the processing time.
Select by DNS Name	Provides for the selection of Telnet sessions by their DNS name rather than IP address or SLU name.
Select by SLUName	Provides for the selection of Telnet sessions by SLUName rather than IP address.
Select by host application name	Enter the host application whose Telnet activity you wish to monitor. Examples of applications are: e-mail, TSO, or a selected database application that users access from your regional sales offices or bank branches.
Select by bytes in/out	Enter a value for bytes transferred in to the monitored Telnet sessions and a value for bytes transferred out by the monitored Telnet sessions. In order to be displayed when this filter is in effect, the Telnet session must satisfy both selected criteria.

Select by session status	Telnet sessions may be displayed by their connection status. Possible TCP connection states are: "Established", "Listen", "Syn-sent", "Syn-received", "Fin-wait-1", "Fin-wait-2", "Close-wait", "Closing", or "Last-ack".

After you have set the parameters, click the Submit button from the filter screen to open the Telnet Monitor screen.



Host IP: 243 137.72.43.243

Telnet Monitor September 10, 2002 11:01 AM

AutoRefresh: off Refresh: 0 seconds

Total Sessions: 6

Address	Connect ID	Status	LU Name	Application	Bytes Out	Bytes In
137.72.43.81	676335	Established	SC0TCP05	A06TSO06	73	69
137.72.43.81	676336	Established	SC0TCP06	A06TSO07	73	69
137.72.43.105	676330	Established	SC0TCP04	A06TSO05	73	69
137.72.43.105	676329	Established	SC0TCP03	A06TSO04	73	69
137.72.43.114	674985	Established	SC0TCP02	A06TSO03	73	69
137.72.43.114	674981	Established	SC0TCP01	A06TSO01	73	69

Figure 65. Telnet Monitor Screen

You can switch back and forth from the filter screen to the main screen as required.

The following information is provided for each monitored device:

Address	IP address of the resource connected to the Telnet session.
Connect ID	The connection identifier assigned to this session.
Status	The status of this session. For more information, please refer to *Appendix A: TCP Connect States*.
LU Name	SNA LU name associated with this Telnet session
Application	SNA application name associated with this Telnet session
Bytes Out	Bytes sent to the remote IP address from the MVS TCP/IP stack
Bytes In	Bytes sent from the remote IP address to the MVS TCP/IP stack

Starting the Telnet Monitor

To use the Real-Time Telnet Monitor, perform the following steps:

1. Click on the Monitor tab.
2. Click the Telnet hyperlink from under Telnet Monitor.
3. Enter any desired filters to limit the number of Telnet sessions from the filter page.
4. Click Submit. The Telnet Monitor screen appears. Use the Change Host option if a different Host is desired.
5. To stop monitoring at any time and return to the SysPoint Home Page, click the SysPoint button on the main menu bar.

SessionLog Expert

The SessionLog Expert allows viewing of *near time* or current time sessions, i.e. sessions that are either currently live or have recently happened. The definition of *recently* is determined by the installation and is set in the parameters for the FTP or SMF exits. The records for these sessions are held in memory by the monitor executing on the MVS host. The data for the logs comes from exits provided by SMF. For further information on the determination of how many such records to hold, please refer to the *Tivoli NetView Performance Monitor for TCP/IP Installation Guide*.

The fact that the data is held in memory at the Host Monitor means that if you restart the Host Monitor, any data that it was saving in memory is lost. Also, if too much data is kept, the installation may find that the Host Monitor is using too much storage.

To view the session logs, click on the SessionLog tab and then select the log to be viewed by clicking the corresponding hyperlink under either the FTP or Telnet and API section:

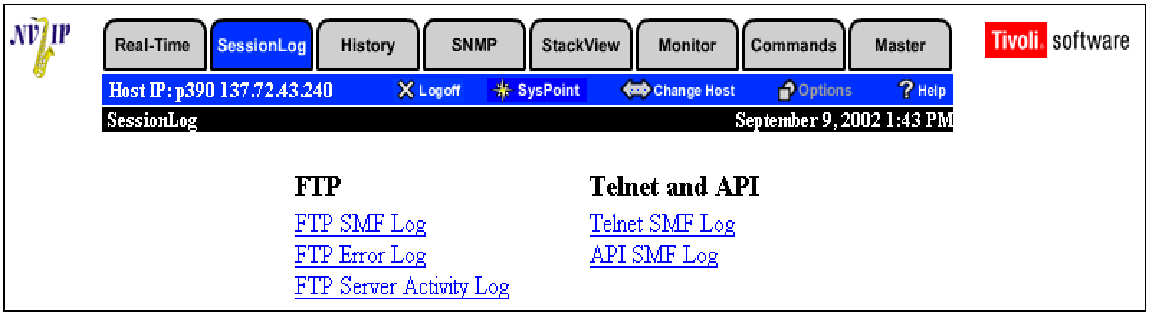
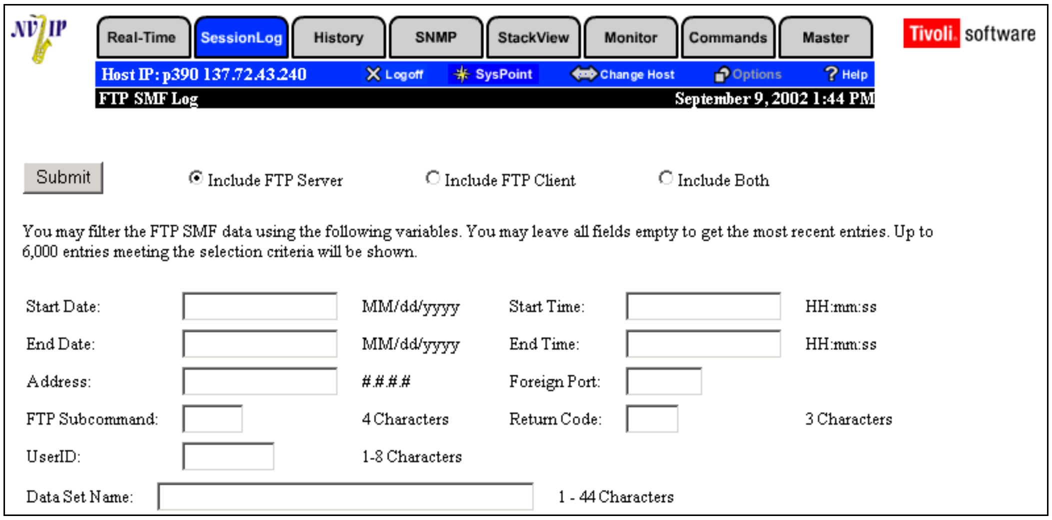


Figure 66. SessionLog Main Screen

FTP SMF Log

The FTP SMF Log provides details on completed FTPs. The data for this report is from the SMF exit. Data is provided for both FTP Client and FTP Server. An FTP Client is a Host who receives FTPs from a PC. An FTP Server is a Host who sends FTPs to a PC.

Filter the data to view only the desired FTPs. In the FTP SMF Log Filter screen below, the user has selected Include Both in order to view both FTP Servers and FTP Clients.



Host IP: p390 137.72.43.240

FTP SMF Log September 9, 2002 1:44 PM

● Include FTP Server ○ Include FTP Client ○ Include Both

You may filter the FTP SMF data using the following variables. You may leave all fields empty to get the most recent entries. Up to 6,000 entries meeting the selection criteria will be shown.

Start Date: MM/dd/yyyy Start Time: HH:mm:ss
End Date: MM/dd/yyyy End Time: HH:mm:ss
Address: #.#.#.# Foreign Port:
FTP Subcommand: 4 Characters Return Code: 3 Characters
UserID: 1-8 Characters
Data Set Name: 1 - 44 Characters

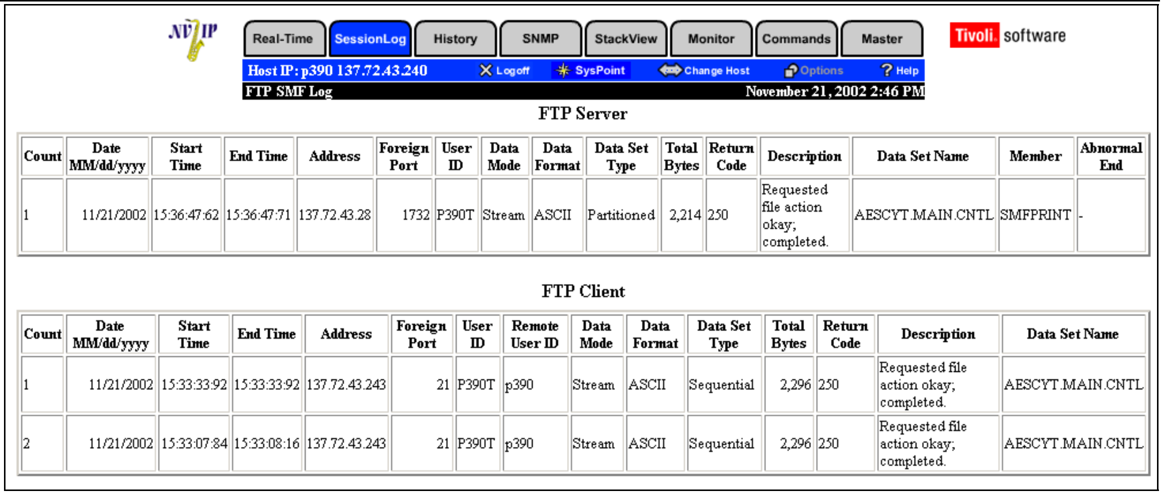
Figure 67. FTP SMF Log Filter

You may set any or all filters described below to choose only the data you want to see:

Start Date	Select FROM this date of transmission (mm/dd/yyyy)
Start Time	Select FROM this time of transmission (hh:mm:ss)
End Date	Select TO this date of transmission (mm/dd/yyyy)
End Time	Select TO this time of transmission (hh:mm:ss)
Address	Select records only for this IP address
Foreign Port	Select records only for this remote port number
FTP Subcommand	Select records only for this type of FTP subcommand. Valid subcommands include: STOR, REN, DELE, etc.
Return Code	Select records only for this return code
User ID	Select records only for this User ID
Data Set Name	Select records only for this data set name
Include FTP Server/Client/ Both	Include records for only FTP Servers, only FTP Clients, or both. FTP Server: data set is sent TO a remote IP address from a Host (Host acts as Server) FTP Client: data set is received by a Host FROM a remote IP address (Host acts as Client)

Access the FTP SMF Log by clicking the FTP SMF Log hyperlink under FTP in the SessionLog tab, entering relevant data in the FTP SMF Log Filter screen, and clicking the Submit button.

In the FTP SMF Log below, the user selected "Include Both" on the Filter Page and the Log displays both FTP Server and FTP Client data.



Host IP: p390 137.72.43.240

FTP SMF Log November 21, 2002 2:46 PM

FTP Server

Count	Date MM/dd/yyyy	Start Time	End Time	Address	Foreign Port	User ID	Data Mode	Data Format	Data Set Type	Total Bytes	Return Code	Description	Data Set Name	Member	Abnormal End
1	11/21/2002	15:36:47:62	15:36:47:71	137.72.43.28	1732	P390T	Stream	ASCII	Partitioned	2,214	250	Requested file action okay; completed.	AESCYT.MAIN.CNTL	SMFPRINT	-

FTP Client

Count	Date MM/dd/yyyy	Start Time	End Time	Address	Foreign Port	User ID	Remote User ID	Data Mode	Data Format	Data Set Type	Total Bytes	Return Code	Description	Data Set Name
1	11/21/2002	15:33:33:92	15:33:33:92	137.72.43.243	21	P390T	p390	Stream	ASCII	Sequential	2,296	250	Requested file action okay; completed.	AESCYT.MAIN.CNTL
2	11/21/2002	15:33:07:84	15:33:08:16	137.72.43.243	21	P390T	p390	Stream	ASCII	Sequential	2,296	250	Requested file action okay; completed.	AESCYT.MAIN.CNTL

Figure 68. FTP SMF Log – Main Panel

The fields on this report are:

FTP Server/Client	
Count	An Index number for each set of data.
Date	Start date of transmission (mm/dd/yyyy)
Start /End Time	Start/End time of transmission (hh:mm:ss)
Address	Remote IP address
Foreign Port	Remote port number
User ID	Local User ID
Remote User ID	Remote User ID. This field displays only in the FTP Clients table.
Data Mode	May be Stream, Block or Compressed
Data Format	Format of the data: ASCII or EBCDIC
Data Set Type	May be: PDS, Sequential or Hierarchical File System
Total Bytes	Byte count of transmission
Return Code	Numeric return code sent to this FTP client/server
Description	Translation of numeric return code sent to this FTP client/server
Data Set Name	Name of the data set transferred
Member	PDS member name -- available only for FTP Server records
Abnormal End	ABEND information – available only for FTP Server records

Using the FTP SMF Log

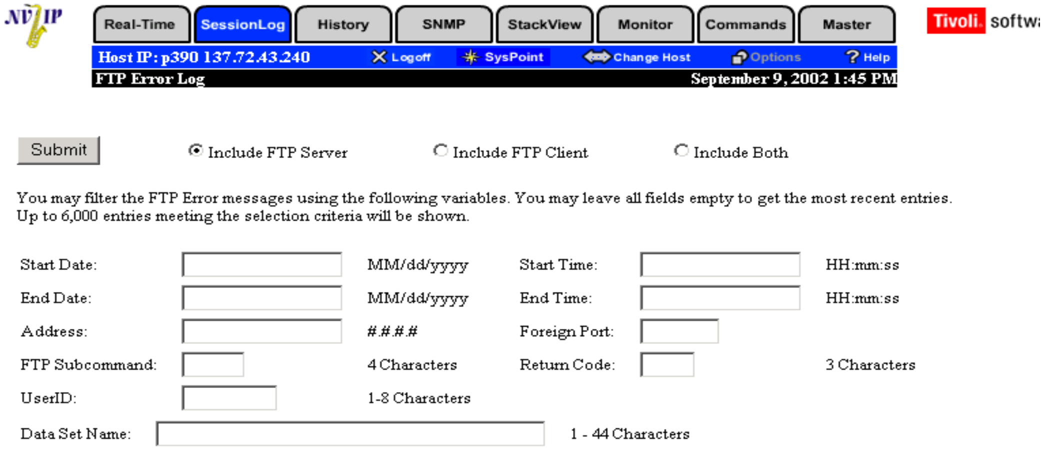
To use the FTP SMF Log, perform the following steps:

1. Click on the SessionLog tab. The SessionLog main screen appears.
2. Click the hyperlink for FTP SMF Log under FTP.
3. Click the Change Host button below the navigation bar if you want to change to a different Host. Select a different Host from the Change Host screen and click Submit.
4. Enter any desired filters in the SMF Log screen or just click the Submit button.
5. To return to the SysPoint Home Page, click the SysPoint button below the navigation bar.

FTP Error Log

The FTP Error Log provides details on FTP errors and is a subset of the FTP SMF Log. The data for this report is from the SMF exit. If an FTP is hung, you will not see an entry for it on this report; the Real-Time Monitoring function will detect such problems. If the FTP server detects an error, you will see that FTP here as well as FTP login failures.

Filter the data to view only the desired FTP errors.



Host IP: p390 137.72.43.240

FTP Error Log September 9, 2002 1:45 PM

● Include FTP Server ○ Include FTP Client ○ Include Both

You may filter the FTP Error messages using the following variables. You may leave all fields empty to get the most recent entries. Up to 6,000 entries meeting the selection criteria will be shown.

Start Date:		MM/dd/yyyy	Start Time:		HH:mm:ss
End Date:		MM/dd/yyyy	End Time:		HH:mm:ss
Address:		#.#.#.#	Foreign Port:		
FTP Subcommand:		4 Characters	Return Code:		3 Characters
UserID:		1-8 Characters			
Data Set Name:		1 - 44 Characters			

Figure 69. FTP Error Log – Filter

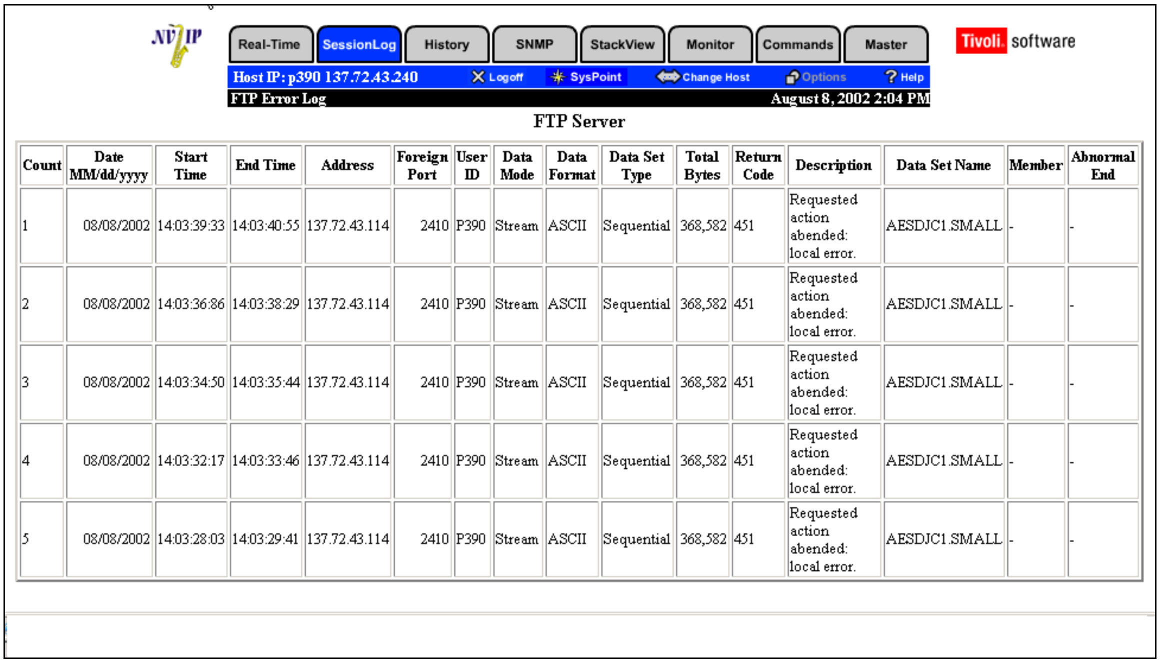
You may select any or all filters described below to choose only the data you want to see:

Start Date	Start date of transmission (mm/dd/yyyy)
Start Time	Start time of transmission (hh:mm:ss)
End Date	End date of transmission (mm/dd/yyyy)
End Time	End time of transmission (hh:mm:ss)
Address	Select records only for this IP address
Foreign Port	Select records only for this remote port number

FTP Subcommand	Select records only for this type of FTP subcommand. Valid subcommands include: STOR, REN, DELE, etc.
Return Code	Select records only for this return code
User ID	Select records only for this User ID
Data Set Name	Select records only for this data set name
Include FTP Server/Client/ Both	Include records only for FTP Server or Client FTP Server: a data set is sent TO the host from a remote IP address FTP Client: a data set is sent FROM the host to a remote IP address

Using the FTP Error Log

The FTP Error Log provides details on FTP errors. The report displays all reply codes where 250 = untrue. The data for this report is from the SMF exit.



Host IP: p390 137.72.43.240

FTP Error Log August 8, 2002 2:04 PM

FTP Server

Count	Date MM/dd/yyyy	Start Time	End Time	Address	Foreign Port	User ID	Data Mode	Data Format	Data Set Type	Total Bytes	Return Code	Description	Data Set Name	Member	Abnormal End
1	08/08/2002	14:03:39:33	14:03:40:55	137.72.43.114	2410	P390	Stream	ASCII	Sequential	368,582	451	Requested action abended: local error.	AESDJC1.SMALL	-	-
2	08/08/2002	14:03:36:86	14:03:38:29	137.72.43.114	2410	P390	Stream	ASCII	Sequential	368,582	451	Requested action abended: local error.	AESDJC1.SMALL	-	-
3	08/08/2002	14:03:34:50	14:03:35:44	137.72.43.114	2410	P390	Stream	ASCII	Sequential	368,582	451	Requested action abended: local error.	AESDJC1.SMALL	-	-
4	08/08/2002	14:03:32:17	14:03:33:46	137.72.43.114	2410	P390	Stream	ASCII	Sequential	368,582	451	Requested action abended: local error.	AESDJC1.SMALL	-	-
5	08/08/2002	14:03:28:03	14:03:29:41	137.72.43.114	2410	P390	Stream	ASCII	Sequential	368,582	451	Requested action abended: local error.	AESDJC1.SMALL	-	-

Figure 70. FTP Error Log – Main Panel

The fields on this report are:

Count	FTP error number
Date	Start date of transmission (mm/dd/yyyy)
Start /End Time	Start/End time of transmission (hh:mm:ss)
Address	Remote IP address
Foreign Port	Remote port number
User ID	Local User ID

Remote User ID	Remote User ID -- available only for FTP Client records
Data Mode	May be Stream, Block or Compressed
Data Format	Format of the data: ASCII or EBCDIC
Data Set Type	Data Set organization: PDS, Sequential or Hierarchical File System
Total Bytes	Byte count of transmission
Return Code	Numeric return code sent to this FTP client/server. For more information, please refer to *Appendix B, FTP Replies*.
Description	Description of numeric return code sent to this FTP client/server
Data Set Name	Name of the data set transferred
Member	PDS member name -- available only for FTP Server records
Abnormal End	ABEND information – available only for FTP Server records

To use the FTP Error Log, perform the following steps:

1. Click on the SessionLog tab. The SessionLog screen appears:
2. Click the FTP Error Log hyperlink under FTP.
3. Click the Change Host button below the navigation tabs if a different Host is desired. Select a different Host from the Change Host screen and click Submit.
4. Enter any filters desired in the SMF Error screen or simply click the Submit button.
5. To return to the SysPoint Home Page, click the SysPoint button below the navigation bar.

FTP Server Activity Log

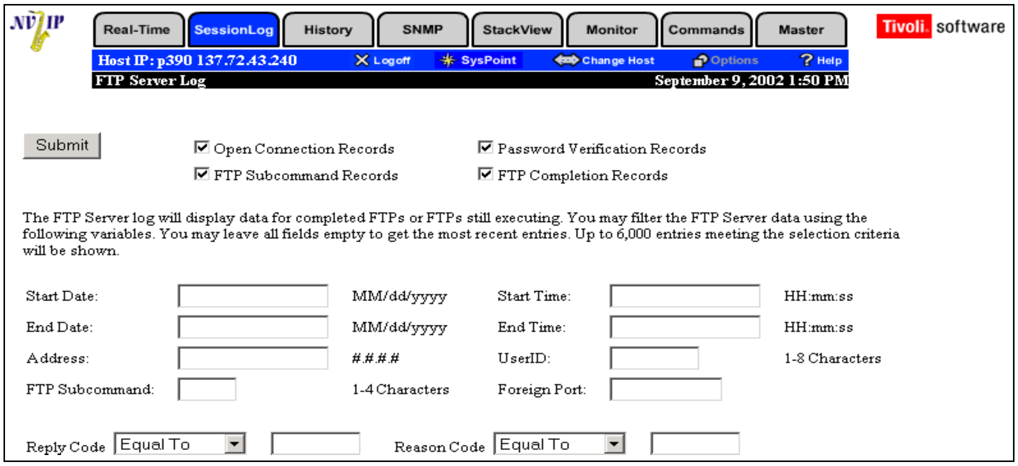
The FTP Server Activity Log displays data for FTPs that are still in progress, as well as those FTPs that have completed. The FTP command enables you to transfer data sets between your local host and any host that supports TCP/IP. Information shown in the FTP Server Log includes the commands typed in for each FTP during the progress of the session.

In the log, you may select four kinds of events:

Open connection	The initial stage of FTP logon, or whenever the user executes an OPEN command to open a new connection. This record contains the IP address.
Password verification	Immediately after the user enters the password. The password is not shown.
FTP Subcommand	Whenever the user enters an FTP command - Get, Put, Delete, etc. In this type of event, you may see an "Arg" field that may contain additional information such as the data set name being transferred. To view more FTP subcommands and explanation, please select FTP subcommands.
FTP Completion (POST)	The completion of the FTP commands RETR, STOR, STOU, APPE, DELE and RNTO. This record contains the reply code, directory type (MVS or HFS), file type (SEQ, JES or SQL), and the close reason code (file transfer completion code) of the FTP command. The close reason code contains the following information: 0 – Transfer completed normally. 4 – Transfer completed with errors; a reply text string will also be displayed. 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. Note: This record is generated by the FTPOSTPR exit, which is available only in OS/390 2.10, and z/OS 1.1 and later releases.

A sample output of the FTP Server Activity Log follows:

```
FTP Open Connection, IP=137.72.43.26,Port=1050
FTP LOGIN, USER=P390
FTP CMD=USER ,USER=  ,ARG=p390
FTP CMD=PASS ,USER=P390 ,ARG=
FTP CMD=TYPE ,USER=P390 ,ARG=A
FTP CMD=PORT ,USER=P390 ,ARG=137,72,43,26,4,27
FTP CMD=RETR ,USER=P390 ,ARG= aes.t40djc.c(aest002)
FTP CMD=CWD ,USER=P390T ,ARG= AESCYT1.MAIN.C
```



Host IP: p390 137.72.43.240

FTP Server Log September 9, 2002 1:50 PM

☑ Open Connection Records
☑ Password Verification Records
☑ FTP Subcommand Records
☑ FTP Completion Records

The FTP Server log will display data for completed FTPs or FTPs still executing. You may filter the FTP Server data using the following variables. You may leave all fields empty to get the most recent entries. Up to 6,000 entries meeting the selection criteria will be shown.

Start Date: MM/dd/yyyy
Start Time: HH:mm:ss
End Date: MM/dd/yyyy
End Time: HH:mm:ss
Address: #.#.#.#
UserID: 1-8 Characters
FTP Subcommand: 1-4 Characters
Foreign Port:
Reply Code Equal To
Reason Code Equal To

Figure 71. FTP Server Log Filter

You may select the following fields to filter the log:

Start Date	Select FROM this date of transmission. (mm/dd/yyyy)
Start Time	Select FROM this time of transmission. (hh:mm:ss)
End Date	Select TO this date of transmission. (mm/dd/yyyy)
End Time	Select TO this time of transmission. (hh:mm:ss)
Address	Select records only for this IP address.
User ID	Select records only for this User ID.
Foreign Port	Select records only for this remote port number.
FTP Subcommand	Select records only for this type of FTP subcommand. Valid subcommands include: STOR, REN, DELE, etc. Select FTP subcommands to view more FTP subcommands/explanations.
FTP Reply Code	Select FTP Completion records with a reply code that is either equal to or not equal to the specified value.
FTP Reason Code	Select FTP Completion records with a reason code that is either equal to or not equal to the specified value. Valid values are: 0, 4, 8, 12 and 16.

The following is a listing of FTP subcommands and their functions:

Subcommand	**Description**
?	Provides information to use FTP.
!	Passes an OS/390 UNIX System Services command to the local OS/390 shell. This command must be executed while using FTP in the OS/390 shell.
ACcount	Sends host-dependent account information.
APpend	Appends a data set on your local host to a file on the foreign host.
AScii	Sets the transfer type to ASCII.
BIG5	Sets the transfer type to BIG5. BIG is the minimum abbreviation for BIG5.
Binary	Sets the transfer type to IMAGE.
Block	Sets the data transfer mode to block mode. This is equivalent specifying the MODE B subcommand.
CD	Changes the working directory.
CDUp	Changes to the parent of the current working directory.
Close	Disconnects from the foreign host.
COMpress	Sets the data transfer mode to compressed mode. This is equivalent to specifying the MODE C subcommand.
CWd	Changes the working directory. (Synonymous with CD)
DEBug	Toggles or sets internal debug options.
DELEte	Deletes a single file on the foreign host.
DELImit	Displays the delimiter character between the file_name and file_type.
Dir	Lists the directory entries for files on the foreign.
Ebcdic	Sets the transfer type to EBCDIC.
Euckanji	Sets the transfer type to EUCKANJI.
File	Sets the file structure to file. This is equivalent to specifying the STRUCTURE F subcommand.
Get	Copies a file from the foreign host to your local host.
GLob	Toggles globbing (the expansion of metacharacters in file names) for the MDELETE, MGET, and MPUT subcommands.
Hangeul	Sets the transfer type to HANGEUL.
Help	Displays help information for FTP.
Ibmkanji	Sets the transfer type to IBMKANJI.

JIS78kj	Sets the transfer type to JIS78KJ.
JIS83kj	Sets the transfer type to JIS83KJ.
Ksc5601	Sets the transfer type to KSC5601.
LCd	Changes the current directory on the local host.
Lmkdir	Creates a PDS on the local host.
LOCSIte	Specifies information that is used by the local host to provide services specific to that host system.
LOCSTat	Displays FTP status information for the local host.
LPwd	Displays the name of the active working directory on the local host.
LS	Lists the names of files on the foreign host.
Mdelete	Deletes multiple files on the foreign host.
Mget	Copies multiple files from the foreign host to your local host.
Mkdir	Creates a directory on the foreign host.
Mode	Specifies the mode or data format of the transfer.
Mput	Copies multiple files on your local host to the foreign host.
Noop	Checks whether the foreign host is still responding.
Open	Opens a connection to a foreign host.
Pass	Supplies a password to the foreign host.

When you are finished entering parameters, click the Submit button to open the Server Activity Log screen.

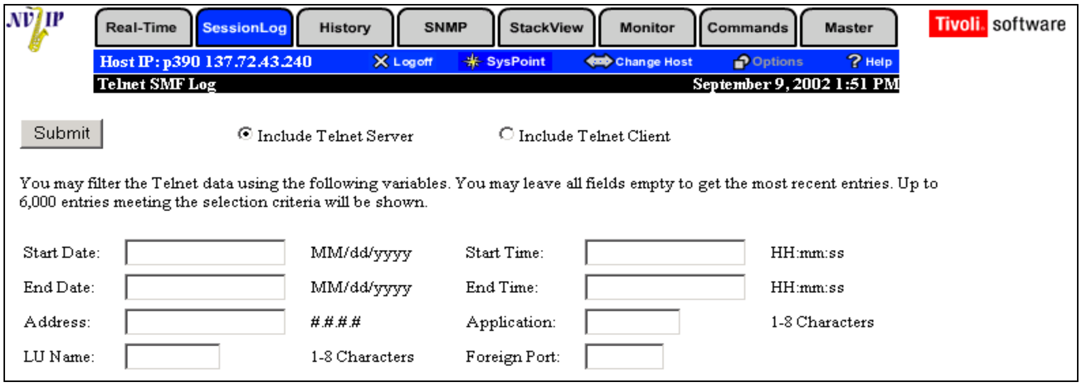
Telnet and API

The system maintains these Telnet and API logs:

- Telnet SMF Log
- API SMF Log (CICS, Web server, MQSeries)

Telnet SMF Log

The Telnet SMF Log shows the details on Telnet sessions, either completed or still active. The data for this report is from the SMF exit. Logon/logoff events are captured. Both Telnet Client and Telnet Server sessions are reported. Telnet Server sessions refer to the use of Telnet on the mainframe. Telnet Client sessions refer to the use of a Telnet Server running at a remote IP host (address). You may filter the data to view only the Telnet sessions you wish, or you may simply press Submit for the latest entries. Use of a filter is recommended to provide a more meaningful display with a shorter processing time.



Host IP: p390 137.72.43.240

Telnet SMF Log September 9, 2002 1:51 PM

● Include Telnet Server ○ Include Telnet Client

You may filter the Telnet data using the following variables. You may leave all fields empty to get the most recent entries. Up to 6,000 entries meeting the selection criteria will be shown.

Start Date: MM/dd/yyyy Start Time: HH:mm:ss

End Date: MM/dd/yyyy End Time: HH:mm:ss

Address: #.#.#.# Application: 1-8 Characters

LU Name: 1-8 Characters Foreign Port:

Figure 72. Telnet SMF Log Filter

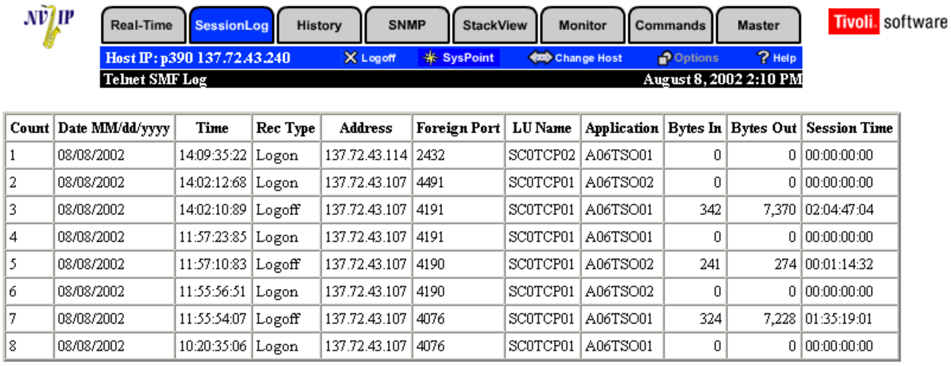
Enter filters and then click Submit to begin. Available filters are:

Start Date	Select FROM this date of logon or logoff (mm/dd/yyyy)
Start Time	Select FROM this time of logon or logoff (hh:mm:ss)
End Date	Select TO this date of logon or logoff (mm/dd/yyyy)
End Time	Select TO this time of logon or logoff (hh:mm:ss)
Address	Select records only for this remote IP address
Application	Select records only for this SNA application name -- available only for Telnet Server records. ***Note:*** You must enter the full Application Name. Wildcards are not supported.
LUName	Select records only for this SNA logical unit name -- available only for Telnet Server records

Foreign Port	Select records only for this remote port number
Include Telnet Server/Client	Include records only for Telnet Server or Client Telnet Server is when Telnet on the mainframe is used. Telnet Client is when a Telnet Server running at a remote IP host (address) is used.

Telnet SMF Log Main Panel

Access the main panel of the Telnet SMF Log by clicking Submit from the Telnet SMF Log. The main panel shows the actual Telnet sessions that have recently completed or are still in session.



Count	Date MM/dd/yyyy	Time	Rec Type	Address	Foreign Port	LU Name	Application	Bytes In	Bytes Out	Session Time
1	08/08/2002	14:09:35:22	Logon	137.72.43.114	2432	SC0TCP02	A06TSO01	0	0	00:00:00:00
2	08/08/2002	14:02:12:68	Logon	137.72.43.107	4491	SC0TCP01	A06TSO02	0	0	00:00:00:00
3	08/08/2002	14:02:10:89	Logoff	137.72.43.107	4191	SC0TCP01	A06TSO01	342	7,370	02:04:47:04
4	08/08/2002	11:57:23:85	Logon	137.72.43.107	4191	SC0TCP01	A06TSO01	0	0	00:00:00:00
5	08/08/2002	11:57:10:83	Logoff	137.72.43.107	4190	SC0TCP01	A06TSO02	241	274	00:01:14:32
6	08/08/2002	11:55:56:51	Logon	137.72.43.107	4190	SC0TCP01	A06TSO02	0	0	00:00:00:00
7	08/08/2002	11:55:54:07	Logoff	137.72.43.107	4076	SC0TCP01	A06TSO01	324	7,228	01:35:19:01
8	08/08/2002	10:20:35:06	Logon	137.72.43.107	4076	SC0TCP01	A06TSO01	0	0	00:00:00:00

Figure 73. Telnet SMF Main Panel

The fields on the main page of the Telnet SMF Log are:

Count	Refers to where that record falls in the list of records displayed
Date	Date of logon or logoff (mm/dd/yyyy)
Time	Time of logon or logoff (hh:mm:ss)
Rec Type	Type of record: logon or logoff
Address	Remote IP address
Foreign Port	Remote port number
LUName	SNA logical unit name -- available only for Telnet Server records
Application	Application name -- available only for Telnet Server records
Bytes In	Number of bytes in to the MVS host -- available only for Telnet Server records
Bytes Out	Number of bytes out to remote port -- available only for Telnet Server records
Session Time	Duration of session. (hh:mm:ss.tt) -- available only for Telnet Server

	records
NJE	NJE node name -- available only for Telnet Client records
STC Name	Started task qualifier name -- available only for Telnet Client records

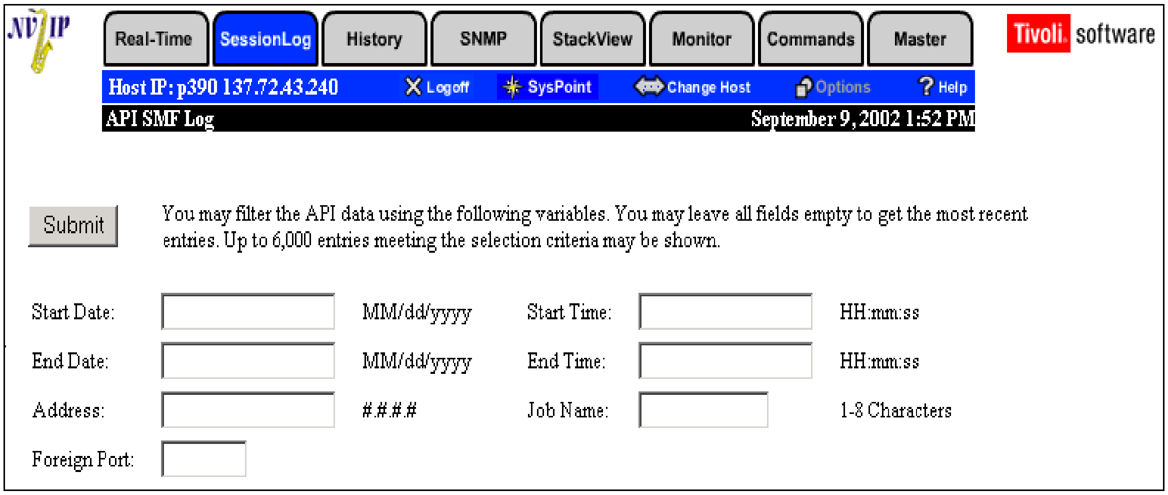
Using the Telnet SMF Log

To use the Telnet SMF Log, perform the following steps:

1. Click on the SessionLog tab.
2. Click the Telnet SMF Log hyperlink under Telnet and API. Use the Change Host option if you want to specify a different Host for this session.
3. Enter any Enter any filters desired or simply press the Submit button.

API SMF Log (CICS, Web server, MQSeries)

The API SMF Log shows the details on any socket-attached sessions that are completed or are still active. The data for this report is from the SMF exit. Initiation and termination events are captured. You may filter the data to view only the API sessions you wish, or you may simply press Submit for the latest entries. Use of a filter is recommended to provide a more meaningful display with a shorter processing time.



Host IP: p390 137.72.43.240

API SMF Log

September 9, 2002 1:52 PM

You may filter the API data using the following variables. You may leave all fields empty to get the most recent entries. Up to 6,000 entries meeting the selection criteria may be shown.

Start Date: MM/dd/yyyy
Start Time: HH:mm:ss
End Date: MM/dd/yyyy
End Time: HH:mm:ss
Address: #.#.#.#
Job Name: 1-8 Characters
Foreign Port:

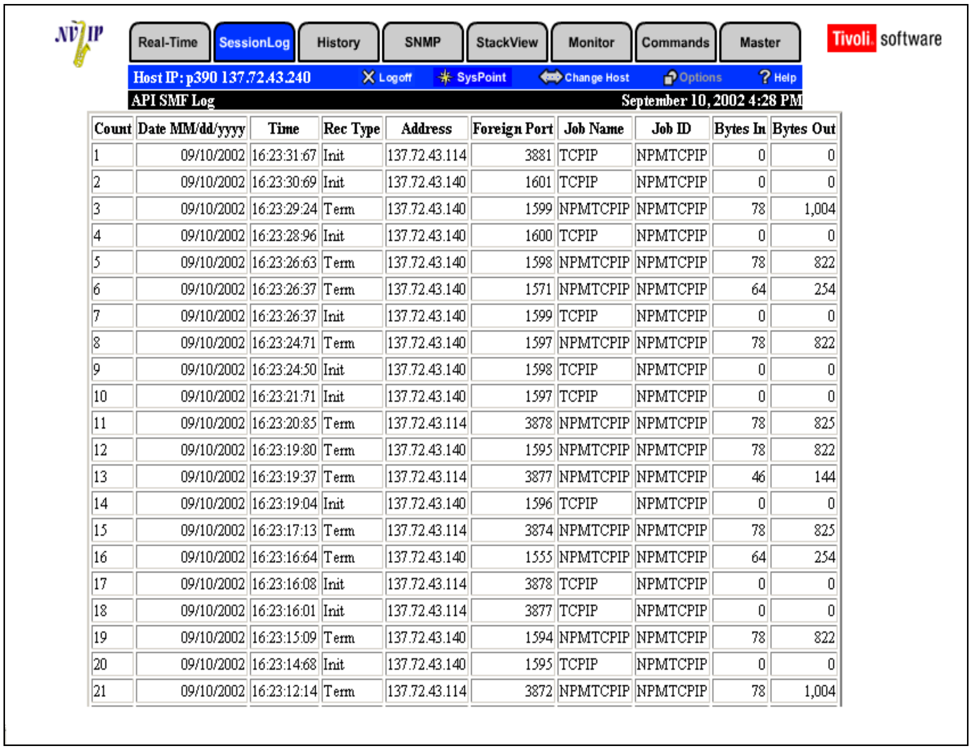
Figure 74. API SMF Log Filter

Filter descriptions are:

Start Date	Select FROM this date of initiation or termination (mm/dd/yyyy)
Start Time	Select FROM this time of initiation or termination (hh:mm:ss)
End Date	Select TO this date of initiation or termination (mm/dd/yyyy)
End Time	Select TO this time of initiation or termination (hh:mm:ss)
Address	Select only records for this IP address
JobName	Select only records for this jobname
Foreign Port	Select only records for this remote port number

Using the API SMF Log

The API SMF Log shows the details on any socket-attached sessions that are completed or are still active. The data for this report is from the SMF exit. Initiation and termination events are captured.



Host IP: p390 137.72.43.240

API SMF Log September 10, 2002 4:28 PM

Count	Date MM/dd/yyyy	Time	Rec Type	Address	Foreign Port	Job Name	Job ID	Bytes In	Bytes Out
1	09/10/2002	16:23:31:67	Init	137.72.43.114	3881	TCPIP	NPMTCPIP	0	0
2	09/10/2002	16:23:30:69	Init	137.72.43.140	1601	TCPIP	NPMTCPIP	0	0
3	09/10/2002	16:23:29:24	Term	137.72.43.140	1599	NPMTCPIP	NPMTCPIP	78	1,004
4	09/10/2002	16:23:28:96	Init	137.72.43.140	1600	TCPIP	NPMTCPIP	0	0
5	09/10/2002	16:23:26:63	Term	137.72.43.140	1598	NPMTCPIP	NPMTCPIP	78	822
6	09/10/2002	16:23:26:37	Term	137.72.43.140	1571	NPMTCPIP	NPMTCPIP	64	254
7	09/10/2002	16:23:26:37	Init	137.72.43.140	1599	TCPIP	NPMTCPIP	0	0
8	09/10/2002	16:23:24:71	Term	137.72.43.140	1597	NPMTCPIP	NPMTCPIP	78	822
9	09/10/2002	16:23:24:50	Init	137.72.43.140	1598	TCPIP	NPMTCPIP	0	0
10	09/10/2002	16:23:21:71	Init	137.72.43.140	1597	TCPIP	NPMTCPIP	0	0
11	09/10/2002	16:23:20:85	Term	137.72.43.114	3878	NPMTCPIP	NPMTCPIP	78	825
12	09/10/2002	16:23:19:80	Term	137.72.43.140	1595	NPMTCPIP	NPMTCPIP	78	822
13	09/10/2002	16:23:19:37	Term	137.72.43.114	3877	NPMTCPIP	NPMTCPIP	46	144
14	09/10/2002	16:23:19:04	Init	137.72.43.140	1596	TCPIP	NPMTCPIP	0	0
15	09/10/2002	16:23:17:13	Term	137.72.43.114	3874	NPMTCPIP	NPMTCPIP	78	825
16	09/10/2002	16:23:16:64	Term	137.72.43.140	1555	NPMTCPIP	NPMTCPIP	64	254
17	09/10/2002	16:23:16:08	Init	137.72.43.114	3878	TCPIP	NPMTCPIP	0	0
18	09/10/2002	16:23:16:01	Init	137.72.43.114	3877	TCPIP	NPMTCPIP	0	0
19	09/10/2002	16:23:15:09	Term	137.72.43.140	1594	NPMTCPIP	NPMTCPIP	78	822
20	09/10/2002	16:23:14:68	Init	137.72.43.140	1595	TCPIP	NPMTCPIP	0	0
21	09/10/2002	16:23:12:14	Term	137.72.43.114	3872	NPMTCPIP	NPMTCPIP	78	1,004

Figure 75. API SMF Log Screen

The fields on the main page of the API SMF Log are:

Count	Refers to where that record falls in the list of records displayed
Date	Date of initiation or termination (mm/dd/yyyy)
Time	Time of initiation or termination (hh:mm:ss)
Rec Type	Type of record: initiation or termination
Address	Remote IP address
Foreign Port	Remote port number
Job Name	Name of job or task • For interactive TSO API usage: the user's TSO User ID • For batch submitted jobs: the name of the JOB card • For started procedures: the name of the procedure
Job ID	For socket API applications, the JES job identifier (name of address space)
Bytes In	Number of bytes in to the MVS host
Bytes Out	Number of bytes out to remote port

To use the API SMF Log, perform the following steps:

1. Click on the SessionLog tab.
2. Click the API SMF Log hyperlink under Telnet and API. Use the Change Host option to specify a different Host for this session.
3. Enter any filters desired or simply press the Submit button.

The fields available on the performance options are:

AutoRefresh	Automatically refresh the screen by the refresh interval without any user action required.
Refresh Interval (seconds)	Determines the refresh interval for new data being displayed on the screen. Minimum refresh interval is 30 seconds. The maximum is 400 seconds. Avoid setting a local interval value less than the Host Monitor interval value.
Response Time Threshold	Enter a value for the response time threshold for all devices being monitored. The threshold settings affect only the current viewing session. They do not affect Alerting at the Host.

SNMP MIB Browser

Simple Network Management Protocol (SNMP) was designed as an answer to the communication problems brought about by different network platforms, protocols, and proprietary network operating systems. Although designed as a temporary solution, it has become the network management protocol of choice.

SNMP exchanges network information through messages known as PDU (protocol data units). From a high-level perspective, the PDU is seen as an object containing variables consisting of both titles and values. SNMP uses five types of PDUs to monitor a network: two deal with setting terminal data, two deal with reading terminal data, and one, the trap, is used for monitoring network events such as start-ups and shut-downs.

The greatest advantage in using SNMP is its simple design. This makes it easy to implement on a large network, for it neither takes a long time to set up nor puts a great deal of stress on the network. In addition, its easy-to-use features allow you to quickly program variables you would like to have monitored in your network. The expandability of SNMP continues to be an asset in the ever more complicated Intranet and Internet networking environments of today's business world.

As a result of its popularity, almost all major vendors of Internet hardware design their products to support SNMP.

The SNMP Public MIB variables available in NV4IP are:

System	Provides generic configuration information, such as device description, agent's hardware and software, how long ago the agent was started/re-started, device name, physical location, and device services
IP (G)	Contains information on the IP subsystem of a managed node such as whether the device is acting as a router or a host, default TTL for packets, datagrams delivered, discarded, timeout value and so forth
ICMP (G)	Uses counters to keep track of the message types generated and received by this local ICMP entity including received, sent, received in error or not sent due to error
UDP (G)	Provides four counters and a table for datagram delivery, destined for unknown ports, discarded due to format errors, and sent from UDP group
TCP (G)	Identifies the retransmission algorithm, maximum/minimum retransmission timeouts, and number of active/passive opens, resets, connections, etc.
Interface (G)	Contains generic information on the interface layers such as- interface description, interface type, MTU size, transmission rate, media specific address etc.
Route Table	Contains an entry for each route known to the entity.

The SNMP private MIB variables available in NV4IP are:

IBM2216	Contains the table in the MIB module for objects used to manage the IBM 2216 device. The table contains information about PCI adapters in the IBM 2216 equipment.
CISCO CIP	Describes the MIB module for objects used to manage the CICSO Mainframe Channel Connection cards. The values can be accessed to determine the general state of the CMCC.
CISCO CIP Channel (*subscreen of CISCO CIP*)	Provides information on the MIB module for objects used to manage the Cisco Mainframe Channel Connection (CMCC) cards. The Channel table contains a list of objects pertaining to the channel or daughter board on the CMCC card. Click an Index hyperlink in the CISCO CIP screen to access this subscreen.
CISCO SubChannel (*subscreen of CISCO CIP Channel*)	Contains the list of objects pertaining to each host connection. Click an Index hyperlink in the CISCO CIP Channel subscreen to access this subscreen.
TN3270 Global	Describes the MIB module for objects used to manage the TN3270 server.
TN3270 PU Table (*subscreen of TN3270 Global*)	Contains the table in the MIB module for objects used to manage the TN3270 server. The PU table holds objects that describe the PU configuration parameters not defined in the NAU MIB, APPN MIB or DLUR MIB. Click an Index hyperlink in TN3270 Global to access this subscreen.
TN3270 LU Table (*subscreen of TN3270 PU Table*)	Contains the table in the MIB module for objects used to manage the TN3270 server. The LU table helps map LU to client IP address/port. Click an Index hyperlink in the TN3270 LU Table to access this subscreen.
TN3270E Config	Contains the Configuration table in the MIB module for objects used to manage the TN3270E server. The Configuration table contains information about the general state of the server.
TN3270E Statistics	Contains a set of statistics concerning global TN3270E server performance. An entry can be global with respect to a single TN3270E server or it can be specified at the port level.
TN3270E TCP	Contains the table in the MIB module for objects used to manage the TN3270E server. This table has an entry for each TN3270(E) client connection that is active at a TN3270E server.
TN3270E SNA Server Map Table (*subscreen of TN3270E Statistics and TN3270E TCP)*	Contains the table in the MIB module for objects used to manage the TN3270E server. This table defines the mapping of an SLUName to a PLUName.

OSA Express (G)	Contains one entry per OSA Express device interface.
OSA Performance (G)	Provides performance information per each LPAR's utilization of an OSA-Express adapter.
OSA Ethernet (G)	Represents the Ethernet ports associated with the OSA Express Channel Table entries for Ethernet adapters.

Using SNMP MIB

To access SNMP MIB Browser, perform the following steps:

1. Click the SNMP tab from anywhere in the application. The SNMP Browser main screen displays in a second browser window. You may maximize or change the size of the new browser window to suit your preference.
2. Enter the IP address of an SNMP-capable device in the text box labeled Address. The MIBs on this address are interrogated.
3. If desired, change the community name by entering it at the text box for Community Name. The community name is password-protected and your entry will display in asterisks, so be sure to type carefully.

   The default community name is "public". Many installations change the name for security purposes. Only a community name with read authority is required for NV4IP.
4. Select the MIB type desired from the MIB Type drop-down list box. A (G) displays after the MIB type if graphs are available for that type.

   You may want to start with the System MIB to make sure you have access to the device.

   > ***Note:*** To view system group information for an address, enter the IP address in the Address box and then select System as the MIB Type. The device must have SNMP capability.
5. Do one or more of the following:
   - Click the View Changes checkbox to view the delta from one time interval to the next.
   - Click the View Graphs checkbox to view any graphs that are available.
   - Click the Graphs on Top checkbox to view graphs at the top of the page and the tabular MIB fields at the bottom. Or to reverse the display and view the tabular MIB fields at the top of the page and the graphs at the bottom, leave the Graphs on Top checkbox unchecked.

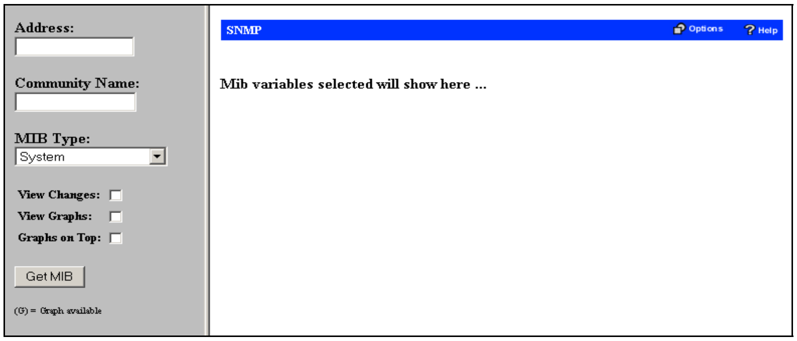
     In either case, the View Graphs checkbox must also be checked in order to display graphs.

   You can quickly scroll to the bottom of the page to view the other format (Graph or MIB fields) by clicking the Graphs or Report link at the top of the screen.

6. Click the Get MIB button. A message appears on the second frame in the SNMP window indicating that the search for information has started. Please wait until either the desired MIB information appears on the screen (in the second frame) or an error message appears. For some MIBs, this may take a few minutes.
7. To view other MIBs for the selected address, select a different MIB type from the MIB Type drop-down list and click the Get MIB button.
8. When you have finished viewing the MIBs, close the SNMP MIB Browser window by clicking the "x" close box in the upper right corner of the window. You are returned to the previous window and the navigation bar displays, from which you can access other NV4IP functions.

SNMP MIB Browser Main Panel

All SNMP MIBs are accessed from the main panel. The main panel consists of two frames. The first frame contains the requested information and operational parameters while the second frame shows the result of the requested display. The following figure shows the SNMP MIB Main Panel as it appears after clicking the SNMP tab:



MIB Type: System

Mib variables selected will show here ...

Figure 76. SNMP MIB Browser - Main Panel

The fields on the main panel are:

Address	IP address of device to be queried.
Community Name	Read community name of device. This is similar to a password and your entry will display as asterisks, so type carefully.
MIB Type	The MIB to view. See beginning of this section for listing of supported MIBs.
View Changes	View the delta from one time to the next.
View Graphs	View graphs for this MIB, if available.
Graphs on Top	Check this box to display graphs at the top of the report, or leave unchecked to display the tabular MIB fields first.

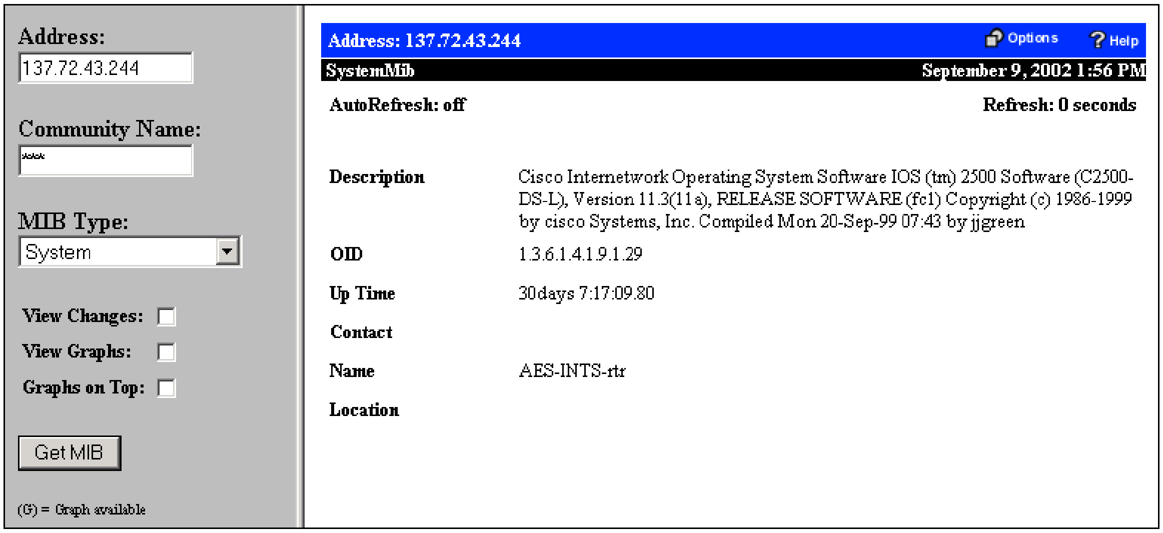
SNMP Options

SNMP options include parameters that are applied to all SNMP functions. When you click on the Options button from the title bar, you are given two options. You may proceed by clicking on SNMP Options, or you may click Cancel to return to the previous screen. If you proceed, you can set SNMP parameters using the following fields:

Time Out Value (Seconds)	The maximum number of seconds that can elapse while trying to retrieve MIB information before an error message appears.
Number of Retries	The maximum number of times a retrieval attempt will be made without having to reenter the information.

System

The System group is the managed node itself. It is supposed to summarize the specific MIB modules, which are implemented by this node. Implementation of the System group is mandatory for all networks. If an agent is not configured to have a value for any of these variables, a string of length 0 is returned.



Address: 137.72.43.244

Community Name: ***

MIB Type: System

View Changes: ☐

View Graphs: ☐

Graphs on Top: ☐

Address: 137.72.43.244

SystemMib September 9, 2002 1:56 PM

AutoRefresh: off Refresh: 0 seconds

Description	Cisco Internetwork Operating System Software IOS (tm) 2500 Software (C2500-DS-L), Version 11.3(11a), RELEASE SOFTWARE (fc1) Copyright (c) 1986-1999 by cisco Systems, Inc. Compiled Mon 20-Sep-99 07:43 by jjgreen
OID	1.3.6.1.4.1.9.1.29
Up Time	30days 7:17:09.80
Contact	
Name	AES-INTS-rtr
Location	

Figure 77. SNMP Browser: System Group

The fields on the System group display are:

Description	System Description. A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating system, and networking software. It is mandatory that this contain only printable ASCII characters.
OID	System Object ID. The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprise subtree (1.3.6.1.4.1) and provides an easy, unambiguous means for determining what kind of box is being managed. For example, if vendor Flintstones, Inc. was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its Fred Router product.
UpTime	System Up Time. The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
Contact	System Contact. The textual identification of the contact person for this managed node, together with information on how to contact this person.

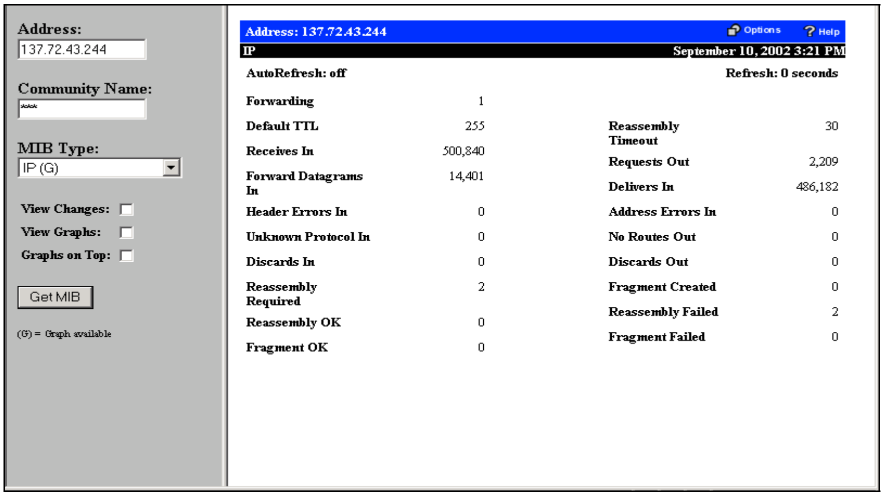
Name	System Name. An administratively assigned name for this managed node. By convention, this is the node's fully qualified domain name.
Location	System Location. The physical location of this node (e.g., telephone closet, 3rd floor).

IP (G)

The IP objects are the statistics and gateway routing tables for the IP layer. The "(G) after "IP" indicates that graphs are available. The graphs consist of several scalars and four tables. They track the datagram information in terms of datagrams forwarded, discarded due to format errors, discarded due to misdelivery, discarded due to resource limitations and so forth. The IP Routing table is part of this group and its contents are discussed separately.

IP MIB Information

The initial IP MIB information is available upon clicking Get MIB with the MIB type set to IP. The route table is actually a part of the IP MIB and may be viewed by selecting the Route Table MIB Type.



Address: 137.72.43.244

Community Name: ***

MIB Type: IP (G)

View Changes: ☐

View Graphs: ☐

Graphs on Top: ☐

Address: 137.72.43.244

IP September 10, 2002 3:21 PM

AutoRefresh: off Refresh: 0 seconds

Forwarding	1		
Default TTL	255	Reassembly Timeout	30
Receives In	500,840	Requests Out	2,209
Forward Datagrams In	14,401	Delivers In	486,182
Header Errors In	0	Address Errors In	0
Unknown Protocol In	0	No Routes Out	0
Discards In	0	Discards Out	0
Reassembly Required	2	Fragment Created	0
Reassembly OK	0	Reassembly Failed	2
Fragment OK	0	Fragment Failed	0

Figure 78. SNMP Browser: IP Group

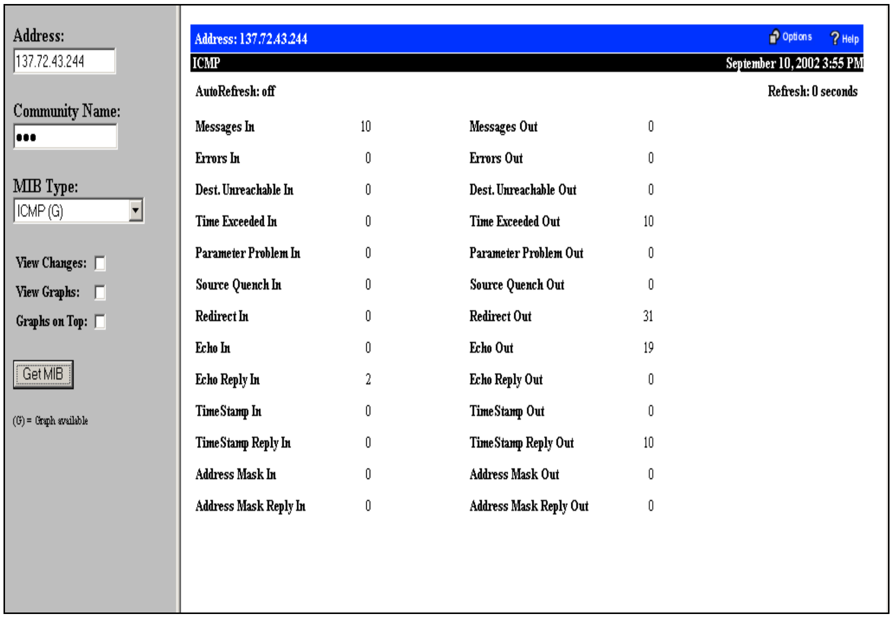
The fields on the IP MIB Information screen are:

Forwarding	Indicates whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP hosts do not (except those source-routed via the host). The options are: 1 = forwarding (acting as a gateway), 2 = not forwarding (not acting as a gateway).
Default TTL	The default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol. The values may be 1-255.
Reassembly Timeout	The maximum number of seconds that received fragments are held while awaiting reassembly at this entity.
Receives In	The total number of input datagrams received from interfaces, including those received in error.
Requests Out	The total number of IP datagrams, which local IP user-protocols (including ICMP), supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
Forward Datagrams In	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities that do not act as IP Gateways, this counter includes only those packets, which were source-routed via this entity, and the source-route option processing was successful.
Delivers In	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
Header Errors In	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
Address Errors In	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Unknown Protocols In	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

No Routes Out	The number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in ipForwDatagrams that meet this "no-route" criterion, including any datagrams that a host cannot route because all its default gateways are down.
Discards In	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
Discards Out	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but they were discarded (e.g., for lack of buffer space). Note that this counter includes datagrams counted in ipForwDatagrams if any such packets meet this discretionary discard criterion.
Reassembly Required	The number of IP fragments received that needed to be reassembled at this entity.
Fragment Created	The number of IP datagram fragments generated as a result of fragmentation at this entity.
Reassembly OK	The number of IP datagrams successfully reassembled.
Reassembly Failed	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragment OK	The number of IP datagrams that have been successfully fragmented at this entity.
Fragment Failed	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.

ICMP (G)

The ICMP objects (Internet Control Message Protocol) are the input and output error and control message statistics for the IP layer. The (G) indicates that graphs are available. The ICMP group consists of twenty-six counters that track the number of times this message type was generated by and received by the local ICMP entity. The other counters keep track of the total messages received, sent, received in error, or not sent due to error.



Address: 137.72.43.244

Community Name: ●●●

MIB Type: ICMP (G)

View Changes: ☐

View Graphs: ☐

Graphs on Top: ☐

(G) = Graph available

Address: 137.72.43.244

ICMP September 10, 2002 3:55 PM

AutoRefresh: off

Refresh: 0 seconds

Messages In	10	Messages Out	0
Errors In	0	Errors Out	0
Dest. Unreachable In	0	Dest. Unreachable Out	0
Time Exceeded In	0	Time Exceeded Out	10
Parameter Problem In	0	Parameter Problem Out	0
Source Quench In	0	Source Quench Out	0
Redirect In	0	Redirect Out	31
Echo In	0	Echo Out	19
Echo Reply In	2	Echo Reply Out	0
TimeStamp In	0	TimeStamp Out	0
TimeStamp Reply In	0	TimeStamp Reply Out	10
Address Mask In	0	Address Mask Out	0
Address Mask Reply In	0	Address Mask Reply Out	0

Figure 79. SNMP Browser: ICMP Group

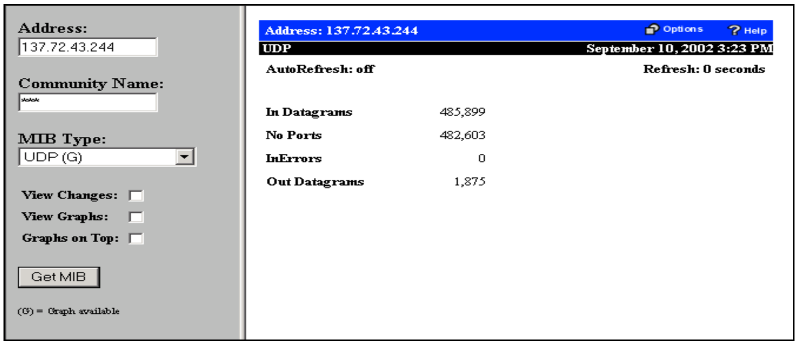
The fields on the ICMP MIB Information screen are:

	IN	OUT
Messages	ICMP In Messages. The total number of ICMP messages the entity received. Note that this counter includes all those counted by icmpInErrors.	ICMP Out Messages. The total number of ICMP messages this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
Errors	ICMP In Errors. The number of ICMP messages that the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).	ICMP Out Errors. The number of ICMP messages that this entity did not send due to problems discovered within ICMP, such as a lack of buffers. This value should not include errors discovered outside the ICMP layer, such as the inability of IP to route the resultant datagram. In some implementations no types of error exist that contribute to this counter's value.

	IN	OUT
Dest. Unreachable	ICMP In Dest. Unreaches. The number of ICMP Destination Unreachable messages received.	ICMP Out Destination Unreachable. The number of ICMP Destination Unreachable messages sent.
Time Exceeded	ICMP In Time Exceeds. The number of ICMP Time Exceeded messages received.	ICMP Out Time Exceeds. The number of ICMP Time Exceeded messages sent.
Parameter Problem	ICMP In Parameter Problems. The number of ICMP Parameter Problem messages received.	ICMP Out Parameter Problems. The number of ICMP Parameter Problem messages sent.
Source Quench	ICMP In Source Quenches. The number of ICMP Source Quench messages received.	ICMP Out Source Quenches. The number of ICMP Source Quench messages sent.
Redirect	ICMP In Redirects. The number of ICMP Redirect messages received.	ICMP Out Redirects. The number of ICMP Redirect messages sent.
Echo	ICMP In Echoes. Echo (request) messages received.	ICMP Out Echoes. The number of ICMP Echo (request) messages sent.
Echo Reply	ICMP In Echo Replies. The number of ICMP Echo Reply messages received.	ICMP Out Echo Replies. The number of ICMP Echo Reply messages sent.
TimeStamp	ICMP In Timestamps. The number of ICMP Timestamp (request) messages received.	ICMP Out Timestamps. The number of ICMP Timestamp (request) messages sent.
TimeStamp Reply	ICMP In Timestamp Replies. The number of ICMP Timestamp Reply messages received.	ICMP Out Timestamp Replies. Number of ICMP Timestamp Reply messages sent.
Address Mask	ICMP In Address Mask. The number of ICMP Address Mask Request messages received.	ICMP Out Address Masks. Number of ICMP Address Mask Request messages sent.
Address Mask Reply	ICMP In Address Mask Replies. The number of ICMP Address Mask Reply messages received.	ICMP Out Address Mask Replies. Number of ICMP Address Mask Reply messages sent.

UDP (G)

The UDP objects (User Datagram Protocol) are the datagram statistics of the UDP layer. The (G) indicates that graphs are available. The UDP group counts the datagrams received, those sent out, those discarded due to format errors, and those destined for unknown ports.



Address: 137.72.43.244

Community Name: ***

MIB Type: UDP (G)

View Changes: ☐

View Graphs: ☐

Graphs on Top: ☐

(G) = Graph available

Address: 137.72.43.244

UDP September 10, 2002 3:23 PM

AutoRefresh: off

Refresh: 0 seconds

In Datagrams	485,899
No Ports	482,603
InErrors	0
Out Datagrams	1,875

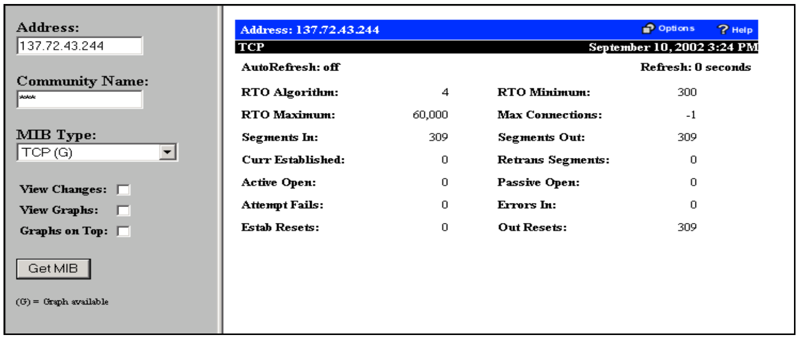
Figure 80. SNMP Browser: UDP Group

The fields on the UDP MIB Information screen are:

In Datagrams	UDP In Datagrams. The total number of UDP datagrams delivered to UDP users.
No Ports	UDP No Ports. The total number of received UDP datagrams for which there was no application at the destination port.
In Errors	UDP In Errors. The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Out Datagrams	UDP Out Datagrams. The total number of UDP datagrams sent from this entity.

TCP (G)

The TCP objects (Transmission Control Protocol) are the data transmission statistics and connection data for the TCP layer. The (G) indicates that graphs are available. Objects that represent information about a particular TCP connection are transient; the objects exist only as long as the specified connection is in use. It provides information on retransmissions, opens, connections, and segments.



Address: 137.72.43.244
Community Name: ***
MIB Type: TCP (G)
View Changes: ☐
View Graphs: ☐
Graphs on Top: ☐
(G) = Graph available

Address: 137.72.43.244
TCP September 10, 2002 3:24 PM
AutoRefresh: off Refresh: 0 seconds

RTO Algorithm:	4	RTO Minimum:	300
RTO Maximum:	60,000	Max Connections:	-1
Segments In:	309	Segments Out:	309
Curr Established:	0	Retrans Segments:	0
Active Open:	0	Passive Open:	0
Attempt Fails:	0	Errors In:	0
Estab Resets:	0	Out Resets:	309

Figure 81. SNMP Browser - TCP Group

The fields on the TCP MIB Information screen are:

RTO Algorithm	TCP Retrans. Timeout Algorithm. The algorithm used to determine the timeout value for retransmitting unacknowledged octets.
RTO Minimum	TCP Retrans. Timeout Minimum. The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is Rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
RTO Maximum	TCP Retrans. Timeout Maximum. The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is Rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
Max Connections	TCP Maximum Connections. The limit on the total number of TCP connections the entity supports. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
Segments In	TCP In Segments. The total number of segments received, including those received in error. This count includes segments received on currently established connections.

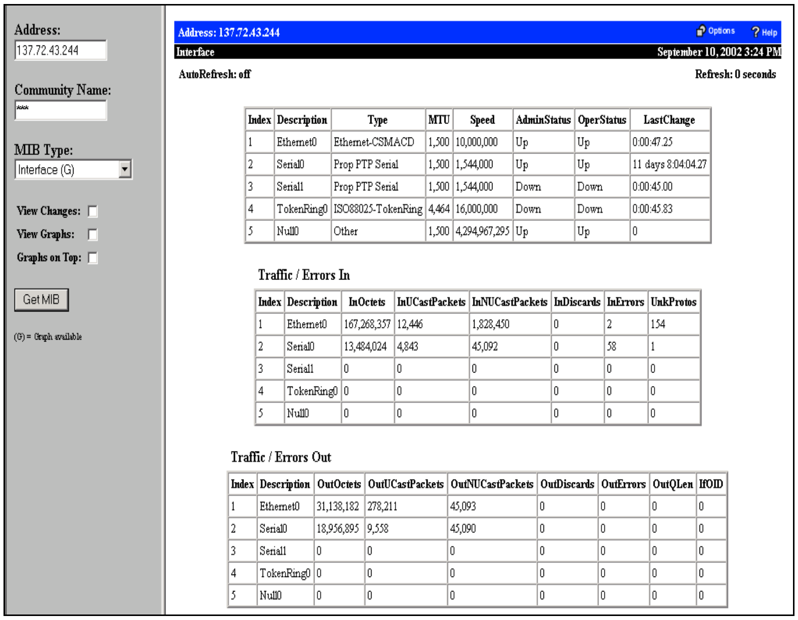
Segments Out	TCP Out Segments. The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Curr Established	TCP Current Established. The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
Retrans Segments	TCP Retransmit Segments. The total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Active Open	TCP Active Open. The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Passive Open	TCP Passive Open. The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Attempt Fails	TCP Attempt Fails. The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Errors In	TCP In Errors. The total number of segments received in error, for example, bad TCP checksums.
Estab Resets	TCP Established Resets. The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
Out Resets	TCP Out Resets. The number of TCP segments sent containing the RST flag.

Interface (G)

The Interfaces table contains information on the entity's interfaces. The (G) indicates that graphs are available. Each interface is thought of as being attached to a subnetwork. Note that this term should not be confused with subnet that refers to an addressing partitioning scheme used in the Internet suite of protocols.

The Interfaces Table has two subtables:

- Traffic/Errors in
- Traffic/Errors out



Address: 137.72.43.244

Community Name: ***

MIB Type: Interface (G)

View Changes: ☐

View Graphs: ☐

Graphs on Top: ☐

(G) = Graph available

Address: 137.72.43.244

Interface

September 10, 2002 3:24 PM

AutoRefresh: off

Refresh: 0 seconds

Index	Description	Type	MTU	Speed	AdminStatus	OperStatus	LastChange
1	Ethernet0	Ethernet-CSMACD	1,500	10,000,000	Up	Up	0:00:47.25
2	Serial0	Prop PTP Serial	1,500	1,544,000	Up	Up	11 days 8:04:04.27
3	Serial1	Prop PTP Serial	1,500	1,544,000	Down	Down	0:00:45.00
4	TokenRing0	ISO88025-TokenRing	4,464	16,000,000	Down	Down	0:00:45.83
5	Null0	Other	1,500	4,294,967,295	Up	Up	0

Traffic / Errors In

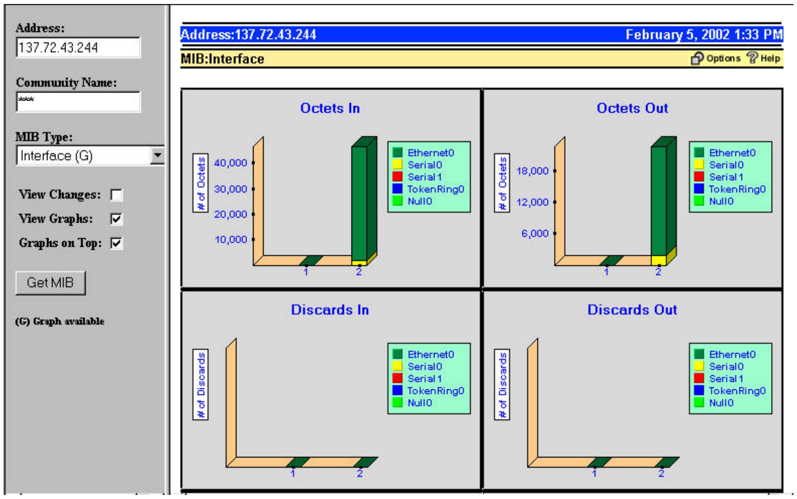
Index	Description	InOctets	InUCastPackets	InNUCastPackets	InDiscards	InErrors	UnkProtos
1	Ethernet0	167,268,357	12,446	1,828,450	0	2	154
2	Serial0	13,484,024	4,843	45,092	0	58	1
3	Serial1	0	0	0	0	0	0
4	TokenRing0	0	0	0	0	0	0
5	Null0	0	0	0	0	0	0

Traffic / Errors Out

Index	Description	OutOctets	OutUCastPackets	OutNUCastPackets	OutDiscards	OutErrors	OutQLen	IfOID
1	Ethernet0	31,138,182	278,211	45,093	0	0	0	0
2	Serial0	18,956,895	9,558	45,090	0	0	0	0
3	Serial1	0	0	0	0	0	0	0
4	TokenRing0	0	0	0	0	0	0	0
5	Null0	0	0	0	0	0	0	0

Figure 82. SNMP Browser: Interfaces Table

You may also graph many of the fields on the Interfaces table. For example, in the following figure Octets In/Octets Out and Discards In/Discards Out are graphed:



Address: 137.72.43.244

Community Name: ****

MIB Type: Interface (G)

View Changes: ☐

View Graphs: ☑

Graphs on Top: ☑

(G) Graph available

Address:137.72.43.244 February 5, 2002 1:33 PM

MIB:Interface

Figure 83. SNMP Browser: Interfaces Table Graph

The fields on the Interfaces Table for the selected IP are:

Index	A unique value for each interface. Its value ranges between 1 and the value of ifNumber. The value for each interface must remain constant at least from one reinitialization of the entity's network management system to the next reinitialization.
Description	A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface.
Type	The type of interface, distinguished according to the physical/link protocol(s) immediately "below" the network layer in the protocol stack.
MTU	The size of the largest datagram that can be sent/received on the interface specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.
Speed	An estimate of the interface's current bandwidth in bits per second. For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth.
AdminStatus	Administrative Status. The desired state of the interface. The testing (3) state indicates that no operational packets can be passed.
OperStatus	Operational Status. The current operational state of the interface. The testing (3) state indicates that no operational packets can be passed.

LastChange	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, then this object contains a zero value.

TRAFFIC/ ERRORS IN subtable

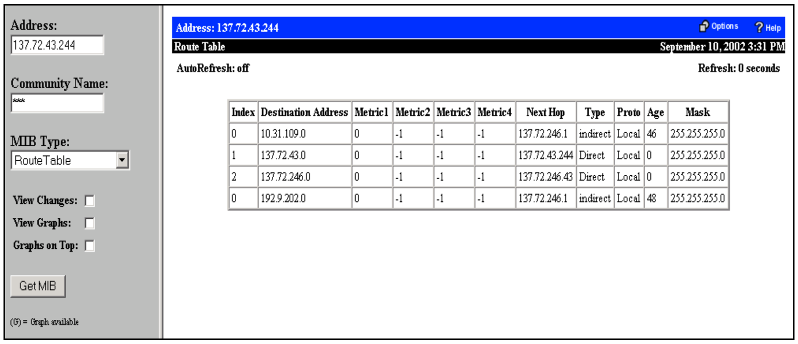
Index	A unique value for each interface. Its value ranges between 1 and the value of ifNumber. The value for each interface must remain constant at least from one reinitialization of the entity's network management system to the next reinitialization.
Description	A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface.
InOctets	The total number of octets received on the interface, including framing characters.
InUCastPackets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
In NUCastPackets	The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
InDiscards	The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
InErrors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
UnkProtos	The number of packets received via the interface that were discarded because of an unknown or unsupported protocol.

TRAFFIC/ ERRORS OUT subtable

Index	A unique value for each interface. Its value ranges between 1 and the value of ifNumber. The value for each interface must remain constant at least from one reinitialization of the entity's network management system to the next reinitialization.
Description	A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface.
OutOctets	The total number of octets transmitted out of the interface, including framing characters.
OutUCastPackets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
OutNUCastPackets	The total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.
OutDiscards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
OutErrors	The number of outbound packets that could not be transmitted because of errors.
OutQLen	The length of the output packet queue (in packets).
IfOID	Interface Specific OID. A reference to MIB definitions specific to the particular media being used to realize the interface. For example, if an Ethernet realizes the interface, then the value of this object refers to a document defining objects specific to Ethernet. If this information is not present, its value should be set to the OBJECT IDENTIFIER 0 0, which is a syntactically valid object identifier, and any conformant implementation of ASN.1 and BER must be able to generate and recognize this value.

Route Table

The IP route table is available from the main SNMP MIB Browser screen by selecting Route Table from the MIB Type drop-down list and pressing Get MIB. The IP route table contains an entry for each route presently known to this entity/managed node.



Address: 137.72.43.244

Community Name: ***

MIB Type: RouteTable

View Changes: ☐

View Graphs: ☐

Graphs on Top: ☐

Address: 137.72.43.244

Route Table September 10, 2002 3:31 PM

AutoRefresh: off Refresh: 0 seconds

Index	Destination Address	Metric1	Metric2	Metric3	Metric4	Next Hop	Type	Proto	Age	Mask
0	10.31.109.0	0	-1	-1	-1	137.72.246.1	indirect	Local	46	255.255.255.0
1	137.72.43.0	0	-1	-1	-1	137.72.43.244	Direct	Local	0	255.255.255.0
2	137.72.246.0	0	-1	-1	-1	137.72.246.43	Direct	Local	0	255.255.255.0
0	192.9.202.0	0	-1	-1	-1	137.72.246.1	indirect	Local	48	255.255.255.0

Figure 84. IP Route Table

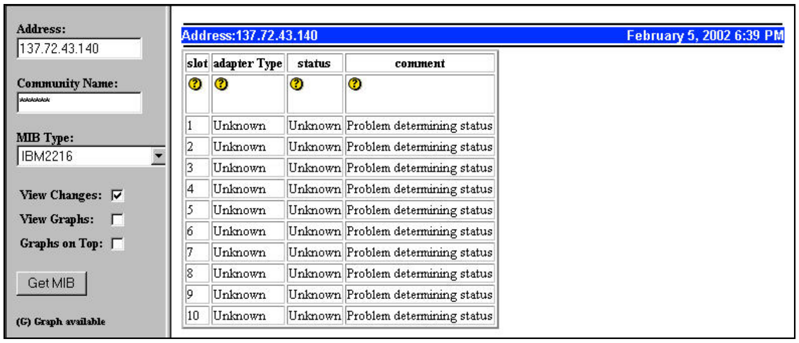
The fields on the IP Route Table are:

Index	Route Interface Index. The index value, which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
Destination Address	Route Destination. The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.
Metric1	Route Metric 1. The primary routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.
Metric2	Route Metric 2. An alternate routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.
Metric3	Route Metric 3. An alternate routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.

Metric4	Route Metric 4. An alternate routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.
Next Hop	Route Next Hop. The IP address of the next hop of this route. (In the case of a route bound to an interface that is realized via a broadcast media, the value of this field is the agent's IP address on that interface.)
Type	Route Type. The type of route. Note that the values Direct(3) and Indirect(4) refer to the notion of direct and indirect routing in the IP architecture. Possible values are: • Other (1) -- none of the following • Invalid (2) -- an invalidated route • Direct (3) -- route to directly connected (sub-network) • Indirect (4) -- route to a non-local host/network/sub-network
Proto	Route Protocol. The routing mechanism via which this route was learned. Inclusion of values for gateway routing protocols is not intended to imply that hosts should support those protocols. Possible values are: • Other (1) -- none of the following • Local (2) -- non-protocol information, e.g., manually configured entries • NetMgmt (3) -- set via a network management protocol • ICMP (4) -- obtained via ICMP
Age	Route Age. The number of seconds since this route was last updated or otherwise determined to be correct. Note that no semantics of too old can be implied except through knowledge of the routing protocol by which the route was learned.
Mask	Route Mask. Indicate the mask to be logically ANDed with the destination address before being compared to the value in the ipRouteDest field.

IBM 2216 Table

This describes the table containing information about PCI adapters in the IBM2216 equipment.


Address: 137.72.43.140

Community Name: ******

MIB Type: IBM2216

View Changes: ☑

View Graphs: ☐

Graphs on Top: ☐

(G) Graph available

Address:137.72.43.140 February 5, 2002 6:39 PM

slot	adapter Type	status	comment
1	Unknown	Unknown	Problem determining status
2	Unknown	Unknown	Problem determining status
3	Unknown	Unknown	Problem determining status
4	Unknown	Unknown	Problem determining status
5	Unknown	Unknown	Problem determining status
6	Unknown	Unknown	Problem determining status
7	Unknown	Unknown	Problem determining status
8	Unknown	Unknown	Problem determining status
9	Unknown	Unknown	Problem determining status
10	Unknown	Unknown	Problem determining status

Figure 85. IBM 2216 PU Table

The fields on the IBM 2216 Table are:

Slot The number identifying a slot location where an adapter can be inserted.

Adapter Type The type of adapter that is inserted into this slot. If no adapter is present, the variable takes the value not present (2). The adapter types are:

……

2: Not-present
3: ATM-MMF-Lic294
4: ATM-MMF-Lic284
5: ATM-SMF-Lic295
6: ATM-SMF-Lic293
7: Token-Ring-Lic280
8: ESCON-Lic287
9: ISDN-T1J1-Lic283
10: ISDN-E1-Lic292
11: Serial-RS232-Lic282
12: Serial-V35-Lic290
13: Serial-X21-Lic291
14: Ethernet-Lic281
15: Ethernet-Fast-Lic288
16: Serial-HSSI-Lic289
17: FDDI-Lic286
18: ISDN-T1J1-Lic297
19: ISDN-E1-Lic298
20: Parallel-Channel-Lic299

21: ISDN-BRI-ST-Lic262
22: ISDN-BRI-U-Lic261
23: Serial-RVX-Lic260
24: Comp-Encrypt-Single-Lic263
25: Comp-Encrypt-Dual-Lic264

Status The operational status of this PCI adapter. The status is:

- Unknown (1): If there was problem determining the operational status of the adapter.
- Not-configured (2): If the adapter inserted in the slot is recognized but no router configuration exists.
- Not-present (3): If no adapter is currently inserted.
- Does-not-apply (4): If this adapter does not contain an operational state.
- Enable-pending (5): If commands have been executed to enable the adapter but have not been completed.
- Enabled (6): If commands have been successfully executed to enable the adapter.

- Disable-pending (7): If commands have been executed to disable the adapter but have not been completed.
- Disabled (8): If commands have been successfully executed to disable the adapter.
- Not-initialized (9): If the adapter has not completed its initialization.
- Unknown-device (10): If the adapter inserted in the slot can not be recognized.
- Hardware-error (11): If the adapter can not be used nor made ready to be used.
- Not-powered (12): If the adapter has had a problem
- obtaining power from its slot.
- Diagnostics (13): If the adapter is currently undergoing diagnostics.
- WRS-available (14): If the adapter is currently configured and available for WAN restoration.

Misconfigured (15): If the adapter is inserted in the slot but the router configuration is of a different type.

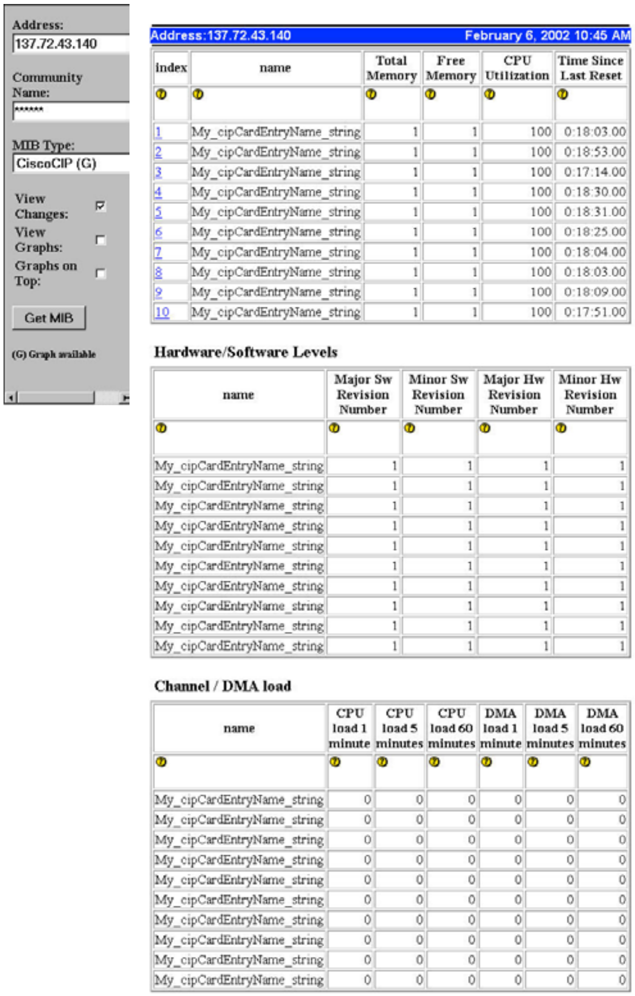
Comment Descriptive text about information in the table.

CISCO CIP (G)

The CISCO CIP card table describes the MIB module for objects used to manage the Cisco Mainframe Channel Connection (CMCC) cards. The (G) indicates that graphs are available. The card table contains a list of values for the CMCC card used to determine the general state of the CMCC.

The CISCO CIP card Table has two subtables:

- Hardware/Software Levels
- Channel/DMA Load



Address: 137.72.43.140

Community Name: ******

MIB Type: CiscoCIP (G)

View Changes: ☑

View Graphs: ☐

Graphs on Top: ☐

(G) Graph available

Address:137.72.43.140 February 6, 2002 10:45 AM

index	name	Total Memory	Free Memory	CPU Utilization	Time Since Last Reset
1	My_cipCardEntryName_string	1	1	100	0:18:03.00
2	My_cipCardEntryName_string	1	1	100	0:18:53.00
3	My_cipCardEntryName_string	1	1	100	0:17:14.00
4	My_cipCardEntryName_string	1	1	100	0:18:30.00
5	My_cipCardEntryName_string	1	1	100	0:18:31.00
6	My_cipCardEntryName_string	1	1	100	0:18:25.00
7	My_cipCardEntryName_string	1	1	100	0:18:04.00
8	My_cipCardEntryName_string	1	1	100	0:18:03.00
9	My_cipCardEntryName_string	1	1	100	0:18:09.00
10	My_cipCardEntryName_string	1	1	100	0:17:51.00

Hardware/Software Levels

name	Major Sw Revision Number	Minor Sw Revision Number	Major Hw Revision Number	Minor Hw Revision Number
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1

Channel / DMA load

name	CPU load 1 minute	CPU load 5 minutes	CPU load 60 minutes	DMA load 1 minute	DMA load 5 minutes	DMA load 60 minutes
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0

Figure 86. CISCO CIP card Table

The fields on the CISCO CIP card are:

Index	The index into the card table (not physical chassis slot number, matches the Cisco chassis MIB card index).
Name	Configured name for the Cisco Mainframe Channel Connection (CMCC).
Total Memory	Total memory on the card.
Free Memory	Amount of memory not in use.
CPU Utililization	The average, over the last minute, of the percentage of time that this processor was running. This includes time spent on non-productive polling and time used by routine maintenance tasks. This value is not a measure of the processor's ability to handle more work, which is represented by the CPU Load information. The ability to handle more work could also be affected by DMA and channel load, represented by the DMA Load and Channel Adapter Load statistics.
Time Since Last Reset	Amount of time the Cisco Mainframe Channel Connection (CMCC) has been running since the last reset.
UP Time	Amount of time the Cisco Mainframe Channel Connection (CMCC) has been running.

HARDWARE/ SOFTWARE LEVELS subtable

Name	Configured name for the Cisco Mainframe Channel Connection (CMCC).
Major SW Revision Number	The major software revision number for the software loaded on the Cisco Mainframe Channel Connection (CMCC) card.
Minor SW Revision Number	The minor software revision number for the software loaded on the Cisco Mainframe Channel Connection (CMCC) card.
Major HW Revision Number	The major hardware revision number for the software loaded on the Cisco Mainframe Channel Connection (CMCC) card.
Minor HW Revision Number	The minor hardware revision number for the software loaded on the Cisco Mainframe Channel Connection (CMCC) card.

CHANNEL/ DMA LOAD subtable

Name	Configured name for the Cisco Mainframe Channel Connection (CMCC).

CPU Load 1 Min	The average, over the last minute, of the percentage of time that this processor was utilized to transfer data. It does not include idle time or time used by routine maintenance tasks.
CPU Load 5 Min	The average, over the last 5 minutes, of the percentage of time that this processor was utilized to transfer data. It does not include idle time or time used by routine maintenance tasks.
CPU Load 60 Min	The average, over the last 60 minutes, of the percentage of time that this processor was utilized to transfer data. It does not include idle time or time used by routine maintenance tasks.
DMA Load 1 Min	The average, over the last minute, of the percentage of time the DMA controller was being used to transfer data between the Cisco Mainframe Channel Connection (CMCC) card and the route processor.
DMA Load 5 Min	The average, over the last 5 minutes, of the percentage of time the DMA controller was being used to transfer data between the Cisco Mainframe Channel Connection (CMCC) card and the route processor.
DMA Load 60 Min	The average, over the last 60 minutes, of the percentage of time that the DMA controller was being used to transfer data between the Cisco Mainframe Channel Connection (CMCC) card and the route processor.

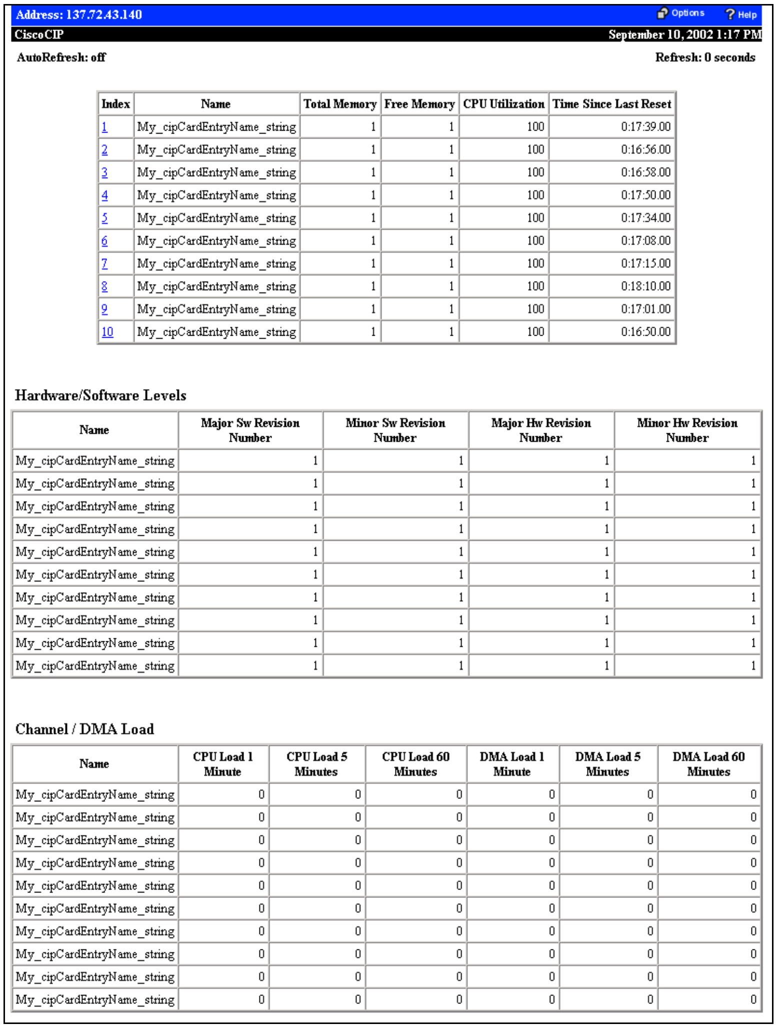
CISCO CIP Channel (*subscreen of CiscoCIP*)

The CISCO CIP Channel subscreen describes the MIB module for objects used to manage the Cisco Mainframe Channel Connection (CMCC) cards. The Channel table contains a list of objects pertaining to the channel or daughter board on the CMCC card.

The CISCO CIP Channel subscreen may be accessed from the CISCO CIP screen by simply clicking an Index number hyperlink.

The CISCO CIP Channel Table has two subtables:

- Errors
- Load and Statistics



AutoRefresh: off

Refresh: 0 seconds

Index	Name	Total Memory	Free Memory	CPU Utilization	Time Since Last Reset
1	My_cipCardEntryName_string	1	1	100	0:17:39.00
2	My_cipCardEntryName_string	1	1	100	0:16:56.00
3	My_cipCardEntryName_string	1	1	100	0:16:58.00
4	My_cipCardEntryName_string	1	1	100	0:17:50.00
5	My_cipCardEntryName_string	1	1	100	0:17:34.00
6	My_cipCardEntryName_string	1	1	100	0:17:08.00
7	My_cipCardEntryName_string	1	1	100	0:17:15.00
8	My_cipCardEntryName_string	1	1	100	0:18:10.00
9	My_cipCardEntryName_string	1	1	100	0:17:01.00
10	My_cipCardEntryName_string	1	1	100	0:16:50.00

Hardware/Software Levels

Name	Major Sw Revision Number	Minor Sw Revision Number	Major Hw Revision Number	Minor Hw Revision Number
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1
My_cipCardEntryName_string	1	1	1	1

Channel / DMA Load

Name	CPU Load 1 Minute	CPU Load 5 Minutes	CPU Load 60 Minutes	DMA Load 1 Minute	DMA Load 5 Minutes	DMA Load 60 Minutes
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0
My_cipCardEntryName_string	0	0	0	0	0	0

Figure 87. CISCO CIP Channel Table

The fields on the CIP Channel Table are:

Index	Indicates which daughter board or channel is being referenced for a particular Cisco Mainframe Channel Connection (CMCC) card.
Type	Indicates the channel path interface type.
Status	Indicates whether the microcode for the daughter board has been successfully loaded and is executing.
Signal	For ESCON, this field indicates if a light has been seen on the fiber and synchronization has been established. For the Parallel Channel Adapter (PCA), which provides the Bus and Tag connection, this field indicates if Operational out has been sensed.
Online	For ESCON, this field indicates if a path has been established with at least one channel. For PCA, this field indicates if the Parallel Channel Adapter (PCA) is online to the channel. That is, it responds to at least one device address.

ERRORS subtable

Type	Indicates the channel path interface type.
Incidents	Counts the number of times the ESCON Processor recovers from an internal error.
Code Violation	The number of recognized code-violation errors. A trap is issued when this number exceeds the bit error rate threshold for ESCON. The bit error rate threshold is set at 15-error burst within a 5-minute period. An error burst is the time period of 1.5 seconds plus or minus 0.05 seconds during which one or more code violation errors occur.
Signal or Sync Loss	The number of link failures recognized as a result of a loss of signal or loss of synchronization that persisted longer than the link interval duration, the link interval duration is one second with a tolerance of +1.5 seconds and -0 seconds.
NOSs	The number of link failures recognized as a result of the not-operational sequence (NOS).
Sequence Timeouts	The number of link failures recognized as a result of a connection recovery timeout or response timeout occurring while in transmit OLS state.

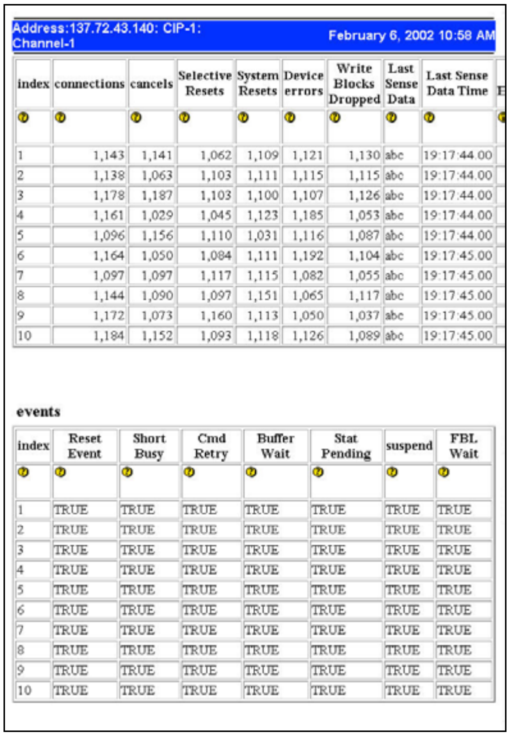
Invalid Sequences	The number of link failures recognized as a result of an invalid sequence for Link-Level-Facility State. Either a UD or UDR sequence was recognized while in wait-for-offline-sequence state.
Trap Cause	Indicates the reason for the last link failure. • liStatus indicates that the daughter board status has changed. • liImplicitIncident indicates that a condition that may cause the recognition of a link incident in the attached node has been recognized. • liBERthreshold indicates that the code violation error rate exceeded the threshold. • liSignalOrSyncLoss indicates a loss of signal or loss of synchronization that persisted longer than the link interval duration. • liNotOperationalSequence indicates the recognition of not-operational sequence, usually due to the operator taking the channel offline. • liSequenceTimeout indicates a connection recovery timeout or response timeout occurring while in transmit OLS state. • linvalidSequence indicates a UD or UDR sequence was recognized while in wait-for-offline-sequence state.
LOAD AND STATISTICS subtable	
Type	Indicates the channel path interface type.
Last Stat	This object indicates how old the statistics are.
Next Stat	This object indicates when statistics will next be read.
Channel Load 1 Min	The average, over the last minute, of the percentage of time the channel adapter was busy communicating to a host.
Channel Load 5 Min	The average, over the last 5 minutes, of the percentage of time the channel adapter was busy communicating to a host.
Channel Load 60 Min	The average, over the last 60 minutes, of the percentage of time the channel adapter was busy communicating to a host.

CISCO Sub-Channel (subscreen of CISCO CIP Channel)

The investigation of CISCO CIPs may be continued by viewing the subchannels belonging to a particular channel by type. This MIB is accessed from the CISCO CIP Channel subscreen by simply clicking an Index number hyperlink.

The Cisco Sub-Channel Table has one subtable:

- Events



Address:137.72.43.140: CIP-1: Channel-1

February 6, 2002 10:58 AM

index	connections	cancels	Selective Resets	System Resets	Device errors	Write Blocks Dropped	Last Sense Data	Last Sense Data Time
1	1,143	1,141	1,062	1,109	1,121	1,130	abc	19:17:44.00
2	1,138	1,063	1,103	1,111	1,115	1,115	abc	19:17:44.00
3	1,178	1,187	1,103	1,100	1,107	1,126	abc	19:17:44.00
4	1,161	1,029	1,045	1,123	1,185	1,053	abc	19:17:44.00
5	1,096	1,156	1,110	1,031	1,116	1,087	abc	19:17:44.00
6	1,164	1,050	1,084	1,111	1,192	1,104	abc	19:17:45.00
7	1,097	1,097	1,117	1,115	1,082	1,055	abc	19:17:45.00
8	1,144	1,090	1,097	1,151	1,065	1,117	abc	19:17:45.00
9	1,172	1,073	1,160	1,113	1,050	1,037	abc	19:17:45.00
10	1,184	1,152	1,093	1,118	1,126	1,089	abc	19:17:45.00

events

index	Reset Event	Short Busy	Cmd Retry	Buffer Wait	Stat Pending	suspend	FBL Wait
1	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
2	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
3	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
4	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
5	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
6	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
7	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
8	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
9	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
10	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE

Figure 88. CISCO Sub-Channel

The fields on the CIP Entry Table for a SubChannel are:

Index	CHECK TEXT: Indicates which daughter board or channel is being referenced for a particular Cisco Mainframe Channel Connection (CMCC) card.
Connections	Number of times a device was connected to the subchannel. For some devices, this value correlates with the number of start subchannels.
Cancels	Number of halt subchannels
Selective Resets	Number of selective resets.
System Resets	Number of system resets.
Device Errors	Number of device level errors.
Write Blocks	Number of times a block was received by the channel and a

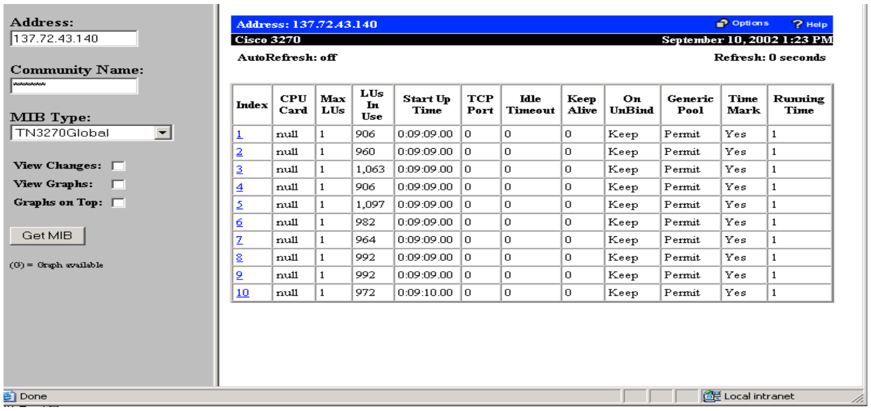
Dropped	router buffer was not available so the block was discarded.
Last Sense Data	Last sense data sent to the channel by this device.
Last Sense Data Time	The time when the last sense data was sent to the channel by this device.
CU Busies	Number of control unit busies sent to the channel when this device was requested.
Cmd Retries	Number of times the subchannel went into command retry state. The sum of this value and the connections value gives the number of start subchannels.

EVENTS subtable

Index	Indicates which daughter board or channel is being referenced for a particular Cisco Mainframe Channel Connection (CMCC) card.
Reset Event	Device state after a system reset that is cleared by resetting event unit check.
Short Busy	A transient state that a device can get into during processing of various resets.
Cmd Retry	Device state that occurs if the mainframe tries to write data to the CMCC when the CMCC has no buffers for it, or if the mainframe performs a read operation when the CMCC doesn't have any data to send.
Buffer Wait	Device state that occurs if the mainframe tries to write data to the CMCC when it has insufficient buffers for all of the write operation.
Stat Pending	Indicates that the CMCC has status to present for a particular device. The indication is cleared when the mainframe accepts the status.
Suspend	Device task has suspended data transfer for a particular device.
FBL Wait	Device state that occurs when the mainframe tries to write data to the CMCC and the CMCC has no buffers for all of the write operation.

TN3270 Global

TN3270 Global describes the MIB module for objects used to manage the TN3270 server. The Global table contains information about the general state of the server.



Address: 137.72.43.140

Community Name: ******

MIB Type: TN3270Global

View Changes: ☐

View Graphs: ☐

Graphs on Top: ☐

(G) = Graph available

Address: 137.72.43.140

Cisco 3270 September 10, 2002 1:23 PM

AutoRefresh: off

Refresh: 0 seconds

Index	CPU Card	Max LUs	LUs In Use	Start Up Time	TCP Port	Idle Timeout	Keep Alive	On UnBind	Generic Pool	Time Mark	Running Time
1	null	1	906	0:09:09.00	0	0	0	Keep	Permit	Yes	1
2	null	1	960	0:09:09.00	0	0	0	Keep	Permit	Yes	1
3	null	1	1,063	0:09:09.00	0	0	0	Keep	Permit	Yes	1
4	null	1	906	0:09:09.00	0	0	0	Keep	Permit	Yes	1
5	null	1	1,097	0:09:09.00	0	0	0	Keep	Permit	Yes	1
6	null	1	982	0:09:09.00	0	0	0	Keep	Permit	Yes	1
7	null	1	964	0:09:09.00	0	0	0	Keep	Permit	Yes	1
8	null	1	992	0:09:09.00	0	0	0	Keep	Permit	Yes	1
9	null	1	992	0:09:09.00	0	0	0	Keep	Permit	Yes	1
10	null	1	972	0:09:10.00	0	0	0	Keep	Permit	Yes	1

Figure 89. TN3270 Global Table

The fields on the TN3270 Global table are:

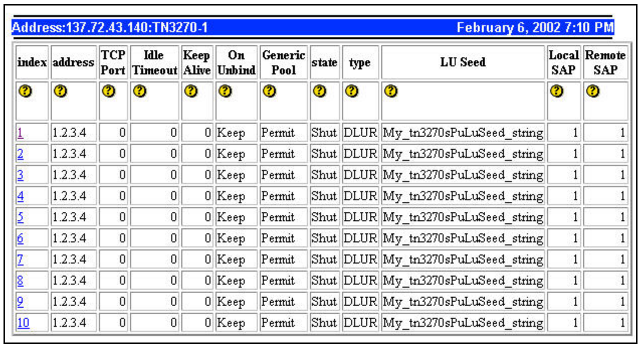
Index	Uniquely identifies each TN3270 server instance. This index value shall not be reused when the server is shut down and a new instance invoked. Click an Index hyperlink to access the TN3270 PU Table.
CPU Card	Identity of the board running the server.
Max LUs	Maximum number of LUs supported by the server.
LUs In Use	Number of LUs currently in use on the server.
Start Up Time	TN3270 server started timestamp.
TCP Port	Default TCP port of this TN3270 Server, inherited by the PU if this PU doesn't have the TCP port explicitly defined in the router configuration.
Idle Timeout	Number of seconds of LU inactivity, from either host or client, before the TN3270 session is disconnected. Zero seconds means that LU sessions, by default, are not disconnected when inactive, regardless of the amount of idle time spent.
Keep Alive	The number of seconds of inactivity from the client side that the TN3270 Server allows to elapse before sending DO-TIMING-MARK to the TN3270 client. If the client does not reply within 30 minutes of such a TIMING-MARK sending, the server disconnects the TN3270 session. Zero seconds indicates that no keepalives will be sent.
On UnBind	The Unbind Action variable indicates whether or not a TN3270 session will be disconnected upon UNBIND. Keep indicates that no automatic disconnect will be made by the server upon receipt of an UNBIND. Disconnect indicates that the session will be disconnected upon receipt of an UNBIND.

Generic Pool	The Generic Pool variable indicates whether or not leftover LUs will be made available to TN3270 sessions that do not request a specific LU or LU pool.
Timing Mark	The Timing Mark variable indicates whether to send a timing mark to solicit a response before sending a response to the host. By using timing mark, an application determines the response time from the client. Some existing clients do not implement the timing mark correctly and do not work with this server if this parameter is sent.
Running Time	Total time elapsed since start of TN3270 server.

TN3270 PU Table (*subscreen of TN3270 Global*)

The TN3270 PU Table is contained in the MIB module for objects used to manage the TN3270 server and is accessed by clicking an Index hyperlink in the TN3270 Global screen.

The PU table contains objects that describe the PU configuration parameters not defined in the NAU MIB, APPN MIB or DLUR MIB. The Global Table contains general information about the state of the server, while the PU table goes one level down to look at the devices per card attached to the server.



Address:137.72.43.140:TN3270-1 February 6, 2002 7:10 PM

index	address	TCP Port	Idle Timeout	Keep Alive	On Unbind	Generic Pool	state	type	LU Seed	Local SAP	Remote SAP
?	?	?	?	?	?	?	?	?	?	?	?
1	1.2.3.4	0	0	0	Keep	Permit	Shut	DLUR	My_tn3270sPuLuSeed_string	1	1
2	1.2.3.4	0	0	0	Keep	Permit	Shut	DLUR	My_tn3270sPuLuSeed_string	1	1
3	1.2.3.4	0	0	0	Keep	Permit	Shut	DLUR	My_tn3270sPuLuSeed_string	1	1
4	1.2.3.4	0	0	0	Keep	Permit	Shut	DLUR	My_tn3270sPuLuSeed_string	1	1
5	1.2.3.4	0	0	0	Keep	Permit	Shut	DLUR	My_tn3270sPuLuSeed_string	1	1
6	1.2.3.4	0	0	0	Keep	Permit	Shut	DLUR	My_tn3270sPuLuSeed_string	1	1
7	1.2.3.4	0	0	0	Keep	Permit	Shut	DLUR	My_tn3270sPuLuSeed_string	1	1
8	1.2.3.4	0	0	0	Keep	Permit	Shut	DLUR	My_tn3270sPuLuSeed_string	1	1
9	1.2.3.4	0	0	0	Keep	Permit	Shut	DLUR	My_tn3270sPuLuSeed_string	1	1
10	1.2.3.4	0	0	0	Keep	Permit	Shut	DLUR	My_tn3270sPuLuSeed_string	1	1

Figure 90. TN3270 PU Table

The fields on the TN3270 PU Table are:

Index	Index used to uniquely identify each Node instance. This is the same as snaNodeAdminIndex in the NAU MIB. Click the Index hyperlink to access the TN3270 LU Table.
Address	The IP address of this TN3270 server.
TCP Port	The TCP port of this TN3270 server Telnet session.
Idle Timeout	The number of seconds of LU inactivity, from either host or client, before the TN3270 session is disconnected. Zero seconds means that LU sessions, by default, are not disconnected when inactive, regardless of the amount of idle time spent. 65535 (not valid in server context) indicates that the idletime value should be taken from the server context.
Keep Alive	The number of seconds of inactivity from the client side that the TN3270 Server allows to elapse before sending DO-TIMING-MARK to the TN3270 client. If the client does not reply within thirty minutes of such a TIMING-MARK sending, the server disconnects the TN3270 session. Zero seconds indicates that no keepalives will be sent. 65535 (not valid in server context) indicates that the default keepalive value for an LU is taken from whatever value had been defined in the server context for this CIP card.

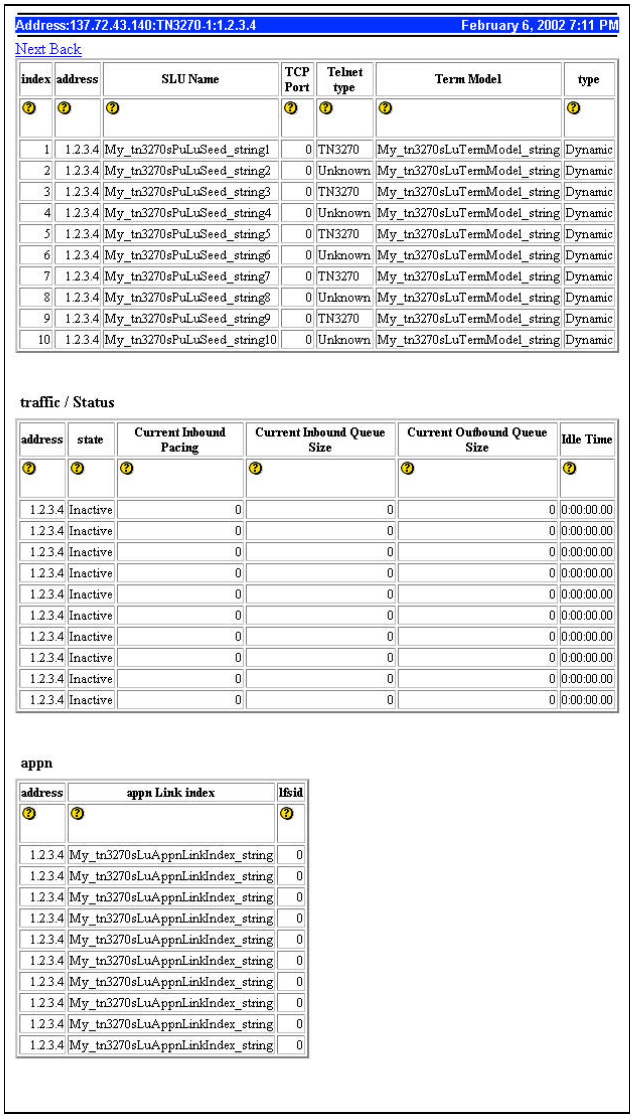
On UnBind	The On Unbind variable indicates whether or not a TN3270 session will be disconnected upon UNBIND. Keep indicates that no automatic disconnect will be made by the server upon receipt of an UNBIND. Disconnect indicates that the session will be disconnected upon receipt of an UNBIND. Inherit indicates that the default keepalive value of a LU is taken from whatever value had been defined in the server context for this CIP card.
Generic Pool	The Generic Pool variable indicates whether or not leftover LUs will be made available to TN3270 sessions, which do not request a specific LU or LU pool. A "leftover" LU is defined as one for which both of the following conditions hold true: the SSCP did not send an ACTLU during PU startup, and the PU controlling the LU is capable of carrying PSID vectors on NMVT messages (thus allowing DDDLU operation for that LU).
State	The Status value identifies the current PU state. This has a different meaning for direct and DLUR PU before the link station is established. For DLUR PU, the PU is in reset state, for direct PU, this will be either sending a TEST or an XID.
Type	Type defines whether the connection to the host is via DLUR or direct link. LuSend, LMAC/SAP, and RMAC/SAP in this table are undefined if the connection to the host is via DLUR.
PU-LU Send	For Direct PU this defines the LU name prefix (LU seed), which is concatenated with the localddr to form a unique name.
Local SAP Address	SAP address of the local direct node.
Remote SAP Address	SAP address of the remote node. Valid for direct PU only.

TN3270 LU Table (*subscreen of TN3270 PU Table*)

The TN3270 LU table provides information on each LU associated with the selected PU in the PU Table. The TN3270 LU table is accessed by clicking an Index hyperlink in the TN3270 PU Table.

The LU Table has two subtables:

- Traffic/Status
- APPN



Address:137.72.43.140:TN3270-1:1.2.3.4 February 6, 2002 7:11 PM

Next Back

index	address	SLU Name	TCP Port	Telnet type	Term Model	type
?	?	?	?	?	?	?
1	1.2.3.4	My_tn3270sPuLuSeed_string1	0	TN3270	My_tn3270sLuTermModel_string	Dynamic
2	1.2.3.4	My_tn3270sPuLuSeed_string2	0	Unknown	My_tn3270sLuTermModel_string	Dynamic
3	1.2.3.4	My_tn3270sPuLuSeed_string3	0	TN3270	My_tn3270sLuTermModel_string	Dynamic
4	1.2.3.4	My_tn3270sPuLuSeed_string4	0	Unknown	My_tn3270sLuTermModel_string	Dynamic
5	1.2.3.4	My_tn3270sPuLuSeed_string5	0	TN3270	My_tn3270sLuTermModel_string	Dynamic
6	1.2.3.4	My_tn3270sPuLuSeed_string6	0	Unknown	My_tn3270sLuTermModel_string	Dynamic
7	1.2.3.4	My_tn3270sPuLuSeed_string7	0	TN3270	My_tn3270sLuTermModel_string	Dynamic
8	1.2.3.4	My_tn3270sPuLuSeed_string8	0	Unknown	My_tn3270sLuTermModel_string	Dynamic
9	1.2.3.4	My_tn3270sPuLuSeed_string9	0	TN3270	My_tn3270sLuTermModel_string	Dynamic
10	1.2.3.4	My_tn3270sPuLuSeed_string10	0	Unknown	My_tn3270sLuTermModel_string	Dynamic

traffic / Status

address	state	Current Inbound Pacing	Current Inbound Queue Size	Current Outbound Queue Size	Idle Time
?	?	?	?	?	?
1.2.3.4	Inactive	0	0	0	0:00:00.00
1.2.3.4	Inactive	0	0	0	0:00:00.00
1.2.3.4	Inactive	0	0	0	0:00:00.00
1.2.3.4	Inactive	0	0	0	0:00:00.00
1.2.3.4	Inactive	0	0	0	0:00:00.00
1.2.3.4	Inactive	0	0	0	0:00:00.00
1.2.3.4	Inactive	0	0	0	0:00:00.00
1.2.3.4	Inactive	0	0	0	0:00:00.00
1.2.3.4	Inactive	0	0	0	0:00:00.00
1.2.3.4	Inactive	0	0	0	0:00:00.00

appn

address	appn Link index	lfsid
?	?	?
1.2.3.4	My_tn3270sLuAppnLinkIndex_string	0
1.2.3.4	My_tn3270sLuAppnLinkIndex_string	0
1.2.3.4	My_tn3270sLuAppnLinkIndex_string	0
1.2.3.4	My_tn3270sLuAppnLinkIndex_string	0
1.2.3.4	My_tn3270sLuAppnLinkIndex_string	0
1.2.3.4	My_tn3270sLuAppnLinkIndex_string	0
1.2.3.4	My_tn3270sLuAppnLinkIndex_string	0
1.2.3.4	My_tn3270sLuAppnLinkIndex_string	0
1.2.3.4	My_tn3270sLuAppnLinkIndex_string	0
1.2.3.4	My_tn3270sLuAppnLinkIndex_string	0

Figure 91. TN3270 LU Table

Use the Back and Next buttons on the screen to open a TN3270 LU Table for the previous or for the next OID listed in the Index column of the TN3270 PU Table.

For example, if you clicked Index hyperlink 2 in the TN3270 PU Table screen to get to the current screen, click Back to go to Index hyperlink 1 or Next to go to Index hyperlink 3.

The fields on the LU Table screen are:

Index	Index used to uniquely identify each LU associated with the selected PU. (or . . . "each node instance?"
Address	The IP address of the TN3270 client connected to this LU.
SLU Name	The name of the secondary LU.
TCP Port	The TCP port of the client for this LU Telnet session.
Telnet Type	The Telnet Type indicates whether the negotiated TN3270 session is TN3270, TN3270E or never connected.
Term Model	Terminal type or model number of the incoming TN3270 client.
Type	Indicates whether the LU is dynamic or static: (1) Dynamic. LU is configured as DDDLU. (2) Static. LU is configured as specific. The host sends an ACTLU as soon as the PU is active.

TRAFFIC/ STATUS subtable

Address	The IP address of the TN3270 client connected to this LU.
State	Current LU state of the client:

Inactive	LU didn't receive ACTLU.
Active	LU received ACTLU and acknowledged positively.
PSdt	LU is bound but there is no SDT yet.
act/session	LU is bound and in session.
PActlu	Telnet connects in and is awaiting ACTLU.
PNotifyAve	Awaiting host notify-available response
pNotifyUa	Awaiting host notify-unavailable response.
pReset	Waiting for a buffer to send DACTLU response.
pPsid	Awaiting a NMVT Reply psid response.
pBind	Waiting for the host to send a bind.
pUnbind	Awaiting host unbind response.

	UnbindWt	Waiting client acknowledgement of disconnect.
	SdtWt	Awaiting client's acknowledgement of an SDT.
Current Inbound Pacing	The number of inbound frames allowed to be sent to the host without receiving a pacing response from the host.	
Current Inbound Queue Size	After the inbound pacing credit is exhausted, the inbound data is queued. This is the number of inbound frames queued waiting for a host pacing response.	
Current Outbound Queue Size	The number of TCP packets in the server queued for transmission to the client.	
Idle Time	Time since last activity was recorded on this LU.	

APPN subtable

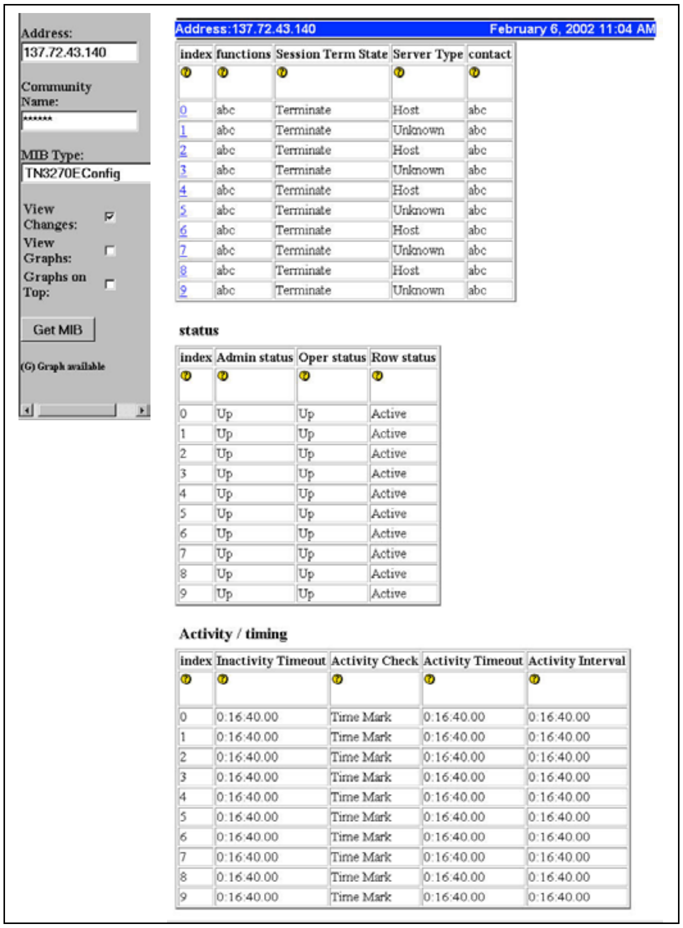
Address	The IP address of the TN3270 client connected to this LU.
APPN Link Index	Only valid for DLUR LU. The link index into an APPN MIB for the link on which the bind flowed.
LFSID	Session identifier on a PU 2.1 link.
Events	An array of octets indicating the latest events that happened in this LU. Octet 1 is the most recent event, octet 2 is the next most recent event, and so on. Although the maximum number of events kept is 16, the actual number of events kept may be lower than that value. When more events are generated than can be kept, the oldest ones are discarded. Events are: 1 Inactivity timer expired 2 Dynamic timer expired 3 ACTLU from host 4 Bind from host 5 Clear from host 6 DACTLU from host 7 Hierarchical reset from PU (warn ACTPU) 8 SDT from host 9 Unbind from host 10 Notify response from host 11 Reply psid negative response from host 12 Reply psid pos response from host 13 Unbind response from host 14 Hierarchical reset from PU 15 Connect from client 16 Disconnect from client 17 Timing-mark response from client 18 Flow control timer expired 19 Negative response to host 20 Negative response from host 21 Data contention happened 22 No buffer to send response 23 Receive a SNA response while inbound
LU Nail	Indicates whether this LU has been configured (Nailed) for a specific TN3270 client: TRUE LU is nailed to the client IP address. FALSE LU is not nailed to the client IP address.

TN3270EConfig

This describes the MIB module for objects used to manage the TN3270E server. The TN3270E Configuration Table contains information about the general state of the server.

The TN3270 Configuration Table has two subtables:

- Status
- Activity/Timing


Address:
137.72.43.140

Community Name:
******

MIB Type:
TN3270EConfig

View Changes: ☑
View Graphs: ☐
Graphs on Top: ☐

Address:137.72.43.140 February 6, 2002 11:04 AM

index	functions	Session Term State	Server Type	contact
0	abc	Terminate	Host	abc
1	abc	Terminate	Unknown	abc
2	abc	Terminate	Host	abc
3	abc	Terminate	Unknown	abc
4	abc	Terminate	Host	abc
5	abc	Terminate	Unknown	abc
6	abc	Terminate	Host	abc
7	abc	Terminate	Unknown	abc
8	abc	Terminate	Host	abc
9	abc	Terminate	Unknown	abc

status

index	Admin status	Oper status	Row status
0	Up	Up	Active
1	Up	Up	Active
2	Up	Up	Active
3	Up	Up	Active
4	Up	Up	Active
5	Up	Up	Active
6	Up	Up	Active
7	Up	Up	Active
8	Up	Up	Active
9	Up	Up	Active

Activity / timing

index	Inactivity Timeout	Activity Check	Activity Timeout	Activity Interval
0	0:16:40.00	Time Mark	0:16:40.00	0:16:40.00
1	0:16:40.00	Time Mark	0:16:40.00	0:16:40.00
2	0:16:40.00	Time Mark	0:16:40.00	0:16:40.00
3	0:16:40.00	Time Mark	0:16:40.00	0:16:40.00
4	0:16:40.00	Time Mark	0:16:40.00	0:16:40.00
5	0:16:40.00	Time Mark	0:16:40.00	0:16:40.00
6	0:16:40.00	Time Mark	0:16:40.00	0:16:40.00
7	0:16:40.00	Time Mark	0:16:40.00	0:16:40.00
8	0:16:40.00	Time Mark	0:16:40.00	0:16:40.00
9	0:16:40.00	Time Mark	0:16:40.00	0:16:40.00

Figure 92. TN3270E Configuration Table

The fields on the TN3270E configuration table are:

Index	This is the index into the configuration table.
Functions	This object indicates the functions supported by the TN3270E server.

Session Term State	The current state for determining what a TN3270E server should do when a TN3270 Session terminates: **Terminate** => Terminate TCP connection **LuSessionPend** => Do not drop the TCP Connection associated with a client when their TN3270 Session ends. Processing should redrive session initialization as if the client was first connecting. **QueueSession** => QUEUESESSION deals with CLSDST-Pass. An example is the easiest explanation. Assume APPL1 does a CLSDST-Pass to APPL2. Then the client logs off APPL Without QUEUESESSION the connection would now be broken. With QUEUESESSION the TN3270E server keeps the LU around after getting the APPL2 unbind waiting for a bind from APPL1.
Server Type	This object indicates the type of TN3270E server. The existence of MIB tables and objects that will be defined by follow-on MIBs may be predicated on whether the TN3270E server can be local to the same host as a Target Application (host:1) or will always be remote (gateway:2).
Contact	This object provides a scratch pad for a TN3270E server administrator for storing information for later retrieval.

STATUS subtable

Index	This is the index into the configuration table.
Admin Status	The desired state of the TN3270E server: **Up (1)** - Activate a TN3270E server. **Down (2)-** Informs the associating TN3270E server to gracefully terminate its processing. **Stop Immediate (3)** - Informs the associating TN3270E server to terminate immediately. Implementation as to the exact semantics of either down (2) or Stop Immediate (3) processing is left as implementation dependent. A TN3270E server that does not distinguish between down or Stop Immediate transitions should not support Stop Immediate.
Oper Status	The current operational state of a TN3270E server: **Up** - The corresponding TN3270E server is active. **Down** - The corresponding TN3270E server is inactive.

Row Status	This object allows entries to be created and deleted in the TN3270ESrvrConfTable. The values may be: 1 : Active 2 : Not In Service 3 : Not Ready 4 : Create And Go 5 : Create And Wait 6 : Destroy An entry in this table is deleted by setting this object to Destroy(6).

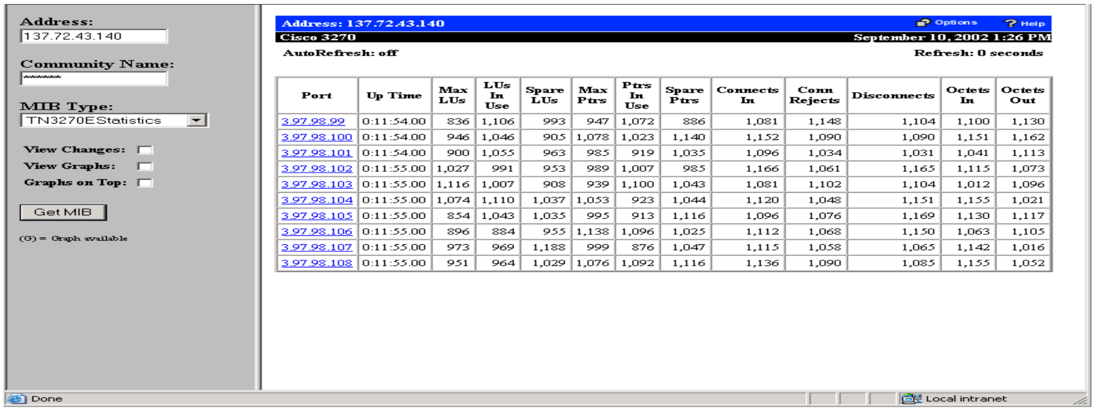
ACTIVITY/ TIMING subtable

Inactivity Timeout	The inactivity time-out specified in seconds. When a connection has been inactive for the number of seconds specified by this object it is closed. The default of 0 means no inactivity time-out.
Activity Check	This object is intended to enable either TIMEMARK or NOP processing.
Activity Timeout	The TIMEMARK or NOP processing time-out specified in seconds. Note that a value of 0 is not allowed for this object since the function that uses this object relies on TN3270ESrvrConfActivityCheck for function enablement.
Activity Interval	The scan interval to be used by a TN3270E server. TIMEMARK or NOP processing scans the Telnet sessions on the interval provided by this object looking for sessions that have been idle for more than the value provided by TN3270ESrvrConfActivityTimeout. Note that a value of 0 is not allowed for this object since the function that uses it relies on TN3270ESrvrConfActivityCheck for function enablement.

TN3270E Statistics

The TN3270E Server Statistics Table defines a set of statistics concerning global TN3270E server performance. An entry can be global with respect to a single TN3270E server or can be specified at a port level. Refer to the text description for tn3270eSrvrStatsPort.

It is possible that a TN3270E server implementation may not be structured to support resource usage on a port basis but provide statistics via an entry in the Server Statistics table for each port. The recommended approach for this is to provide a global entry (a value of 0 for TN3270eSrvrStatsPort) with: TN3270eSrvrStatsMaxLus, TN3270eSrvrStatsMaxLus, Tn3270eSrvrStatsLusInUse, TN3270eSrvrStatsSpareLus, TN3270eSrvrStatsMaxPtrs, TN3270eSrvrStatsPtrsInUse, TN3270eSrvrStatsSparePtrs set at this layer but set to zero at the port layer.


Address: 137.72.43.140

Community Name: ********

MIB Type: TN3270EStatistics

View Changes: ☐
View Graphs: ☐
Graphs on Top: ☐

(G) = Graph available

Address: 137.72.43.140

Cisco 3270 September 10, 2002 1:26 PM

AutoRefresh: off Refresh: 0 seconds

Port	Up Time	Max LUs	LUs In Use	Spare LUs	Max Ptrs	Ptrs In Use	Spare Ptrs	Connects In	Conn Rejects	Disconnects	Octets In	Octets Out
3.97.98.99	0:11:54.00	836	1,106	993	947	1,072	886	1,081	1,148	1,104	1,100	1,130
3.97.98.100	0:11:54.00	946	1,046	905	1,078	1,023	1,140	1,152	1,090	1,090	1,151	1,162
3.97.98.101	0:11:54.00	900	1,055	963	985	919	1,035	1,096	1,034	1,031	1,041	1,113
3.97.98.102	0:11:55.00	1,027	991	953	989	1,007	985	1,166	1,061	1,165	1,115	1,073
3.97.98.103	0:11:55.00	1,116	1,007	908	939	1,100	1,043	1,081	1,102	1,104	1,012	1,096
3.97.98.104	0:11:55.00	1,074	1,110	1,037	1,053	923	1,044	1,120	1,048	1,151	1,155	1,021
3.97.98.105	0:11:55.00	854	1,043	1,035	995	913	1,116	1,096	1,076	1,169	1,130	1,117
3.97.98.106	0:11:55.00	896	884	955	1,138	1,096	1,025	1,112	1,068	1,150	1,063	1,105
3.97.98.107	0:11:55.00	973	969	1,188	999	876	1,047	1,115	1,058	1,065	1,142	1,016
3.97.98.108	0:11:55.00	951	964	1,029	1,076	1,092	1,116	1,136	1,090	1,085	1,155	1,052

Figure 93. TN3270E Statistics Table

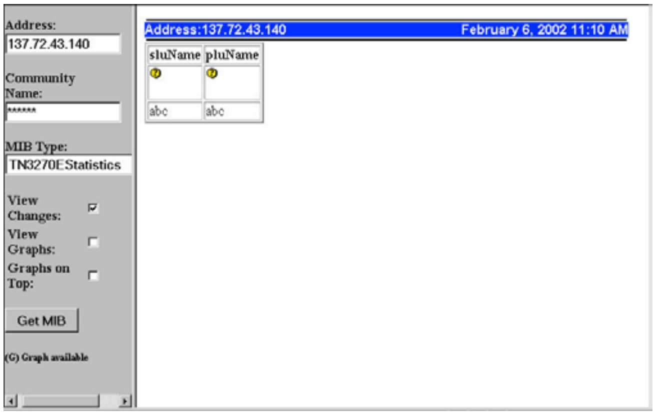
The fields on the TN3270E Server Statistics Table are:

Port	Indicates the port that the corresponding statistics are for. Implementation of collection of these statistics on a port basis is not mandatory. An implementation may limit itself to keeping this data on a global basis by using a value of 0. This column is a hyperlink to the TN3270E SNA Server Map Table, which defines the mapping of an SLUName to a PLUName.
Up Time	Indicates when either usage of an associating port becomes active (TN3270eSrvrStatsPort non-zero) or if the entry is being kept on a global basis the time that the TN3270E server becomes active. The value of this object does not get reset based on port usage status changes or changes to TN3270eSrvrPortOperStatus.
Max LUs	States the maximum number of LUs for use by a TN3270E server.
LUs in Use	Indicates the current number of LUs in use by a TN3270E server.

Spare LUs	Shows the number of free LUs for a particular TN3270E server. It is possible that the difference between TN3270eSrvrStatsMaxLUs and TN3270eSrvrStatsLUsInUse does not equal TN3270eSrvrStatsSpareLUs. An LU may exist but not be usable by a client connection.
Max Ptrs	Lists the maximum number of printer resources for use by a TN3270E server.
Ptrs in Use	Indicates the current number of printer resources in use by a TN3270E server.
Spare Ptrs	States the number of free printer resources for a particular TN3270E server. It is possible that the difference between TN3270eSrvrStatsMaxPtrs and TN3270eSrvrStatsPtrsInUse does not equal TN3270eSrvrStatsSparePtrs. A printer resource may exist but not be usable by a client connection.
Connects In	Lists the number of client connections received by a TN3270E server.
Conn Rejects	Shows the number of client connections disconnected by a TN3270E server.
Disconnects	Indicates the number of client connections disconnected by a TN3270E server.
Octets In	States the number of octets received from TN3270 and TN3270E clients.
Octets Out	Lists the number of octets sent to TN3270 and TN3270E clients.

TN3270E SNA Server Map Table (*subscreen of TN3270E Statistics*)

The TN3270E SNA Server Map Table defines the mapping of an SLUName to a PLUName. Access the TN3270E SNA Server Map Table by clicking the Port hyperlink from the TN3270EStatistics table.



Address: 137.72.43.140

Community Name: ******

MIB Type: TN3270EStatistics

View Changes: ☑

View Graphs: ☐

Graphs on Top: ☐

Address:137.72.43.140 February 6, 2002 11:10 AM

sluName	pluName
abc	abc

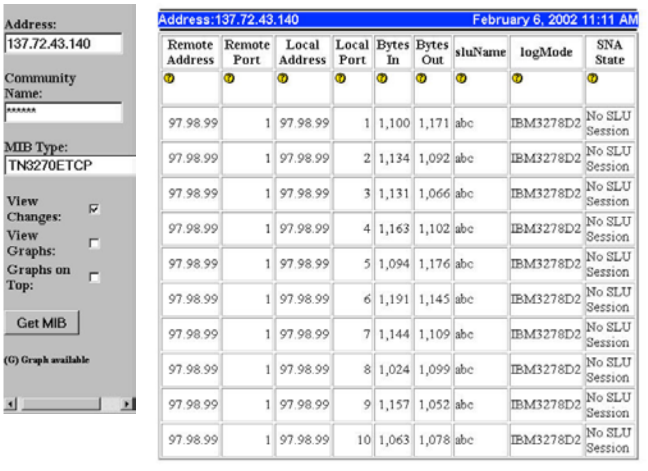
Figure 94. TN3270E SNA Map Table

The fields on the TN3270E SNA Map Table are:

SLUName	The name of the secondary LU (SLU) as it is known in the SNA network. This name is sent by the SSCP on the Activate Logical Unit (ACTLU) request.
PLUName	When there is a currently active LU-LU session for this connection, this object returns the primary LU (PLU) name from the BIND. When there is no active LU-LU session or when the PLU name is unavailable for some other reason, this object is empty.

TN3270E TCP

The TN3270E TCP table describes the MIB module for objects used to manage the TN3270E server. This table has an entry for each TN3270(E) client connection that is active at the TN3270E server. The table was originally modeled after the TCPConnTable and was modified to support different client address types. It is indexed first by the remote address and port as opposed to local address and port, thus enabling use of a SNMP GET-NEXT operation while using only the remote address and port.



Address: 137.72.43.140

Community Name: ******

MIB Type: TN3270ETCP

View Changes: ☑

View Graphs: ☐

Graphs on Top: ☐

Address:137.72.43.140 February 6, 2002 11:11 AM

Remote Address	Remote Port	Local Address	Local Port	Bytes In	Bytes Out	sluName	logMode	SNA State
97.98.99	1	97.98.99	1	1,100	1,171	abc	IBM3278D2	No SLU Session
97.98.99	1	97.98.99	2	1,134	1,092	abc	IBM3278D2	No SLU Session
97.98.99	1	97.98.99	3	1,131	1,066	abc	IBM3278D2	No SLU Session
97.98.99	1	97.98.99	4	1,163	1,102	abc	IBM3278D2	No SLU Session
97.98.99	1	97.98.99	5	1,094	1,176	abc	IBM3278D2	No SLU Session
97.98.99	1	97.98.99	6	1,191	1,145	abc	IBM3278D2	No SLU Session
97.98.99	1	97.98.99	7	1,144	1,109	abc	IBM3278D2	No SLU Session
97.98.99	1	97.98.99	8	1,024	1,099	abc	IBM3278D2	No SLU Session
97.98.99	1	97.98.99	9	1,157	1,052	abc	IBM3278D2	No SLU Session
97.98.99	1	97.98.99	10	1,063	1,078	abc	IBM3278D2	No SLU Session

Figure 95. TN3270E TCP Table

The fields on the TN3270E TCP table are:

Remote Address	The remote address associated with a TN3270E client. TN3270ETcpConnRemAddrType indicates the address type (IPv4 or IPv6 for example). If a TN3270 (E) client is connected to its server via a proxy client the address represented by the value of this object should be the remote client's address, not the proxy client's address.
Remote Port	The remote port associated with a TN3270E client. If a TN3270 (E) client is connected to its server via a proxy client the port represented by the value of this object should be the remote client's port, not the proxy client's port.
Local Address	The local address associated with a TN3270E client. TN3270ETcpConnRemAddrType indicates the address type (IPv4 or IPv6 for example).
Local Port	The local port associated with a TN3270E client.
Bytes In	The number of bytes received by the server from TCP for this connection.

Bytes Out	The number of bytes sent to TCP for this connection.
SLUName	LU/Printer secondary name for connecting a client into an SNA network.
Logmode	Indicates the device type if negotiated with client. This object is also known as Logmode. May be one of the following: 0 : Unknown 1 : IBM3278D2 2 : IBM3278D2E 3 : IBM3278D3 4 : IBM3278D3E 5 : IBM3278D4 6 : IBM3278D4E 7 : IBM3278D5 8 : IBM3278D5E 9 : IBMDynamic 10: IBM3287D1
SNA State	The current state of the SNA side of the end-to-end TN3270 connection. The following states are defined: 0 : Unknown – the true state is not known. 1 : No SLU Session – the SLU has neither an SSCP-LU nor an LU-LU session active. 2 : SSCP LU Session – the SSCP-LU session for the SLU is active, but the SLU is not currently in session with a PLU. 3 : LU LU Session – the SLU currently has an active session with a PLU.

OSA Express

OSA-Express Fast Ethernet (FENET), OSA-Express 155 ATM and OSA-Express Gigabit Ethernet (GbE) are the newest features in the lineup of Local Area Network (LAN) adapters offered under the covers of S/390 Parallel Enterprise Server Generation 5 and Generation 6.

OSA-Express has one physical network adapter or OSA port. Its physical port can be attached directly to a LAN. This integration of channel path with network port makes OSA-Express a unique type of S/390 channel, recognized by the hardware I/O configuration as one of the following:

- OSD (QDIO)
- OSE (non QDIO)

Reports for the following are shown:

- Processor utilization
- Physical PCI bus utilization
- Ethernet port diagnostics

There are three OSA-Express type variables:

- OSAExpress (G)
- OSAPerformance (G)
- OSAEthernet (G)

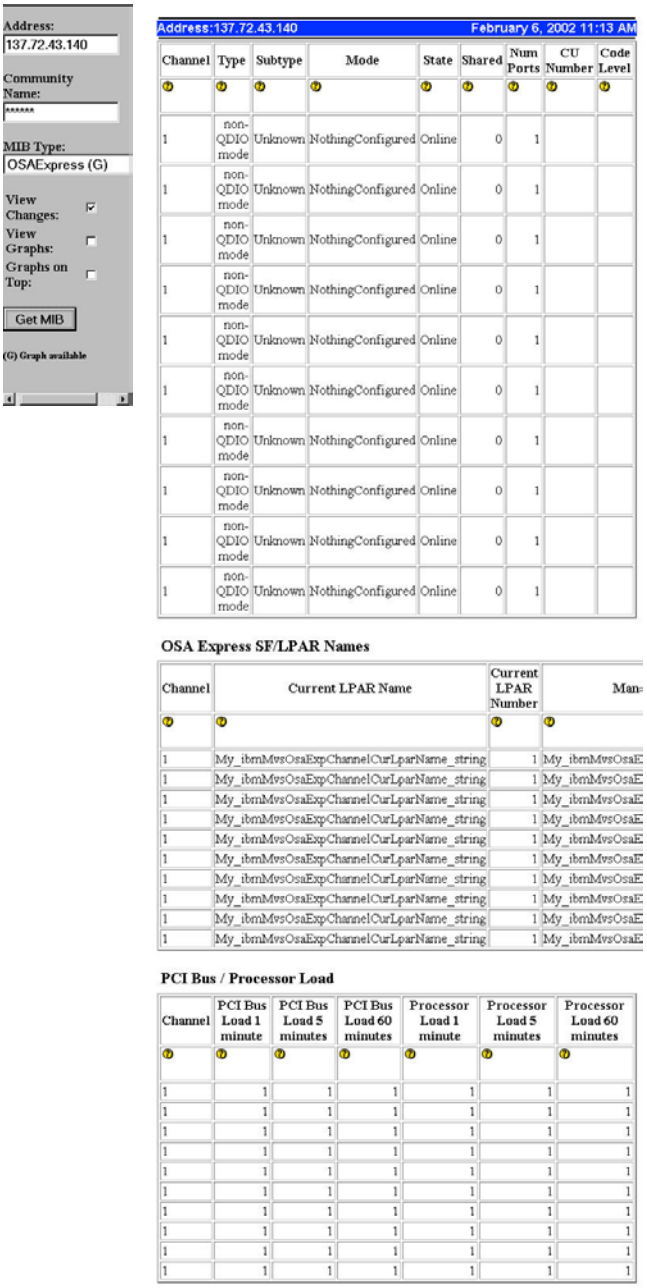
The (G) after each variable indicates that graphs are available.

OSAExpress (G)

One entry in this table exists per OSA-Express Device Interface in the OSA Express table. The (G) indicates that graphs are available. If the values for objects ibmMvsOsaExpCurLparName/Num are not the same as the values for objects ibmMvsOsaExpManLparName/Num then the OSA/SF running in the current LPAR is not the managing OSA/SF for this Device. The utilization object values are reset when the CHPID is reset. The processor utilization objects are the sum of the per LPAR processor utilization values in the corresponding osaexpPerfTable entries for the adapter.

The OSA Express Table has two subtables:

- OSA Express SF/LPAR Names
- PCI Bus/Processor Load



Address: 137.72.43.140

Community Name: ******

MIB Type: OSAExpress (G)

View Changes: ☑

View Graphs: ☐

Graphs on Top: ☐

Address:137.72.43.140 February 6, 2002 11:13 AM

Channel	Type	Subtype	Mode	State	Shared	Num Ports	CU Number	Code Level
1	non-QDIO mode	Unknown	NothingConfigured	Online	0	1		
1	non-QDIO mode	Unknown	NothingConfigured	Online	0	1		
1	non-QDIO mode	Unknown	NothingConfigured	Online	0	1		
1	non-QDIO mode	Unknown	NothingConfigured	Online	0	1		
1	non-QDIO mode	Unknown	NothingConfigured	Online	0	1		
1	non-QDIO mode	Unknown	NothingConfigured	Online	0	1		
1	non-QDIO mode	Unknown	NothingConfigured	Online	0	1		
1	non-QDIO mode	Unknown	NothingConfigured	Online	0	1		
1	non-QDIO mode	Unknown	NothingConfigured	Online	0	1		
1	non-QDIO mode	Unknown	NothingConfigured	Online	0	1		

OSA Express SF/LPAR Names

Channel	Current LPAR Name	Current LPAR Number	Man
1	My_ibmMvsOsaExpChannelCurLparName_string	1	My_ibmMvsOsaE
1	My_ibmMvsOsaExpChannelCurLparName_string	1	My_ibmMvsOsaE
1	My_ibmMvsOsaExpChannelCurLparName_string	1	My_ibmMvsOsaE
1	My_ibmMvsOsaExpChannelCurLparName_string	1	My_ibmMvsOsaE
1	My_ibmMvsOsaExpChannelCurLparName_string	1	My_ibmMvsOsaE
1	My_ibmMvsOsaExpChannelCurLparName_string	1	My_ibmMvsOsaE
1	My_ibmMvsOsaExpChannelCurLparName_string	1	My_ibmMvsOsaE
1	My_ibmMvsOsaExpChannelCurLparName_string	1	My_ibmMvsOsaE
1	My_ibmMvsOsaExpChannelCurLparName_string	1	My_ibmMvsOsaE
1	My_ibmMvsOsaExpChannelCurLparName_string	1	My_ibmMvsOsaE

PCI Bus / Processor Load

Channel	PCI Bus Load 1 minute	PCI Bus Load 5 minutes	PCI Bus Load 60 minutes	Processor Load 1 minute	Processor Load 5 minutes	Processor Load 60 minutes
1	1	1	1	1	1	1
1	1	1	1	1	1	1
1	1	1	1	1	1	1
1	1	1	1	1	1	1
1	1	1	1	1	1	1
1	1	1	1	1	1	1
1	1	1	1	1	1	1
1	1	1	1	1	1	1
1	1	1	1	1	1	1
1	1	1	1	1	1	1

Figure 96. OSA Express Table

The fields on the OSA Express Table are:

Channel	The channel number for this interface.
Type	For OSA-Express adapters supporting QDIO mode, the value is osd (17). For OSA-Express adapters supporting non-QDIO mode, the value will be ose (16).

SubType	The channel subtype indicates how the channel is configured. The values possible are: 1 : Unknown 2 : Gigabit EtherNet 3 : Fast Ethernet 4 : ATM Native 5 : ATM LAN Emulation 6 : No Ports Defined 7 : One Logical Ethernet Port 8 : One Logical Token Ring Port 9 : Two Logical Ethernet Ports 10 : Two Logical Token Ring Ports 11 : Logical Ethernet And Token Ring Ports 12 : Logical Token Ring And Ethernet Ports
Mode	The configured mode of the OSA-Express adapter. The values possible are: 1: Nothing Configured 2: Pass Thru Mode 3: SNA Mode 4: Pass Thru And SNA 5: ATM LE Pass Thru 6: ATM LE SNA 7: ATM LE Passthru And SNA 8: ATM Native 9: QDIO
State	Hardware channel state: online, not installed, or offline.
Shared	An OSA-Express Channel can be shared across multiple LPARs. This object indicates if this channel is currently being shared.
Num Ports	Number of physical ports on the OSA-Express Channel.
CU Number	The control unit number associated with the OSA-Express Channel.
Code Level	This is the firmware (or micro code level) of the OSA adapter. For example, OSA adapter level 05.60 would be represented as 0560 by this object.

OSA EXPRESS SF/LPAR NAMES subtable

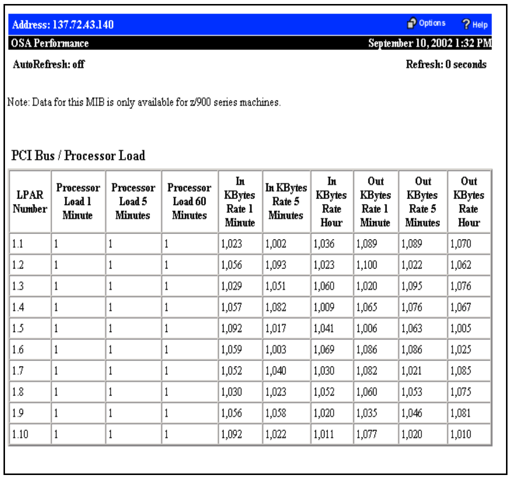
Channel	The channel number for this interface.
Current LPAR Name	LPAR name of the OSA/SF from which this data was retrieved.
Current LPAR Number	LPAR number of the OSA/SF from which this data was retrieved.
Managing LPAR Name	LPAR name of the OSA Support Facility managing this channel. Only one OSA/SF can manage a OSA-Express Channel within an MVS Sysplex even though multiple OSA/SFs can retrieve information from the same OSA-Express Channel.
Managing LPAR Number	LPAR number of the OSA Support Facility managing this channel (set to 0xFFFF if not being managed by a OSA/SF).

PCI BUS/ PROCESSOR LOAD subtable

Channel	The channel number for this interface.
PCI Bus Load 1 Minute	The average, over a 1-minute interval, of the percentage of time that the PCI bus was utilized to transfer data. It does not include idle time or time used by routine maintenance tasks. The range of valid values for this object is 0 to 100%. A value of -1 indicates that the value could not be retrieved from the adapter.
PCI Bus Load 5 Minutes	The average, over a 5-minute interval, of the percentage of time that the PCI bus was utilized to transfer data. It does not include idle time or time used by routine maintenance tasks. The range of valid values for this object is 0 to 100%. A value of -1 indicates that the value could not be retrieved from the adapter.
PCI Bus Load 60 Minutes	The average, over an hour interval, of the percentage of time that the PCI bus was utilized to transfer data. It does not include idle time or time used by routine maintenance tasks. The range of valid values for this object is 0 to 100%. A value of -1 indicates that the value could not be retrieved from the adapter.

OSA Performance (G)

The OSA Performance table provides performance information per each LPAR's utilization of an OSA-Express adapter. The (G) indicates that graphs are available. The values are reset when the adapter CHPID is reset.



Address: 137.72.43.140

OSA Performance September 10, 2002 1:32 PM

AutoRefresh: off Refresh: 0 seconds

Note: Data for this MIB is only available for z/900 series machines.

PCI Bus / Processor Load

LPAR Number	Processor Load 1 Minute	Processor Load 5 Minutes	Processor Load 60 Minutes	In KBytes Rate 1 Minute	In KBytes Rate 5 Minutes	In KBytes Rate Hour	Out KBytes Rate 1 Minute	Out KBytes Rate 5 Minutes	Out KBytes Rate Hour
1.1	1	1	1	1,023	1,002	1,036	1,089	1,089	1,070
1.2	1	1	1	1,056	1,093	1,023	1,100	1,022	1,062
1.3	1	1	1	1,029	1,051	1,060	1,020	1,095	1,076
1.4	1	1	1	1,057	1,082	1,009	1,065	1,076	1,067
1.5	1	1	1	1,092	1,017	1,041	1,006	1,063	1,005
1.6	1	1	1	1,059	1,003	1,069	1,086	1,086	1,025
1.7	1	1	1	1,052	1,040	1,030	1,082	1,021	1,085
1.8	1	1	1	1,030	1,023	1,052	1,060	1,053	1,075
1.9	1	1	1	1,056	1,058	1,020	1,035	1,046	1,081
1.10	1	1	1	1,092	1,022	1,011	1,077	1,020	1,010

Figure 97. OSA Performance Table

The fields on the OSA Peformance Table are:

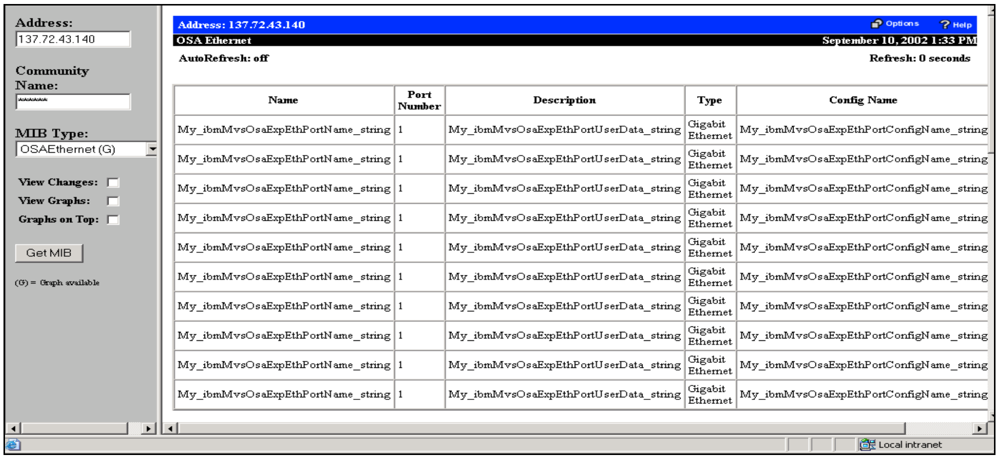
LPAR Number	LPAR number of the LPAR to which the performance objects apply.
Processor Load 1 Minute	The average percentage of time that the CHPID Processor was utilized to transfer data for a specific LPAR over a 1-minute interval. It does not include idle time or time used by routine maintenance tasks. The range of valid values for this object is 0 to 100%. A value of -1 indicates that the value could not be retrieved from the adapter.
Processor Load 5 Minutes	The average percentage of time that the CHPID Processor was utilized to transfer data for a specific LPAR over a 5-minute interval. It does not include idle time or time used by routine maintenance tasks. The range of valid values for this object is 0 to 100%. A value of -1 indicates the value could not be retrieved from the adapter.
Processor Load 60 Minutes	The average percentage of time that the CHPID Processor was utilized to transfer data for a specific LPAR over a one-hour interval. It does not include idle time or time used by routine maintenance tasks. The range of valid values for this object is 0 to 100%. A value of -1 indicates that the value could not be retrieved from the adapter.
In KBytes Rate	The average number of inbound kilobytes processed for a specific LPAR over a 1-minute interval. When the

1 Minute	ibmMvsOsaExpPerfProcessorUtil1Min object for a specific LPAR has a value of -1, the interval data could not be retrieved from the adapter and this object has a value of zero.
In KBytes Rate **5 Minutes**	The average number of inbound kilobytes processed for a specific LPAR over a 5-minute interval. When the ibmMvsOsaExpPerfProcessorUtil5Min object for a specific LPAR has a value of -1, then the interval data could not be retrieved from the adapter and this object has a value of zero.
In KBytes Rate **60 Minutes**	The average number of inbound kilobytes processed for a specific LPAR over a 5-minute interval. When the ibmMvsOsaExpPerfProcessorUtil5Min object for a specific LPAR has a value of -1, then the interval data could not be retrieved from the adapter and this object has a value of zero.
Outbound KBytes Rate **1 Minute**	The average number of outbound kilobytes processed for a specific LPAR over a 1-minute interval. When the ibmMvsOsaExpPerfProcessorUtil1Min object for a specific LPAR has a value of -1, then the interval data could not be retrieved from the adapter and this object has a value of zero.
Out KBytes Rate **5 Minutes**	The average the number of outbound kilobytes processed for a specific LPAR over a 5-minute interval. When the ibmMvsOsaExpPerfProcessorUtil5Min object for a specific LPAR has a value of -1, then the interval data could not be retrieved from the adapter and this object has a value of zero.
Out KBytes Rate **60 Minutes**	The average number of outbound kilobytes processed for a specific LPAR over a one-hour interval. When the ibmMvsOsaExpPerfProcessorUtilHour object for a specific LPAR has a value of -1, then the interval data could not be retrieved from the adapter and this object has a value of zero.

OSA Ethernet (G)

The OSA Ethernet Table is intended to represent the Ethernet ports associated with the OSA Express Channel Table entries for Ethernet adapters. The (G) indicates that graphs are available. Each OSA-Express Channel has one or more ports. The OSA Ethernet Table has three subtables:

- Configuration
- Traffic/Errors
- MAC Addresses



Address: 137.72.43.140

Community Name: ******

MIB Type: OSAEthernet (G)

View Changes: ☐
View Graphs: ☐
Graphs on Top: ☐

(G) = Graph available

Address: 137.72.43.140

OSA Ethernet September 10, 2002 1:33 PM

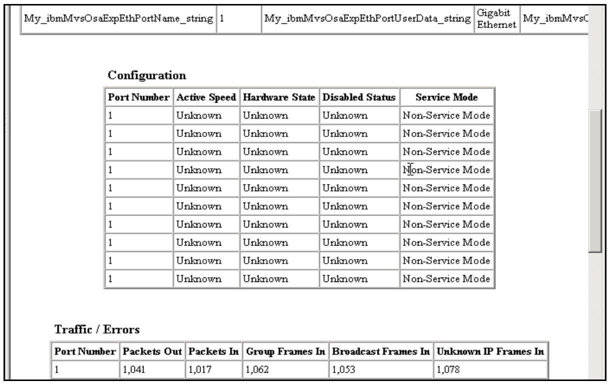
AutoRefresh: off Refresh: 0 seconds

Name	Port Number	Description	Type	Config Name
My_ibmMvsOsaExpEthPortName_string	1	My_ibmMvsOsaExpEthPortUserData_string	Gigabit Ethernet	My_ibmMvsOsaExpEthPortConfigName_string
My_ibmMvsOsaExpEthPortName_string	1	My_ibmMvsOsaExpEthPortUserData_string	Gigabit Ethernet	My_ibmMvsOsaExpEthPortConfigName_string
My_ibmMvsOsaExpEthPortName_string	1	My_ibmMvsOsaExpEthPortUserData_string	Gigabit Ethernet	My_ibmMvsOsaExpEthPortConfigName_string
My_ibmMvsOsaExpEthPortName_string	1	My_ibmMvsOsaExpEthPortUserData_string	Gigabit Ethernet	My_ibmMvsOsaExpEthPortConfigName_string
My_ibmMvsOsaExpEthPortName_string	1	My_ibmMvsOsaExpEthPortUserData_string	Gigabit Ethernet	My_ibmMvsOsaExpEthPortConfigName_string
My_ibmMvsOsaExpEthPortName_string	1	My_ibmMvsOsaExpEthPortUserData_string	Gigabit Ethernet	My_ibmMvsOsaExpEthPortConfigName_string
My_ibmMvsOsaExpEthPortName_string	1	My_ibmMvsOsaExpEthPortUserData_string	Gigabit Ethernet	My_ibmMvsOsaExpEthPortConfigName_string
My_ibmMvsOsaExpEthPortName_string	1	My_ibmMvsOsaExpEthPortUserData_string	Gigabit Ethernet	My_ibmMvsOsaExpEthPortConfigName_string
My_ibmMvsOsaExpEthPortName_string	1	My_ibmMvsOsaExpEthPortUserData_string	Gigabit Ethernet	My_ibmMvsOsaExpEthPortConfigName_string
My_ibmMvsOsaExpEthPortName_string	1	My_ibmMvsOsaExpEthPortUserData_string	Gigabit Ethernet	My_ibmMvsOsaExpEthPortConfigName_string

Figure 98. OSA Ethernet Table

The fields on OSA Ethernet are:

Name	Specifies the port name that must also be entered at the connection manager on the host and the application. Port name is specifed to OSA/SF as a config file parameter (PCM_NAME). This value is also specified via ILMI as the value of the atmfPortMyIfName object. Does not apply to an ATM OSA-2 adapter configured for ATM IP Forwarding mode, or an OSA-Express ATM155 adapter configured for QDIO LAN Emulation mode.
Port Number	Port number, starts at 0.
Description	Configured port description provided by the user.
Type	The physical port type. May be Gigabit Ethernet or Fast Ethernet.
Config Name	Name of configuration.
Config Speed	The configured port speed. For OSA-Express Gigabit Ethernet adapters the port speed cannot be configured so the value of this object is 1000MbFullDuplex(7). 0: Auto Negotiate 1: Half Duplex 10Mb 2: Full Duplex 10Mb 3: Half Duplex 100Mb 4: Full Duplex 100Mb 7: Full Duplex 1000Mb



My_ibmMvsOsaExpEthPortName_string	1	My_ibmMvsOsaExpEthPortUserData_string	Gigabit Ethernet	My_ibmMvs

Configuration

Port Number	Active Speed	Hardware State	Disabled Status	Service Mode
1	Unknown	Unknown	Unknown	Non-Service Mode
1	Unknown	Unknown	Unknown	Non-Service Mode
1	Unknown	Unknown	Unknown	Non-Service Mode
1	Unknown	Unknown	Unknown	Non-Service Mode
1	Unknown	Unknown	Unknown	Non-Service Mode
1	Unknown	Unknown	Unknown	Non-Service Mode
1	Unknown	Unknown	Unknown	Non-Service Mode
1	Unknown	Unknown	Unknown	Non-Service Mode
1	Unknown	Unknown	Unknown	Non-Service Mode
1	Unknown	Unknown	Unknown	Non-Service Mode

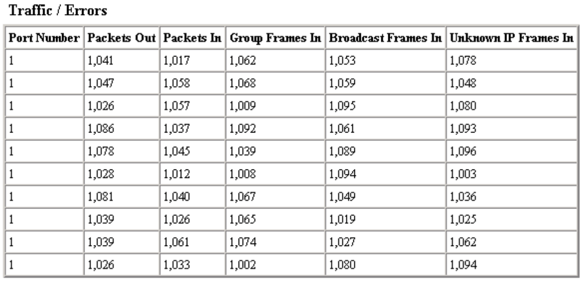
Traffic / Errors

Port Number	Packets Out	Packets In	Group Frames In	Broadcast Frames In	Unknown IP Frames In
1	1,041	1,017	1,062	1,053	1,078

Figure 99. OSA Ethernet Configuration Subtable

CONFIGURATION subtable

Port Number	Port number, starts at 0.
Active Speed	The actual port speed. 0: Unknown 1: Half Duplex 10Mb 2: Full Duplex 10Mb 3: Half Duplex 100Mb 4: Full Duplex 100Mb 7: Full Duplex 1000Mb
Hardware State	The hardware state of the port: 1 - Unknown port hardware state. 2 - OSA has detected a loss of signal on the link. (A likely cause of this condition is an improperly installed or missing cable connection on the port). For OSA-Express ATM, this condition can also be caused by registration failure. 3 - Port is disabled. The reason for the port being disabled is set in object Disabled Status. 4 - Port is enabled.
Disabled Status	When the value of Hardware State is disabled(3), this object explains the reason for the disabled state. The value for this object may be a combination of the following: 0x0001 Disabled internal port failure 0x0002 Disabled service processor request 0x0004 Disabled network request 0x0008 Disabled OSA/SF request 0x0010 Disabled configuration change 0x0020 Disabled link failure threshold exceeded 0x0040 Disabled port temporarily disabled When the value of Hardware State is not disabled(3), the value of this object is zero.
Service Mode	May be Non-service Mode or Service Mode.



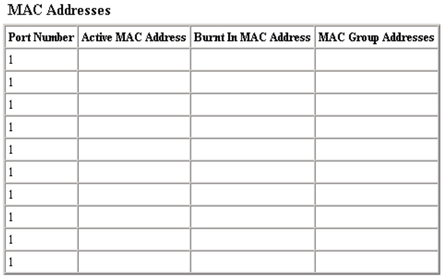
Traffic / Errors

Port Number	Packets Out	Packets In	Group Frames In	Broadcast Frames In	Unknown IP Frames In
1	1,041	1,017	1,062	1,053	1,078
1	1,047	1,058	1,068	1,059	1,048
1	1,026	1,057	1,009	1,095	1,080
1	1,086	1,037	1,092	1,061	1,093
1	1,078	1,045	1,039	1,089	1,096
1	1,028	1,012	1,008	1,094	1,003
1	1,081	1,040	1,067	1,049	1,036
1	1,039	1,026	1,065	1,019	1,025
1	1,039	1,061	1,074	1,027	1,062
1	1,026	1,033	1,002	1,080	1,094

Figure 100. OSA Ethernet Traffic/Errors Subtable

TRAFFIC/ERRORS subtable

Port Number	Port number, starts at 0.
Packets Out	The count of the total number of packets transmitted from this port. A CHPID reset causes this value to be reset to zero.
Packets In	The count of the total number of packets received by this port. A CHPID reset causes this value to be reset to zero.
Group Frames In	The count of the total number of group frames received by this port. A CHPID reset causes this value to be reset to zero.
Broadcast Frames In	The count of the total number of broadcast frames received by this port. A CHPID reset causes this value to be reset to zero.
Unknown IP Frames In	The count of the total number of packets that were discarded because they did not have a matching IP address and there was no primary or secondary router default defined. This object is not supported for Fast Ethernet adapters so the value is zero.



MAC Addresses

Port Number	Active MAC Address	Burnt In MAC Address	MAC Group Addresses
1			
1			
1			
1			
1			
1			
1			
1			
1			
1			

Figure 101. OSA Ethernet MAC Addresses Subtable

MAC ADDRESSES subtable

Port Number	Port number, starts at 0.
Active MAC Address	A 6 byte OCTET STRING that contains the current MAC address in use on the adapter.
Burnt In MAC Address	A 6 byte OCTET STRING that contains the adapter's burned in MAC address.
MAC Group Addresses	This field contains the active Group Addresses. An individual Group Address is 6 bytes long. Therefore, this field is actually 32 times (OCTET STRING(SIZE(6)) + 2 bytes of padding) long.

(This page intentionally left blank.)

History Reports

NV4IP views the TCP/IP network performance from the enterprise level to the remote user connection. Performance indicators are available for workload, usage, and response time. The history reports are available immediately after the Host Monitor is brought up.

There are nine types of history reports under four categories that provide the following information:

Workload and Performance

Base History	Sample-based workload and response time.
Thru99 EE History	Interval-based throughput summaries for Enterprise Extender (UDP-based) data traffic by port.
Thru99 Link History	Interval-based throughput summaries for TCP/IP data traffic to/from IP channel links.

Expert Reports

API Expert	Session-based Socket applications.
FTP Performance Expert	Session-based FTP (client or server).
Telnet Expert	Session-based Telnet (client or server).

Buffer

(CSM) History	Usage and Alerts for CSM buffer pools.
VTAM Buffer History	Usage and trends for VTAM buffer pools.

TraceRoute

TraceRoute History	Session-based results of the TraceRte command for any defined critical resources that have exceeded their performance threshold parameters.

In addition to the difference in the type of data collected, the method of data collection differs between history reports. The Base History data is collected using a sampling method. The Host Monitor writes SMF records at regular intervals detailing the number of active sessions, byte counts, etc. This type of report indicates how many concurrent sessions there are at any instant and the changes in data flow over time. These reports are particularly valuable for long sessions with varying amounts of data transferred.

The Thru99 EE and Link History reports introduce an alternative RMF-like interval snapshot recording method for data being sent or received. The Thru99 Link History report provides interval-based reports for data sent/received over each of the stack's defined IP to IP or IP to channel links. The Thru99 EE History report provides interval-based reports for any of the specifically assigned UDP ports being utilized for Enterprise Extender (EE), which uses UDP over SNA. The default 15-minute interval snapshots allow you to correlate traditional RMF-style host-based activity and workload reports with critical link traffic, and to compare specific throughput levels with their respective stack and CPU workload timeframes.

The Expert Reports (API, FTP, or Telnet) use a session-based method for calculating their reports. The data for these reports is from the SMF records produced by the TCP/IP stack. Session-based counting means that session counts are done based on session initiation and termination records. The session is recorded at the time it finishes, and if no session termination record exists for whatever reason, there will not be a record of the session. The session may have lasted for 8 hours, but it is recorded at the time it terminates. These reports are particularly valuable if you have very short sessions such as with Web server applications or would like to obtain a count of the total number of sessions.

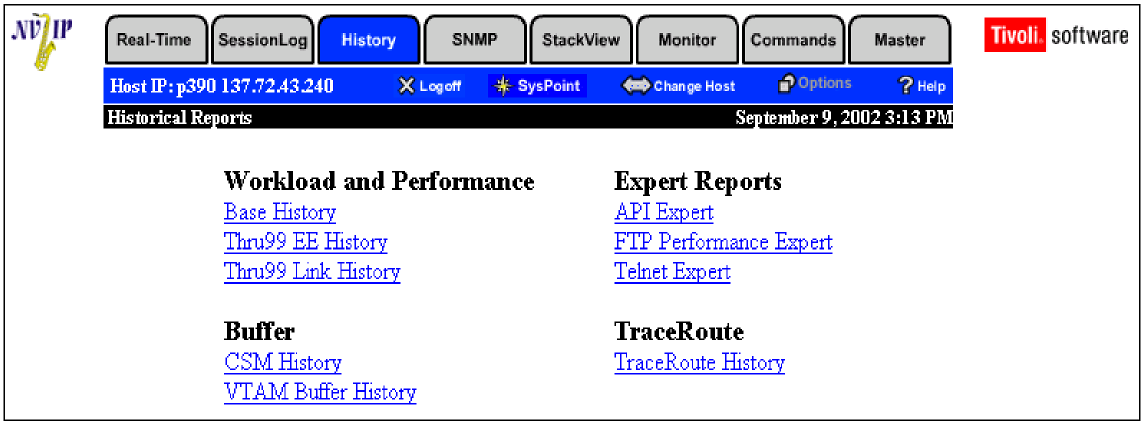
The Buffer reports (CSM History and VTAM Buffer History) are collected from the host. The appropriate interval command must have been set at the host to activate data collection for the VTAM Buffer History report. Data for the TraceRoute History report is collected from the host if the AUTOTRACEROUTE command has previously been set at the host. Data results from a TraceRoute command issued at the workstation is not included in the TraceRoute History report.

In summary, to view real-time data on a sampling basis, view the Real-Time Reports. These reports are available for gathering and monitoring network data in the daily work environment before it has become part of the historical database used by the Base History Reports function. The Real-Time reports are available as soon as the Host Monitor has been active for a short period of time.

If you plan to perform specific historical traffic level analysis by viewing time slices of active sessions taken in a sampling mode, use the History tab's Base History reports. To analyze a specific application or application usage, use the Expert Reports for API, FTP, or Telnet. To view buffer usage by either the Communications Storage Manager or VTAM, use the Buffer reports. To see which critical resources either exceeded the response time threshold or were unavailable, use the TraceRoute History report.

For an alternative method of looking at "near time" activity, view the SessionLog reports for specific application activity. SessionLog reports show API, FTP, or Telnet sessions in a log or sequential format, which are currently in progress or have recently completed. The Thru99 reports will complement any of the above reports, as well as other host-centric RMF reports currently being generated.

To access a report, click on the appropriate tab and then click a hyperlink under the section for the type of report you want to view. The figure below shows the Historical Reports screen accessed by clicking the History tab.



Host IP: p390 137.72.43.240

Historical Reports

September 9, 2002 3:13 PM

Workload and Performance
Base History
Thru99 EE History
Thru99 Link History

Expert Reports
API Expert
FTP Performance Expert
Telnet Expert

Buffer
CSM History
VTAM Buffer History

TraceRoute
TraceRoute History

Figure 102. Historical Reports Screen

Workload and Performance Reports

Workload and performance contains these reports:

- **Base History**
- **Thru99 EE History**
- **Thru99 Link History**

Base History Reports

Trending and historical reports for TCP/IP requires, at a minimum, reporting on workload and response time. Workload for TCP/IP may be measured as sessions or bytes either for an application or for a particular client. The reports provided by NV4IP provide a baseline measurement of your network activity.

The Base History Reports provide three categories of reporting:

Workload	Shows the workload creating the most demand on your system. Available reports are: • Top Clients (Bytes) • Bytes by Application • Sessions by Application
Usage	Shows the absolute usage per interval chosen for applications and clients. For an application, the report indicates which clients (addresses) were using that application. For a client, the report indicates which applications the client was using. Available reports are: • Application Usage Details • Client Usage Details
Response Time	Provides information on the average response times for a particular address, the network, and in terms of network performance relative to service goals. • Response Time for Network • Response Time for Resource • Service Level for Response Time

Base History Workload Reports

The Base History Workload Reports show the workload creating the most demand on your system. All reports are available in both graphical and tabular formats.

A brief description of each Workload Report follows:

Top Clients (Bytes)	Clients sending the most bytes over the selected time period.
Bytes by Application	Number of bytes sent and received per application
Sessions by Application	Number of sessions per application.

Top Clients (Bytes)

The Top Clients (Bytes) report shows the clients who are sending the most bytes over the selected time period (interval) for the particular clients chosen. The clients are the remote IP addresses using an application within the TCP/IP address space selected. The Total Bytes represents the sum of the bytes sent and received.

Graphical Report – Top Clients (Bytes)

Data may be viewed by the week, day, hour, or year. Use Options/Change Graph to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

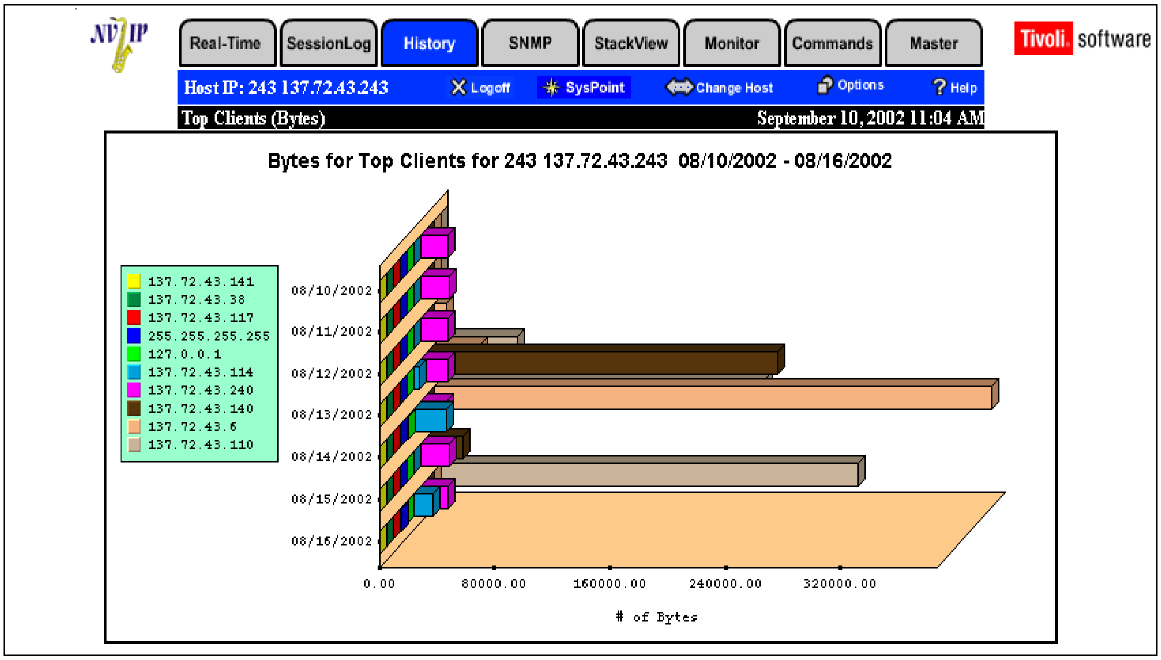


Figure 103. Top Clients (Bytes)

Tabular Report – Top Clients (Bytes)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top Clients (Bytes) tabular report are:

Name/Address	Remote IP address of any socket-attached OLTP application using the selected TCP/IP address space.
Time	Date of session.
Number of Bytes	Sum of bytes sent and received.

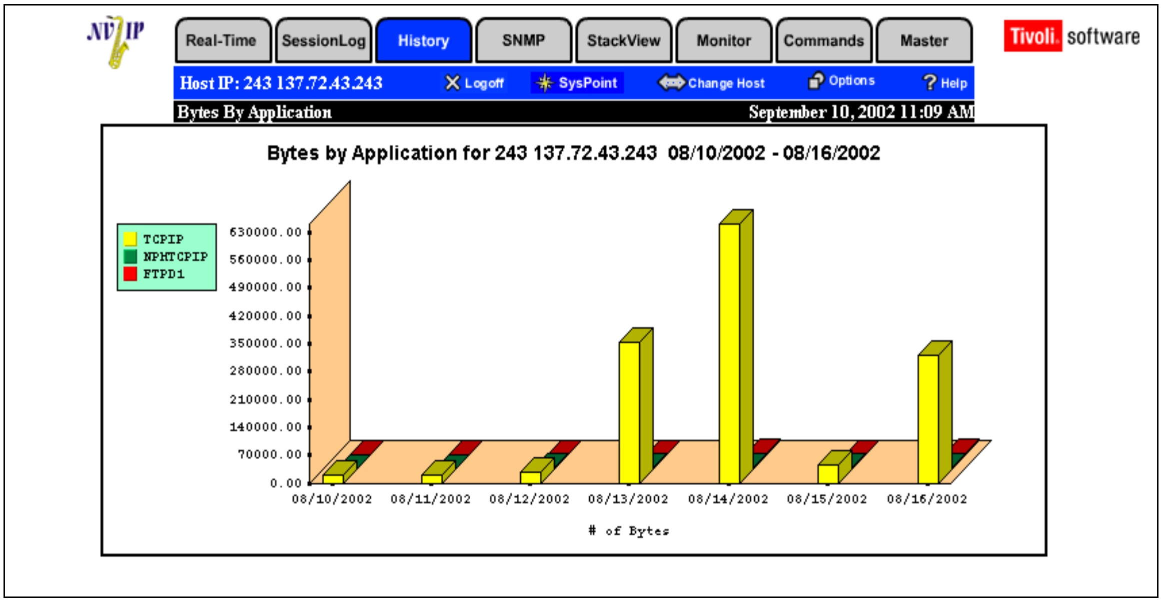
Bytes by Application

The Bytes by Application report shows the number of bytes sent and received per application as well as the total number of bytes for the interval chosen. The number of bytes is the sum of the bytes sent and received. Applications include Telnet, e-mail, or any other socket-attached OLTP applications using the selected TCP/IP address space.

Graphical Report – Bytes by Application

Data may be viewed by the week, day, hour, or year. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

The X-axis lists the application while the Y-axis shows the total number of bytes sent and received. Refer to the legend to determine the exact data for each value. Rest the mouse on a column to see the detail for that value.



Host IP: 243 137.72.43.243

Bytes By Application

September 10, 2002 11:09 AM

Figure 104. Bytes by Application

Tabular Report - Bytes by Application

The tabular report format provides the same basic information as the graphical report format.

The fields on the Bytes by Application tabular report are:

Application	Any socket-attached OLTP application using the selected TCP/IP address space.
Time	Date of session count.
Number of Bytes	Sum of bytes sent and received.

Sessions by Application

Sessions by Application shows the number of sessions per application for the interval selected. The session number is the number of remote IP addresses using the application. A client may have more than one session. Applications include Telnet, e-mail, or any other socket-attached OLTP applications using the selected TCP/IP address space.

Graphical Report – Sessions by Application

Data may be viewed by the week, day, hour, or year. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

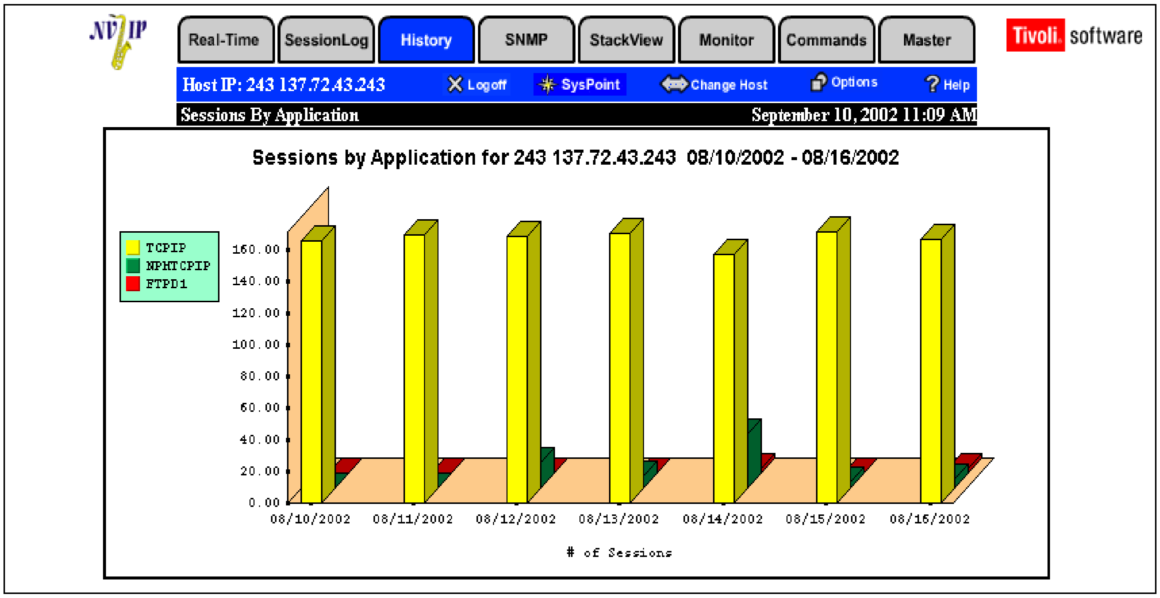


Figure 105. Sessions by Application

Tabular Report – Sessions by Application

The tabular report provides the same basic information as the graphical report format.

The fields on the Sessions by Application tabular report are:

Application	Any socket-attached OLTP application using the selected TCP/IP address space.
Time	Date of session count.
Number of Sessions	Number of active sessions per application for the interval chosen.

Base History Usage Reports

The Usage Reports provide information on the absolute usage per interval chosen for applications and clients. For an application, the report indicates which clients (addresses) were using that application. For a client, the report indicates which applications the client was using.

A brief description of each Usage Report follows:

Application Usage Details	The client (IP address) using the application for the interval selected, including the number of bytes in and out
Client Usage Details	The TCP/IP applications used by a particular client (IP address) for the interval selected, including the number of bytes in and out

Application Usage Details

Application Usage Details shows the client (IP address) using the application for the interval selected. The number of bytes in and out is also shown. A client may have more than one session. Applications include Telnet, e-mail, or any other socket-attached OLTP applications using the selected TCP/IP address space. To use this report, the application name must be specified as a parameter to the selection.

Tabular Report Format – Application Usage Details

This report is available only in a tabular report format. Each entry represents one session.

The fields on the Application Usage Details tabular report are:

Address	IP address of client using the application during the interval selected.
Name	DNS name of client using the application during the interval selected. This parameter is only available if the Use DNS name option is used. If no DNS name is available, the IP address is shown.
Bytes In	Number of bytes in to the application during the session.
Bytes Out	Number of bytes out to the client during the session.

Client Usage Details

Client Usage Details shows the TCP/IP applications used by a particular client (IP address) for the interval selected. The number of bytes in and out is also shown. A client may have more than one session. Applications include Telnet, e-mail, or any other socket-attached OLTP applications using the selected TCP/IP address space. To use this report, the IP address must be specified as a parameter to the selection.

Tabular Report Format – Client Usage Details

This report is available only in a tabular report format. Each entry represents the total count. That is, there may have been more than one session during that interval.

The fields on the Client Usage Details tabular report are:

Application	Name of application used by the client during the interval selected.
Bytes In	Number of bytes in to the application during the session.
Bytes Out	Number of bytes out to the client during the session.

Base History Response Time Reports

The Response Time reports provide information on the average response times for the test done by the host and on the varying number of bytes sent in the tests set up through the Master workstation. The reports show the times per packet sent for the addresses that are being monitored. Reports are available in graphic and tabular formats.

A brief description of each report follows:

Response Time for Network	Response time by the number of bytes sent through the customized test for the devices monitored for the interval chosen. This is the aggregate time over the network for the customized tests.
Response Time for Resource	Maximum, minimum, and average response times for the devices monitored for the interval chosen.
Service Level for Response Time	Shows the critical resources that have exceeded the user - defined service goals for response time. Service goals are set in the Response Time for Resource(s).

Response Time for Network

The Response Time for Network report shows the response time by the number of bytes sent through the customized test for all devices monitored for the interval chosen. The packet lengths and frequency are set in the Master.

Graphical Report – Response Time for Network

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

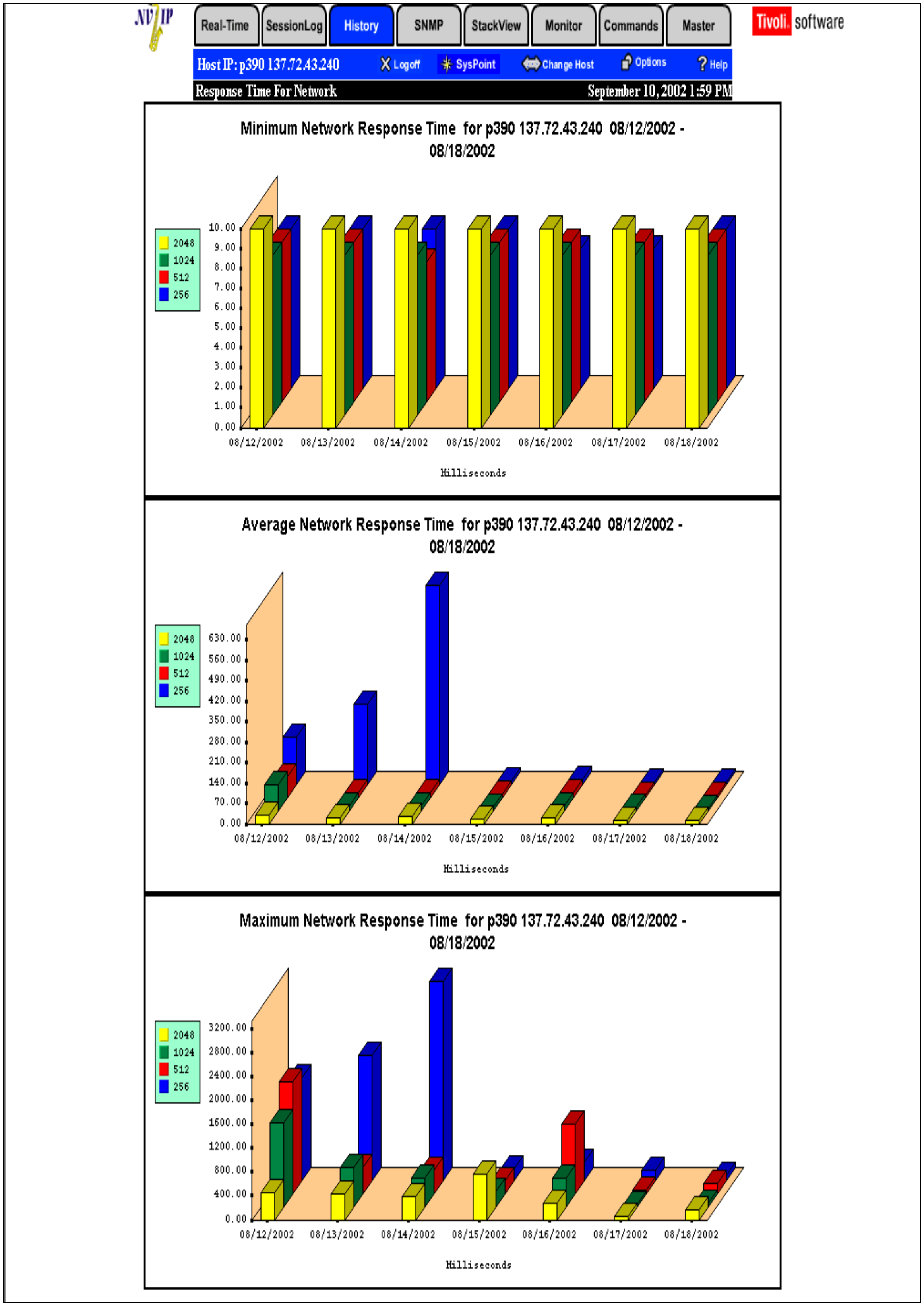


Figure 106. Response Time for Network

Reviewing the Response Time for Network report helps determine if there are bottlenecks in the network caused by fragmentation. For example, a certain network component may be set up for a maximum segment size of 512 Kbytes. Packets less than 512 are not segmented; packets greater than 512 Kbytes are segmented. There may be a significant difference in response time between those packets which are less than 512 and those greater than 512.

Tabular Report - Response Time for Network

The tabular report format provides the same basic information as the graphical report format.

Each record of information consists of three lines on the Response Time for Network tabular report. The three lines must be used together to provide the following information:

Packet Size	The size of the packet at the time of measurement.
Minimum (Min) response time	Minimum (Min) response time shown by packet size.
Average (Avg) response time	Average (Avg) response time shown by packet size.
Maximum (Max) response time	Maximum (Max) response time shown by packet size.
Time	Date of the measurement.

Response Time for Resource

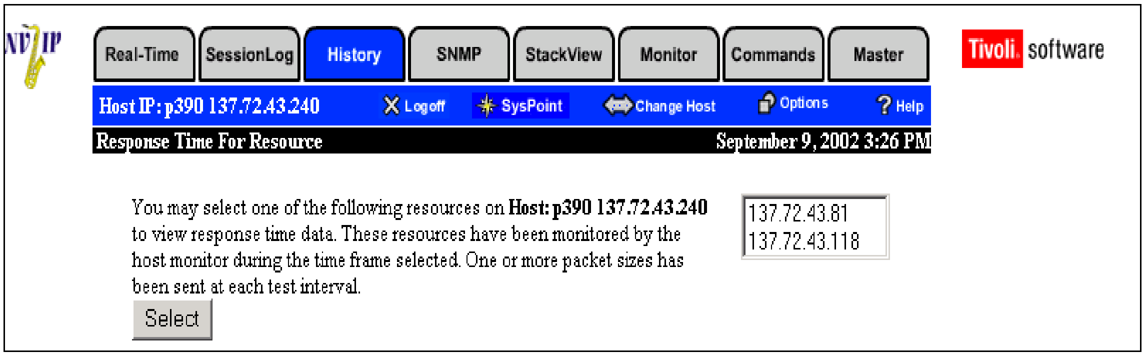
The Response Time for Resource report shows the maximum, minimum, and average response times for a particular device monitored for the interval chosen. Data is shown for the selected time period for each packet size selected in the Master.

Perform the following steps:

1. Select Response Time for Resource from the Report drop-down menu.
2. Specify the desired filters.
3. Click the Submit button. You have the option to select from a list of resources on your host machine.
4. Select one resource and click the Submit button to view a graph or report.

Graphical Report – Response Time for Resource

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



You may select one of the following resources on **Host: p390 137.72.43.240** to view response time data. These resources have been monitored by the host monitor during the time frame selected. One or more packet sizes has been sent at each test interval.

137.72.43.81
137.72.43.118

Figure 107. Response Time for Resource Filter

Tabular Report – Response Time for Resource

The tabular report format provides the same basic information as the graphical report format.

Each record of information consists of three lines on the Min, Avg, Max Response Time tabular report. The three lines must be used together to provide the following information:

Packet Size	The size of the packet at the time of measurement.
Minimum (Min) response time	Minimum (Min) response time shown by packet size.
Average (Avg) response time	Average (Avg) response time shown by packet size.
Maximum (Max) response time	Maximum (Max) response time shown by packet size.
Time	Date of the measurement.

Service Level for Response Time

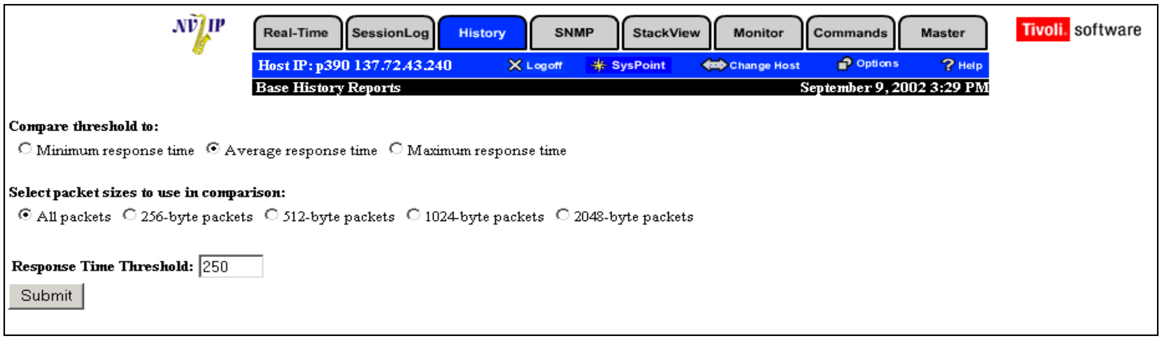
The Service Level for Response Time shows the critical resources that have exceeded the user-defined service goal for response time.

Perform the following steps:

1. Select Service Level for Response Time from the Report drop-down menu.
2. Specify the desired filters.
3. Click the Submit button. You have the following options:
   - Compare the response time threshold to the minimum, average, or maximum response time
   - Compare the service goal against all packet sizes or one specific size
   - Specify a response time threshold
4. Specify your options.
5. Click the Submit button to view the graph or report.

Graphical Report – Service Level for Response Time

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Base History Reports September 9, 2002 3:29 PM

Compare threshold to:

○ Minimum response time ● Average response time ○ Maximum response time

Select packet sizes to use in comparison:

● All packets ○ 256-byte packets ○ 512-byte packets ○ 1024-byte packets ○ 2048-byte packets

Response Time Threshold: 250

Submit

Figure 108. Service Level for Response Time

Tabular Report – Service Level for Response Time

The tabular report format provides the same basic information as the graphical report format.

The fields on the Service Level for Response Time report are

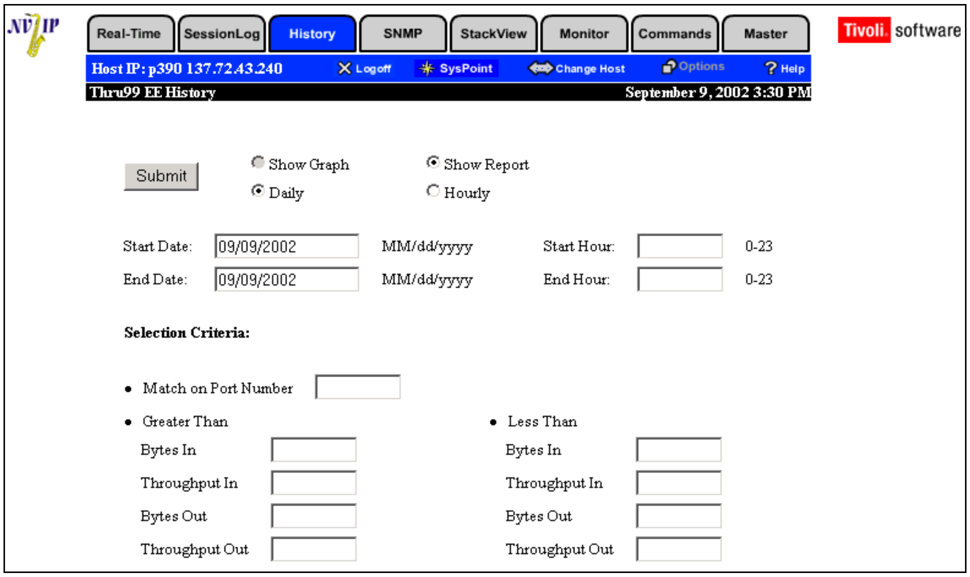
SUMMARY		**DETAIL**	
Address	IP address of device exceeding the response time threshold	**Address**	IP address of device exceeding the response time threshold
Count	The number of times threshold was exceeded	**Response Time**	The response time at the time the threshold was exceeded
		Packet	The packet size (in bytes) sent at the time the threshold was exceeded

Thru99 EE History Report

The Thru99 EE History report allows you to view interval-based summaries for any of the specifically assigned UDP Enterprise Extender (EE) ports being utilized by EE, which uses UDP over SNA. The default 15-minute interval snapshots allow you to correlate traditional RMF-style host-based activity and workload reports with critical link traffic, and to compare specific throughput levels with their respective stack and CPU workload timeframes. The Thru99 EE History report can be used with any of the other history reports or with host-centric RMF reports currently being generated.

To view a Thru 99 EE History report, perform the following steps:

1. Click on the History tab.
2. Click the Thru 99 EE History hyperlink under Workload and Performance. The Thru99 EE History screen appears.



Host IP: p390 137.72.43.240

Thru99 EE History September 9, 2002 3:30 PM

○ Show Graph ● Show Report

● Daily ○ Hourly

Start Date: 09/09/2002 MM/dd/yyyy Start Hour: 0-23

End Date: 09/09/2002 MM/dd/yyyy End Hour: 0-23

Selection Criteria:

- Match on Port Number
- Greater Than
  - Bytes In
  - Throughput In
  - Bytes Out
  - Throughput Out
- Less Than
  - Bytes In
  - Throughput In
  - Bytes Out
  - Throughput Out

Figure 109. Thru99 EE History Report Screen

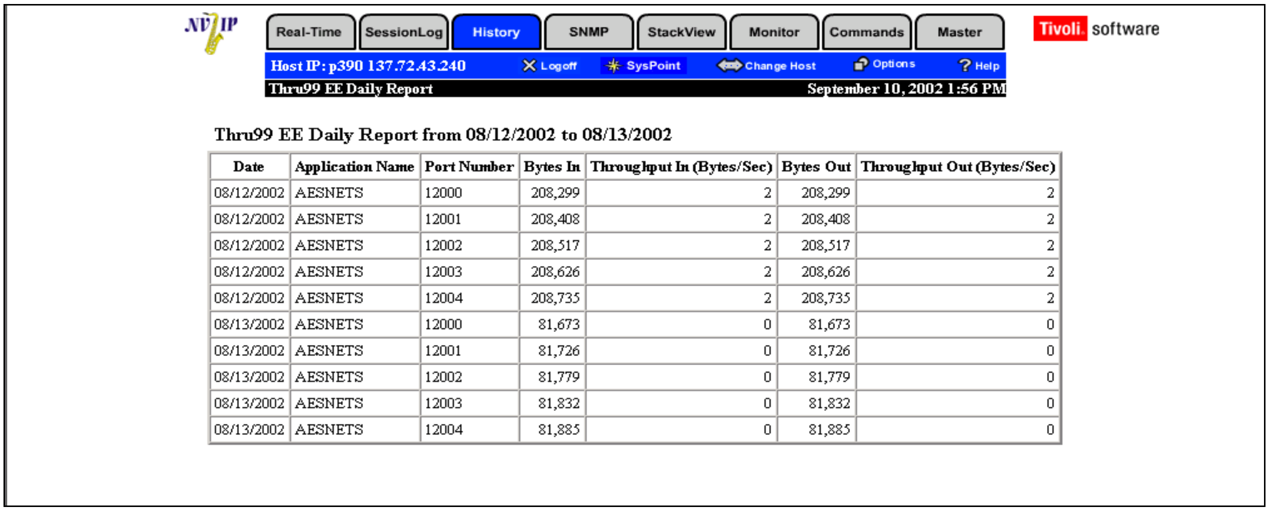
The Thru99 EE History screen provides the following selection criteria for the report you want to view:

- Weekly by Day (known as the Daily report)
- Daily by Hour (known as the Hourly report)
- Start/End Date. If you selected the Hourly report, these fields are not required. The report will display data for today's date unless you specify a different Start Date.
- Start/End Hour (only applies to the Hourly report)
- Match on Port Number

- Greater Than/Less Than:
  - Byes In
  - Throughput In
  - Bytes Out
  - Throughput Out

  The selection criteria is both logical and grouped. For example, you can select Port Number = 12002, and Bytes In > 300,000 AND Throughput Out < 1000.

3. If you selected the Thru99 EE Daily report, the following screen displays:



Host IP: p390 137.72.43.240

Thru99 EE Daily Report September 10, 2002 1:56 PM

Thru99 EE Daily Report from 08/12/2002 to 08/13/2002

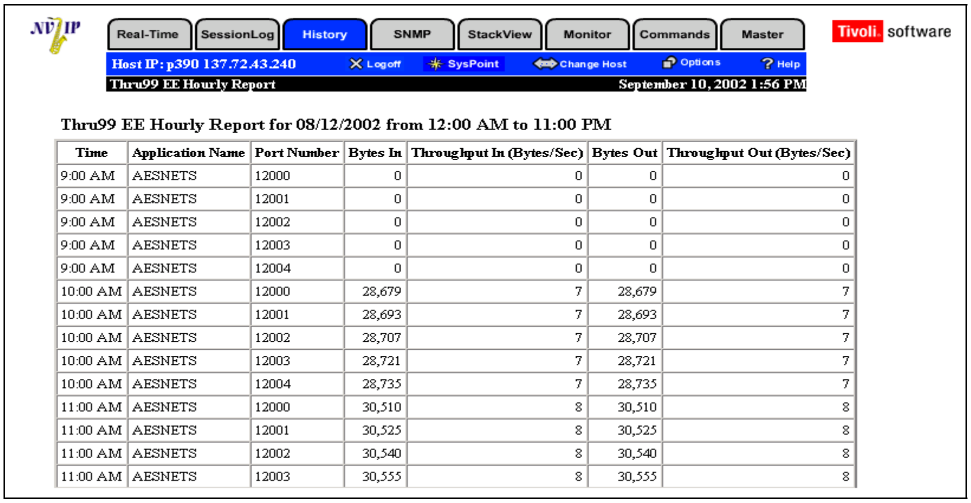
Date	Application Name	Port Number	Bytes In	Throughput In (Bytes/Sec)	Bytes Out	Throughput Out (Bytes/Sec)
08/12/2002	AESNETS	12000	208,299	2	208,299	2
08/12/2002	AESNETS	12001	208,408	2	208,408	2
08/12/2002	AESNETS	12002	208,517	2	208,517	2
08/12/2002	AESNETS	12003	208,626	2	208,626	2
08/12/2002	AESNETS	12004	208,735	2	208,735	2
08/13/2002	AESNETS	12000	81,673	0	81,673	0
08/13/2002	AESNETS	12001	81,726	0	81,726	0
08/13/2002	AESNETS	12002	81,779	0	81,779	0
08/13/2002	AESNETS	12003	81,832	0	81,832	0
08/13/2002	AESNETS	12004	81,885	0	81,885	0

Figure 110. Thru99 EE Daily Report

The fields in the Thru99 EE Daily report are:

Date	The date the data was reported.
Application Name	The VTAM application name for EE on that system.
Port Number	The number of the assigned EE port. By default, five port numbers are assigned: 12000-120004.
Bytes In	The number of bytes sent in to the assigned EE port on the date reported.
Throughput In Bytes/Sec	Throughput for bytes sent in to the assigned EE port on the date reported.
Bytes Out	The number of bytes sent out through the assigned EE port on the date reported.
Throughput Out Bytes/Sec	Throughput for bytes sent out through the assigned EE port on the date reported.

4. If you selected the Thru99 EE Hourly report, the following screen displays:



Thru99 EE Hourly Report for 08/12/2002 from 12:00 AM to 11:00 PM

Time	Application Name	Port Number	Bytes In	Throughput In (Bytes/Sec)	Bytes Out	Throughput Out (Bytes/Sec)
9:00 AM	AESNETS	12000	0	0	0	0
9:00 AM	AESNETS	12001	0	0	0	0
9:00 AM	AESNETS	12002	0	0	0	0
9:00 AM	AESNETS	12003	0	0	0	0
9:00 AM	AESNETS	12004	0	0	0	0
10:00 AM	AESNETS	12000	28,679	7	28,679	7
10:00 AM	AESNETS	12001	28,693	7	28,693	7
10:00 AM	AESNETS	12002	28,707	7	28,707	7
10:00 AM	AESNETS	12003	28,721	7	28,721	7
10:00 AM	AESNETS	12004	28,735	7	28,735	7
11:00 AM	AESNETS	12000	30,510	8	30,510	8
11:00 AM	AESNETS	12001	30,525	8	30,525	8
11:00 AM	AESNETS	12002	30,540	8	30,540	8
11:00 AM	AESNETS	12003	30,555	8	30,555	8

Figure 111. Thru99 EE Hourly Report

The fields in the Thru99 EE Hourly report are:

Time	The time the data was reported. By default, data is reported every 15 minutes.
Application Name	Name of the EE application the data was sent out to.
Port Number	The number of the assigned EE port. By default, five port numbers are assigned: 12000-120004.
Bytes In	The number of bytes sent in to the assigned EE port at the time the data was reported.
Throughput In Bytes/Sec	Throughput for bytes sent in to the assigned EE port at the time the data was reported.
Bytes Out	The number of bytes sent out through the assigned EE port at the time the data was reported.
Throughput Out Bytes/Sec	Throughput for bytes sent out through the assigned EE port at the time the data was reported.

5. When you are finished viewing the report, click the Back Button on your browser to return to the Thru99 EE History screen.

Thru99 Link History Report

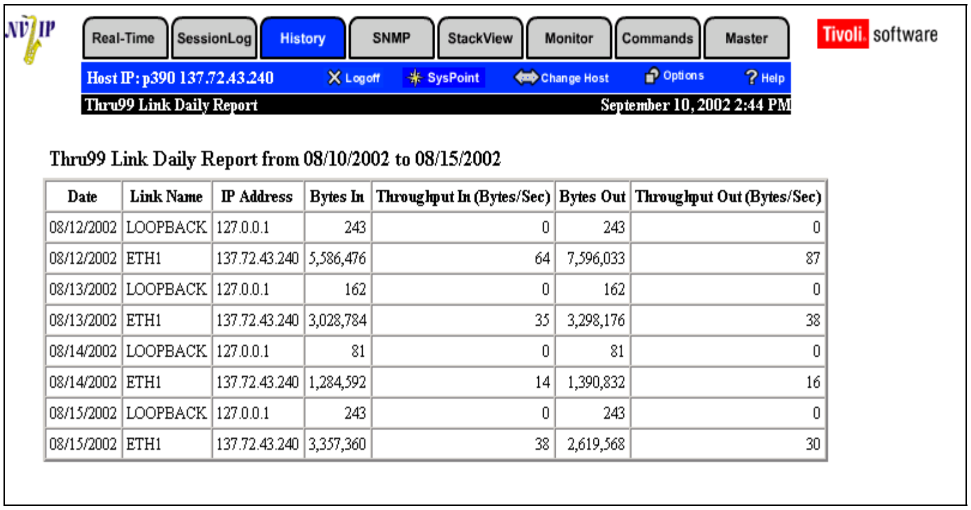
The Thru99 Link History report allows you to view interval-based summaries for data sent or received over each of a stack's IP to IP or IP to channel links. The Thru99 Link History report can be used with any of the other history reports or with host-centric RMF reports currently being generated.

To view a Thru 99 Link History report, perform the following steps:

1. Click on the History tab.
2. Click on the Thru 99 Link History hyperlink under Workload and Performance. The Thru99 Link History screen displays with the following selection criteria for the report you want to view:
   - Weekly by Day (known as the Daily report)
   - Daily by Hour (known as the Hourly report)
   - Start/End Date. If you selected the Hourly report, these fields are not required. The report will display data for today's date unless you specify a different Start Date.
   - Start/End Hour (applies only to the Hourly report)
   - Match on Link Name
   - Greater Than/Less Than:
     - Byes In
     - Throughput In
     - Bytes Out
     - Throughput Out

   The selection criteria is both logical and grouped. For example, you can select Link Name = ETH1, and Bytes In > 200,000 AND Throughput Out < 1000.

3. If you selected the Thru99 Link Daily report, the following screen displays:



Thru99 Link Daily Report from 08/10/2002 to 08/15/2002

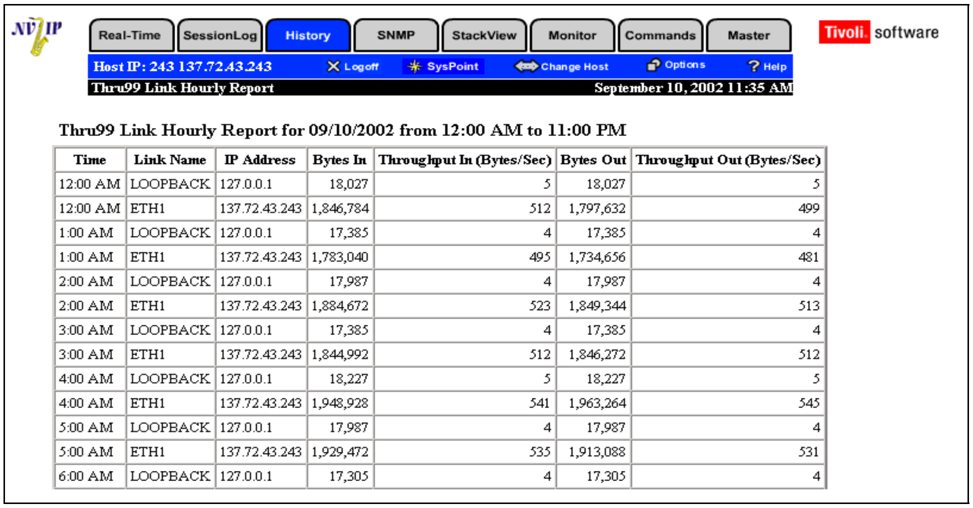
Date	Link Name	IP Address	Bytes In	Throughput In (Bytes/Sec)	Bytes Out	Throughput Out (Bytes/Sec)
08/12/2002	LOOPBACK	127.0.0.1	243	0	243	0
08/12/2002	ETH1	137.72.43.240	5,586,476	64	7,596,033	87
08/13/2002	LOOPBACK	127.0.0.1	162	0	162	0
08/13/2002	ETH1	137.72.43.240	3,028,784	35	3,298,176	38
08/14/2002	LOOPBACK	127.0.0.1	81	0	81	0
08/14/2002	ETH1	137.72.43.240	1,284,592	14	1,390,832	16
08/15/2002	LOOPBACK	127.0.0.1	243	0	243	0
08/15/2002	ETH1	137.72.43.240	3,357,360	38	2,619,568	30

Figure 112. Thru99 Link Daily Report

The fields in the Thru99 Link Daily report are:

Date	The date the data was reported.
Link Name	The name of the link used by the stack.
IP Address	Internet Protocol address used for the stack.
Bytes In	The number of bytes sent in on the date reported.
Throughput In Bytes/Sec	Throughput for bytes sent in on the date reported.
Bytes Out	The number of bytes sent out on the date reported.
Throughput Out Bytes/Sec	Throughput for bytes sent out on the date reported.

4. If you selected the Thru99 Link Hourly report, the following screen displays:



Thru99 Link Hourly Report for 09/10/2002 from 12:00 AM to 11:00 PM

Time	Link Name	IP Address	Bytes In	Throughput In (Bytes/Sec)	Bytes Out	Throughput Out (Bytes/Sec)
12:00 AM	LOOPBACK	127.0.0.1	18,027	5	18,027	5
12:00 AM	ETH1	137.72.43.243	1,846,784	512	1,797,632	499
1:00 AM	LOOPBACK	127.0.0.1	17,385	4	17,385	4
1:00 AM	ETH1	137.72.43.243	1,783,040	495	1,734,656	481
2:00 AM	LOOPBACK	127.0.0.1	17,987	4	17,987	4
2:00 AM	ETH1	137.72.43.243	1,884,672	523	1,849,344	513
3:00 AM	LOOPBACK	127.0.0.1	17,385	4	17,385	4
3:00 AM	ETH1	137.72.43.243	1,844,992	512	1,846,272	512
4:00 AM	LOOPBACK	127.0.0.1	18,227	5	18,227	5
4:00 AM	ETH1	137.72.43.243	1,948,928	541	1,963,264	545
5:00 AM	LOOPBACK	127.0.0.1	17,987	4	17,987	4
5:00 AM	ETH1	137.72.43.243	1,929,472	535	1,913,088	531
6:00 AM	LOOPBACK	127.0.0.1	17,305	4	17,305	4

Figure 113. Thru99 Link Hourly Report

The fields in the Thru99 Link Hourly report are:

Time	The time the data was reported. By default, data is reported every 15 minutes.
Link Name	The name of the link used by the stack.
IP Address	Internet Protocol address used for the stack.
Bytes In	The number of bytes sent in at the time the data was reported.
Throughput In Bytes/Sec	The throughput for bytes sent in at the time the data was reported.
Bytes Out	The number of bytes sent out at the time the data was reported.
Throughput Out Bytes/Sec	The throughput for bytes sent out at the time the data was reported.

When you are finished viewing the report, click the Back button on your browser to return to the Thru99 Link History report.

Expert Reports

Expert Reports contains these three categories of reports:

- API Expert
- FTP Performance Expert
- Telnet Expert

API Expert Reports (CICS, Web server, MQSeries)

This product views the TCP/IP network performance from the enterprise level to the remote user connection. Performance indicators are available for workload, usage, and response time. The API Expert Reports become available when the Host Monitor is started.

The API Expert is structured to allow you to view both a global and detailed view of API activity. API includes all socket-attached application activity. Clearly, if your installation is using any such application, for example, CICS sockets, Web server, MQSeries, or even this product, you will be interested in the historical performance statistics presented here.

The data provided is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it is recorded at the time it terminates.

If you wish to view time slices of active sessions taken in a sampling mode, please review the Base History reports. You may also want to look at "near time" API activity by viewing the SessionLog API reports. The SessionLog API reports show sessions that are currently in progress or have recently completed.

The API Expert Reports provide two categories of reporting:

Activity (Address Based Reports)	
Total API Usage	Total API session and byte activity for the time period chosen.
Top API Users – Sessions/Bytes	View the top API addresses performing the session and byte activity for the time period chosen (by sessions or bytes).
Selected API User	View the details of any API address for the time period chosen by sessions and bytes.
Selected API User – Detail List	View the sessions or bytes for a specific API address for the time period chosen.
Application Based Reports	
Top API Applications –	View the top applications accessed via API.

Sessions/Bytes	
Selected API Application	Statistics for any application accessed via API.

To view an API Expert Report, perform the following steps:

1. Click on the History tab.
2. Click the API Expert hyperlink under Expert Reports. The API Expert Reports screen appears.
3. Choose Show Graph or Show Report.
4. Select the report you wish to view.
5. Select the type of report, that is, the time slice, you wish to view: Weekly by Day or Daily by Hour.
6. Select if you want to view by DNS name or address. This only applies to the top API user reports.
7. Select the starting time using the twenty-four clock if you are doing the daily by hour report and wish to start at an hour other than 0.
8. Enter how many bytes, clients, applications, or specific name / address you would like to view:
   - For the Total report category, enter the minimum bytes, if desired.
   - For Top reports, enter between 1 to 250 data points if you are requesting a report or enter between 1-20 if you are requesting a graph.
   - For Selected User reports, enter the IP address.
   - For Selected Application reports, enter the API Application name to be viewed.
9. Click Submit. The report screen appears.
10. Use the Back Arrow on your browser to move between screens.

Note: Each type of report has corresponding required fields. See each report type section for more information.

Activity (Address Based Reports) for API usage

Activity (Address Based) Reports offer information regarding either total API usage or API usage by address through the following reports:

- Total API Usage
- Top API Users (Sessions/Bytes)
- Selected API User
- Selected API User – Detail List

Total API Usage

This report allows you to view the total API activity for the time period chosen. API includes any socket-attached application.

The data provided is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it is recorded at the time it terminates.

If you wish to view time slices of active sessions taken in a sampling mode, please review the Base History reports. You may also want to look at "near time" API activity by viewing the SessionLog API reports. The SessionLog API reports show sessions that are currently in progress or have recently completed.

If you enter the minimum bytes filter, these reports show the total number of sessions or bytes per API session exceeding the number of bytes entered for the interval chosen. You may use this report to show you when most sessions exceeding a certain byte limit take place. For example, you may want to see when API sessions with over 5 megabytes took place.

Graphical Report – Total API Usage

Data may be viewed weekly by day, or daily by hour. Required field is Start Date. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

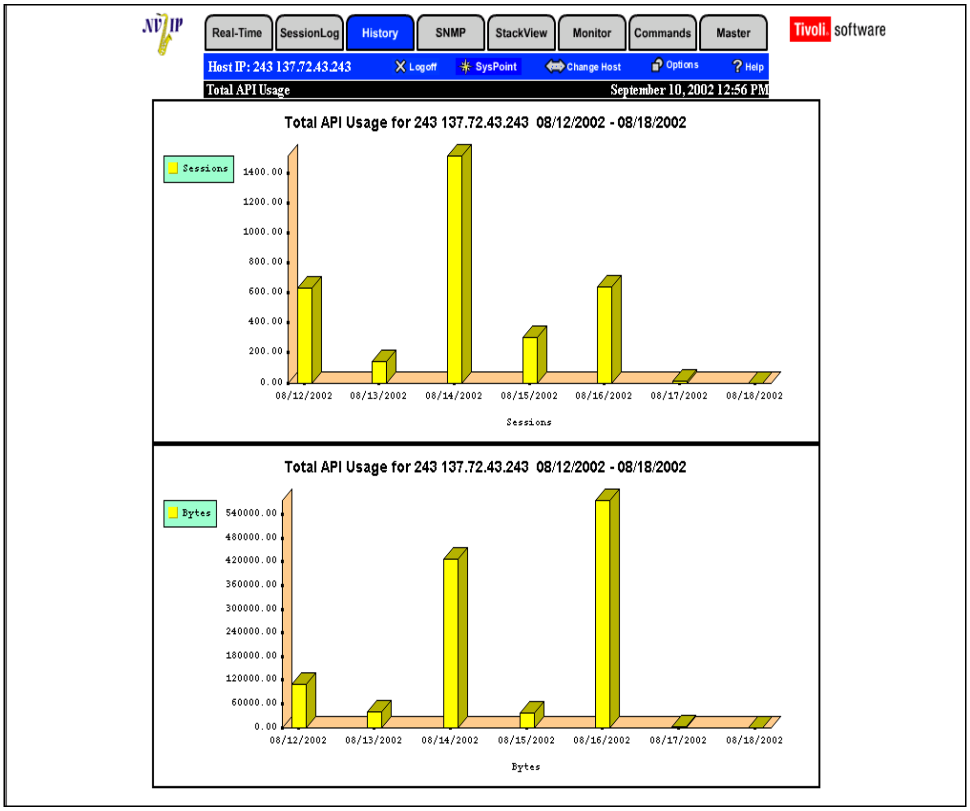


Figure 114. Total API Usage

Tabular Report – Total API Usage

The tabular report format provides the same basic information as the graphical report format.

The fields on the Total API Usage tabular reports are:

Time	Interval during which when the API session terminated.
Number of Bytes	Total number of bytes.
Number of Sessions	Total number of sessions.

Top API Users - Sessions/Bytes

These reports allow you to view the most active API users (addresses) for the time period chosen. API includes any socket-attached application.

The data provided is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it is recorded at the time it terminates.

If you wish to view time slices of active sessions taken in a sampling mode, please review the Base History reports. You may also want to look at "near time" API activity by viewing the SessionLog API reports. The SessionLog API reports show sessions that are currently in progress or have recently completed.

Graphical Report – Top API Users – Sessions/Bytes

Data may be viewed weekly by day, or daily by hour. Required fields are Start Date and How Many. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

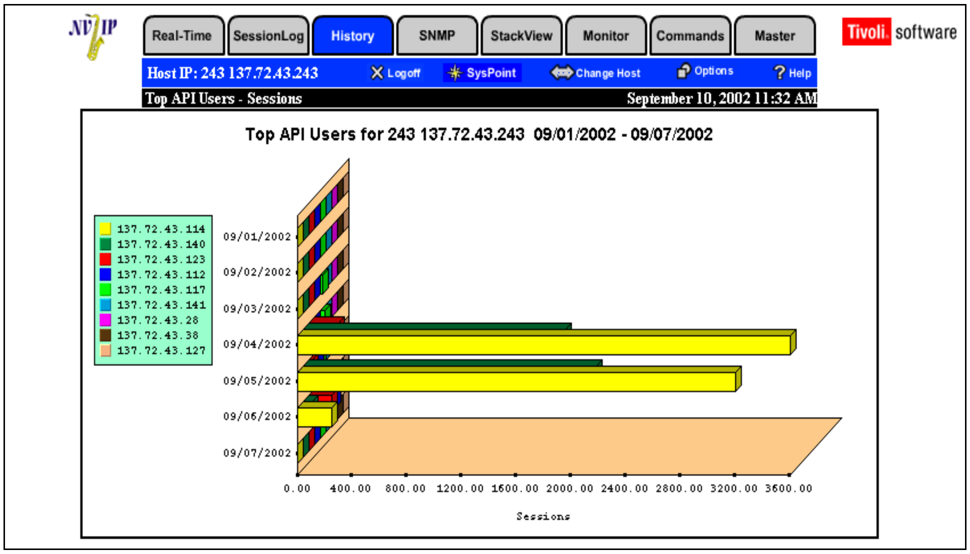


Figure 115. Top API Users - Sessions

Tabular Report - Top API Users – Sessions/Bytes

The tabular report format provides the same basic information as the graphical report format.

The fields on the Total API Users (Sessions/Bytes) tabular reports are:

Address	IP address initiating the API session.
Time	Interval during which the API session terminated.
Number of Bytes	Total number of bytes.
Number of Sessions	Total number of sessions.

Selected API User

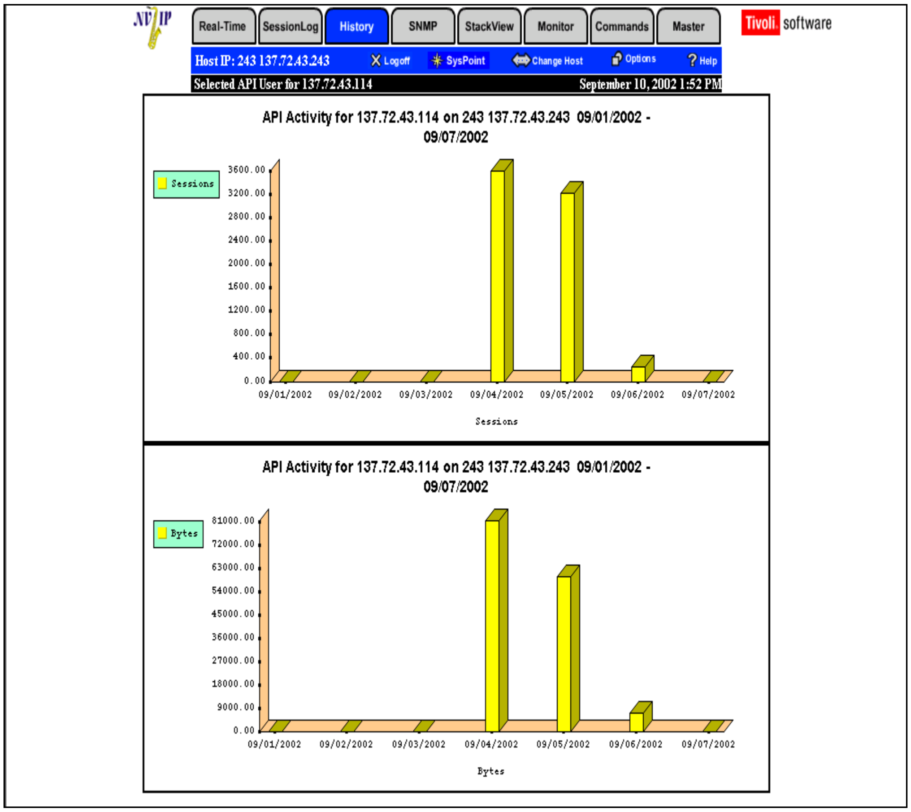
This report allows you to view data for a specific API user (address) for the time period chosen. API includes any socket-attached application.

The data provided is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it is recorded at the time it terminates.

If you wish to view time slices of active sessions taken in a sampling mode, please review the Base History reports. You may also want to look at "near time" API activity by viewing the SessionLog API reports. The SessionLog API reports show sessions that are currently in progress or have recently completed.

Graphical Report – Selected API User

Data may be viewed weekly by day, or daily by hour. Required fields are Start Date and Address. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: 243 137.72.43.243

Selected API User for 137.72.43.114 September 10, 2002 1:52 PM

Figure 116. Selected API User

Tabular Report - Selected API User

The tabular report format provides the same basic information as the graphical report format.

The fields on the Selected API User tabular report are:

Address	IP address initiating the API session.
Time	Interval during which the API session ended.
Number of Bytes	Total number of bytes.
Number of Sessions	Total number of sessions.

Selected API User - Detail List

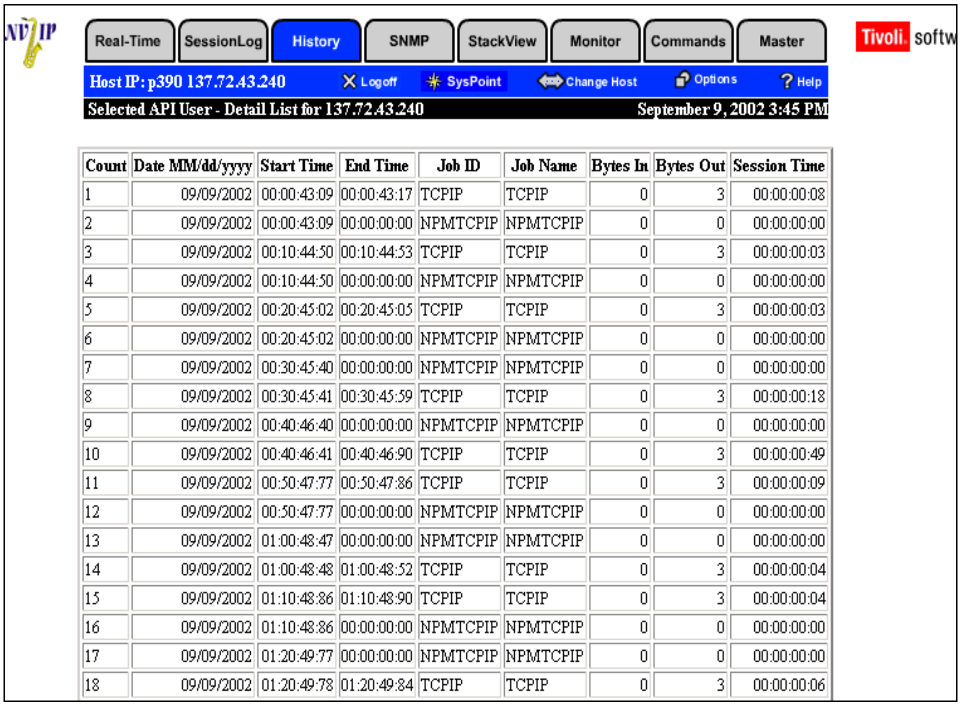
This report allows you to view the API sessions for a selected user for the time period chosen. API includes any socket-attached application.

The data provided is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it will be recorded at the time it terminates.

If you wish to view time slices of active sessions taken in a sampling mode, please review the Base History reports. You may also want to look at "near time" API activity by viewing the SessionLog API reports. The SessionLog API reports will show sessions that are currently in progress or have recently completed.

Tabular Report – Selected API User – Detail List

This report is available in tabular format only. Required fields are Start Date and Address.



Selected API User - Detail List for 137.72.43.240 September 9, 2002 3:45 PM

Count	Date MM/dd/yyyy	Start Time	End Time	Job ID	Job Name	Bytes In	Bytes Out	Session Time
1	09/09/2002	00:00:43:09	00:00:43:17	TCPIP	TCPIP	0	3	00:00:00:08
2	09/09/2002	00:00:43:09	00:00:00:00	NPMTCPIP	NPMTCPIP	0	0	00:00:00:00
3	09/09/2002	00:10:44:50	00:10:44:53	TCPIP	TCPIP	0	3	00:00:00:03
4	09/09/2002	00:10:44:50	00:00:00:00	NPMTCPIP	NPMTCPIP	0	0	00:00:00:00
5	09/09/2002	00:20:45:02	00:20:45:05	TCPIP	TCPIP	0	3	00:00:00:03
6	09/09/2002	00:20:45:02	00:00:00:00	NPMTCPIP	NPMTCPIP	0	0	00:00:00:00
7	09/09/2002	00:30:45:40	00:00:00:00	NPMTCPIP	NPMTCPIP	0	0	00:00:00:00
8	09/09/2002	00:30:45:41	00:30:45:59	TCPIP	TCPIP	0	3	00:00:00:18
9	09/09/2002	00:40:46:40	00:00:00:00	NPMTCPIP	NPMTCPIP	0	0	00:00:00:00
10	09/09/2002	00:40:46:41	00:40:46:90	TCPIP	TCPIP	0	3	00:00:00:49
11	09/09/2002	00:50:47:77	00:50:47:86	TCPIP	TCPIP	0	3	00:00:00:09
12	09/09/2002	00:50:47:77	00:00:00:00	NPMTCPIP	NPMTCPIP	0	0	00:00:00:00
13	09/09/2002	01:00:48:47	00:00:00:00	NPMTCPIP	NPMTCPIP	0	0	00:00:00:00
14	09/09/2002	01:00:48:48	01:00:48:52	TCPIP	TCPIP	0	3	00:00:00:04
15	09/09/2002	01:10:48:86	01:10:48:90	TCPIP	TCPIP	0	3	00:00:00:04
16	09/09/2002	01:10:48:86	00:00:00:00	NPMTCPIP	NPMTCPIP	0	0	00:00:00:00
17	09/09/2002	01:20:49:77	00:00:00:00	NPMTCPIP	NPMTCPIP	0	0	00:00:00:00
18	09/09/2002	01:20:49:78	01:20:49:84	TCPIP	TCPIP	0	3	00:00:00:06

Figure 117. Selected API User - Detail List

The fields on the Selected API User - Detail List tabular report are:

Count	Refers to where that record falls in the list of records displayed
Date	Start date of session (mm/dd/yyyy)
Start Time	Start time of session (hh:mm:ss)
End Time	End time of session (hh:mm:ss)
Job ID	For socket API applications, the JES job identifier (name of address space)
JobName	Name of job or task • For interactive TSO API usage: the user's TSO user ID • For batch submitted jobs: the name of the JOB card • For started procedures: the name of the procedure
Bytes In	Bytes in to MVS TCP/IP
Bytes Out	Bytes out to the remote IP address
Session Time	The duration of the session (hh:mm:ss)

Application Based Reports for API

Application Based Reports offer information regarding API applications through the following reports:

- Top API Applications – Sessions/Bytes
- Selected API Application

Top API Applications - Sessions/Bytes

These reports allow you to view the API applications that had the most sessions for the time period chosen, either by sessions, or by bytes. API includes any socket-attached application except Telnet or FTP.

The data provided is session-based. That is, the session counts are done based on a session initiation and termination record. The session is recorded at the time it finishes; if no session termination record exists for whatever reason, there will not be a record of the session. The session may have lasted for 8 hours, but it is recorded at the time it terminates.

If you wish to view time slices of active sessions taken in a sampling mode, please review the Base History reports. You may also want to look at "near time" API activity by viewing the SessionLog API reports. The SessionLog API reports show sessions that are currently in progress or have recently completed.

Graphical Report - Top API Applications - Sessions/Bytes

Data may be viewed weekly by day, or daily by hour. Required fields are Start Date and How Many. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

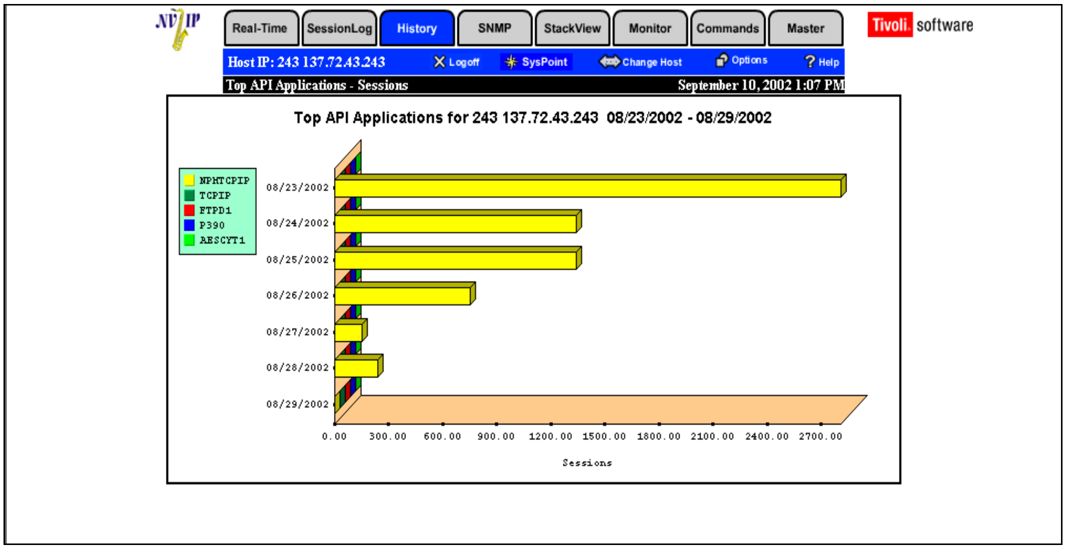


Figure 118. Top API Applications - Sessions

Tabular Report - Top API Applications - Sessions/Bytes

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top API Applications (Sessions/Bytes) tabular reports are:

Application Name	API application name.
Time	Interval during which the API session terminated.
Number of Bytes	Total number of bytes.
Number of Sessions	Total number of sessions.

Selected API Application

This report allows you to view the sessions or bytes for a specific API application for the time period chosen. API includes any socket-attached application.

The data provided is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it is recorded at the time it terminates.

If you wish to view time slices of active sessions taken in a sampling mode, please review the Base History reports. You may also want to look at "near time" API activity by viewing the SessionLog API reports. The SessionLog API reports show sessions that are currently in progress or have recently completed.

Graphical Report - Selected API Application

Data may be viewed weekly by day, or daily by hour. Required fields are Start Date and Application Name. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

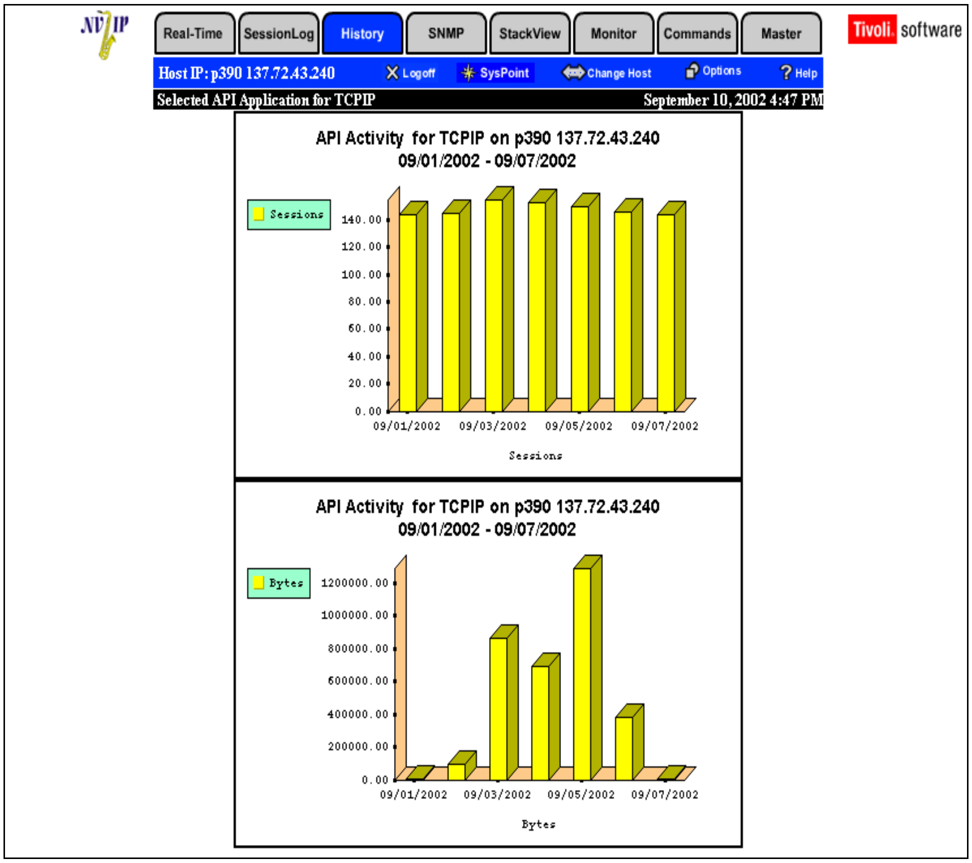


Figure 119. Selected API Application

Tabular Report - Selected API Application

The tabular report format provides the same basic information as the graphical report format.

The fields on the Selected API Application/STC tabular report are:

Time	Interval during which the API session terminated.
Number of Bytes	Total number of bytes.
Number of Sessions	Total number of sessions.

FTP Performance Expert Reports

The FTP Performance Expert is structured to allow you to view both global and detailed views of FTP activity. FTP is the Internet standard for file transfer and is one of the most frequently used functions of TCP/IP. You may not know if you have problems with FTP in your network. FTP jobs may be failing at night, users may be resubmitting multiple jobs, or submitting jobs which conflict with other usage. You may want to find users who are submitting excessively long jobs or who submit jobs that always fail for some reason. The FTP Performance Expert Reports allow you to find answers to these and many other questions.

The FTP Performance Expert is a historical reporting function designed to allow global network views as well as detailed views of FTP activity. The FTP Expert Reports provide three categories of reporting:

Activity (Address Based Reports)

Total FTP	Total FTP client and server session and byte activity for the time period chosen. The total sessions report includes both data transfer and non-data transfer sessions.
Top FTP	View the top FTP client and server addresses performing the session and byte activity for the time period chosen.
Selected User	View the details of any FTP client or server address for the time period chosen.

Data Set Based Reports

Top Data Set Activity	View the top data sets accessed for FTPs.
Any Data Set Activity	Any data set accessed for FTPs. Either FTP client or server sessions may be selected for the time period chosen.
Data Set by Type Activity	FTP activity by the type of data set: SEQ, SQL, or JES.

Failure Based Reports

Total Failures	All the failed FTP jobs for a chosen time period. Either FTP client or server sessions may be selected.
Top Failing Addresses	Top addresses submitting failing FTP jobs for a chosen time period.
Data Set Failures	Top data sets against which failing FTP jobs were submitted for a chosen time period.

Activity (Address Based Reports) for FTP

The Activity (Address Based) reports allow you to view the total FTP client and server session and byte activity for the time period chosen. Total sessions include both data transfer and non-data transfer sessions. An example of a non-data transfer FTP session may be a RENAME function. A non-data transfer session has no bytes associated with it. Information is provided in three views: total activity, top activity, and detail.

Total FTP - Bytes/Sessions Reports List

The Total FTP reports allow you to view the total FTP client and server session and byte activity for the time period chosen. The available reports are:

- Total Sessions
- Total Bytes

Top FTP User Reports List

The Top FTP User reports show the top FTP client and server addresses performing the session and byte activity for the time period chosen. The available reports are:

- Top FTP Users (All Sessions)
- Top FTP Users (Data Sessions)
- Top FTP Users (Bytes)

Selected User Reports List

The Selected User provides the details regarding any FTP client or server address for the time period chosen. Details of all FTPs performed by the address may be viewed by selecting the Selected User - Detail List. The available reports are:

- Selected User (All Sessions)
- Selected User (Data Sessions)
- Selected User (Bytes)
- Selected User - Detail List
- Selected User - FTP Diagnostic

Total FTP Bytes/Sessions Reports

The Total FTP Bytes/Sessions reports allow you to view the total FTP client and server session and byte activity for the time period chosen. Whether the report displays both data and non-data sessions depends upon the report type and the parameters selected. Total Sessions shows both types of sessions while the Total Bytes shows only data sessions.

You may use the minimum bytes parameter with these reports to view sessions greater than a particular number of bytes. For example, you may want to see the number of sessions that exceeded one megabyte or one gigabyte.

To view a Total FTP Bytes/Sessions report, perform the following steps:

1. Click on the History tab.
2. Click the FTP Performance Expert hyperlink under Expert Reports. The FTP Performance Expert main screen appears. Use the Change Host option if reporting for a different host is desired in this session.
3. Select Graph or Report type.
4. Select Weekly by Day or Daily by Hour.
5. Select FTP server or FTP client records to view.
6. Select the category of Total FTP report to view (session or bytes).
7. Set the report day, month, and year to start viewing.
8. Select the minimum number of bytes, if desired.
9. Click Submit. The selected report appears.
10. Click Back on the browser to select another function from the FTP Performance Expert main screen.

Total FTP Sessions

The Total FTP Sessions report shows the total number of sessions per FTP client and server for the interval chosen. Both data transfer and non-data transfer sessions are included. This report shows you the times of heaviest use of FTP at your installation in terms of number of sessions. The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view either the Total Bytes report or sessions with traffic over a certain number of bytes to obtain a balanced picture of activity.

Graphical Report - Total FTP Sessions

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

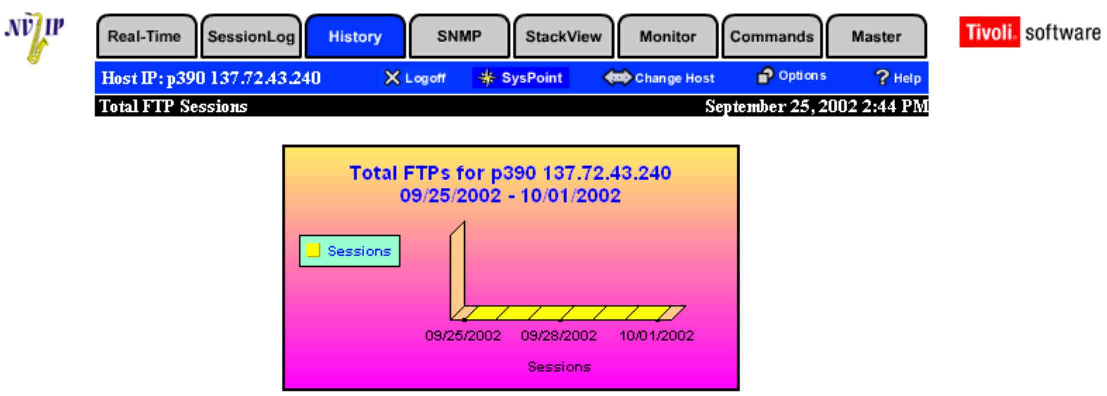


Figure 120. Total FTP Sessions

Tabular Report - Total FTP Sessions

The tabular report format provides the same basic information as the graphical report format.

The fields on the Total FTP Sessions report are:

Time	Calendar date or hour for which total activity is reported.
Sessions	Number of sessions, data and non-data, for the selected time period based on the host acting as a server or a client.

Total FTP Bytes

The Total FTP Bytes report shows the total number of bytes per FTP client and server for the interval chosen. Only data transfer sessions are included. This report shows you the times of heaviest use of FTP at your installation in terms of bytes transmitted. The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view the Total Sessions report to obtain a balanced picture of activity.

Graphical Report - Total FTP Bytes

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

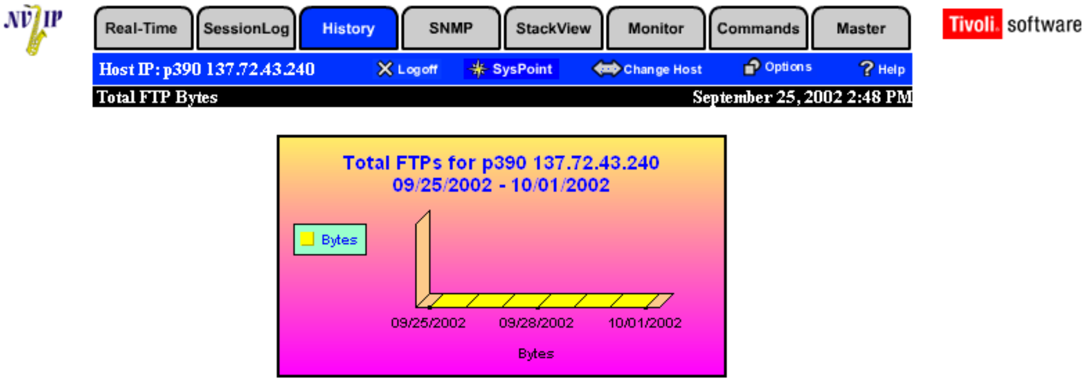


Figure 121. Total FTP Bytes

Tabular Report - Total FTP Bytes

The tabular report format provides the same basic information as the graphical report format. The fields on the Total FTP Bytes report are:

Time	Calendar date or hour for which total activity is reported.
Bytes	Number of bytes transferred for the selected time period based on the selected resource acting as a server or a client.

Top FTP User Reports

The Top FTP User reports allow you to view the top FTP client and server addresses performing the session and byte activity for the time period chosen. The data transfer being initiated by the remote IP address defines an FTP server session. The data transfer being initiated by the MVS TCP/IP host defines an FTP client session. Often, an FTP client session is a batch job. The total session's reports include both data transfer and non-data transfer sessions. An example of a non-data transfer FTP session may be a RENAME function. A non-data transfer session has no bytes associated with it.

These reports show the total number of sessions per FTP client or server for the number of top addresses chosen. Both data transfer and non-data transfer sessions are included. You may use these reports to show you who the heaviest users of FTP are at your installation in terms of the number of sessions.

The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions, which perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view some of the other reports in this section, such as Top FTP Users (Bytes) or Top FTP Users (Data Sessions), to obtain a balanced picture of activity.

To obtain a Top FTP Users report, perform the following steps:

1. Click on the History tab.
2. Click the FTP Performance Expert hyperlink under Expert Reports. The FTP Performance Expert main screen appears. Use the Change Host option if reporting for a different host is desired in this session.
3. Select Graph or Report type.
4. Select Weekly by Day or Daily by Hour.
5. Select FTP server or FTP client records to view.
6. Select the category of Top FTP Users Report to view (all sessions, data sessions, or bytes).
7. Set the report day, month, and year to start viewing.
8. Select the number of top users on which to report.
9. Click Submit. The selected report appears.
10. Click Back on the browser to select another function from the FTP Performance Expert main screen.

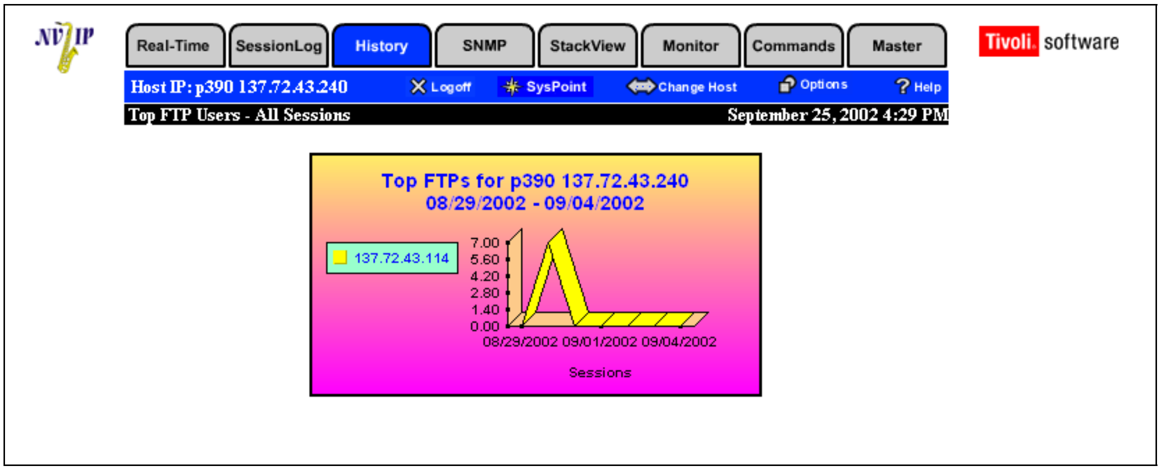
Top FTP Users (All Sessions)

The Top FTP Users (All Sessions) report shows the total number of sessions per FTP client or server for the number of top addresses chosen. Both data transfer and non-data transfer sessions are included. This report shows the heaviest users of FTP at your installation in terms of number of sessions.

The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view some of the other reports in this section, such as Top FTP Users (Bytes) or Top FTP Users (Data Sessions), to obtain a balanced picture of activity.

Graphical Report – Top FTP Users (All Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Top FTP Users - All Sessions

September 25, 2002 4:29 PM

Figure 122. Top FTP Users (All Sessions)

Tabular Report – Top FTP Users (All Sessions)

The tabular report format provides the same basic information as the graphical report.

The fields on the Top FTP Users (All Sessions) report are:

Name/Address	IP addresses listed in descending order.
Time	Calendar date or hour for which activity is reported.
All Sessions	Shows the total number of sessions per FTP client or server for the number of top addresses chosen. Data and non-data transfer sessions are included in the count.

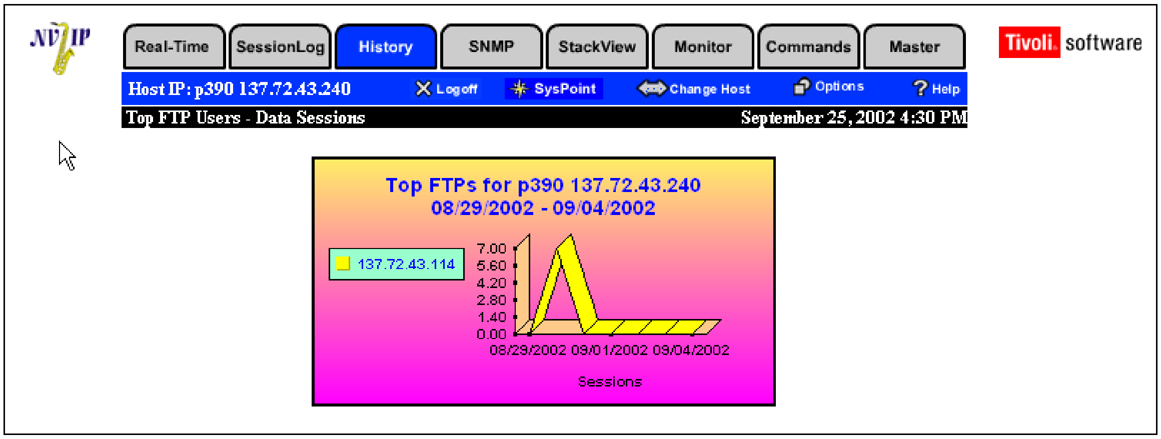
Top FTP Users (Data Sessions)

The Top FTP Users (Data Sessions) report shows the total number of sessions per FTP client or server for the number of top addresses chosen. Only data transfer sessions are included. This report shows you who the heaviest users of FTP are at your installation in terms of number of data transfer sessions.

The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view the Top FTP Users (All Sessions) to obtain a balanced picture of activity. Then if you want more detail about a particular address, select the Options (Show Detail) button to view all the FTPs performed by that address for the time period chosen.

Graphical Report - Top FTP Users (Data Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Top FTP Users - Data Sessions

September 25, 2002 4:30 PM

Figure 123. Top FTP Users (Data Sessions)

Tabular Report - Top FTP Users (Data Sessions)

The tabular report format provides the same basic information as the graphical report format.

The report is divided into sections by IP address order for the selected time period. The fields on the Top FTP Users (Data Sessions) report are:

Name/Address	IP addresses listed in descending order.
Time	Calendar date for which activity is reported.
Data Sessions	Shows the total number of sessions per FTP client or server for the number of top addresses chosen. Only data transfer sessions are included.

Top FTP Users (Bytes)

The Top FTP Users (Bytes) report shows the total number of bytes per FTP client or server for the number of top addresses chosen. Only data transfer sessions are included. This report shows you who the heaviest users of FTP are at your installation in terms of number of bytes transferred.

The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view the Top FTP Users (All Sessions) to obtain a balanced picture of activity.

Graphical Report - Top FTP Users (Bytes)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

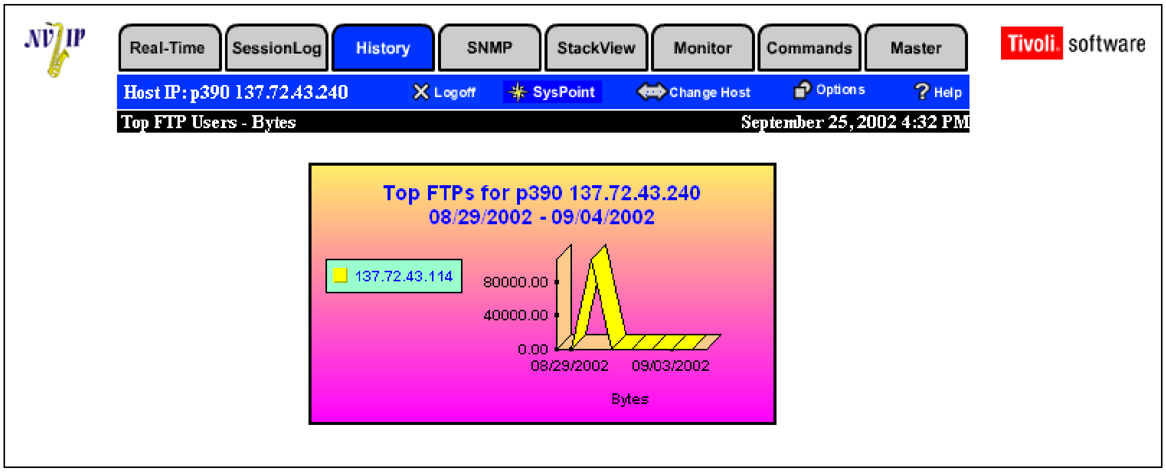


Figure 124. Top FTP Users (Bytes)

Tabular Report - Top FTP Users (Bytes)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top FTP Users (Bytes) report are:

Name/Address	IP addresses listed in descending order.
Time	Calendar date for which activity is reported.
Total Bytes	Shows the total bytes per FTP client or server for the number of top addresses chosen.

Selected User Reports

The Selected User reports allow you to view the details of any FTP client or server address for the time period chosen. The total sessions include both data transfer and non-data transfer sessions. An example of a non-data transfer FTP session may be a RENAME function. A non-data transfer session has no bytes associated with it. In addition, details of all FTPs performed by the address may be viewed by selecting Selected User Detail List.

To obtain a Selected User report, perform the following steps:

1. Click on the History tab.
2. Click the FTP Performance Expert hyperlink under Expert Reports. The FTP Performance Expert main screen appears. Use the Change Host option if reporting for a different host is desired in this session.
3. Select Graph or Report type.
4. Select Weekly by Day or Daily by Hour.
5. Select FTP server or FTP client records to view.
6. Select the category of Selected Users report to view (all sessions, data sessions, or bytes).
7. Set the report day, month, and year to start viewing.
8. Enter the IP address of the user desired.
9. Click Submit. The selected report appears.
10. Click Back on the browser to select another function from the FTP Performance Expert main screen.

Selected User (All Sessions)

The Selected User (All Sessions) report shows the total number of sessions per FTP client or server for the address chosen. Both data transfer and non-data transfer sessions are included. This report shows the FTP activity of any desired user.

Graphical Report - Selected User (All Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

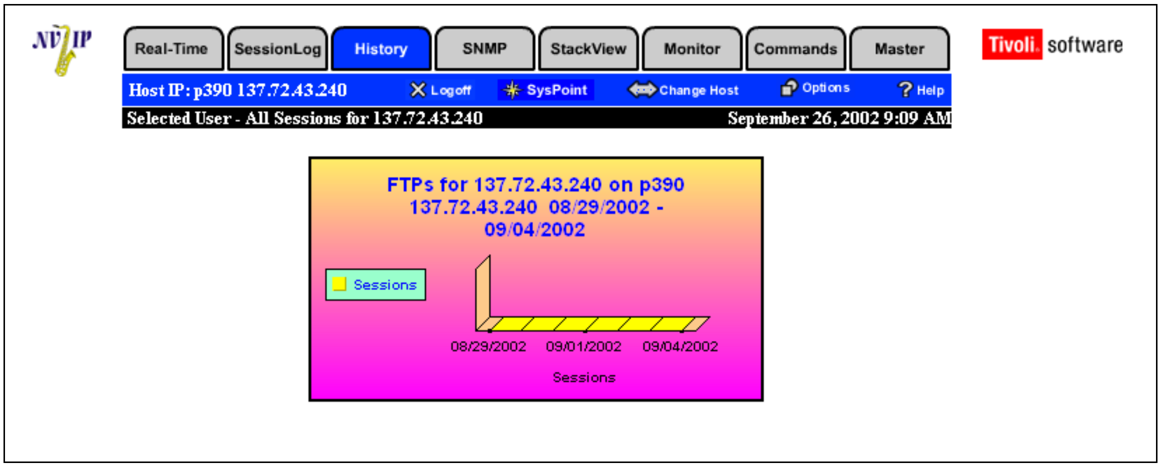

NV IP
Real-Time
SessionLog
History
SNMP
StackView
Monitor
Commands
Master
Tivoli software
Host IP: p390 137.72.43.240
Logoff
SysPoint
Change Host
Options
Help
Selected User - All Sessions for 137.72.43.240
September 26, 2002 9:09 AM
FTPs for 137.72.43.240 on p390 137.72.43.240 08/29/2002 - 09/04/2002
Sessions
08/29/2002
09/01/2002
09/04/2002
Sessions

Figure 125. Selected User (All Sessions)

Tabular Report - Selected User (All Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Selected User (All Sessions) display are:

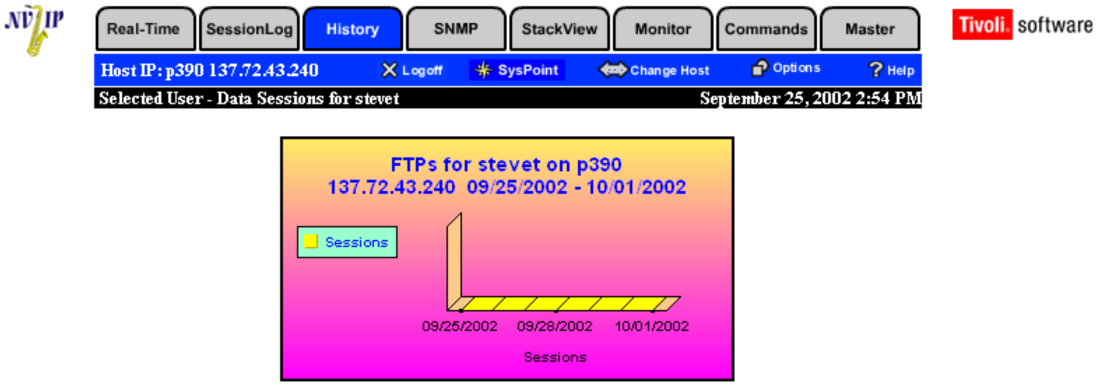
Time	Calendar date or hour for which activity is reported.
Sessions	Shows the total number of sessions per FTP client or server for the selected address. Data and non-data transfer sessions are included.

Selected User (Data Sessions)

The Selected User (Data Sessions) report shows the total number of sessions per FTP client or server for the address chosen. Only data transfer sessions are included. This report shows the data transfer activity of any user. If you want more detail about a particular address, you may view all the FTPs performed by that address for the time period chosen by selecting the Options (Show Detail) button. For more information, view Selected User (All Sessions).

Graphical Report - Selected User (Data Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Selected User - Data Sessions for stevet

September 25, 2002 2:54 PM

Figure 126. Selected User (Data Sessions)

Tabular Report - Selected User (Data Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Selected User (Data Sessions) report are:

Address	IP address
Time	Calendar date or hour for which activity is reported
Sessions	Shows the total number of data sessions per FTP client or server for the selected address

Selected User (Bytes)

The Selected User (Bytes) report shows the total number of bytes as well as the data transfer rate in Kbytes/second per FTP client or server for the address chosen. Only data transfer sessions are included. This report shows the bytes transferred activity of any user.

Graphical Report - Selected User (Bytes)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

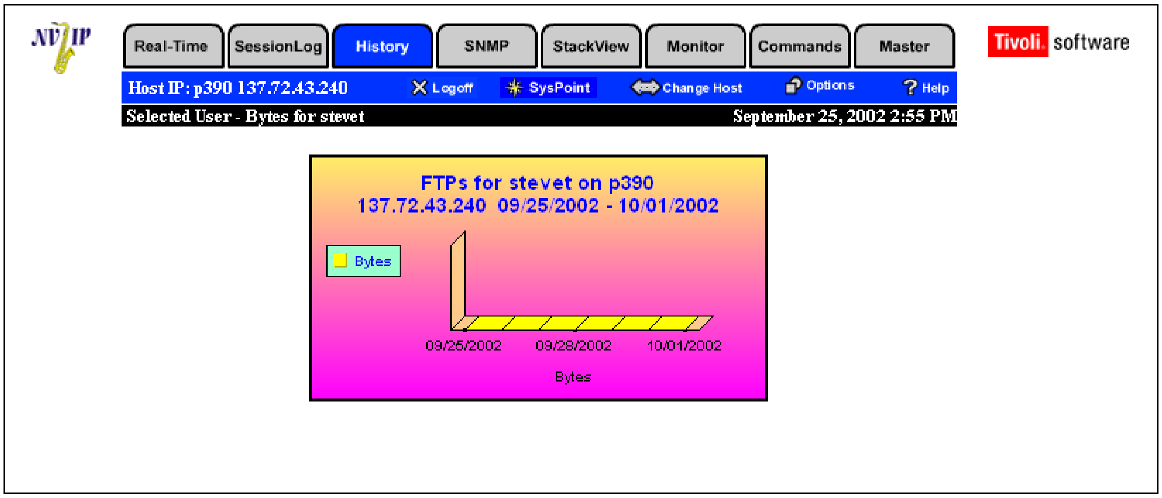


Figure 127. Selected User (Bytes)

Tabular Report - Selected User (Bytes)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Selected User (Bytes) report are:

Time	Calendar date or hour for which activity is reported.
Total Bytes	Shows the total number of bytes transferred per FTP client or server activity for the selected address.

Selected User - Detail List

The Selected User - Detail List shows the details of FTP activity per client. The dates and times of all jobs per FTP client or server are shown for the address chosen. Further details of each FTP activity, as well as information on the data set, member, abnormal end, byte count, or total transmission time may be also be available from this report. View the Selected User - FTP Diagnostic report for a description. To get to the diagnostic report, click on the hyperlink.

Tabular Report - Selected User - Detail List

This report is available only in a tabular report format.

The fields on the Selected User - Detail List tabular report are:

Start Date	Beginning reporting date for FTP activity.
Start Time	Time in hours:minutes:seconds:milliseconds the activity began.
End Date	Ending reporting date for the FTP activity
End Time	Time in hours:minutes:seconds:milliseconds the activity ended.
Data Set Name	Data set name of the file involved in the transaction.
Member	If a partitioned data set, the specific member involved in the transaction.
Total Bytes	Number of bytes transferred in this session.
Return Code	Last return code sent to this client by the FTP server, wherever the FTP server workload resides (the termination code for the operation)
Return Code Description	Textual description of the last return code
Transmit Time	Length of time in hours:minutes:seconds:milliseconds this transmission took
Abnormal End	The ABEND code received if the action was not successfully completed
Throughput Kbytes/sec	Data transfer rate in Kbytes per second.

Selected User - FTP Diagnostic Report

The Selected User - FTP Diagnostic report shows the details of FTP activity per FTP. This report is available either from the Selected User - Detail List or as its own selection. The dates and times of all jobs per FTP client or server are shown for the address chosen. Information on the data set, the member, abnormal end, byte count, total transmission time, FTP subcommand, local User ID, data set format, data set mode, data set type, second data set, or second member may be available.

This report is available only in a tabular report format.

Tabular Report - Selected User - FTP Diagnostic Report

The fields on the Selected User - FTP Diagnostic report are:

Start Date	Beginning reporting date for FTP activity
End Date	Ending reporting date for the FTP activity
Start Time	Time in hours:minutes:seconds:milliseconds the activity began
End Time	Time in hours:minutes:seconds:milliseconds the activity ended
Data Set name	Data set name of the file involved in the transaction
Member	If a partitioned data set, the specific member involved in the transaction
User ID	Local or remote User ID. For example, the TSO ID job was initiated under by the logon profile
2nd Data Set Name	First 44 bytes of the name of the second file involved in the transaction, for example on a RENAME command
2nd Member	If a partitioned data set, the specific member involved in the transaction
FTP Subcommand	Four byte code for the FTP command executed: STOR(e), REN(ame), or DELE(te)
Transmit Time	Lapsed time which the transfer required
Bytes	Total bytes transferred/transmitted
Data Format	Text format used for system processing: ASCII or EBCDIC
Abnormal End	Reserved for abnormal end information
Data Mode	Method of transfer: stream, block, or compressed
Return Code	Last return code sent to this client by the FTP server, wherever the FTP server workload resides (the termination code for the operation)

Data Set Type	Structure of transferred file: sequential, partitioned, or HFS (Hierarchical File System)
Description	Description of numeric return code (shows the status of the FTP action)

Data Set Based Reports

The Data Set Based reports provide information on the top data sets per total number of sessions for data and non-data sessions, selected data set activity regardless of frequency of use, and detail information on activity by data set type.

Either FTP client or server sessions may be selected for the time period chosen. Total sessions include both data transfer and non-data transfer sessions. An example of a non-data transfer FTP session may be a RENAME function. A non-data transfer session has no bytes associated with it.

Top Data Set Activity Reports List

The Top Data Set Activity reports allow you to view the top data sets accessed for FTPs. The available reports are:

- Top Data Set Activity (All Sessions)
- Top Data Set Activity (Data Sessions)
- Top Data Set Activity (Bytes)
- Selected Data Set Activity Reports

Selected Data Set Activity Reports List

The Selected Data Set Activity reports allow you to view selected data set activity accessed for FTPs. The available reports are:

- Selected Data Set Activity (All Sessions)
- Selected Data Set Activity (Data Sessions)
- Selected Data Set Activity (Bytes)
- SEQ/JES/SQL Activity Reports

SEQ/SQL/ JES Activity Reports List

The SEQ/JES/SQL Activity Reports allows you to view the FTP activity by the type of data set: SEQ, SQL, or JES. The available reports are:

- SEQ/JES/SQL Activity (All Sessions)
- SEQ/JES/SQL Activity (Data Sessions)
- SEQ/JES/SQL Activity (Bytes)

Top Data Set Activity Reports

The Top Data Set Activity reports allow you to view the top data sets accessed for FTPs. Either FTP client or server sessions may be selected for the time period chosen. The total sessions report includes both data transfer and non-data transfer sessions. An example of a non-data transfer FTP session may be a RENAME function. A non-data transfer session has no bytes associated with it.

To obtain a Top Data Set Activity report, perform the following steps:

1. Click on the History tab.
2. Click the FTP Performance Expert hyperlink under Expert Reports. The FTP Performance Expert main screen appears. Use the Change Host option if reporting for a different host is desired in this session.
3. Select Graph or Report type.
4. Select Weekly by Day or Daily by Hour.
5. Select FTP server or FTP client records to view.
6. Select the category of Top Data Set Activity report to view (all sessions, data sessions, or bytes).
7. Set the report day, month, and year to start viewing.
8. Select the number of top users on which to report.
9. Click Submit. The selected report appears.
10. Click Back on the browser to select another function from the FTP Performance Expert main screen.

Top Data Set Activity (All Sessions)

The Top Data Set Activity (All Sessions) report shows the total number of sessions per FTP client or server for the number of top data sets chosen. Both data transfer and non-data transfer sessions are included. This report shows which are the most heavily used data sets at your installation in terms of number of sessions.

The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view some of the other reports in this section, such as the Top Data Set Activity (Bytes) or Top Data Set Activity (Data Sessions), to obtain a balanced picture of activity.

Graphical Report - Top Data Set Activity (All Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

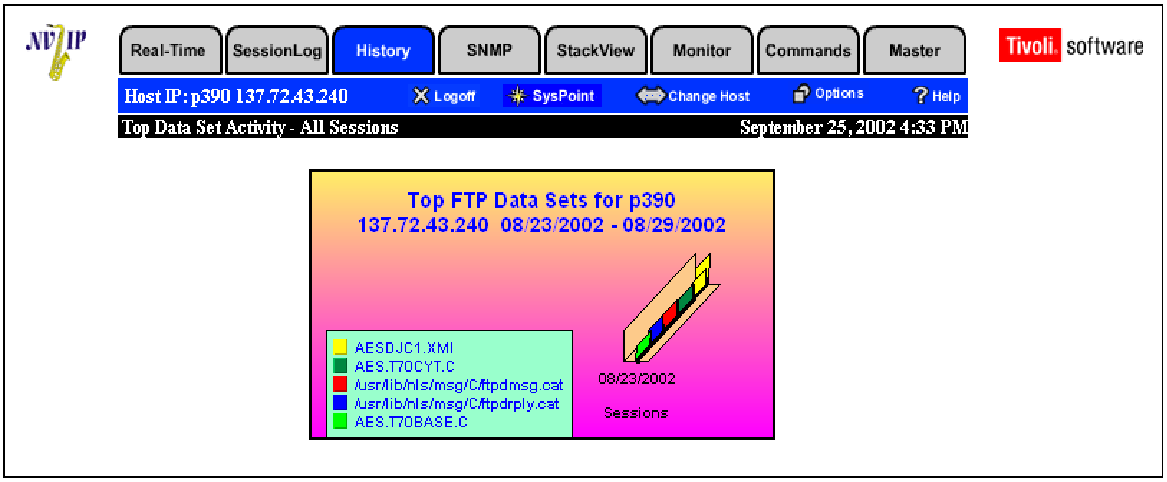


Figure 128. Top Data Set Activity (All Sessions)

Tabular Report - Top Data Set Activity (All Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top Data Set Activity (All Sessions) report are:

Data Set	Data set name for which the selected host/remote device acted as a server
Time	Calendar date or hour for which activity is reported
All Sessions	Shows the total number of sessions involving this data set per FTP client or server activity for the selected device

Top Data Set Activity (Data Sessions)

The Top Data Set Activity (Data Sessions) shows the total number of sessions per FTP client or server for the number of top data sets chosen. Only data transfer sessions are included. This report shows the most heavily used FTP data sets at your installation in terms of number of data transfer sessions. The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view the Top Data Set Activity (All Sessions) to obtain a balanced picture of activity.

Graphical Report - Top Data Set Activity (Data Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

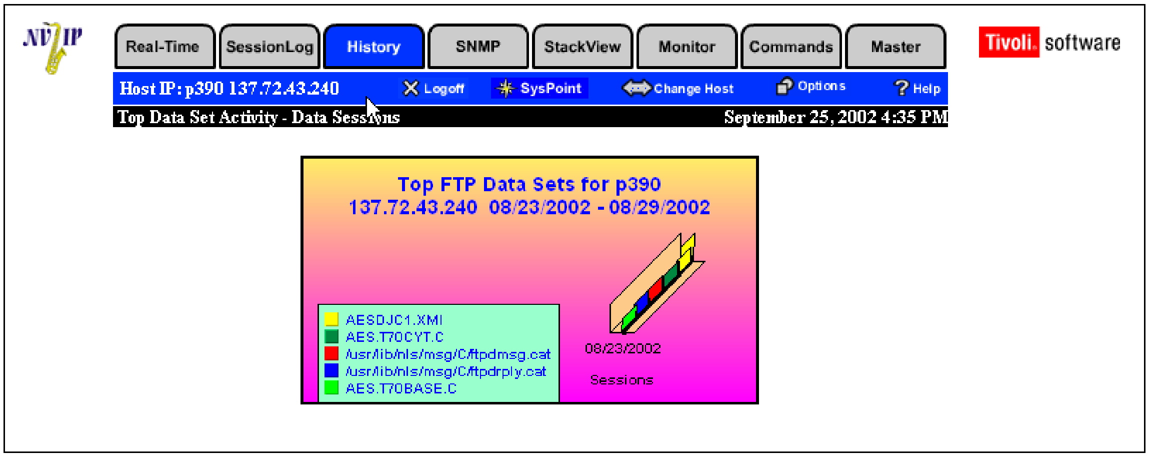


Figure 129. Top Data Set Activity (Data Sessions)

Tabular Report - Top Data Set Activity (Data Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top Data Set Activity (Data Sessions) report are:

Data Set	Data set name for which the selected host/remote device acted as a server/client
Time	Calendar date or hour for which activity is reported
Data Sessions	Shows the total number of sessions involving this data set per FTP client or server activity for the selected device

Top Data Set Activity (Bytes)

The Top Data Set Activity (Bytes) report shows the total number of bytes per FTP client or server for the number of top data sets chosen. Only data transfer sessions are included. This report shows which are the most heavily data sets used FTP at your installation in terms of number of bytes transferred.

The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view the Top Data Set Activity (All Sessions) to obtain a balanced picture of activity.

Graphical Report - Top Data Set Activity (Bytes)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

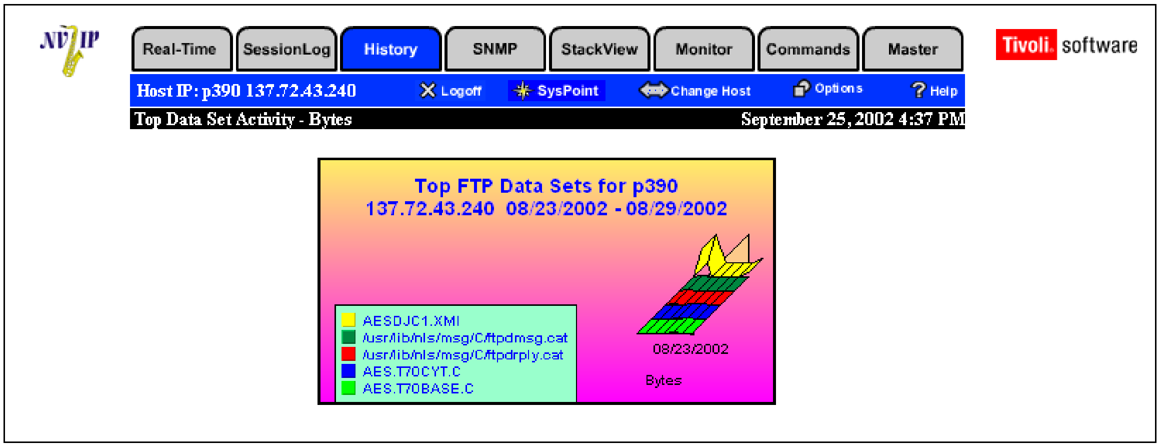


Figure 130. Top Data Set Activity (Bytes)

Tabular Report - Top Data Set Activity (Bytes)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top Data Set Activity (Bytes) report are:

Data Set	One of the top data set names for which the selected host/remote device acted as a server/client
Time	Calendar date or hour for which activity is reported
Bytes	Total number of bytes per FTP client or server for top data sets chosen

Selected Data Set Activity Reports

The Selected Data Set Activity reports allow you to view any Data Set accessed for FTPs. Either FTP client or server sessions may be selected for the time period chosen. The total sessions include both data transfer and non-data transfer sessions. An example of a non-data transfer FTP session may be a RENAME function. A non-data transfer session has no bytes associated with it.

To obtain a Selected Data Set Activity report, perform the following steps:

1. Click on the History tab.
2. Click the FTP Performance Expert hyperlink under Expert Reports. The FTP Performance Expert main screen appears. Use the Change Host option if reporting for a different host is desired in this session.
3. Select Graph or Report type.
4. Select Weekly by Day or Daily by Hour.
5. Select FTP server or FTP client records to view.
6. Select the category of Selected Data Set Activity report to view (all sessions, data sessions, or bytes).
7. Set the report day, month, and year to start viewing.
8. Select the name of the data set on which to report.
9. Click Submit. The selected report appears.
10. Click Back on the browser to select another function from the FTP Performance Expert main screen.

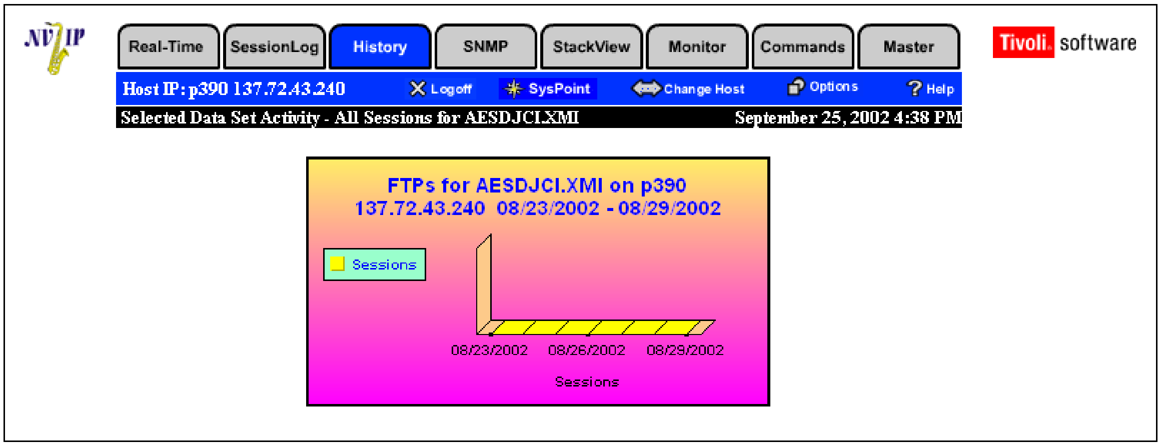
Selected Data Set Activity (All Sessions)

The Selected Data Set Activity (All Sessions) report shows the total number of sessions per FTP client or server for the data set chosen. Both data transfer and non-data transfer sessions are included. This report shows the FTP activity for the data set in terms of number of sessions.

The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view some of the other reports in this section, such as Selected Data Set Activity (Bytes) Selected Data Set Activity (Data Sessions), to obtain a balanced picture of activity.

Graphical Report - Selected Data Set Activity (All Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Selected Data Set Activity - All Sessions for AESDJCI.XMI September 25, 2002 4:38 PM

Figure 131. Selected Data Set Activity (All Sessions)

Tabular Report - Selected Data Set Activity (All Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Selected Data Set Activity (All Sessions) report are:

Time	Calendar date for which activity is reported.
All Sessions	Total number of sessions per FTP client or server for the data sets chosen.

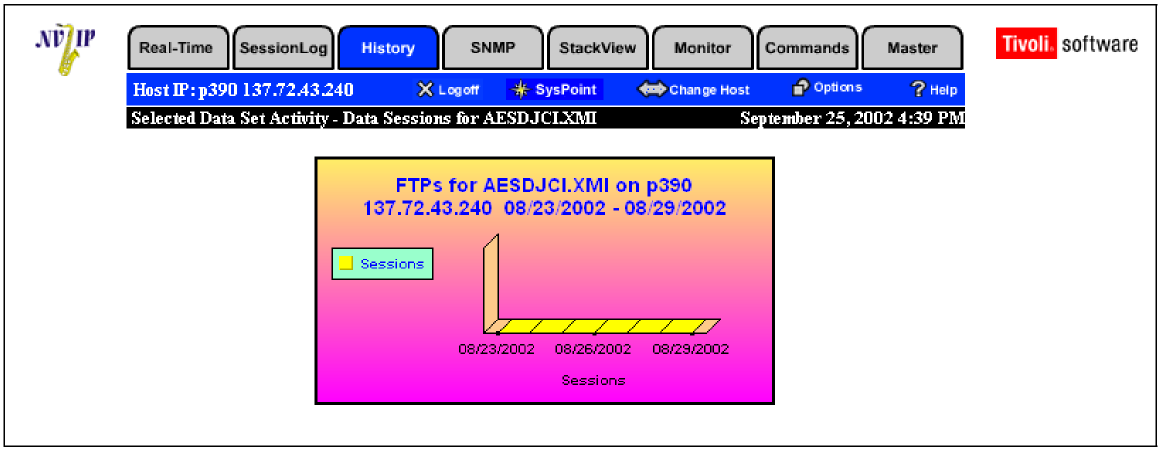
Selected Data Set Activity (Data Sessions)

The Selected Data Set Activity (Data Sessions) report shows the total number of sessions per FTP client or server for the specific data set chosen. Only data transfer sessions are included. This report shows the activity of the FTP data set at your installation in terms of number of data transfer sessions.

The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view the Selected Data Set Activity (All Sessions) to obtain a balanced picture of activity.

Graphical Report - Selected Data Set Activity (Data Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Selected Data Set Activity - Data Sessions for AESDJCI.XMI September 25, 2002 4:39 PM

Figure 132. Selected Data Set Activity (Data Sessions)

Tabular Report - Selected Data Set Activity (Data Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Selected Data Set Activity (Data Sessions) report are:

Time	Calendar date or hour for which activity is reported
Data Sessions	Total number of data transfer sessions per FTP client or server for the data sets chosen

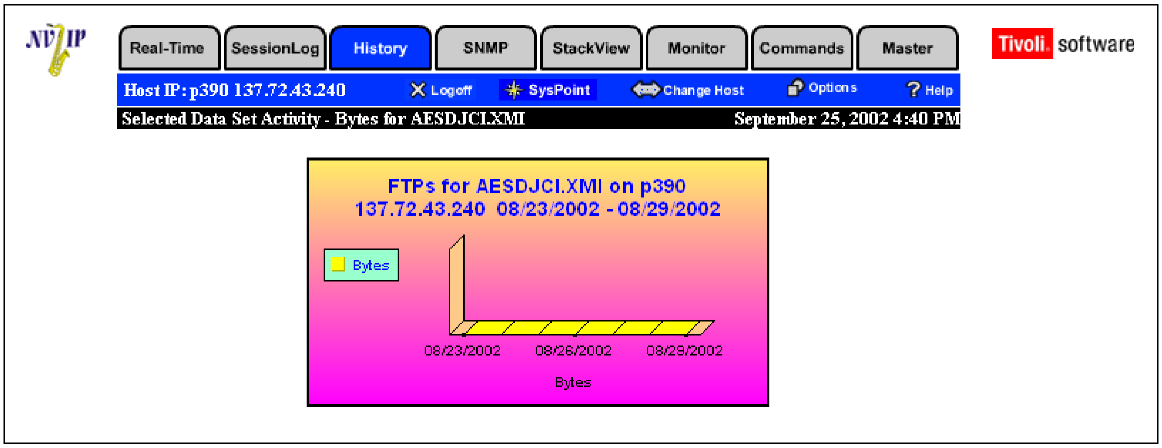
Selected Data Set Activity (Bytes)

The Selected Data Set Activity (Bytes) report shows the total number of bytes per FTP client or server for the data set chosen. Only data transfer sessions are included. This report shows you which FTP data sets are the most heavily used at your installation in terms of number of bytes transferred.

The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view the Selected Data Set Activity (All Sessions) to obtain a balanced picture of activity.

Graphical Report - Selected Data Set Activity (Bytes)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Selected Data Set Activity - Bytes for AESDJCI.XMI September 25, 2002 4:40 PM

Figure 133. Selected Data Set Activity (Bytes)

Tabular Report - Selected Data Set Activity (Bytes)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Selected Data Set Activity (Bytes) report are:

Time	Calendar date or hour for which activity is reported.
Bytes	Total number of bytes transferred per FTP client or server session type for the data set chosen.

SEQ/SQL/JES Activity Reports

The SEQ/SQL/JES Activity reports allow you to view the FTP activity by the type of data set (SEQ, SQL, or JES) for the selected FTP server. The total sessions include both data transfer and non-data transfer sessions. An example of a non-data transfer FTP session may be a RENAME function. A non-data transfer session has no bytes associated with it.

To obtain a SEQ/SQL/JES Activity report, perform the following steps:

1. Click on the History tab.
2. Click the FTP Performance Expert hyperlink under Expert Reports. The FTP Performance Expert main screen appears. Use the Change Host option if reporting for a different host is desired in this session.
3. Select Graph or Report type.
4. Select Weekly by Day or Daily by Hour.
5. Select FTP server or FTP client records to view.
6. Select the category of SEQ/SQL/JES Activity report to view (all sessions, data sessions, or bytes).
7. Set the report day, month, and year to start viewing.
8. Select the type of data set on which to report: SEQ, SQL, or JES.
9. Click Submit. The selected report appears.
10. Click Back on the browser to select another function from the FTP Performance Expert main screen.

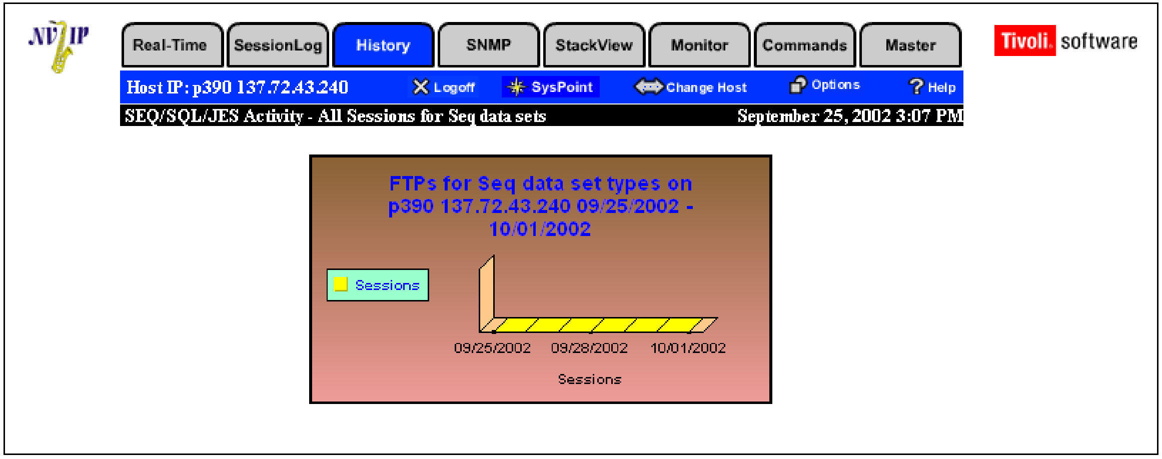
SEQ/SQL/JES Activity Report (All Sessions)

The SEQ/SQL/JES Activity (All Sessions) report shows the total number of sessions per FTP server for SEQ, SQL, and JES data sets. Both data transfer and non-data transfer sessions are included. This report shows the most heavily used data sets at your installation in terms of number of sessions.

The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view some of the other reports in this section, such as SEQ/SQL/JES Activity (Bytes) or SEQ/SQL/JES Activity (Data Sessions), to obtain a balanced picture of activity.

Graphical Report - SEQ/SQL/JES Activity Report (All Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

SEQ/SQL/JES Activity - All Sessions for Seq data sets September 25, 2002 3:07 PM

Figure 134. SEQ/SQL/JES Activity (All Sessions)

Tabular Report - SEQ/SQL/JES Activity Report (All Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the SEQ/SQL/JES Activity (All Sessions) report are:

Time	Calendar date or hour for which activity is reported
All Sessions	Total number of session types per FTP server selected (data and non-data sessions are included in the count)

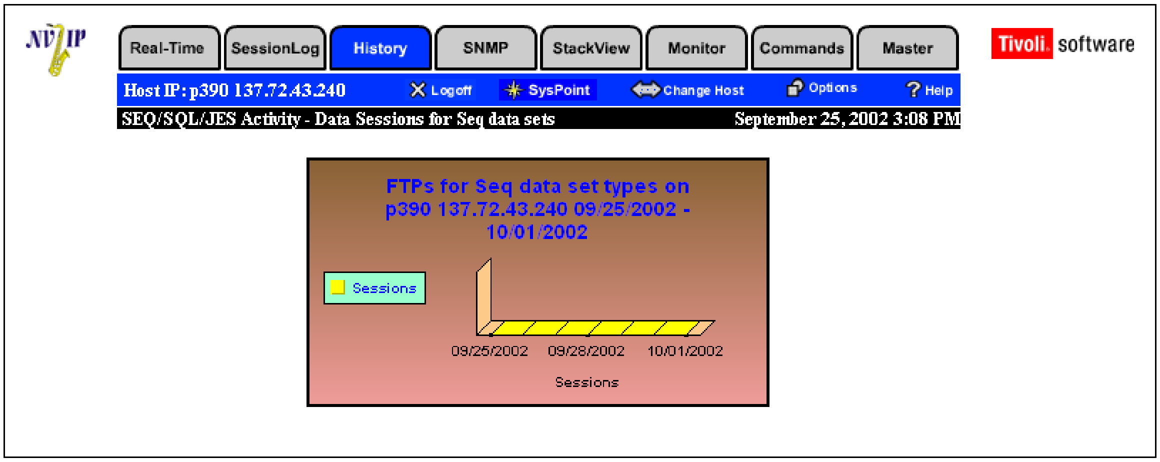
SEQ/SQL/JES Activity (Data Sessions)

The SEQ/SQL/JES Activity (Data Sessions) report shows the total number of sessions per FTP client or server for SEQ, SQL, and JES data sets. Only data transfer sessions are included. This report shows which are the most heavily used FTP data sets at your installation in terms of number of data transfer sessions.

The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view the SEQ, SQL, and JES Activity (All Sessions) to obtain a balanced picture of activity.

Graphical Report - SEQ/SQL/JES Activity (Data Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

SEQ/SQL/JES Activity - Data Sessions for Seq data sets September 25, 2002 3:08 PM

Figure 135. SEQ/SQL/JES Activity (Data Sessions)

Tabular Report - SEQ/SQL/JES Activity (Data Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the SEQ/SQL/JES Activity (Data Sessions) report are:

Time	Calendar date or hour for which activity is reported
Data Sessions	Total number of data session transfer types per FTP server selected for the specific date

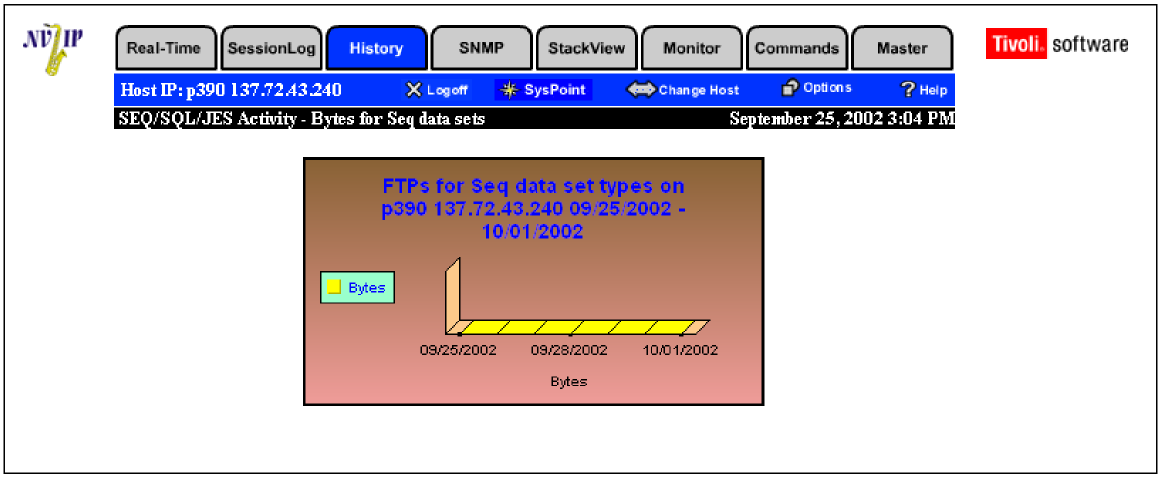
SEQ/SQL/JES Activity (Bytes)

The SEQ/SQL/JES Activity (Bytes) report shows the total number of bytes per FTP client or server for SEQ, SQL, and JES data sets. Only data transfer sessions are included. This report shows which are the most heavily used FTP data sets at your installation in terms of number of bytes transferred.

The total number of sessions may or may not correlate with the period of highest amount of bytes transmitted. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME), or many failed FTP sessions. You may wish to view the FTP SEQ, SQL, and JES Activity (All Sessions) to obtain a balanced picture of activity.

Graphical Report - SEQ/SQL/JES Activity (Bytes)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

SEQ/SQL/JES Activity - Bytes for Seq data sets September 25, 2002 3:04 PM

Figure 136. SEQ/SQL/JES Activity (Bytes)

Tabular Report - SEQ/SQL/JES Activity (Bytes)

The tabular report format provides the same basic information as the graphical report format.

The fields on the SEQ/SQL/JES Activity (Bytes) report are:

Time	Calendar date or hour which activity is reported
Bytes	Total bytes transferred per data set type per the selected FTP client or server

Failure Based Reports

The Failure Based reports provide an overall view as well as address and data set failure information. The Total Failures reports allow you to view all the failed FTP jobs for a chosen time period. The Top Failing Users reports allow you to view the top addresses submitting failing FTP jobs for a chosen time period. The Top Failing Data Sets reports allow you to view the top data sets against which failing FTP jobs were submitted for a chosen time period.

Either FTP client or server sessions may be selected. You may also choose to view all failures or only failures that do not include user aborts. Total sessions include both data transfer and non-data transfer sessions. An example of a non-data transfer FTP session may be a RENAME function. A non-data transfer session has no bytes associated with it.

Total Failures Reports List

The Total Failures reports allow you to view all the failed FTP jobs for a chosen time period. The available reports are:

- Total Failures (All Sessions)
- Total Failures (Data Sessions)
- Total Failures (Bytes)

Top Failing Users Reports List

The FTP Top Failing Addresses reports allow you to view the top addresses submitting failing FTP jobs for a chosen time period. The available reports are:

- Top Failing Users (All Sessions)
- Top Failing Users (Data Sessions)
- Top Failing Users (Bytes)

Top Failing Data Sets Reports List

The Top Failing Data Sets reports allow you to view the top data sets against which failing FTP jobs were submitted for a chosen time period. You may also choose to view all failures or only failures that do not include user aborts. The available reports are:

- Top Failing Data Sets (All Sessions)
- Top Failing Data Sets (Data Sessions)
- Top Failing Data Sets (Bytes)

Total Failures Reports

The Total Failures reports allow you to view all the failed FTP jobs for a chosen time period. Either FTP client or server sessions may be selected. Total sessions include both data transfer and non-data transfer sessions. An example of a non-data transfer FTP session may be a RENAME function. A non-data transfer session has no bytes associated with it.

To obtain a Total Failures report, perform the following steps:

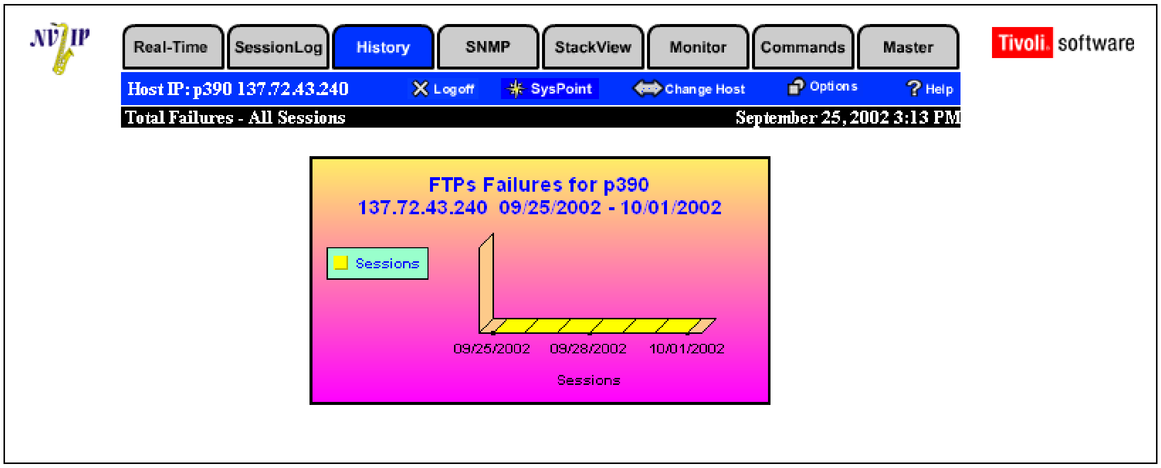
1. Click on the History tab.
2. Click the FTP Performance Expert hyperlink under Expert Reports. The FTP Performance Expert main screen appears. Use the Change Host option if reporting for a different host is desired in this session.
3. Select Graph or Report type.
4. Select Weekly by Day or Daily by Hour.
5. Select FTP server or FTP client records to view.
6. Select the category of Total Failures report to view (all sessions, data sessions, or bytes).
7. Set the report day, month, and year to start viewing.
8. Select whether you wish to include user aborts in the count of failures.
9. Click Submit. The selected report appears.
10. Click Back on the browser to select another function from the FTP Performance Expert main screen.

Total Failures (All Sessions)

The Total Failures (All Sessions) report shows the total number of failing sessions per FTP client or server for all FTP jobs. Both data transfer and non-data transfer sessions are included. This report shows failures in the network of which no one is aware. The total number of sessions may not all be data transfer sessions. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME). It may be these sessions that are failing. You may wish to view some of the other reports in this section, such as Total Failures (Bytes) or Total Failures (Data Sessions), to obtain a balanced picture of activity.

Graphical Report - Total Failures (All Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Total Failures - All Sessions

September 25, 2002 3:13 PM

Figure 137. Total Failures (All Sessions)

Tabular Report - Total Failures (All Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Total Failures (All Sessions) report are:

Time	Calendar date or hour for which activity is reported
All Sessions	Total number of failed sessions per FTP client or server for all FTP jobs, data and non-data

Total Failures (Data Sessions)

The Total Failures (Data Sessions) report shows the total number of failing sessions per FTP client or server for data transfer FTP sessions. Non-data transfer sessions are not included. This report shows failures in your network of which you may not be aware. The total number of sessions may not all be data transfer sessions. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME). It may be these sessions that are failing. You may wish to view some of the other reports in this section, for example Total Failures (Bytes) or Total Failures (All Sessions), to obtain a balanced picture of activity.

Graphical Report - Total Failures (Data Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

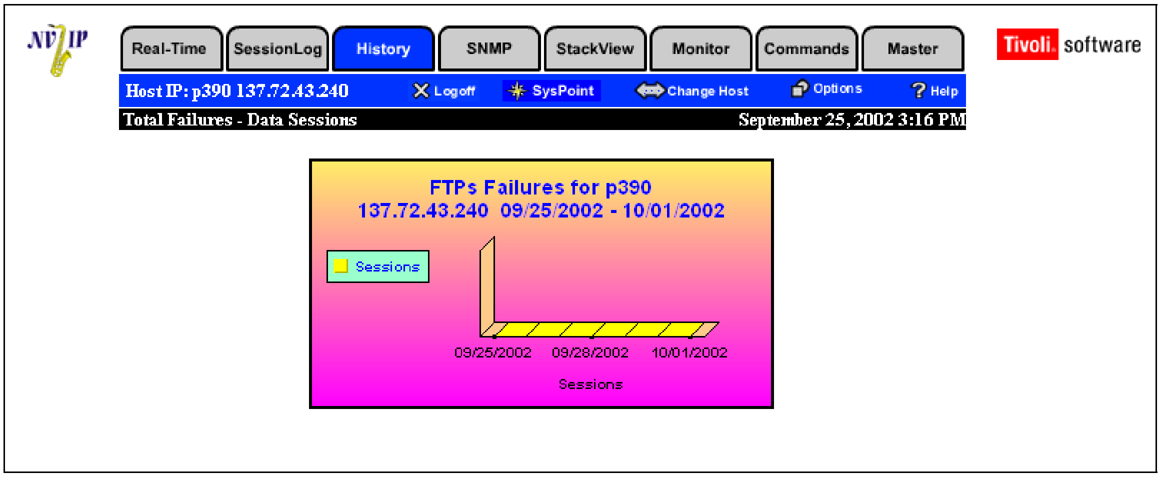


Figure 138. Total Failures (Data Sessions)

Tabular Report - Total Failures (Data Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Total Failures (Data Sessions) report are:

Time	Calendar date or hour for which activity is reported
Data Sessions	Total number of failed sessions per FTP client or server for data transfer FTP jobs

Total Failures (Bytes)

The Total Failures (Bytes) report shows the total number of bytes per failing sessions per FTP client or server for data transfer FTP sessions. Non-data transfer sessions are not included. This report shows failures in your network of which you may not be aware. The total number of sessions may not all be data transfer sessions. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME). It may be these sessions that are failing. You may wish to view some of the other reports in this section, for example Total Failures (Data Sessions) or Total Failures (All Sessions), to obtain a balanced picture of activity.

Graphical Report - Total Failures (Bytes)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

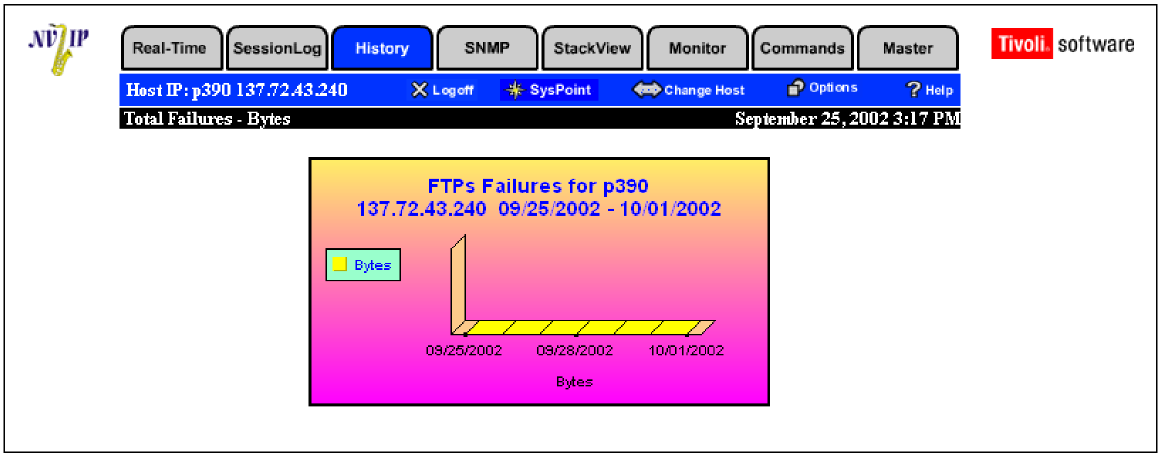


Figure 139. Total Failures (Bytes)

Tabular Report Total Failures (Bytes)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Total Failures (Bytes) report are:

Time	Calendar date or hour for which activity is reported
Bytes	Number of bytes sent for the failing FTP transmission

Top Failing Users Reports

The Top Failing Users reports allow you to view the top addresses submitting failing FTP jobs for a chosen time period. Either FTP client or server sessions may be selected. You may also choose to view all failures or only failures that do not include user aborts. The total sessions count includes both data transfer and non-data transfer sessions. An example of a non-data transfer FTP session may be a RENAME function. A non-data transfer session has no associated with it. To obtain a Top Failing Users report, perform the following steps:

1. Click on the History tab.
2. Click the FTP Performance Expert hyperlink under Expert Reports. The FTP Performance Expert main screen appears. Use the Change Host option if reporting for a different host is desired in this session.
3. Select Graph or Report type.
4. Select Weekly by Day or Daily by Hour.
5. Select FTP server or FTP client records to view.
6. Select the category of Top Failing Users report to view (all sessions, data sessions, or bytes).
7. Set the report day, month, and year to start viewing.
8. Select the number of top failing users on which to report.
9. Select whether you wish to include user aborts in the count of failures.
10. Click Submit. The selected report appears.
11. Click Back on the browser to select another function from the FTP Performance Expert main screen.

Top Failing Users (All Sessions)

The Top Failing Users (All Sessions) report shows the top addresses with failing sessions per FTP client or server for all FTP jobs. Both data transfer and non-data transfer sessions are included. You may choose to include all failures or only those that were not aborted by the user. This report shows the addresses in your network which are most often experiencing FTP failures.

The failures may be for many reasons. You may wish to view the Selected User - Detail List from the Selected User - FTP Diagnostic report for more information on these failures. The total number of sessions may not all be data transfer sessions. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME). It may be these sessions that are failing. You may wish to view some of the other reports in this section, for example Top Failing Users (Bytes) or Top Failing Users (Data Sessions), to obtain a balanced picture of activity.

Graphical Report - Top Failing Users (All Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

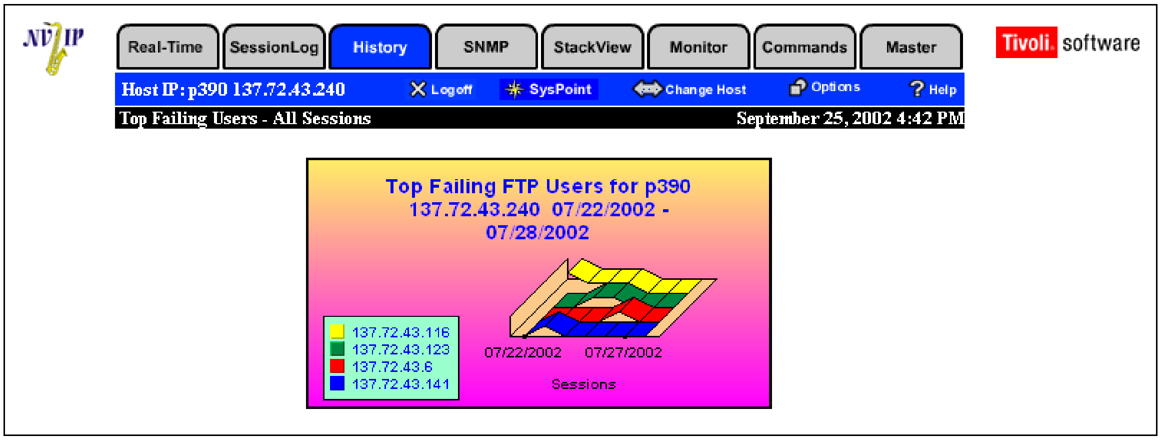


Figure 140. Top Failing Users (All Sessions)

Tabular Report - Top Failing Users (All Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top Failing Users (All Sessions) report are:

Name/Address	Lists failing IP addresses for the selected server or client
Time	Calendar date or hour for which activity is reported
All Sessions	Total number of failed sessions per IP address by date for the selected FTP client or server

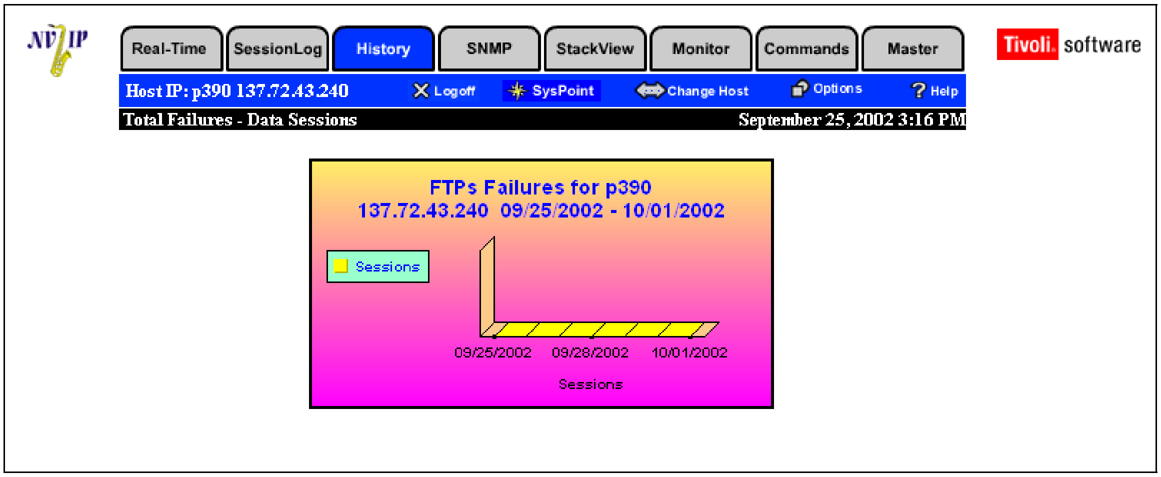
Top Failing Users (Data Sessions)

This report shows the top addresses with failing sessions per FTP client or server for all FTP jobs. Only data transfer sessions are included. You may choose to include all failures or only those that were not aborted by the user. This report shows you the addresses in your network which are most often experiencing FTP failures. The failures may be for many reasons.

You may wish to view the Selected User - Detail List from the Selected User - FTP Diagnostic report for more information on these failures. The total number of sessions may not all be data transfer sessions. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME). It may be these sessions that are failing. You may wish to view some of the other reports in this section, such as Top Failing Users (Bytes) or Top Failing Users (All Sessions), to obtain a balanced picture of activity.

Graphical Report - Top Failing Users (Data Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Total Failures - Data Sessions

September 25, 2002 3:16 PM

FTPs Failures for p390
137.72.43.240 09/25/2002 - 10/01/2002

Figure 141. Top Failing Users – Data Sessions

Tabular Report - Top Failing Users (Data Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top Failing Users (Data Sessions) report are:

Name/Address	Lists failing IP addresses for the selected server or client
Time	Calendar date or hour for which activity is reported
Data Sessions	Total number of failed sessions per IP address by date for the selected FTP client or server

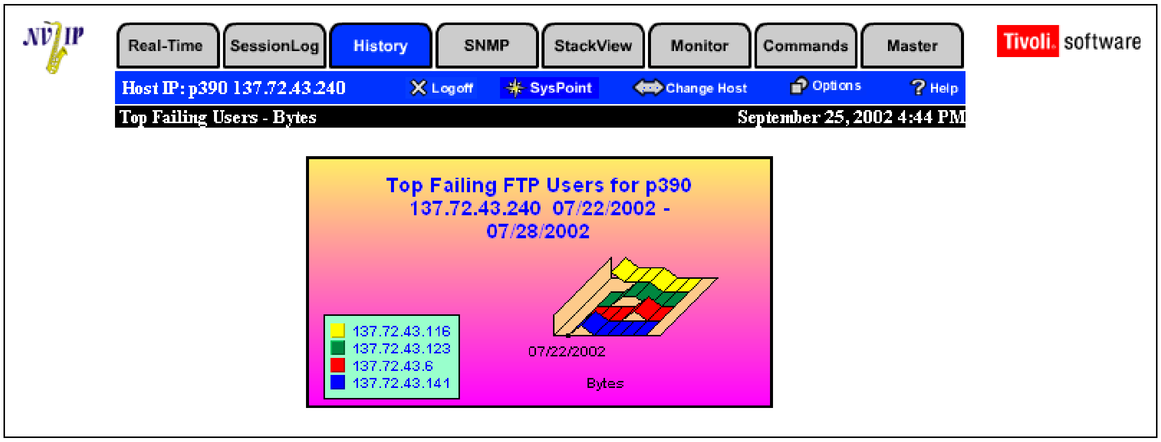
Top Failing Users (Bytes)

This report shows the bytes for the top addresses with failing sessions per FTP client or server for all FTP jobs. Only data transfer sessions are included. You may choose to include all failures or only those that were not aborted by the user. This report is used to show the addresses in your network which are most often experiencing FTP failures.

The failures may be for many reasons. You may wish to view the Selected User - Detail List from the Selected User - FTP Diagnostic report for more information on these failures. The total number of sessions may not all be data transfer sessions. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME). It may be these sessions that are failing. You may wish to view some of the other reports in this section, such as Top Failing Addresses (Data Sessions) or Top Failing Addresses (All Sessions), to obtain a balanced picture of activity.

Graphical Report - Top Failing Users (Bytes)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Top Failing Users - Bytes

September 25, 2002 4:44 PM

Figure 142. Top Failing Users - Bytes

Tabular Report - Top Failing Users (Bytes)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top Failing Users (Bytes) report are:

Name/Address	Lists failing IP addresses for the selected server or client
Time	Calendar date or hour for which activity is reported
Bytes	Number of bytes sent for the failing FTP transmission

Top Failing Data Set Reports

The Top Failing Data Sets reports allow you to view the top data sets against which failing FTP jobs were submitted for a chosen time period. Either FTP client or server sessions may be selected. You may also choose to view all failures or only failures that do not include user aborts. The total sessions graph/report includes both data transfer and non-data transfer sessions. An example of a non-data transfer FTP session may be a RENAME function. A non-data transfer session has no bytes associated with it.

To obtain a Top Failing Data Sets report, perform the following steps:

1. Click on the History tab.
2. Click the FTP Performance Expert hyperlink under Expert Reports. The FTP Performance Expert main screen appears. Use the Change Host option if reporting for a different host is desired in this session.
3. Select Graph or Report type.
4. Select Weekly by Day or Daily by Hour.
5. Select FTP server or FTP client records to view.
6. Select the category of Top Failing Data Sets report to view (all sessions, data sessions, or bytes).
7. Set the report day, month, and year to start viewing.
8. Select the number of top failing data sets on which to report.
9. Select whether you wish to include user aborts in the count of failures.
10. Click Submit. The selected report appears.
11. Click Back on the browser to select another function from the FTP Performance Expert main screen.

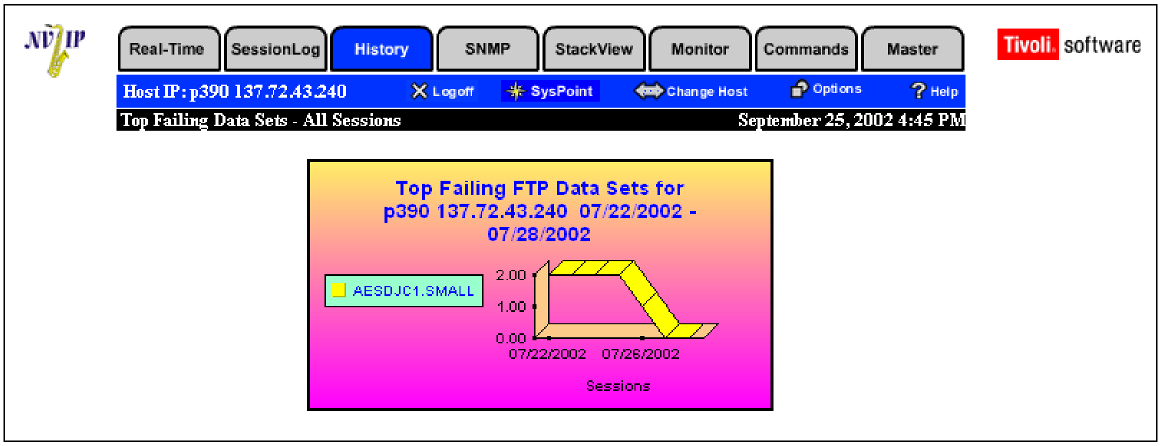
Top Failing Data Sets (All Sessions)

The Top Failing Data Sets (All Sessions) report shows the top data sets with failing sessions per FTP client or server for all FTP jobs. Both data transfer and non-data transfer sessions are included. You may choose to include all failures or only those that were not aborted by the user. This report shows you the data sets in your network which are most often experiencing FTP failures.

The total number of sessions may not all be data transfer sessions. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME). It may be these sessions that are failing. You may wish to view some of the other reports in this section, such as Top Failing Data Sets (Bytes) or Top Failing Data Sets (Data Sessions), to obtain a balanced picture of activity.

Graphical Report - Top Failing Data Sets (All Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Top Failing Data Sets - All Sessions

September 25, 2002 4:45 PM

Figure 143. Top Failing Data Sets (All Sessions)

Tabular Report - Top Failing Data Sets (All Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top Failing Data Sets (All Sessions) report are:

Data Set	One of the top number of data sets with failing sessions
Time	Calendar date or hour for which activity is reported
All Sessions	Total number of failed sessions per that top failing data set by date

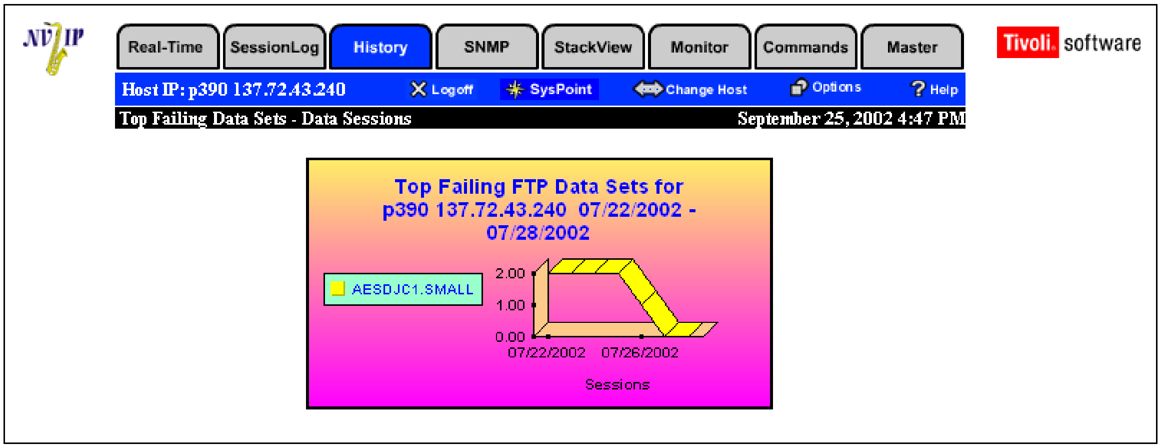
Top Failing Data Sets (Data Sessions)

The Top Failing Data Sets (Data Sessions) shows the top data sets with failing sessions per FTP client or server for all FTP jobs. Only data transfer sessions are included. You may choose to include all failures or only those that were not aborted by the user. This report shows the data sets in your network which are most often experiencing FTP failures.

The total number of sessions may not all be data transfer sessions. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME). It may be these sessions that are failing. You may wish to view some of the other reports in this section, such as Top Failing Data Sets (Bytes) or Top Failing Data Sets (All Sessions), to obtain a balanced picture of activity.

Graphical Report - Top Failing Data Sets (Data Sessions)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Top Failing Data Sets - Data Sessions September 25, 2002 4:47 PM

Figure 144. Top Failing Data Sets (Data Sessions)

Tabular Report - Top Failing Data Sets (Data Sessions)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top Failing Data Sets (Data Sessions) report are:

Data Set	One of the top number of data sets with failing sessions
Time	Calendar date or hour for which activity is reported
Data Sessions	Number of failing data sessions

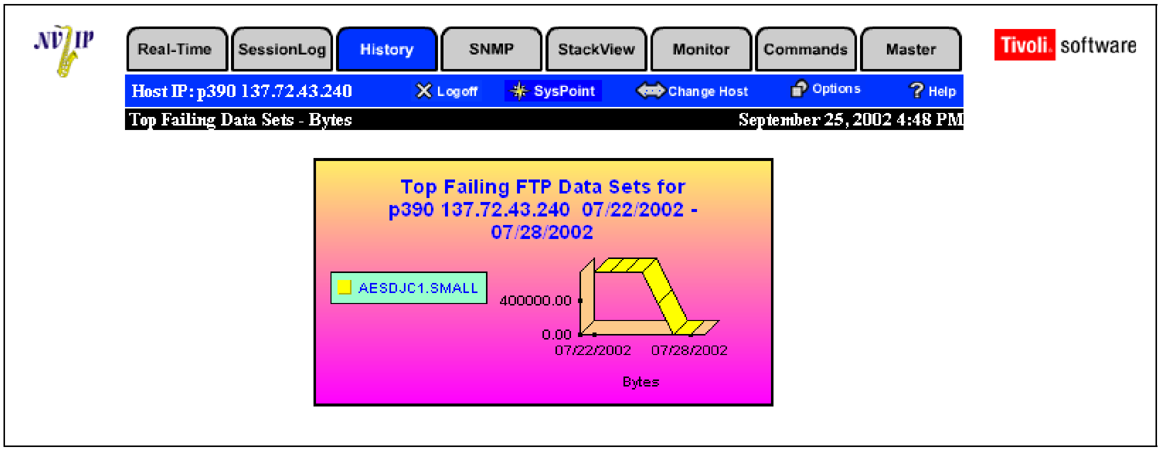
Top Failing Data Sets (Bytes)

The Top Failing Data Sets (Bytes) report shows the number of bytes for the top data sets with failing sessions per FTP client or server for all FTP jobs. Only data transfer sessions are included. You may choose to include all failures or only those that were not aborted by the user. This report shows you the data sets in your network which are most often experiencing FTP failures.

The total number of sessions may not all be data transfer sessions. For example, there may be many FTP sessions that perform non-data transfer activity (RENAME). It may be these sessions that are failing. You may wish to view some of the other reports in this section, such as Top Failing Data Sets (Data Sessions) or Top Failing Data Sets (All Sessions), to obtain a balanced picture of activity.

Graphical Report - Top Failing Data Sets (Bytes)

Data may be viewed by day, by week, or by hour. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Top Failing Data Sets - Bytes

September 25, 2002 4:48 PM

Top Failing FTP Data Sets for p390 137.72.43.240 07/22/2002 - 07/28/2002

Figure 145. Top Failing Data Sets (Bytes)

Tabular Report - Top Failing Data Sets (Bytes)

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top Failing Data Sets (Bytes) report are:

Data Set	One of the top number of data sets with failing sessions.
Time	Calendar date or hour for which activity is reported.
Data Sessions	Number of failing data sessions

Telnet Expert Reports

This product views the TCP/IP network performance from the enterprise level to the remote user connection. Performance indicators are available for Telnet workload and usage. The Telnet Expert Reports become available when the Host Monitor is started.

The Telnet Expert is structured to allow you to view both a global and detailed view of Telnet activity. Telnet, especially TN3270 from the Telnet server, is one of the most frequently used functions of TCP/IP. You may want to know what SNA applications your installation is using, who the top Telnet users are or to diagnose problems with a particular Telnet session. The Telnet Expert Reports allows you to find answers to these and many other questions.

The data provided in these reports is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it is recorded at the time it terminates.

If you wish to view time slices of active sessions taken in a sampling mode, please review the Base History reports. You may also want to look at "near time" Telnet activity by viewing the SessionLog Telnet reports. The SessionLog Telnet reports show sessions that are currently in progress or have recently completed.

The Telnet Expert Reports provide two categories of reporting:

Activity (Address Based Reports)	
Total Telnet Usage	Total Telnet client or server session and byte activity for the time period chosen.
Top Telnet Users	View the top Telnet client or server addresses performing the session and byte activity for the time period chosen.
Selected Telnet Users	View the details of any Telnet client or server address for the time period chosen.
Selected Telnet User – Detail List	View the sessions or bytes for a specific Telnet client or server application for the time period chosen.
Application Based Reports	
Top Telnet Applications/STCs	View the top applications accessed via Telnet.
Selected Telnet Application/STC	Statistics for any application accessed via Telnet.

To view a Telnet Expert Report, perform the following steps:

1. Click on the History tab.
2. Click the Telnet Expert hyperlink under Expert Reports. The Telnet Expert Reports main screen appears.
3. Choose Show Graph or Show Report.
4. Select the report you want to view.
5. Select the time slice you want to view: Weekly by Day or Daily by Hour.
6. Select whether you want to report on Telnet client or Telnet server sessions. A Telnet server session is initiated by the remote IP address. A Telnet client session is initiated by the MVS TCP/IP host.
7. Select if you want to view by DNS name or address. This option only applies to the top Telnet user reports.
8. Select the starting time using the twenty-four hour clock if you are doing the Daily by Hour report and want to start at an hour other than 0.
9. Enter the number of bytes, clients, applications, or the specific name / address you want to view:
    - For the Total report category, enter the minimum bytes
    - For Top reports, enter between 1-250 data points if you are requesting a report, or enter a value between 1-20 if you are requesting a graph.
    - For Selected User reports, enter the IP address.
    - For Selected Application reports, enter the Telnet Application name to be viewed.
    - Click Submit. The selected report appears.
10. Use the Back Arrow on your browser to move between screens.

Activity (Address Based Reports) for Telnet

Activity (Address Based) Reports offer information regarding Telnet clients and servers through the following reports:

- Total Telnet Usage
- Top Telnet Users
- Selected Telnet Users
- Selected Telnet User

Total Telnet Usage Report

These reports allow you to view the total Telnet client or server activity for the time period chosen. A Telnet server session is initiated by the remote IP address. A Telnet client session is initiated by the MVS TCP/IP host. The number of bytes is available for Telnet server sessions only.

The data provided in these reports is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it is recorded at the time it terminates.

If you enter the minimum bytes filter, these reports show the total number of sessions or bytes per Telnet session exceeding the number of bytes entered for the interval chosen. You may use this report to show you when most sessions exceeding a certain byte limit take place. For example, you may want to see when Telnet sessions with over 5 megabytes take place. The number of bytes filter is available for Telnet server sessions only.

Graphical Report - Total Telnet Usage Report

Data may be viewed weekly by day, or daily by hour. Required field is Start Date. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

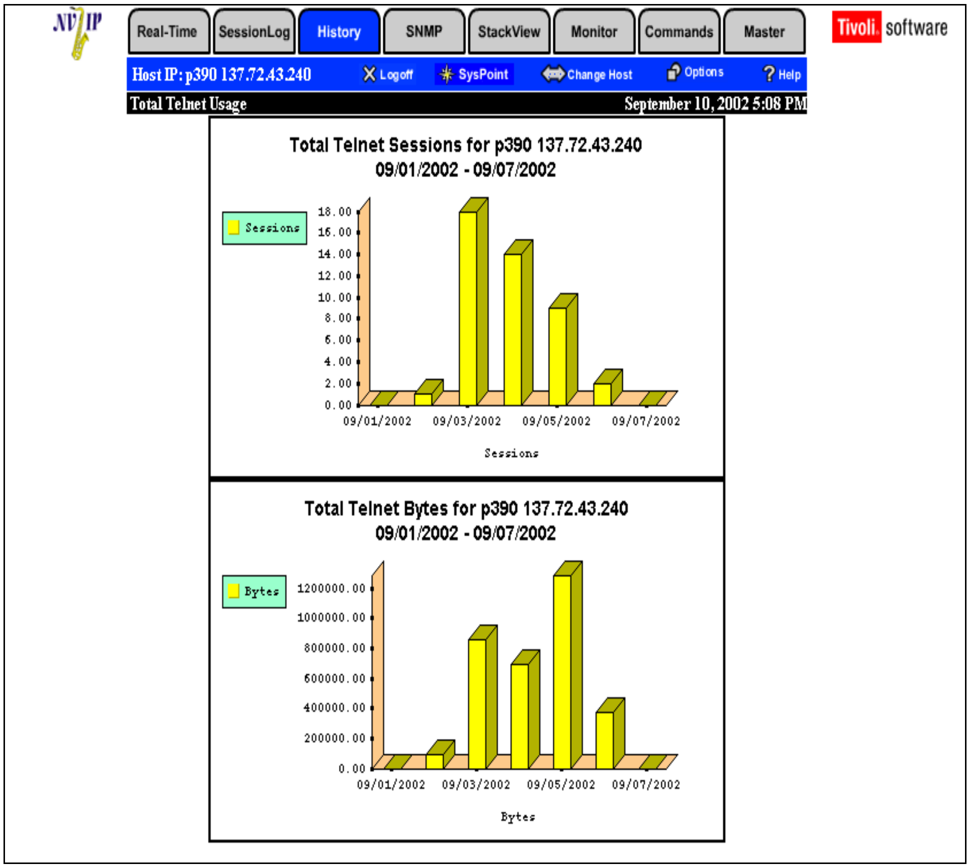


Figure 146. Total Telnet Usage Reports

Tabular Report - Total Telnet Usage Report

The tabular report format provides the same basic information as the graphical report format.

The fields on the Total Telnet Usage tabular report are:

Time	Interval during which the Telnet session ended.
Number of Bytes	Total number of bytes(Telnet server only).
Number of Sessions	Total number of sessions.

Top Telnet Users Report

These reports allow you to view the most active Telnet client or server users for the time period chosen. A Telnet server session is initiated by the remote IP address. A Telnet client session is initiated by the MVS TCP/IP host. The number of bytes is available for Telnet server sessions only.

The data provided in this report is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it is recorded at the time it terminates.

Graphical Report - Top Telnet Users Report

Data may be viewed weekly by day, or daily by hour. Required fields are Start Date and How Many. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

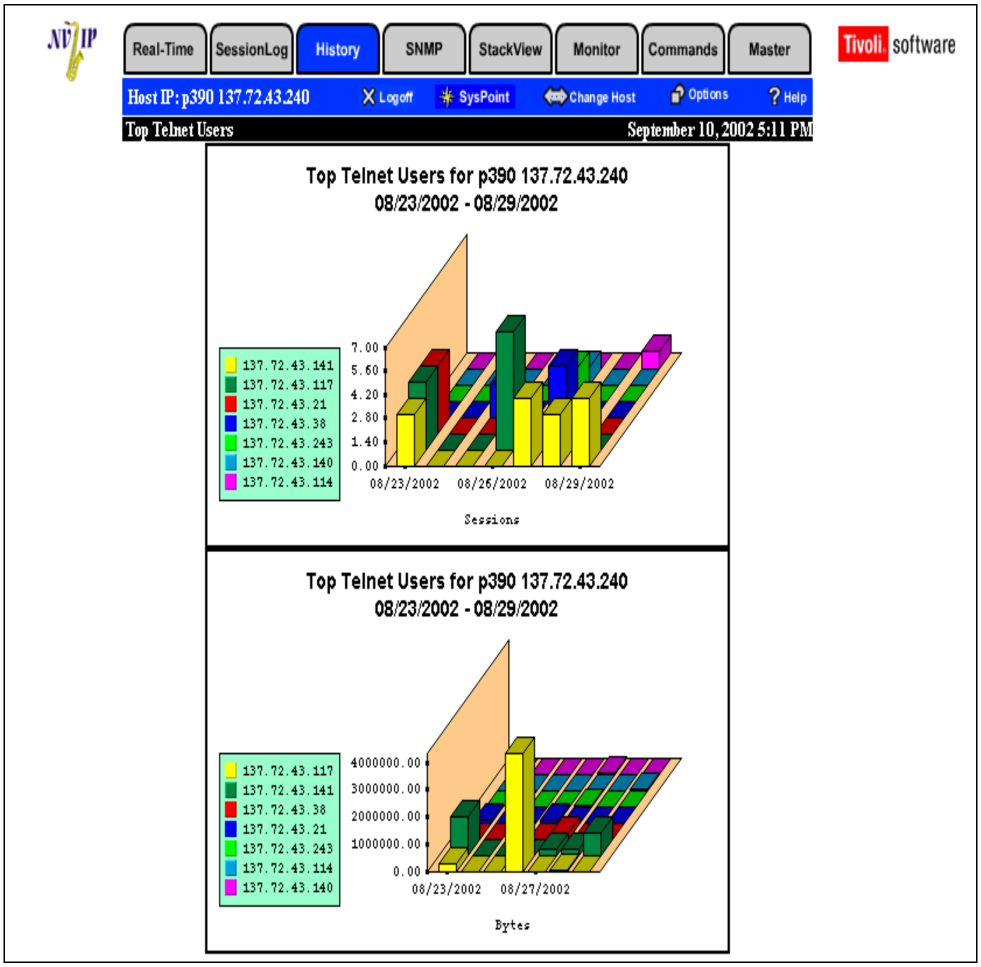


Figure 147. Top Telnet Users Report

Tabular Report - Top Telnet Users Report

The tabular report format provides the same basic information as the graphical report format.

The fields on the Total Telnet Users tabular report are:

Address	IP address initiating the Telnet session.
Time	Interval during which the Telnet session terminated.
Number of Bytes	Total number of bytes (for Telnet server only).
Number of Sessions	Total number of sessions.

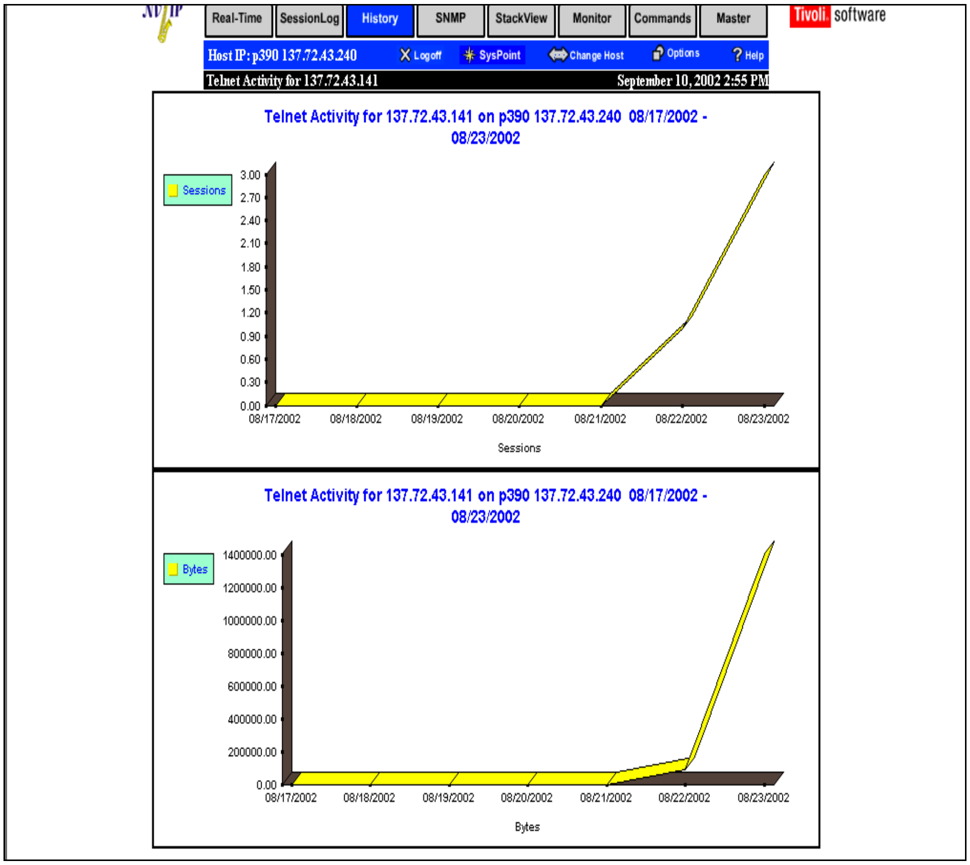
Selected Telnet User Report

This report allows you to view data for a specific Telnet client or server user for the time period chosen. A Telnet server session is initiated by the remote IP address. A Telnet client session is initiated by the MVS TCP/IP host. The number of bytes is available for Telnet server sessions only.

The data provided in this report is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it will be recorded at the time it terminates.

Graphical Report - Selected Telnet User Report

Data may be viewed weekly by day, or daily by hour. Required fields are Start Date and Address. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Telnet Activity for 137.72.43.141 September 10, 2002 2:55 PM

Telnet Activity for 137.72.43.141 on p390 137.72.43.240 08/17/2002 - 08/23/2002

Telnet Activity for 137.72.43.141 on p390 137.72.43.240 08/17/2002 - 08/23/2002

Figure 148. Selected Telnet User Report

Tabular Report - Selected Telnet User Report

The tabular report format provides the same basic information as the graphical report format.

The fields on the Selected Telnet User tabular report are:

Time	Interval during which the Telnet session terminated.
Number of Bytes	Total number of bytes (for Telnet server only).
Number of Sessions	Total number of sessions.

Selected Telnet User – Detail List

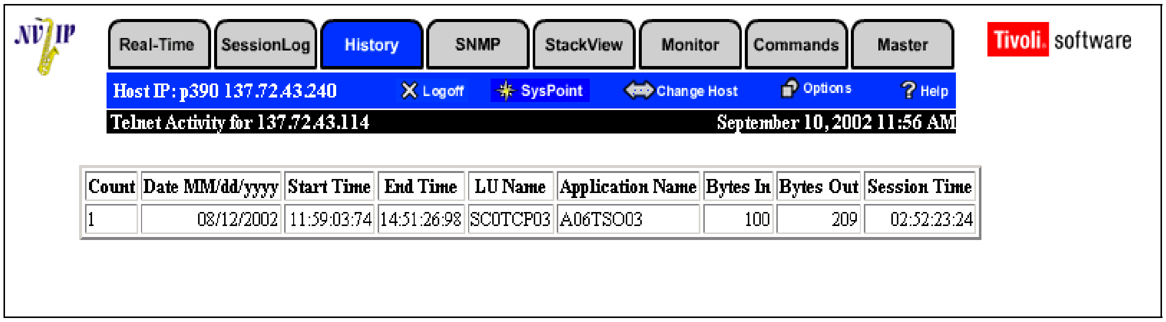
This report allows you to view the Telnet client or server sessions for a selected user for the time period chosen.

The data provided in this report is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it will be recorded at the time it terminates.

This report is available in Tabular Report format only.

Tabular Report - Selected Telnet User – Detail List

The tabular report format provides the same basic information as the graphical report format. Required fields are Start Date and Address.



Host IP: p390 137.72.43.240

Telnet Activity for 137.72.43.114 September 10, 2002 11:56 AM

Count	Date MM/dd/yyyy	Start Time	End Time	LU Name	Application Name	Bytes In	Bytes Out	Session Time
1	08/12/2002	11:59:03:74	14:51:26:98	SC0TCP03	A06TSO03	100	209	02:52:23:24

Figure 149. Selected Telnet User – Detail List

The fields for Telnet server are:

Count	Identifier for the session.
Date	Start date of session (mm/dd/yyyy)
Start Time	Start time of session (hh:mm:ss)
End Time	End time of session (hh:mm:ss)
LU Name	SNA Logical Unit name
Application Name	Name of the Telnet application used
Bytes In	Bytes in to the Telnet server (MVS TCP/IP only). This field is available for Telnet server only.
Bytes Out	Bytes out to the remote IP address. This field is available for Telnet server only.
Session Time	The duration of the session (hh:mm:ss:SS)

The fields for Telnet client sessions are:

Date	Start date of session (mm/dd/yyyy)
Start Time	Start time of session (hh:mm:ss)
End Time	End time of session (hh:mm:ss)
STC Name	STC (user ID)
NJE Node	NJE node name
Session Time	The duration of the session (hh:mm:ss)

Application Based Reports for Telnet

Application Based Reports offer information regarding Telnet applications through the following reports:

- Top Telnet Applications/STCs
- Selected Telnet Application/STC

Top Telnet Applications/STCs

This report allows you to view the Telnet client or server applications that had the most sessions for the time period chosen. A Telnet server session is initiated by the remote IP address. A Telnet client session is initiated by the MVS TCP/IP host. The application reports are available for Telnet server only. The STC (user ID) reports are available for Telnet client only.

The data provided in this report is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it is recorded at the time it terminates.

Graphical Report - Top Telnet Applications/STCs

Data may be viewed weekly by day, or daily by hour. Required fields are Start Date and How Many. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.

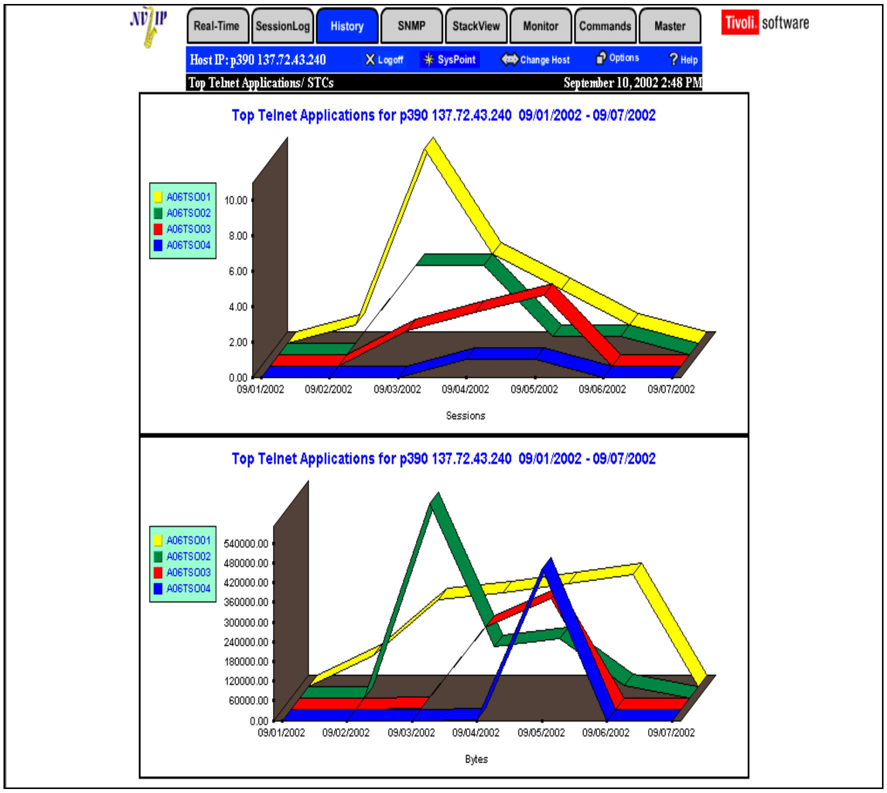


Figure 150. Top Telnet Applications/STCs

Tabular Report - Top Telnet Applications/STCs

The tabular report format provides the same basic information as the graphical report format.

The fields on the Top Telnet Applications/STCs tabular report are:

Application Name	Telnet application name (for Telnet server only).
STC	User ID (for Telnet client only).
Time	Interval during which the Telnet session terminated.
Number of Bytes	Total number of bytes (for Telnet server only).
Number of Sessions	Total number of sessions.

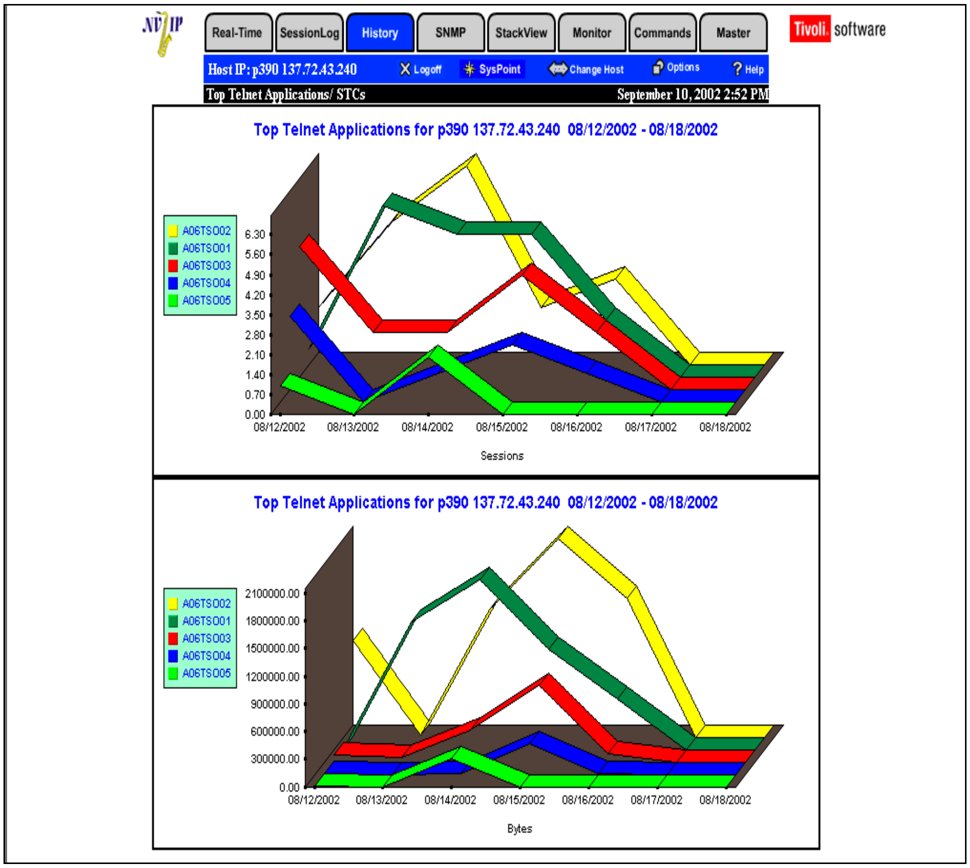
Selected Telnet Application/STC

This report allows you to view the sessions or bytes for a specific Telnet client or server application for the time period chosen. A Telnet server session is initiated by the remote IP address. A Telnet client session is initiated by the MVS TCP/IP host. The application reports are available for Telnet server only. The STC (user ID) reports are available for Telnet client only.

The data provided in this report is session-based. That is, the session counts are done based on a session initiation and termination record. If no session termination record exists for some reason, there will not be a record of the session. Remember also, that the session is recorded at the time that it finishes. The session may have lasted for 8 hours, but it is recorded at the time it terminates.

Graphical Report - Selected Telnet Application/STC

Data may be viewed weekly by day, or daily by hour. Required fields are Start Date and Application/STC Name. Use the Change Graph option to select the type of graph, background, colors, legends, and many other parameters. Charts are available in two or three dimensions.



Host IP: p390 137.72.43.240

Top Telnet Applications/ STCs September 10, 2002 2:52 PM

Figure 151. Selected Telnet Application/STC

Tabular Report - Selected Telnet Application/STC

The tabular report format provides the same basic information as the graphical report format.

The fields on the Selected Telnet Application/STC tabular report are:

Time	Interval during which the Telnet session terminated.
Number of Bytes	Total number of bytes (for Telnet server only).
Number of Sessions	Total number of sessions.

Buffer Reports

Buffer reports include:

- CSM History
- VTAM History

CSM History

The CSM History (Communications Storage Manager) buffer pools are a critical storage resource shared between SNA and TCP/IP. The CSM History includes the following:

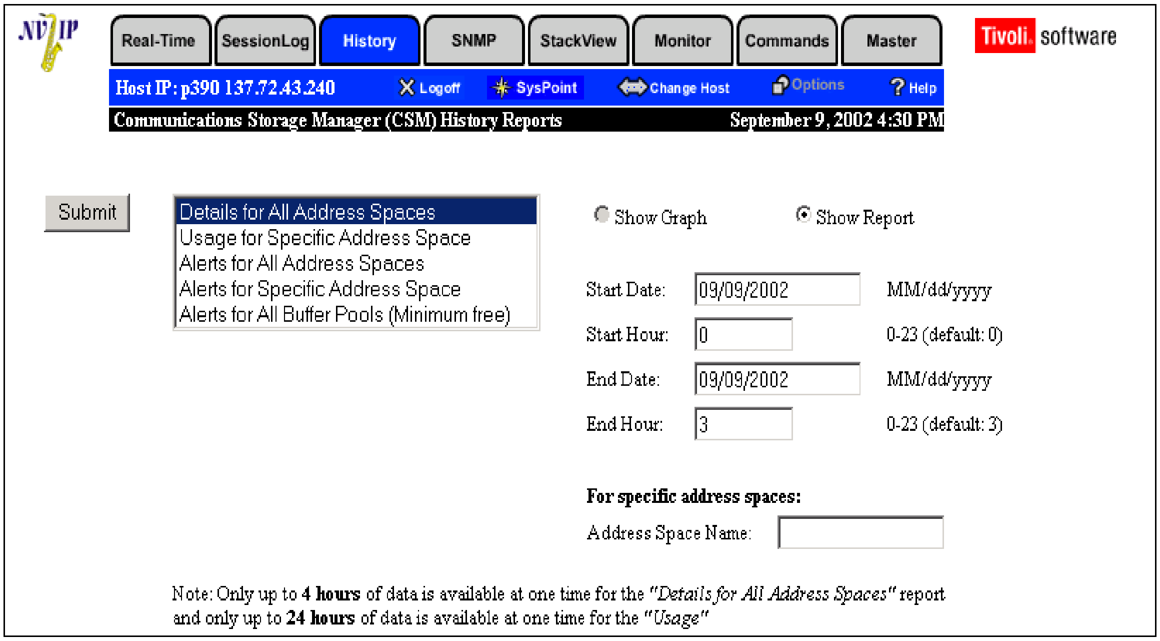
- CSM History Reports
- CSM Details Report
- CSM Address Space Alerts
- CSM Alerts for Buffer Pools

CSM History Reports

The data provided is collected via periodic D NET,CSM,OWNERID=ALL commands issued by the Host Monitor and saved in VSAM data sets. The parameter governing the time interval for the periodic collection is: CSMBUFINTERVAL, set in CONF00.

To view a CSM History Report, perform the following steps:

1. Click on the History tab.
2. Click the CSM History hyperlink under Buffer. The Communications Storage Manager (CSM) History Reports main screen appears.



NV IP
Real-Time
SessionLog
History
SNMP
StackView
Monitor
Commands
Master
Tivoli software
Logoff
SysPoint
Change Host
Options
Help
Submit
Details for All Address Spaces
Usage for Specific Address Space
Alerts for All Address Spaces
Alerts for Specific Address Space
Alerts for All Buffer Pools (Minimum free)

Host IP: p390 137.72.43.240

Communications Storage Manager (CSM) History Reports September 9, 2002 4:30 PM

○ Show Graph ● Show Report

Start Date: 09/09/2002 MM/dd/yyyy

Start Hour: 0 0-23 (default: 0)

End Date: 09/09/2002 MM/dd/yyyy

End Hour: 3 0-23 (default: 3)

For specific address spaces:

Address Space Name:

Note: Only up to **4 hours** of data is available at one time for the *"Details for All Address Spaces"* report and only up to **24 hours** of data is available at one time for the *"Usage"*

Figure 152. Communications Storage Manager (CSM) History Reports Filter

3. Choose Show Graph or Show Report.
4. Select the report you wish to view.
5. Enter the starting date for the data you wish to view.
6. Enter the starting hour for the data you wish to view. If this field is left blank, the starting hour is assumed to be zero (midnight).
7. Select the number of hours of data you wish to view starting at the hour specifed: one hour, two hours, or three hours.
8. To view a report for a specific address space, enter the address space name.
9. To view a report for a specific buffer pool, select the buffer pool name.
10. Click Submit. The report screen appears.
11. Use the Back button on your browser to move between screens.

The historical reports for CSM buffer pools are designed to allow global views of buffer activity as well as detailed views of specific buffer pool or address space activity.

The following reports are provided:

Details for All Address Spaces/Usage for Specific Address Space	Graph or tabular report (All Address Spaces is tabular only) that shows the number of buffers used for all buffer pools for all address spaces or for a particular address space when an ownerid is specified in CSM for the time period chosen.
Alerts for All Address Spaces /Alerts for Specific Address Space	Graph or tabular report of the total ECSA or DSP used when the threshold for ECSA or DSP usage is exceeded for all address spaces or for a specific address space when an ownerid is specified in CSM for the time period chosen.
Alerts for All Buffer Pools (Minimum free)	Graph or tabular report of the total storage used when the storage in the buffer pool falls below the threshold for the minimum percent free in the time period chosen.

Details for All Address Spaces

The Details for All Address Spaces report allows you to view the number of buffers used for all CSM buffer pools for all address spaces or a particular address space for the time period chosen. (The All Address Space report is available in tabular format only.) Only address spaces with an ownerid specified in CSM for the time period chosen is shown.

The data is collected via periodic D NET,CSM,OWNERID=ALL commands issued by the Host Monitor and saved in VSAM data sets. The parameter governing the time interval for the periodic collection is: CSMBUFINTERVAL, set in CONF00.

The fields in this report are:

Date	Date the sample (D NET,CSM,OWNERID=ALL) was taken.
Time	Time the sample (D NET,CSM,OWNERID=ALL) was taken.
Address Space Name	Name of the address space assigned as the ownerid for the CSM buffer pool. This entry displays *TOTAL* to designate the total for all address spaces when no ownerid is specified.
ECSA 4K	The amount of storage, in KB, used by this address space in the ECSA 4K buffer pool.
ECSA 16K	The amount of storage, in KB, used by this address space in the ECSA 16K buffer pool.
ECSA 32K	The amount of storage, in KB, used by this address space in the ECSA 32K buffer pool.
ECSA 60K	The amount of storage, in KB, used by this address space in the ECSA 60K buffer pool.
ECSA 180K	The amount of storage, in KB, used by this address space in the ECSA 180K buffer pool.
DSP 4K	The amount of storage, in KB, used by this address space in the DSP 4K buffer pool.
DSP 16K	The amount of storage, in KB, used by this address space in the DSP16K buffer pool.
DSP 32K	The amount of storage, in KB, used by this address space in the DSP 32K buffer pool.
DSP 60K	The amount of storage, in KB, used by this address space in the DSP 60K buffer pool.
DSP 180K	The amount of storage, in KB, used by this address space in the DSP 180K buffer pool.
Date	Date the sample (D NET,CSM,OWNERID=ALL) was taken.

Alerts for All Address Spaces/Alerts for Specific Address Space

The Alerts for All Address Spaces/Alerts for Specific Address Space reports and graphs allow you to view the Alerts for all address spaces or for a particular address space during the specified time period. Only address spaces with an ownerid specified in CSM for the time period chosen is shown. The Alerts show when the threshold total number of buffers used for ECSA or DSP is exceeded by a particular address space.

The data is collected via Alerting and monitoring performed by the Host Monitor. The Alert threshold for total ECSA and DSP may be set as a parameter to the Host Monitor started task.

The fields in this report are:

Date	Date of Alert.
Time	Time of Alert.
Address Space Name	Name of the address space assigned as the ownerid for the CSM buffer pools when Alert occurred.
Total ECSA	Total amount of storage, in KB or MB, used by this address space in all ECSA buffer pools.
Total DSP	Total amount of storage, in KB or MB, used by this address space in all DSP buffer pools.

CSM Alerts for Buffer Pool

The CSM Alerts for Buffer Pool report or graph allows you to view the total storage used when the storage in the buffer pool falls below the threshold for minimum percent free for the time period chosen.

The data provided in these reports is collected via Alerting and monitoring performed by the Host Monitor. The minimum percent free threshold may be set as a parameter to the Host Monitor started task.

The fields in this report are:

Date	Date of Alert.
Time	Time of Alert.
Buffer Pool Name	Name of the buffer pool (ECSA or DSP).
Storage Used	Total amount of storage, in KB, in use by this buffer pool.
FreeStorage	Total amount of free storage, in KB, for this buffer pool.

Note: The sum of the total storage allocated to all users of a particular pool may be greater than the total amount of storage allocated to that pool. This is due to the existence of multiple instances of a buffer created when an application program issues the IVTCSM ASSIGN_BUFFER macro. The storage displayed for each OWNERID indicates the amount of storage that must be freed by the user to enable the storage to be returned to the buffer pool.

VTAM Buffer History

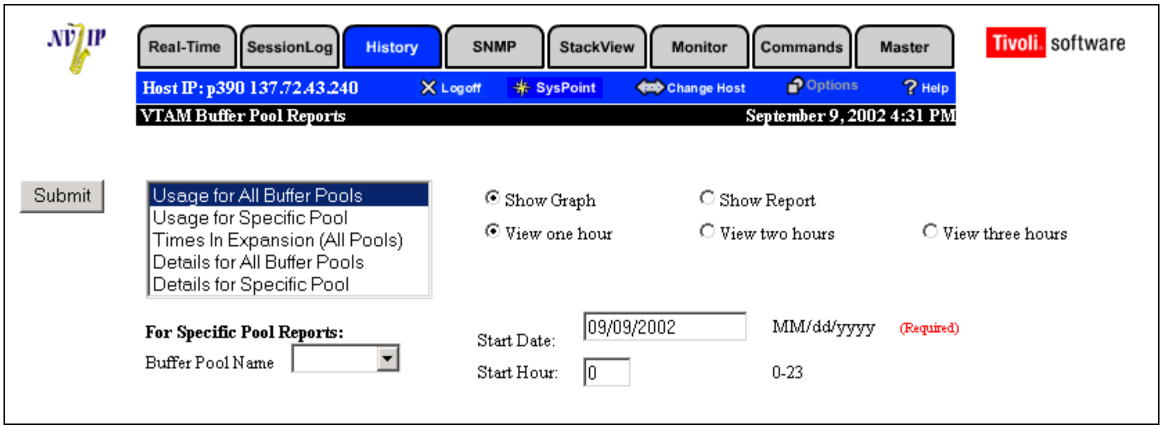
VTAM buffer pools are a critical storage resource shared between SNA and TCP/IP. The VTAM Buffer History reports provide both a global and a detailed view of this shared resource. The reports include:

- Usage for all buffer pools or a specific buffer pool
- Times in Expansion
- Detailed usage per Interval

The data provided in these reports is collected via periodic D NET,BFRUSE commands issued by the Host Monitor and saved in VSAM data sets. The parameter governing the time interval for the periodic collection is: VTAMBUFINTERVAL which is set in CONF00.

To view a VTAM Buffer Pool History Report, perform the following steps:

1. Click on the History tab.
2. Click the VTAM Buffer History hyperlink. The VTAM Buffer Pool Reports main screen appears.



Host IP: p390 137.72.43.240

VTAM Buffer Pool Reports September 9, 2002 4:31 PM

Usage for All Buffer Pools
Usage for Specific Pool
Times In Expansion (All Pools)
Details for All Buffer Pools
Details for Specific Pool

● Show Graph ○ Show Report
● View one hour ○ View two hours ○ View three hours

For Specific Pool Reports:
Buffer Pool Name

Start Date: 09/09/2002 MM/dd/yyyy (Required)
Start Hour: 0 0-23

Figure 153. VTAM Buffer Pool Reports Filter

3. Check either the Show Graph or Show Report radio button.
4. Select the type of report you wish to view from the Report list.
5. Enter a Start Date for the data you wish to view. The year must be four digits.
6. Enter a Start Hour for the data you wish to view. If you do not enter a Start Hour, it is assumed to be zero (midnight).
7. Check one of the View {number} Hours radio boxes for the number of hours of data you wish to view starting at the hour specifed in the Start Hour field.
8. Select a buffer pool name if you are doing a report for a specific buffer pool.
9. Click Submit. The report screen appears if data was found for your selection criteria.
10. Use the Back Arrow on your browser to return to the VTAM Buffer Pool Reports screen.
11. If you would like to view a different type of report, select it from the Report list and repeat Steps 5-10.

The following reports are provided:

Usage for All Buffer Pools	Graphs or tabular reports of the number of buffers used for all buffers for the time period chosen.
Usage for Specific Pool	Graphs or tabular reports of the number of buffers used for a specific buffer for the time period chosen.
Times in Expansion (All Pools)	Graphs or tabular reports of the number of buffers used for all buffers when the buffer pool is in dynamic expansion mode for the time period chosen.
Details for All Buffer Pools	Tabular report of all data gathered for all buffers for the time period chosen.
Details for Specific Pool	Tabular report of all data gathered for a specific buffer for the time period chosen.

VTAM Buffer Pool Usage

The VTAM Buffer Pool Usage reports and graphs allow you to view the buffer usage for all buffer pools or a specific buffer pool for during the specified time period.

The data in these reports is collected via periodic D NET,BFRUSE commands issued by the Host Monitor and saved in VSAM data sets. The parameter governing the time interval for the periodic collection is: VTAMBUFINTERVAL, which is set in CONF00.

Note: You must explicitly set VTAMBUFINTERVAL in CONF00; if you do not, the data will not be collected.

The fields in this report are:

Date	Date the sample (D NET,BFRUSE) was taken.
Time	Time the sample (D NET,BFRUSE) was taken.
Sample #	The sample number within the interval requested.
Buffer Pool Name	Name of the VTAM buffer pool.
Current Used	The number of buffers currently used in the pool.
Current Available	The number of buffers currently available for use.
Max Used	The maximum number of buffers ever used within the pool (since the last SMS trace record was written, if an SMS trace is active).

VTAM Buffer Pool Times in Expansion

The VTAM Times in Expansion reports allow you to view data of the number of buffers used for all buffers when the buffer pool is in dynamic expansion mode during the specified time period.

The data provided in these reports is collected via periodic D NET,BFRUSE commands issued by the Host Monitor and saved in VSAM data sets. The parameter governing the time interval for the periodic collection is VTAMBUFINTERVAL, which is set in CONF00.

Note: You must explicitly set VTAMBUFINTERVAL in CONF00; if you do not, the data will not be collected.

VTAM Buffer Pool Details

The VTAM Buffer Pool Details reports allow you to view all the data collected in a sample for all buffer pools or for a specific buffer pool for a selected time period.

The data in these reports is collected via periodic D NET,BFRUSE commands issued by the Host Monitor and saved in VSAM data sets. The parameter governing the time interval for the periodic collection is: VTAMBUFINTERVAL, which is set in CONF00.

Note: You must explicitly set VTAMBUFINTERVAL in CONF00; if you do not, the data will not be collected.

The fields in this report are:

Date	Date the sample (D NET,BFRUSE) was taken.
Time	Time the sample (D NET,BFRUSE) was taken.
Sample #	The sample number within the interval requested.
Buffer Pool Name	Name of the VTAM buffer pool.
Buffer Size	The size, in bytes, of each buffer. (Note that for certain buffer pools, such as IOBUF, the size displayed might not match the size specified in the buffer pool start options because VTAM increases the size of some buffers for buffer headers that must be added.
Expansion Increment	The number of buffers to be added during each expansion.
Times Expanded	The number of times that the buffer pool has been expanded (since the last SMS trace record was written, if an SMS trace is active).
Expansion Threshold	The number of available buffers at or below which expansion will occur.
Contraction Threshold	The number of available buffers at or above which contraction will be attempted.
Current Total	The number of buffers currently assigned to the pool.
Current Available	The number of buffers currently available for use.
Max Used	The maximum number of buffers ever used within the pool (since the last SMS trace record was written, if an SMS trace is active).
Max Total	The maximum number of buffers ever assigned to the pool (since the last SMS trace record was written, if an SMS trace is active).
Expansion Limit	The maximum size for the pool. Only applies to the IOBuf pool.
Buffers Requested	Number of buffers requested. Only applied to the IOBuf pool.

TraceRoute Reports

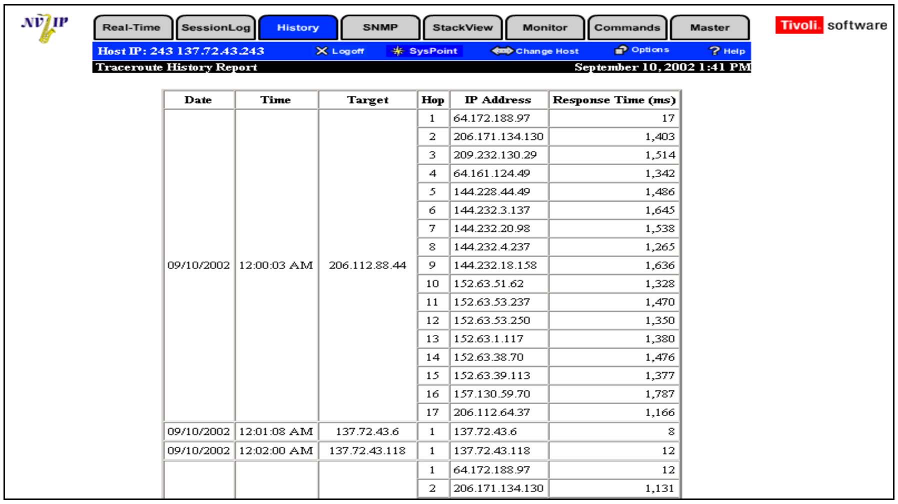
TraceRoute lets you view TCP/IP route and segment information. The TraceRte command sends UDP requests with varying Time to Live values (TTL). It waits for the routers between the local and remote hosts to send TTL exceeded messages. Use it to monitor response time from hop-to-hop and to diagnose network problems.

TraceRoute History

The TraceRoute History report allows you to view the results of the TraceRte command when thresholds for defined critical resources have been exceeded. It also shows availability of devices. When a device has not responded to a PING command, "No Data Found" displays for that device.

The TraceRte command is executed automatically for each device defined as a critical resource when AUTOTRACEROUTE has been set in the CONFxx file on the Host. If AUTOTRACEROUTE has not been set, the TraceRoute History report is not generated. The data provided in these reports is collected via the monitoring and Alerting performed by the Host Monitor.

The Host IP Address displays in the menu bar of the report below the tabs at the top of the screen.



Host IP: 243 137.72.43.243

Traceroute History Report

September 10, 2002 1:41 PM

Date	Time	Target	Hop	IP Address	Response Time (ms)
09/10/2002	12:00:03 AM	206.112.88.44	1	64.172.188.97	17
			2	206.171.134.130	1,403
			3	209.232.130.29	1,514
			4	64.161.124.49	1,342
			5	144.228.44.49	1,486
			6	144.232.3.137	1,645
			7	144.232.20.98	1,538
			8	144.232.4.237	1,265
			9	144.232.18.158	1,636
			10	152.63.51.62	1,328
			11	152.63.53.237	1,470
			12	152.63.53.250	1,350
			13	152.63.1.117	1,380
			14	152.63.38.70	1,476
			15	152.63.39.113	1,377
			16	157.130.59.70	1,787
			17	206.112.64.37	1,166
09/10/2002	12:01:08 AM	137.72.43.6	1	137.72.43.6	8
09/10/2002	12:02:00 AM	137.72.43.118	1	137.72.43.118	12
			1	64.172.188.97	12
			2	206.171.134.130	1,131

Figure 154. TraceRoute History Report

The fields in this report are:

Date	Date the TraceRte command was initiated.
Time	Time the TraceRte command was initiated.
Target	IP Address of the remote destination device.
Hop	The hop numbers of each hop taken, in consecutive order.
IP Address	IP address of each hop.
Response Time (ms)	Response time (ms) between the Host and each hop.

Commands

Command menus are provided in the following categories: Route Display (OSPF, RIP, and Route Table), Route Diagnostic (IP: TraceRoute and Ping; EE/HPR: D NET,APING and D NET,RTPS), USS (D OMVS), and Communication Server (Netstat, VTAM, and Storage). Only Master and Operations Manager users have full command authority. Performance Manager can issue display only commands.

To execute a command, perform the following steps:

1. From the Commands main screen, click the command hyperlink for the command you want to execute:
   - **Route Display Commands**
     - OSPF
     - RIP
     - Route Table
   - **Route Diagnostic Commands**

     IP
     - Ping
     - TraceRoute

     EE/HPR
     - D NET,APING
     - D NET,RTPS
   - **USS Commands**
     - OMVS
   - **Communication Server Commands**
     - Netstat
     - Storage
     - VTAM

Note: You can also access the OMPRoute (OSPF, RIP, and Route Table), Netstat (Gateways and VIPA), and VTAM command menus by clicking their corresponding buttons in the LinkView screen. See the LinkView section for more information.

2. Enter the desired parameters for the command.
3. Click Submit. The command output screen is displayed for the selected link, port, client or address.

Route Display Commands

Route Display Commands include:

- OSPF, RIP and Route Table

OSPF, RIP and Route Table

OSPF and RIP are dynamic Interior Gateway Protocols (IGP), Internet protocols which provide routing information to the routers within an autonomous network. The OMPRoute program application allows you to specify OSPF and/or RIP protocols. The following provides a description of each protocol:

OSPF	OSPF is classified as an Interior Gateway Protocol (IGP). The OSPF protocol is based on link-state or shortest path first (SPF) technology. The OMPROUTE program application implements OSPF Version 2 and the OSPF subagent protocols. OSPF commands may be submitted to display OSPF configuration and state information.
RIP	RIP is an Interior Gateway Protocol (IGP) designed to manage a relatively small network. RIP is based on the Bellman-Ford or the distance-vector algorithm. The OMPROUTE program application implements RIP Version 1 and Version 2 protocols. RIP commands may be submitted to display RIP configuration and state information.
Route Table	You may choose to view the Route Table information. You may view all route table configurations or obtain information about a particular route. When multiple equal-cost routes exist, you may use commands to obtain a list of the next hops. ***Note:*** This is not the TCP/IP route table, but the OMPRoute route table.

Route Diagnostic Commands

Route Diagnostic Commands include;

- (IP) Ping and TraceRoute
- (EE/HPR) D NET,APING and D NET,RTPS

(IP) Ping and TraceRoute

Ping is used to diagnose TCP/IP network problems dealing with availability and response time. The Ping command sends an echo request to a foreign node to determine if the computer is accessible. When the response to the Ping command is received, the elapsed time is displayed. The time does not include the time spent communicating between the user and the TCP/IP address space.

The TraceRte command sends UDP requests with varying Time to Live values (TTL). It waits for the routers between the local and remote hosts to send TTL exceeded messages. Use it to monitor response time from hop-to-hop and to diagnose network problems over routes and segments.

(EE/HPR) D NET,APING and D NET,RTPS

D NET,APING performs a VTAM-based Advanced Peer to Peer Networking (APPN) Ping test from the originating host to the remote host. The D NET,APING command is the VTAM-based equivalent of the TCP/IP Ping command. D NET,APING is used to diagnose APPN availability and response time issues for a specific APPN Transmission Group (TG) that may be defined between two APPN endpoints, or to test network connectivity of Enterprise Extender links.

The D NET,RTPS Route Test provides the ability to quickly perform a VTAM-based RTP (Rapid Transport Protocol) Route Test across the 'HPR or RTPS pipe' for any Enterprise Extender (EE) connection to a specific RTP endpoint. In most EE environments this endpoint will usually be the same destination as the previously defined VTAM Cross Domain (CDRM) and associated Control Point (CP). The new RTP data transport, however, uses UDP and IP between both endpoints instead of SNA.

EE leverages the tactical combination of SNA (Systems Network Architecture) and APPN/HPR (Advanced Peer to Peer Networking/High Performance Routing) on each end of a connection along with TCP/IP. The data is transported quickly and efficiently through the use of UDP over the IP topology network located between the two endpoints. In a corporate environment there may be several different RTP endpoints defined for one EE link. In addition, as with any network link, there may be situations in which you need to determine if a specific EE link is connected and communicating. It is also helpful to know the routing path the link is using, especially when the link may transverse multiple nodes or control points.

The D NET,RTPS Route test is comparable to the TCP/IP-based Tracerte command because it sends multiple "route test" messages that "wrap around" as they reach each node along the pipe's path. This behavior is similar to the Time-to-Live (TTL) feature of the tracert command. As a result of this "wrap-around" behavior, you can easily measure 'internodal' transit times, which can be very helpful in determining current network-based response times going through a specific EE link. From this response time data you can identify any network bottlenecks that may exist in the RTP's path.

Note: The D NET,RTPS Route Test function is only available in z/OS V.1.2 and later. If you are using an earlier version, the D NET,RTPS Route Test will only return a display of the current status of all RTPs. You can utilize the D NET,APING command to test EE connectivity for an APPN Transmission Group regardless of the z/OS version you are using.

USS D OMVS Command

The D OMVS command is a UNIX System Services command used to display and diagnose current OMVS-based settings and associated processes, such as file structures, applications, user services, and servers. D OMVS is usually referred to as UNIX System Services or USS, and runs as a started task under MVS with a default name of BPXOINIT. Many operations have chosen to initiate some or most of their TCP/IP 'stack-based' tasks via USS, including the FTP Daemon (FTPD). Default allocations are made in a Parmlib member for USS (BPXPRMxx), in the same way as in other major MVS subsystems. Maximum values or limits are set for resource types such as the maximum number of concurrent processes (MAXPROCSYS) and the maximum number of concurrent threads (MAXTHREADS).

USS values may apply system-wide or specifically for any single USS-based process. Occasionally these values can reach critical mass and will no longer operate properly as a result. A specific process may not behave properly at other times as well. Because USS is so tightly woven with TCP/IP, this behavior can significantly impact the stability of the TCP/IP stack as well. USS must have at least one Common INET (CINET) routing transport link reachable in order for it to communicate with TCP/IP. Because of this, efficient, proactive use of the D OMVS command may uncover some of these potential problems and corrective action can be taken to alleviate the situation, such as modifying OMVS settings with the SETOMVS command.

Communication Server Commands

Commuication Servers uses these commands:

- Netstat
- Storage
- VTAM

Netstat Command

The Netstat command is used to diagnose network problems and control network activity. It is used to show the status of links, foreign ports, clients, and socket-attached applications. Once you have selected the options desired and setup any necessary filters, submit the command to the TCP/IP on the MVS host you designated.

Storage Commands

Storage commands may be submitted to display shared storage such as CSM or VTAM buffer pools. The Communications Storage Manager (CSM) is a component of VTAM that allows authorized host applications to share data with VTAM and other CSM users without having to physically copy the data. CSM shortages may impact response time. VTAM buffer pools are used by TCP/IP for applications such as CICS sockets, Telnet, FTP and others. The buffer pool types specifically used by TCP/IP include: IOBUF, LFBUF, CRPLBUF, TIBUF, and CRA4.

VTAM Commands

VTAM commands may be submitted to diagnose network problems for resources. You may execute Display (D Net), Vary Active (V Net,Act), Vary Inactive (V Net,Inact), or Modify (F Net) commands. The Display command is available to all users. The other commands require security authorization. If you do not have the appropriate authority, these commands will not display.

Using Route Display Commands

The OMPROUTE program application implements the OSPF protocol described in RFC 1583 (OSPF Version 2), the OSPF subagent protocol described in RFC 1850, and the RIP protocols described in RFC 1058 (RIP Version 1) and in RFC 1723 (RIP Version 2). It provides an alternative to the static TCP/IP gateway definitions by allowing you to specify these dynamic routing protocols. The MVS host running with OMPROUTE becomes an active OSPF or RIP router, or both in a TCP/IP network. Either or both of these routing protocols can be used to dynamically maintain the host routing table. For example, OMPROUTE detects when a route is created, is temporarily unavailable, or if a more efficient route exists. If both OSPF and RIP protocols are used simultaneously, OSPF routes are preferred over RIP routes to the same destination. You can also view route table configuration with the Route Table command under OMPRoute.

Using OSPF (Open Shortest Path First) Commands

OSPF(Open Shortest Path First) is classified as an Interior Gateway Protocol (IGP). This means that it distributes routing information between routers belonging to a single Autonomous System (AS), a group of routers all using a common routing protocol. The OSPF protocol is based on link-state or shortest path first (SPF) technology. It has been designed expressly for the TCP/IP Internet environment, including explicit support for IP subnetting and the tagging of externally derived routing information.

OSPF performs the following tasks:

- Multiple Routes: Provides support for multiple equal-cost routes
- Authentication: Provides for the authentication of routing updates
- IP Multicast: Uses IP multicast when sending or receiving the updates
- Area Routing: Capability Area routing capability enables an additional level of routing protection and a reduction in routing protocol traffic.
- Allows Network Grouping: Allows sets of networks to be grouped together. Such a grouping is called an area. The topology of an area is hidden from the rest of the Autonomous System. This method of hiding information enables a significant reduction in routing traffic. Also, routing within the area is determined only by the area's own topology, lending the area protection from bad routing data. An area is a generalization of an IP subnetted network.
- IP Subnet Configuration: Enables the flexible configuration of IP subnets. Each route distributed by OSPF has a destination and mask. Two different subnets of the same IP network number may have different sizes (that is, different masks). This is commonly referred to as variable length subnetting. A packet is routed to the best (longest or most specific) match. Host routes are considered to be subnets whose masks are "all ones" (0xFFFFFFFF).

- Authenticate OSPF Protocol Exchanges: Can be configured such that all OSPF protocol exchanges are authenticated. This means that only trusted routers can participate in the Autonomous System's routing. A single authentication scheme is configured for each area. This enables some areas to use authentication while others do not. OSPF is a dynamic routing protocol. It quickly detects topological changes in the AS (such as router interface failures) and calculates new loop-free routes after a period of convergence. This period of convergence is short and involves a minimum of routing traffic as compared to RIP protocol.

In a link-state routing protocol, each router maintains a database describing the Autonomous System's topology. Each participating router has an identical database. Each individual piece of this database is a particular router's local state (for example, the router's usable interfaces and reachable neighbors). The router distributes its local state throughout the Autonomous System by flooding.

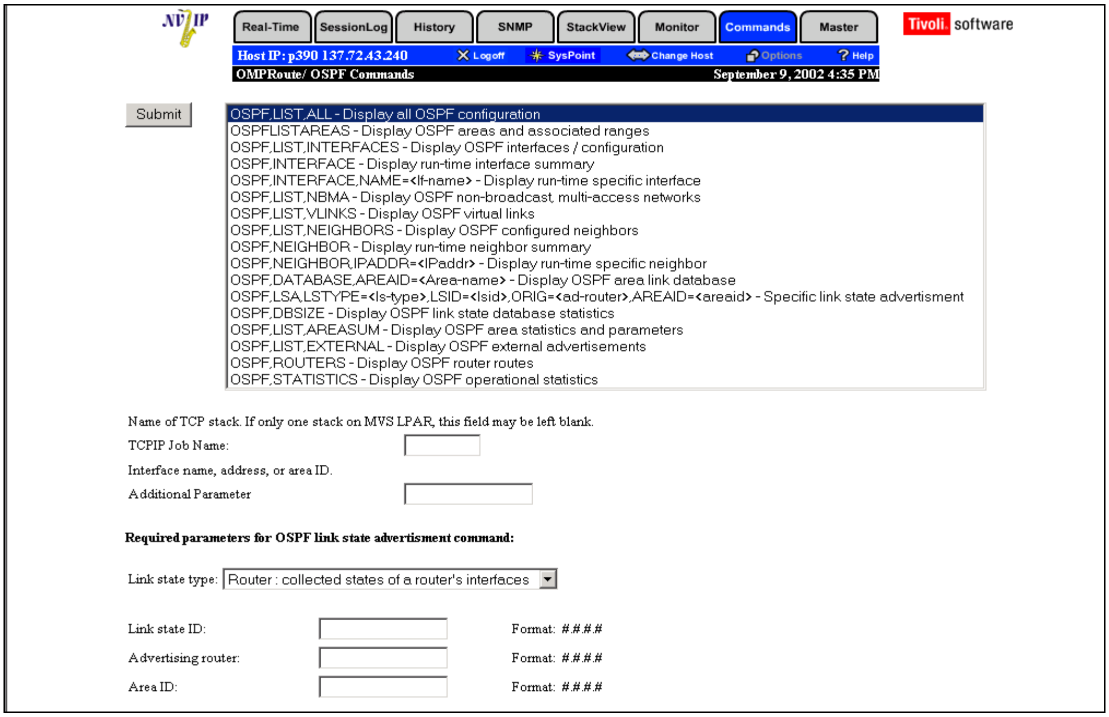
All routers run the exact same algorithm, in parallel. From the topological database, each router constructs a tree of shortest paths with itself as root. This shortest-path tree gives the route to each destination in the Autonomous System. Externally derived routing information appears on the tree as leaves. When several equal-cost routes to a destination exist, the routes (up to four) are added to the TCP/IP stack's route table. The TCP/IP stack uses these equal-cost routes according to the IPCONFIG MULTIPATH statement.

Externally derived routing data (for example, routes learned from the RIP protocol) is passed transparently throughout the Autonomous System. This externally derived data is kept separate from the OSPF protocol's link state data. Each external route can also be tagged by the advertising router, enabling additional information to be passed between routers on the boundaries of the Autonomous System.

Using Assisted OSPF Commands

Complete the following steps:

1. From the Commands main menu, click the OSPF hyperlink under Route Display Commands. The OMPRoute/OSPF Commands main screen appears.



Host IP: p390 137.72.43.240

OMPRoute/ OSPF Commands

September 9, 2002 4:35 PM

OSPF,LIST,ALL - Display all OSPF configuration
OSPFLISTAREAS - Display OSPF areas and associated ranges
OSPF,LIST,INTERFACES - Display OSPF interfaces / configuration
OSPF,INTERFACE - Display run-time interface summary
OSPF,INTERFACE,NAME=<If-name> - Display run-time specific interface
OSPF,LIST,NBMA - Display OSPF non-broadcast, multi-access networks
OSPF,LIST,VLINKS - Display OSPF virtual links
OSPF,LIST,NEIGHBORS - Display OSPF configured neighbors
OSPF,NEIGHBOR - Display run-time neighbor summary
OSPF,NEIGHBOR,IPADDR=<IPaddr> - Display run-time specific neighbor
OSPF,DATABASE,AREAID=<Area-name> - Display OSPF area link database
OSPF,LSA,LSTYPE=<ls-type>,LSID=<lsid>,ORIG=<ad-router>,AREAID=<areaid> - Specific link state advertisment
OSPF,DBSIZE - Display OSPF link state database statistics
OSPF,LIST,AREASUM - Display OSPF area statistics and parameters
OSPF,LIST,EXTERNAL - Display OSPF external advertisements
OSPF,ROUTERS - Display OSPF router routes
OSPF,STATISTICS - Display OSPF operational statistics

Name of TCP stack. If only one stack on MVS LPAR, this field may be left blank.

TCPIP Job Name:

Interface name, address, or area ID.

Additional Parameter

Required parameters for OSPF link state advertisment command:

Link state type: Router : collected states of a router's interfaces ▼

Link state ID: Format: #.#.#.#
Advertising router: Format: #.#.#.#
Area ID: Format: #.#.#.#

Figure 155. OMPRoute/OSPF Commands Main Page

2. Click the down triangle to view a drop-down list of the available OSPF commands.

3. Select a command, for example, DISPLAY TCPIP,<tcpipjobname>, OMPROUTE,OSPF,LIST,ALL

> ***Note:*** If you select DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF, INTERFACE,NAME=<if-name> you must enter the Interface Address parameter in the field provided. The address is appended to the end of the command. For example:
> DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,
> INTERFACE,NAME=1.2.3.4

4. Click Submit. The response to the command appears on the next screen.

5. Use your Web browser's commands to:

   - find a particular string in the output
   - obtain hardcopy of the output
   - return to the main menu by clicking the Back arrow

Assisted OSPF Commands

OMPRoute OSPF commands may be submitted to display OSPF configuration and state information. The following commands are available using the assisted mode. The section following this one describes each command in detail.

- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,ALL**
  Lists all OSPF-related configuration information.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,AREAS**
  Lists all OSPF configured areas and ranges.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,INTERFACES**
  Lists IP addresses and configured parameters for each OSPF interface.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,INTERFACE**
  Displays a summary of run-time statistics and parameters related to all OSPF interfaces.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,INTERFACE, NAME=<if-name>**
  Displays run-time statistics and parameters related to a particular OSPF interface.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,NBMA**
  Displays parameters related to OSPF Non-Broadcast, Multi-Access Networks.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,VLINKS**
  Displays parameters related to OSPF Virtual Links.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,NEIGHBORS**
  Displays parameters related to neighboring routers.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,NEIGHBOR**
  Displays a summary of run-time statistics and parameters related to all neighbors.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,NEIGHBOR, IPADDR=<ip-addr>**
  Displays details of run-time statistics and parameters related to a specific neighbor.
- **DISPLAYTCPIP,<tcpipjobname>,OMPROUTE,OSPF,DATABASE, AREAID=<area-id>**
  Displays a summary of all the advertisements in the OSPF database.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LSA,LSTYPE= ls-type,LSID=lsid, ORIG=ad-router,AREAID=area-id**
  Displays parameters related to a specific OSPF link state advertisement.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,DBSIZE**
  Displays link state database statistics.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,AREASUM**
  Displays OSPF area statistics and parameters.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,EXTERNAL**
  Displays OSPF external advertisements.

- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,ROUTERS**
  Displays all calculated routes to other routers present in the routing table.
- **DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,STATISTICS**
  Displays statistics generated by the OSPF routing protocol.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,ALL

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,ALL command lists all OSPF-related configuration information. A sample output with an explanation of entries follows:

```
EZZ7831I GLOBAL CONFIGURATION 967
TRACE LEVEL: 1, DEBUG LEVEL: 0, SADEBUG LEVEL: 0
STACK AFFINITY:   TCPCS6
OSPF PROTOCOL:   ENABLED
EXTERNAL COMPARISON:  TYPE 1
AS BOUNDARY CAPABILITY: ENABLED
IMPORT EXTERNAL ROUTES: RIP SUB
ORIG. DEFAULT ROUTE:  ALWAYS
DEFAULT ROUTE COST:  (1, TYPE 2)
DEFAULT FORWARD. ADDR: 9.167.100.17
DEMAND CIRCUITS:   ENABLED

EZZ7832I AREA CONFIGURATION
AREA ID   AUTYPE   STUB? DEFAULT-COST IMPORT-SUMMARIES?
0.0.0.0   0=NONE   NO   N/A   N/A
2.2.2.2   0=NONE   NO   N/A   N/A

--AREA RANGES--
AREA ID   ADDRESS   MASK    ADVERTISE?
2.2.2.2   9.167.200.0  255.255.255.0 YES
2.2.2.2   9.167.100.0  255.255.255.0 YES

EZZ78331 INTERFACE CONFIGURATION
IP ADDRESS  AREA  COST RTRNS TRNSDLY PRI HELLO DEAD
9.168.100.3  0.0.0.0  1  10  1  1  20  80
9.167.100.13 2.2.2.2  1  10  1  1  20  80

EZZ7836I VIRTUAL LINK CONFIGURATION
VIRTUAL ENDPOINT  TRANSIT AREA  RTRNS TRNSDLY HELLO DEAD
9.67.100.8   2.2.2.2   20  5  40 160


EZZ7835I NBMA CONFIGURATION
INTERFACE ADDR  POLL INTERVAL
9.168.100.3   120

EZZ7834I NEIGHBOR CONFIGURATION
NEIGHBOR ADDR INTERFACE ADDRESS DR ELIGIBLE?
9.168.100.56  9.168.100.3    YES
9.168.100.70  9.168.100.3    NO
```

The fields for this output are:

TRACE LEVEL	Displays the level of tracing currently in use by OMPROUTE.
DEBUG LEVEL	Displays the level of debugging currently in use by OMPROUTE.
SADEBUG LEVEL	Displays the level of debugging currently in use by OMPROUTE's OSPF SNMP subagent.
STACK AFFINITY	Displays the name of the stack on which OMPROUTE is running.
OSPF PROTOCOL	Displays that OSPF is enabled or disabled.
EXTERNAL COMPARISON	Displays the external route type used by OSPF when importing external information into the OSPF domain and when comparing OSPF external routes to RIP routes.
AS BOUNDARY CAPABILITY	Indicates whether the router will import external routes into the OSPF domain.
IMPORT EXTERNAL ROUTES	Indicates the types of external routes that will be imported into the OSPF domain. Displayed only when AS Boundary Capability is enabled.
ORIG DEFAULT ROUTE	Indicates whether the router will originate a default route into the OSPF domain. The Originate Default Route is displayed only when AS Boundary Capability is enabled.
DEFAULT ROUTE COST	Displays the cost and type of the default route (if advertised). The Default Route Cost is displayed only when AS Boundary Capability is enabled.
DEFAULT FORWARD ADDR	Displays the forwarding address specified in the default route (if advertised). The Default Forwarding Address is displayed only when AS Boundary Capability is enabled.
DEMAND CIRCUITS	Indicates whether demand circuit support is available for OSPF interfaces.

The remainder of the DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,ALL output is described in the following sections: Configured OSPF Areas and Ranges, Configured OSPF Interfaces, Configured OSPF Non-Broadcast, Multi-Access Networks, Configured OSPF Virtual Links, and Configured OSPF Neighbors.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,AREAS

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,AREAS command lists all information concerning configured OSPF areas and their associated ranges.

A sample output with an explanation of entries follows:

```
EZZ7832I AREA CONFIGURATION 115
AREA ID   AUTYPE   STUB? DEFAULT-COST IMPORT-SUMMARIES?

0.0.0.0   0=NONE   NO   N/A   N/A
2.2.2.2   0=NONE   NO   N/A   N/A

--AREA RANGES--
AREA ID   ADDRESS   MASK    ADVERTISE?
2.2.2.2   9.167.200.0  255.255.255.0 YES
2.2.2.2   9.167.100.0  255.255.255.0 YES
```

The fields for this output are:

AREA ID	Displays the area ID.
AUTYPE	Displays the method used for area authentication. "Simple-pass" means a simple password scheme is being used for the area authentication.
STUB?	Indicates whether the area is a stub area.
DEFAULT COST	Displays the cost of the default route configured for the stub area.
IMPORT SUMMARIES?	Indicates whether summary advertisements are to be imported into the stub area.
ADDRESS	Displays the network address for a given range within an area.
MASK	Displays the subnet mask for a given range within an area.
ADVERTISE?	Indicates whether a given range within an area is to be advertised.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF, LIST,INTERFACES

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,INTERFACES command lists, for each OSPF interface, the IP address and configured parameters as coded in the OMPROUTE configuration file. A sample output with an explanation of entries follows:

```
EZZ7833I INTERFACE CONFIGURATION 165
IP ADDRESS  AREA    COST RTRNS TRNSDLY PRI HELLO DEAD
9.168.100.3  0.0.0.0    1  10  1  1  20  80
9.167.100.13 2.2.2.2    1  10  1  1  20  80
```

The fields for this output are:

IP ADDRESS	Indicates the IP address of the interface.
AREA	Indicates the OSPF area to which the interface attaches.
COST	Indicates the TOS 0 cost (or metric) associated with the interface.
RTRNS	Indicates the retransmission interval, which is the number of seconds between retransmissions of unacknowledged routing information.
TRNSDLY	Indicates the transmission delay, which is an estimate of the number of seconds required to transmit routing information over the interface. The number of seconds must be greater than zero.
PRI	Indicates the interface router priority, which is used when selecting the designated router.
HELLO	Indicates the number of seconds between Hello Packets sent from the interface.
DEAD	Indicates the number of seconds after not having received an OSPF Hello packet, that a neighbor is declared to be down.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,INTERFACE

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,INTERFACE command displays current, run-time statistics and parameters related to OSPF interfaces. A single line is printed summarizing each interface. A sample output with explanations of entries follow:

```
EZZ7849I INTERFACES 354
IFC ADDRESS  PHYS  ASSOC. AREA TYPE STATE #NBRS #ADJS
9.168.100.3  CTC1  0.0.0.0   P-P  16  0  0
9.167.100.13 CTC2  2.2.2.2   P-P  16  1  1
UNNUMBERED  VL/0  0.0.0.0   VLINK 16  1  1
```

The fields for this output are:

IFC ADDRESS	Interface IP address.
PHYS	Displays the interface name.
ASSOC AREA	Attached area ID.
TYPE	Can be non-broadcast, multi-access, for example, an ATM connection, VLink (an OSPF virtual link), or VIPA (a Virtual IP Address link).

STATE	Can be one of the following: 1 (down) 2 (backup) 4 (looped back) 8 (waiting) 16 (point-to-point) 32 (DR other) 64 (backup DR) 128 (designated router) For more information about these values, refer to RFC 1583.
#NBRS	Number of neighbors. This is the number of routers whose hellos have been received, plus those that have been configured.
#ADJS	Number of adjacencies. This is the number of neighbors in state Exchange or greater. These are the neighbors with whom the router has synchronized or is in the process of synchronization.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE, OSPF,INTERFACE,NAME=<if-name>

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,INTERFACE,NAME=<if-name> command displays current, run-time statistics and parameters related to a specific OSPF interface. A sample output with explanations of entries follows:

```
EZZ7850I INTERFACE DETAILS 356
  INTERFACE ADDRESS:  9.168.100.3
  ATTACHED AREA:   0.0.0.0
  PHYSICAL INTERFACE:  CTC1
  INTERFACE MASK:   255.255.255.0
  INTERFACE TYPE:   P-P
  STATE:     16
  DESIGNATED ROUTER:  0.0.0.0
  BACKUP DR:    0.0.0.0

DR PRIORITY:  1 HELLO INTERVAL: 20 RXMT INTERVAL: 10
DEAD INTERVAL: 80 TX DELAY:   1 POLL INTERVAL:  0
DEMAND CIRCUIT: OFF HELLO SUPPRESS: OFF SUPPRESS REQ: OFF
MAX PKT SIZE: 556 TOS 0 COST:  1

# NEIGHBORS:  0 # ADJACENCIES:  0 # FULL ADJS.:  0
# MCAST FLOODS: 0 # MCAST ACKS:  0
MC FORWARDING: OFF DL UNICAST:  OFF
NETWORK CAPABILITIES: POINT-TO-POINT
```

The fields for this output are:

INTERFACE ADDRESS	Interface IP address.
ATTACHED AREA	Attached area ID.
PHYSICAL INTERFACE	Displays the interface name.
INTERFACE MASK	Displays interface subnet mask.
INTERFACE TYPE	Can be non-broadcast, multi-access, for example, an ATM connection, VLink (an OSPF virtual link), or VIPA (a Virtual IP Address link).

STATE	Can be one of the following: 1 (down) 2 (backup) 4 (looped back) 8 (waiting) 16 (point-to-point) 32 (DR other) 64 (backup DR) 128 (designated router) For more information about these values, refer to RFC 1583.
DESIGNATED ROUTER	IP address of the designated router.
BACKUP DR	IP address of the backup designated router.
DR PRIORITY	Displays the interface router priority used when selecting the designated router.
HELLO INTERVAL	Displays the current hello interval value.
RXMT INTERVAL	Displays the current retransmission interval value.
DEAD INTERVAL	Displays the current dead interval value.
TX DELAY	Displays the current transmission delay value.
POLL INTERVAL	Displays the current poll interval value.
DEMAND CIRCUIT	Displays the current demand circuit status.
HELLO SUPPRESS	Displays whether Hello Suppression is currently on or off.
SUPPRESS REQ	Displays whether Hello Suppression was requested.
MAX PKT SIZE	Displays the maximum size for an OSPF packet sent out this interface.
TOS 0 COST	Displays the interface TOS 0 cost.
# NEIGHBORS	Number of neighbors. This is the number of routers whose hellos have been received, plus those that have been configured.
# ADJACENCIES	Number of adjacencies. This is the number of neighbors in state Exchange or greater.
# FULL ADJS	Number of full adjacencies. This is the number of neighbors whose state is Full (and therefore with which the router has synchronized databases).
# MCAST FLOODS	Number of link state updates flooded out the interface (not counting retransmissions).
# MCAST ACKS	Number of link state acknowledgments flooded out the interface (not counting retransmissions).
NETWORK CAPABILITIES	Displays the capabilities of the interface.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,NBMA

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,NBMA command lists the interface address and polling interval related to interfaces connected to non-broadcast, multi-access networks.

A sample output follows:

```
EZZ7835I NBMA CONFIGURATION 191
   INTERFACE ADDR  POLL INTERVAL
   9.168.100.3   120
```

The fields for this output are:

INTERFACE ADDRESS	Interface IP address.
POLL INTERVAL	Displays the current poll interval value.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,VLINKS

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,VLINKS command lists all virtual links that have been configured with this router as the endpoint. A sample output with an explanation of entries follows:

```
EZZ7836I VIRTUAL LINK CONFIGURATION 202
VIRTUAL ENDPOINT  TRANSIT AREA  RTRNS TRNSDLY HELLO DEAD
9.67.100.8   2.2.2.2    20  5  40 160
```

The fields for this output are:

VIRTUAL ENDPOINT	Indicates the OSPF router ID of the other endpoint.
TRANSIT AREA	Indicates the non-backbone area through which the virtual link is configured. Virtual links are treated by the OSPF protocol similarly to point-to-point networks.
RTRNS	Indicates the retransmission interval, which is the number of seconds between retransmissions of unacknowledged routing information.
TRNSDLY	Indicates the transmission delay, which is an estimate of the number of seconds required to transmit routing information over the interface. The number of seconds must be greater than zero.
HELLO	Indicates the number of seconds between Hello Packets sent from the interface.
DEAD	Indicates the number of seconds after not having received an OSPF Hello packet, that a neighbor is declared to be down.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF, LIST,NEIGHBORS

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LIST,NEIGHBORS command lists the configured neighbors on non-broadcast networks.

A sample output with an explanation of entries follows:

```
EZZ7834I NEIGHBOR CONFIGURATION 205
   NEIGHBOR ADDR  INTERFACE ADDRESS DR ELIGIBLE?
   9.168.100.56  9.168.100.3   YES
   9.168.100.70  9.168.100.3   NO
```

The fields for this output are:

NEIGHBOR ADDR	Indicates the IP address of the neighbor.
INTERFACE ADDRESS	Indicates the IP address of the interface on which the neighbor is configured.
DR ELIGIBLE?	Indicates whether the neighbor is eligible to become the designated router on the net.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,NEIGHBOR

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,NEIGHBOR command displays the statistics and parameters related to OSPF neighbors. A single line is printed summarizing each neighbor. To view details of a specific neighbor, enter the DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,NEIGHBOR,IPADDR=<ip-addr> command. Following is a sample output with explanations of entries for the summary command:

```
 EZZ7851I NEIGHBOR SUMMARY 358
NEIGHBOR ADDR NEIGHBOR ID  STATE LSRXL DBSUM LSREQ HSUP IFC
9.167.100.17 9.67.100.7  128  0  0  0 OFF CTC2
VL/0   9.67.100.8  128  0  0  0 OFF *
```

The fields for this output are:

NEIGHBOR ADDR	Displays the neighbor's interface IP address.
NEIGHBOR ID	Displays the neighbor OSPF router ID.
STATE	Can be one of the following: 1 (Down) 2 (Attempt) 4 (Init) 8 (2-Way) 16 (ExStart) 32 (Exchange) 64 (Loading) 128 (Full) For more information about these values, refer to RFC 1583.
LSRXL	Displays the size of the current link state retransmission list for this neighbor.
DBSUM	Displays the size of the database summary list waiting to be sent to the neighbor.
LSREQ	Displays the number of link state advertisements that are being requested from the neighbor.
HSUP	Displays whether Hello Suppression is active with the neighbor.
IFC	Displays the name of the interface over which a relationship has been established with this neighbor.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,NEIGHBOR, IPADDR=<ip-addr>

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,NEIGHBOR, IPADDR=<ip-addr> command displays the statistics and parameters related to a specific OSPF neighbor. An IP address must be given and detailed statistics for that neighbor are displayed.

To view a summary of all neighbors, enter the

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,NEIGHBOR command.

Following is a sample output with explanations of entries for a detailed display:

```
EZZ7852I NEIGHBOR DETAILS 360
   NEIGHBOR IP ADDRESS: 9.167.100.17
   OSPF ROUTER ID:   9.67.100.7
   NEIGHBOR STATE:   128
   PHYSICAL INTERFACE:  CTC2
   DR CHOICE:    0.0.0.0
   BACKUP CHOICE:   0.0.0.0
   DR PRIORITY:   1
   NBR OPTIONS:   E
DB SUMM QLEN:  0 LS RXMT QLEN:  0 LS REQ QLEN:  0
LAST HELLO:  1 NO HELLO:  OFF
# LS RXMITS:  1 # DIRECT ACKS:  2 # DUP LS RCVD:  2
# OLD LS RCVD:  0 # DUP ACKS RCVD: 0 # NBR LOSSES:  0
# ADJ. RESETS:  2
```

The fields for this output are:

NEIGHBOR IP ADDRESS	Displays the neighbor's interface IP address.
OSPF ROUTER ID	Neighbor OSPF router ID.
NEIGHBOR STATE	Can be one of the following: 1 (Down) 2 (Attempt) 4 (Init) 8 (2-Way) 16 (ExStart) 32 (Exchange) 64 (Loading) 128 (Full) For more information about these values, refer to RFC 1583.
PHYSICAL INTERFACE	Displays the name of the interface over which a relationship has been established with this neighbor.
DR CHOICE, BACKUP CHOICE, DR PRIORITY	Indicate the values seen in the last hello received from the neighbor.
NBR OPTIONS	Indicates the optional OSPF capabilities supported by the neighbor. These capabilities are denoted by E (processes type 5 externals; when this is not set the area to which the common network belongs has been configured as a stub), T (can route based on TOS), MC (can forward IP multicast datagrams), and DC (can support demand circuits). This field is valid only for those neighbors in state Exchange or greater.

DB SUMM QLEN	Indicates the number of advertisements waiting to be summarized in Database Description packets. It should be zero except when the neighbor is in state Exchange.
LS RXMT QLEN	Indicates the number of advertisements that have been flooded to the neighbor, but not yet acknowledged.
LS REQ QLEN	Indicates the number of advertisements that are being requested from the neighbor in state Loading.
LAST HELLO	Indicates the number of seconds since a hello has been received from the neighbor.
NO HELLO	Indicates whether Hello Suppression is active with the neighbor.
# LS RXMITS	Indicates the number of retransmissions that have occurred during flooding.
# DIRECT ACKS	Indicates responses to duplicate link state advertisements.
# DUP LS RCVD	Indicates the number of duplicate retransmissions that have occurred during flooding.
# OLD LS RCVD	Indicates the number of old advertisements received during flooding.
# DUP ACKS RCVD	Indicates the number of duplicate acknowledgments received.
# NBR LOSSES	Indicates the number of times the neighbor has transitioned to Down state.
# ADJ. RESETS	Counts entries to state ExStart.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,DATABASE, AREAID=<area-id>

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,DATABASE, AREAID=<area-id> command displays a description of the contents of a particular OSPF area link state database. AS external advertisements are omitted from the display. A single line is printed for each advertisement.

Each advertisement is defined by the following three parameters:

- link state type (called Type)
- link state ID (called the LS destination)
- advertising router (called the LS originator)

A sample output with an explanation of entries follows:

```
EZZ7853I AREA LINK STATE DATABASE 352
 TYPE LS DESTINATION  LS ORIGINATOR  SEQNO  AGE XSUM
 1 @9.67.100.7   9.67.100.7  0x80000016 113 0X5D8D
 1 @9.67.100.8   9.67.100.8  0x80000014 88 0XC0AE
 1 @9.167.100.13  9.167.100.13 0x80000013 100 0X4483
 3 @9.167.100.13  9.167.100.13 0x80000001 760 0XF103
    # ADVERTISEMENTS:  4
    CHECKSUM TOTAL:   0X253C1
```

The fields for this output are:

TYPE	Separate LS types are numerically displayed: type 1 (router links advertisements), type 2 (network links advertisements), type 3 (network summaries), and type 4 (AS boundary router summaries).
LS DESTINATION	Indicates what is being described by the advertisement.
LS ORIGINATOR	Indicates the router that originated the advertisement
SEQNO, AGE, and XSUM	It is possible for several instances of an advertisement to be present in the OSPF routing domain at any one time. However, only the most recent instance is kept in the OSPF link state database (and printed by this command). The LS sequence number (Seqno), LS age (Age) and LS checksum (Xsum) fields are compared to see which instance is most recent. The LS age field is expressed in seconds. Its maximum value is 3600.

At the end of the display, the total number of advertisements in the area database is printed, along with a checksum total over all of their contents. The checksum total is simply the 32-bit sum (carries discarded) of the individual advertisement LS checksum fields. This information is used to quickly determine whether two OSPF routers have synchronized databases.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LSA, LSTYPE=ls-type, LSID=lsid,ORIG=ad-router,AREAID=area-id

The following command displays the contents of a single link state advertisement contained in the OSPF database:

```
DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,LSA,LSTYPE=ls-type,
LSID=lsid,ORIG=ad-router,AREAID=area-id
```

For a summary of all the advertisements in the OSPF database, use the following command:

```
DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,DATABASE,
AREAID=<area-id>
```

A link state advertisement is defined by its link state type, link state ID and its advertising router. There is a separate link state database for each OSPF area. Providing an area-ID on the command line tells the software which database you want to search. The different kinds of advertisements depend on the value given for link-state-type and are as follows:

Router links: (link-state-type = 1)	Describe the collected states of a router's interfaces
Network links: (link-state-type = 2)	Describe the set of routers attached to a network
IP Network: (link-state-type = 3)	Describe inter-area routes to networks
ASBR link: (link-state-type = 4)	Describe inter-area routes to AS boundary routers
AS external: (link-state-type = 5)	Describe routes to destinations external to the Autonomous System

Note: The ORIGINATOR only needs to be specified for link-state-types three, four, and five. The AREAID needs to be specified for all link-state-types except five. Link State IDs, originators (specified by their router IDs), and area IDs take the same format as IP addresses. For example, the backbone area can be entered as 0.0.0.0.

```
EZZ7880I LSA DETAILS 220
 LS AGE:   292
 LS OPTIONS:  E,DC
 LS TYPE:   1
 LS DESTINATION (ID): 9.167.100.13
 LS ORIGINATOR: 9.167.100.13
 LS SEQUENCE NO: 0X80000009
 LS CHECKSUM:  0X8F78
 LS LENGTH:  36
 ROUTER TYPE: ABR
 # ROUTER IFCS: 1
   LINK ID:   9.67.100.8
   LINK DATA:  9.167.100.13
   INTERFACE TYPE: 4
     NO. OF METRICS: 0
     TOS 0 METRIC: 2 (2)
```

LS AGE	Indicates the age of the advertisement in seconds.
LS OPTIONS	Indicates the optional OSPF capabilities supported by the piece of the routing domain described by the advertisement. These capabilities are denoted by E (processes type 5 externals; when this is not set, the area to which the advertisement belongs has been configured as a stub), T (can route based on TOS), MC (can forward IP multicast datagrams), and DC (can support demand circuits).

LS TYPE	Classifies the advertisement and dictates its contents: 1 (router links advertisement), 2 (network link advertisement), 3 (summary link advertisement), 4 (summary ASBR advertisement), 5 (AS external link).
LS DESTINATION	Identifies what is being described by the advertisement, dependant on the advertisement type: for router links and ASBR summaries, it is the OSPF router ID; for network links, it is the IP address of the network designated router; for summary links and AS external links, it is a network/subnet number.
LS ORIGINATOR	OSPF router ID of the originating router.
LS SEQUENCE NUMBER	Used to distinguish separate instances of the same advertisement. Should be looked at as a signed 32-bit integer. Starts at 0x80000001, and increments by one each time the advertisement is updated.
LS CHECKSUM	A checksum of advertisement contents, used to detect data corruption.
LS LENGTH	The size of the advertisement in bytes.
ROUTER TYPE	Indicates the level of function of the advertising router. ASBR means that the router is an AS boundary router, ABR that the router is an area border router, and W that the router is a wildcard multicast receiver.
# ROUTER IFCS	The number of router interfaces described in the advertisement.
LINK ID	Indicates what the interface connects to. Depends on Interface type. For interfaces to routers (that is, point-to-point links), the Link ID is the neighbor's router ID. For interfaces to transit networks, it is the IP address of the network designated router. For interfaces to stub networks, it is the network's network/subnet number.
LINK DATA	Four bytes of extra information concerning the link, it is either the IP address of the interface (for interfaces to point-to-point networks and transit networks), or the subnet mask (for interfaces to stub networks).
INTERFACE TYPE	One of the following: 1 (point-to-point connection to another router), 2 (connection to transit network), 3 (connection to stub network), or 4 (virtual link).
NO. OF METRICS	The number of nonzero TOS values for which metrics are provided for this interface. For the OS/390 implementation, this value is always zero.
TOS 0 METRIC	The cost of the interface.

The LS age, LS options, LS type, LS destination, LS originator, LS sequence no, LS checksum, and LS length fields are common to all advertisements. The Router type and # router ifcs are seen only in router links advertisements. Each link in the router advertisement is described by the Link ID, Link Data, and Interface type fields.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,DBSIZE

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,DBSIZE command displays the number of LSAs currently in the link state database, categorized by type. The following is a sample output:

```
EZZ7854I LINK STATE DATABASE SIZE 364
   # ROUTER-LSAS:   5
   # NETWORK-LSAS:   0
   # SUMMARY-LSAS:   7
   # SUMMARY ROUTER-LSAS: 1
   # AS EXTERNAL-LSAS:  5
   # INTRA-AREA ROUTES:  4
   # INTER-AREA ROUTES:  0
   # TYPE 1 EXTERNAL ROUTES: 5
   # TYPE 2 EXTERNAL ROUTES: 0
```

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,AREASUM

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,AREASUM command displays the statistics and parameters for all OSPF areas attached to the router. A sample output with an explanation of entries follows:

```
EZZ7848I AREA SUMMARY 222
AREA ID  AUTHENTICATION #IFCS #NETS #RTRS #BRDRS DEMAND
0.0.0.0   NONE    2  0  2  2 ON
2.2.2.2   NONE    1  0  3  2 ON
```

The fields for this output are:

AREA ID	Indicates the ID of the area.
AUTHENTICATION	Indicates the authentication method being used by the area.
# IFCS	Indicates the number of router interfaces attached to the particular area. These interfaces are not necessarily functional.
# NETS	Indicates the number of transit networks that have been found while doing the SPF tree calculation for this area.
# RTRS	Indicates the number of routers that have been found when doing the SPF tree calculation for this area.
# BRDRS	Indicates the number of area border routers that have been found when doing the SPF tree calculation for this area.
DEMAND	Indicates whether demand circuits are supported in this area.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,EXTERNAL

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,EXTERNAL command lists the AS external advertisements belonging to the OSPF routing domain. One line is printed for each advertisement. Each advertisement is defined by the following three parameters:

Its link state type (always five for AS external advertisements), its link state ID (called the LS destination), and the advertising router (called the LS originator).

A sample output with an explanation of entries follows:

```
EZZ7853I AREA LINK STATE DATABASE 269
TYPE  LS DESTINATION    LS ORIGINATOR    SEQNO       AGE  XSUM
 5    @9.67.100.0       9.67.100.8       0x80000001  4    0X408
 5    @9.169.100.0      9.67.100.8       0x80000001  4    0X73E
 5    @9.169.100.14     9.67.100.8       0x80000001  4    0XE66
 5    @192.8.8.0        9.67.100.8       0x80000001  4    0XAAF
 5    @192.8.8.8        9.67.100.8       0x80000001  4    0X5A4
 # ADVERTISEMENTS:  5
 CHECKSUM TOTAL:   0X 2A026
```

The fields for this output are:

TYPE	Always 5 for AS external advertisements.
LS DESTINATION	Indicates an IP network/subnet number. These network numbers belong to other Autonomous Systems.
LS ORIGINATOR	Indicates the router that originated the advertisement.
SEQNO, AGE, and XSUM	It is possible for several instances of an advertisement to be present in the OSPF routing domain at any one time. However, only the most recent instance is kept in the OSPF link state database (and printed by this command). The LS sequence number (Seqno), LS age (Age), and LS checksum (Xsum) fields are compared to see which instance is most recent. The LS age field is expressed in seconds. Its maximum value is 3600.

At the end of the display, the total number of AS external advertisements is printed, along with a checksum total over all of their contents. The checksum total is simply the 32-bit sum (carries discarded) of the individual advertisement LS checksum fields. This information is used to quickly determine whether two OSPF routers have synchronized databases.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,ROUTERS

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,ROUTERS command displays all routes to other routers that have been calculated by OSPF and are now present in the routing table. A sample output with explanations of entries follows:

```
EZZ7855I OSPF ROUTERS 362
DTYPE RTYPE DESTINATION  AREA   COST  NEXT HOP(S)
BR SPF 9.67.100.8  2.2.2.2   2   9.167.100.17
BR SPF 9.67.100.8  0.0.0.0   2   9.67.100.8
ASBR SPF 9.67.100.8  2.2.2.2   2   9.167.100.17
```

DTYPE	Indicates the destination type: ASBR : Indicates that the destination is an AS boundary router. ABR : Indicates that the destination is an area border router. FADD : Indicates a forwarding address (for external routes).
RTYPE	Indicates the route type and how the route was derived. **SPF** indicates that the route is an intra-area route (comes from the Dijkstra calculation). **SPIA** indicates that it is an inter-area route (comes from considering summary link advertisements).
DESTINATION	Indicates the destination router's OSPF router ID.
AREA	Displays the OSPF area to which the destination router belongs.
COST	Displays the cost to reach the router.
NEXT HOP(S)	Indicates the address of the next router on the path toward the destination host. A number in parentheses at the end of the column indicates the number of equal-cost routes to the destination.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,STATISTICS

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,OSPF,STATISTICS command displays statistics generated by the OSPF routing protocol. The statistics indicate how well the implementation is performing, including its memory and network utilization. Many of the fields displayed are confirmation of the OSPF configuration. A sample output with explanations of entries follows:

```
EZZ7856I OSPF STATISTICS 366
  OSPF ROUTER ID:   9.167.100.13
  EXTERNAL COMPARISON: TYPE 1
  AS BOUNDARY CAPABILITY: NO
  IMPORT EXTERNAL ROUTES: NONE
  ORIG. DEFAULT ROUTE: NO
  DEFAULT ROUTE COST:  (1, TYPE 2)
  DEFAULT FORWARD. ADDR.: 0.0.0.0
ATTACHED AREAS: 2 OSPF PACKETS RCVD: 194
OSPF PACKETS RCVD W/ERRS:  1 TRANSIT NODES ALLOCATED:   82
TRANSIT NODES FREED:   77 LS ADV. ALLOCATED:    53
LS ADV. FREED:     40 QUEUE HEADERS ALLOC:    32
QUEUE HEADERS AVAIL:   32 MAXIMUM LSA SIZE:    528
# DIJKSTRA RUNS:    25 INCREMENTAL SUMM. UPDATES:  0
INCREMENTAL VL UPDATES:   0
MULTICAST PKTS SENT:   227 UNICAST PKTS SENT:    36
LS ADV. AGED OUT:    0 LS ADV. FLUSHED:     10
PTRS TO INVALID LS ADV:   0 INCREMENTAL EXT. UPDATES:  19
```

The fields for this output are:

OSPF ROUTER	ID Displays the router's OSPF router ID.
EXTERNAL COMPARISON	Displays the external route type used by the router when importing external routes.
AS BOUNDARY CAPABILITY	Displays whether external routes will be imported.
IMPORT EXTERNAL ROUTES	Displays the external routes that will be imported.
ORIG. DEFAULT ROUTE	Displays whether the router will advertise an OSPF default route.
DEFAULT ROUTE COST	Displays the cost and type of the default route (if advertised).
DEFAULT FORWARD ADDR	Displays the forwarding address specified in the default route (if advertised).
ATTACHED AREAS	Indicates the number of areas to which that the router has active interfaces.
OSPF PACKETS RCVD	Covers all types of OSPF protocol packets.
TRANSIT NODES	Allocated to store router links and network links advertisements.

LS ADV	Allocated to store summary link and AS external link advertisements.
QUEUE HEADERS	Form lists of link state advertisements. These lists are used in the flooding and database exchange processes; if the number of queue headers allocated is not equal to the number freed, database synchronization with a neighbor is in progress.
MAXIMUM LSA SIZE	The size of the largest link state advertisement that can be sent.
# DIJKSTRA RUNS	Indicates how many times the OSPF routing table has been calculated from scratch.
INCREMENTAL SUMM UPDATES, INCREMENTAL VL UPDATES	Indicate that new summary link advertisements have caused the routing table to be partially rebuilt.
MULTICAST PKTS SENT	Covers OSPF hello packets and packets sent during the flooding procedure.
UNICAST PKTS SENT	Covers OSPF packet retransmissions and the Database Exchange procedure.
LS ADV. AGED OUT	Indicates the number of advertisements that have hit 60 minutes. Link state advertisements are aged out after 60 minutes. Usually they are refreshed before this time.
LS ADV. FLUSHED	Indicates the number of advertisements removed (and not replaced) from the link state database.
INCREMENTAL EXT. UPDATES	Displays the number of changes to external destinations that are incrementally installed in the routing table.

Using RIP Commands

RIP is an Interior Gateway Protocol (IGP) designed to manage a relatively small network. RIP is based on the Bellman-Ford or the distance-vector algorithm. RIP has many limitations and is not suited for every TCP/IP environment. You may wish to read more about RIP in RFCs 1058 and 1723.

RIP uses the number of hops, or hop count, to determine the best possible route to a host or network. The term hop count is also referred to as the metric. In RIP, a hop count of 16 means infinity, or that the destination cannot be reached. This limits the longest path in the network that can be managed by RIP to 15 gateways.

A RIP router broadcasts routing information to its directly connected networks every 30 seconds. It receives updates from neighboring RIP routers every 30 seconds and uses the information contained in these updates to maintain the routing table. If an update has not been received from a neighboring RIP router in 180 seconds, a RIP router assumes that the neighboring RIP router is down and sets all routes through that router to a metric of 16 (infinity). If an update has still not been received from the neighboring RIP router after another 120 seconds, the RIP router deletes from the routing table all of the routes through that neighboring RIP router.

RIP Version 2 is an extension of RIP Version 1 and provides the following features:

- Route Tags to provide EGP-RIP and BGP-RIP interactions: The route tags are used to separate internal RIP routes (routes for networks within the RIP routing domain) from external RIP routes, which may have been imported from an EGP (external gateway protocol) or another IGP. OMPROUTE does not generate route tags, but preserves them in received routes and readvertises them when necessary.
- Variable subnetting support: Variable length subnet masks are included in routing information so that dynamically added routes to destinations outside subnetworks or networks can be reached.
- Immediate Next Hop for shorter paths: Next hop IP addresses, whenever applicable, are included in the routing information to eliminate packets being routed through extra hops in the network. OMPROUTE does generate immediate next hops, but does preserve them if they are included in the RIP packets.
- Multicasting to reduce load on hosts: IP multicast address 224.0.0.9, reserved for RIP Version 2 packets, is used to reduce unnecessary load on hosts which are not listening for RIP Version 2 messages. This support is dependent on interfaces that are multicast-capable.
- Authentication for routing update security: Authentication keys can be configured for inclusion in outgoing RIP Version 2 packets. Incoming RIP Version 2 packets are checked against the configured keys.

- Configuration switches for RIP Version 1 and RIP Version 2 packets: Configuration parameters allow for controlling which version of RIP packets are to be sent or received over each interface. Supernetting support: The supernetting feature is part of Classless InterDomain Routing (CIDR).
- Supernetting provides a way to combine multiple network routes into fewer supernet routes, thus reducing the number of routes in the routing table and in advertisements.

Assisted RIP Commands

OMPROUTE implements the OSPF protocol described in RFC 1583 (OSPF Version 2), the OSPF subagent protocol described in RFC 1850, and the RIP protocols described in RFC 1058 (RIP Version 1) and in RFC 1723 (RIP Version 2). It provides an alternative to the static TCP/IP gateway definitions. The MVS host running with OMPROUTE becomes an active OSPF router, a RIP router, or both in a TCP/IP network. Either or both of these routing protocols can be used to dynamically maintain the host routing table. For example, OMPROUTE detects when a route is created, is temporarily unavailable, or if a more efficient route exists. If both OSPF and RIP protocols are used simultaneously, OSPF routes are preferred over RIP routes to the same destination.

OMPRoute RIP commands may be submitted to display RIP configuration and state information. The following commands are available using the assisted mode:

- DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,LIST,ALL

  This command lists all RIP-related configuration information.
- DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,LIST,INTERFACES

  This command lists IP addresses and configured parameters for each RIP interface.
- DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,LIST,ACCEPTED

  This command lists the routes to be unconditionally accepted, as configured with the ACCEPT_RIP_ROUTE statement.
- DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,INTERFACE, NAME=<if-name>

  This command displays statistics and parameters related to a particular RIP interface.
- DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,FILTERS

  This command displays the Global RIP filters.

To use the assisted RIP commands, perform the following steps:

1. From the Commands main menu, click the RIP hyperlink under Route Display Commands.
2. Click the down triangle to view a drop-down list of the available RIP commands.
3. Select a command, for example:
   DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,LIST,ALL
4. If you are doing the DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP, INTERFACE,NAME=<if-name> you must enter the Interface Address parameter in the field provided. The address is appended to the end of the command. For example,
   DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,INTERFACE,NAME=1.2.3.4
5. Click Submit. The response to the command appears on the next screen.
6. Use your Web browser's commands to:
   - find a particular string in the output,
   - obtain hardcopy of the output, or
   - return to the main menu by clicking the Back arrow.

The following section describes each OMPRoute RIP command in detail.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,LIST,ALL

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,LIST,ALL command lists all RIP-related configuration information. A sample output with explanations of entries follows:

```
 EZZ7843I RIP CONFIGURATION 447
 TRACE LEVEL: 1, DEBUG LEVEL: 0, SADEBUG LEVEL: 0
 STACK AFFINITY: TCPCS6
 RIP: ENABLED
 RIP DEFAULT ORIGINATION: ALWAYS, COST = 1
 PER-INTERFACE ADDRESS FLAGS:
 CTC2    9.167.100.13 RIP VERSION 1
        SEND NET AND SUBNET ROUTES
        RECEIVE NO DYNAMIC HOST ROUTES
        RIP INTERFACE INPUT METRIC: 1
        RIP INTERFACE OUTPUT METRIC: 0
CTC1    9.168.100.3  RIP VERSION 1
        SEND NET AND SUBNET ROUTES
        RECEIVE NO DYNAMIC HOST ROUTES
        RIP INTERFACE INPUT METRIC: 1
        RIP INTERFACE OUTPUT METRIC: 0
 EZZ7844I RIP ROUTE ACCEPTANCE
 ACCEPT RIP UPDATES ALWAYS FOR:
 9.167.100.59
```

The fields for this output are:

TRACE LEVEL	Displays the level of tracing currently in use by OMPROUTE.
DEBUG LEVEL	Displays the level of debugging currently in use by OMPROUTE.
SADEBUG LEVEL	Displays the level of debugging currently in use by OMPROUTE's OSPF SNMP subagent.
STACK AFFINITY	Displays the name of the stack on which OMPROUTE is running.

The remainder of the DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,LIST,ALL output is described in the following sections: Configured RIP Interfaces and RIP Routes to Be Accepted.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP, LIST,INTERFACES

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,LIST,INTERFACES command lists IP addresses and configured parameters for each RIP interface. A sample output with explanations of entries follows:

```
EZZ7843I RIP CONFIGURATION 447
RIP: ENABLED
RIP DEFAULT ORIGINATION: ALWAYS, COST = 1
PER-INTERFACE ADDRESS FLAGS:
CTC2    9.167.100.13 RIP VERSION 1
        SEND NET AND SUBNET ROUTES
        RECEIVE NO DYNAMIC HOST ROUTES
        RIP INTERFACE INPUT METRIC: 1
        RIP INTERFACE OUTPUT METRIC: 0
CTC1    9.168.100.3  RIP VERSION 1
        SEND NET AND SUBNET ROUTES
        RECEIVE NO DYNAMIC HOST ROUTES
        RIP INTERFACE INPUT METRIC: 1
        RIP INTERFACE OUTPUT METRIC: 0
```

The fields for this output are:

RIP	Indicates whether RIP communication is enabled.
RIP DEFAULT ORIGINATION	Indicates the conditions under which RIP supports default route generation and the advertised cost for the default route.
PER-INTERFACE	ADDRESS FLAGS Specifies information about an interface
RIP VERSION ***(Address Flag)***	Specifies whether RIP Version 1 or RIP Version 2 packets are being communicated over this interface.
SEND ***(Address Flag)***	Specifies which types of routes are included in RIP responses sent out this interface.

RECEIVE *(Address Flag)*	Specifies which types of routes are accepted in RIP responses received on this interface.
RIP INTERFACE INPUT METRIC *(Address Flag)*	Specifies the value of the metric added to RIP routes received over this interface.
RIP INTERFACE OUTPUT METRIC *(Address Flag)*	Specifies the value of the metric added to RIP routes advertised over this interface.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP, LIST,ACCEPTED

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,LIST,ACCEPTED command lists the routes to be unconditionally accepted, as configured with the ACCEPT_RIP_ROUTE statement. A sample output follows:

```
EZZ7844I RIP ROUTE ACCEPTANCE
ACCEPT RIP UPDATES ALWAYS FOR:
9.167.100.79  9.167.100.59
```

The fields for this output are:

ACCEPT RIP UPDATES ALWAYS FOR	Indicates the networks, subnets, and hosts for which updates are always accepted.

DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP, INTERFACE,NAME=

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RIP,INTERFACE,NAME= command displays statistics and parameters related to RIP interfaces. Detailed statistics for the interface chosen are displayed.

```
EZZ7860I RIP INTERFACE DETAILS 466
INTERFACE ADDRESS:  9.167.100.13
INTERFACE NAME:   CTC2
SUBNET MASK:   255.255.0.0
MTU      576
DESTINATION ADDRESS: 9.167.100.17
RIP VERSION:   1
IN METRIC:    1  OUT METRIC:    0
RECEIVE NET ROUTES:  YES RECEIVE SUBNET ROUTES: YES
RECEIVE HOST ROUTES: NO SEND DEFAULT ROUTES: NO
SEND NET ROUTES:  YES SEND SUBNET ROUTES:  YES
SEND STATIC ROUTES:  NO SEND HOST ROUTES:  NO
SEND POIS. REV. ROUTES: YES

SEND ONLY: VIRTUAL, DEFAULT

FILTERS: SEND  9.67.100.0 255.255.255.0
  RECEIVE 9.67.101.0 255.255.255.0
```

The fields for this output are:

INTERFACE ADDRESS	Indicates the interface IP address.
INTERFACE NAME	Indicates the interface name.
SUBNET MASK	Indicates the subnet mask.
MTU	Indicates the value of the Maximum Transmission Unit.
DESTINATION ADDRESS	Indicates the RIP identification for the destination router when the interface is point-to-point.
RIP VERSION	Indicates whether RIP Version 1 or RIP Version 2 packets are communicated over this interface.
IN METRIC	Specifies the value of the metric to be added to RIP routes advertised over this interface.
OUT METRIC	Indicates the RIP interface output metric
RECEIVE NET ROUTES	Indicates whether network routes are accepted in RIP responses received over this interface.
RECEIVE SUBNET ROUTES	Indicates whether subnet routes are accepted in RIP responses received over this interface.
RECEIVE HOST ROUTES	Indicates whether host routes are accepted in RIP responses received over this interface.
SEND DEFAULT ROUTES	Indicates whether the default route, if available, is advertised in RIP responses sent over this interface.
SEND NET ROUTES	Indicates whether network routes are advertised in RIP responses sent over this interface.
SEND SUBNET ROUTES	Indicates whether subnet routes are advertised in RIP responses sent over this interface.
SEND STATIC ROUTES	Indicates whether static routes are advertised in RIP responses sent over this interface.
SEND HOST ROUTES	Indicates whether host routes are advertised in RIP responses sent over this interface.
SEND POIS. REV. ROUTES	Indicates whether poisoned reverse routes are advertised in RIP responses sent over this interface. A poisoned reverse route is one with an infinite metric (a metric of 16).
SEND ONLY	Indicates the route-type restrictions on RIP broadcasts for this interface.
FILTERS	Indicates the send and receive filters for this interface.

DISPLAY TCPIP,<tcpipjobname>,RIP,FILTERS

The DISPLAY TCPIP,<tcpipjobname>,RIP,FILTERS command displays the Global RIP filters. A sample output with explanations of entries follows:

```
EZZ78012I GLOBAL RIP FILTERS
SEND ONLY: VIRTUAL, DEFAULT
FILTERS: SEND  9.67.100.0 255.255.255.0
  NORECEIVE 9.67.101.0 255.255.255.0
```

The fields for this output are:

SEND ONLY	Indicates the global route-type restrictions on RIP broadcasts that apply to all RIP interfaces.
FILTERS	Indicates the global send and receive filters that apply to all RIP interfaces.

DISPLAY TCPIP,<TCPIPJOBNAME>,OMPROUTE,RTTABLE

The DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RTTABLE command displays all of the routes in the OMPROUTE routing table. A sample output with explanation of entries follow.

Note: Be aware that this command displays the contents of the working table that is used by OMPROUTE, not the TCP/IP routing table. The contents of the OMPROUTE routing table may contain information different from that in the TCP/IP routing table.

```
EZZ7847I ROUTING TABLE 368
TYPE DEST NET   MASK  COST AGE  NEXT HOP(S)

SBNT 9.0.0.0   FF000000 1  576  NONE
SPE1 9.67.100.0  FFFFFF00 3  571  9.167.100.17
 SPF 9.67.100.7  FFFFFFFF 3  595  9.167.100.17
 SPF 9.67.100.8  FFFFFFFF 2  1270 9.167.100.17
 DIR* 9.167.0.0  FFFF0000 1  1685 9.167.100.13
 SPF 9.167.100.13  FFFFFFFF 2  1292 CTC2
 SPF* 9.167.100.17  FFFFFFFF 1  1684 9.167.100.17
 DIR* 9.168.100.0  FFFFFF00 1  1686 9.168.100.3
 DIR* 9.168.100.4  FFFFFFFF 1  1686 9.168.100.3
SPE1 9.169.100.0  FFFFFF00 3  571  9.167.100.17
SPE1 9.169.100.14  FFFFFFFF 3  571  9.167.100.17
SPE1 192.8.8.0  FFFFFF00 3  571  9.167.100.17
SPE1 192.8.8.8  FFFFFFFF 3  572  9.167.100.17
      0 NETS DELETED, 3 NETS INACTIVE
```

The fields for this output are:

TYPE	Indicates how the route was derived: SBNT: Indicates that the network is subnetted; such an entry is a placeholder only. DIR: Indicates a directly connected network, subnet, or host. RIP: Indicates a route that was learned through the RIP protocol. DEL: Indicates the route has been deleted. STAT: Indicates a statically configured route. SPF: Indicates that the route is an OSPF intra-area route. SPIA: Indicates that the route is an OSPF inter-area route. SPE1: Indicates OSPF external route - type 1. SPE2: Indicates OSPF external route - type 2. RNGE: Indicates a route type that is an active OSPF area address range and is not used in forwarding packets. An asterisk (*) after the route type indicates that the route has a directly connected backup. A percent sign (%) after the route type indicates that RIP updates are always accepted for this network/subnet.
DEST NET	Indicates the IP destination.
MASK	Indicates the IP destination subnet mask.
COST	Indicates the route cost.
AGE	Indicates the time that has elapsed since the routing table entry was last refreshed.
NEXT HOP(S)	Indicates the IP address of the next router on the path toward the destination host. A number in parentheses at the end of the column indicates the number of equal-cost routes to the destination. Use the DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RTTABLE,DEST= command to obtain a list of the next hops.

OMPROUTE Route Expansion Information

Use the DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RTTABLE,DEST=<ip-addr> command to obtain information about a particular route. When multiple equal-cost routes exist, use this command to obtain a list of the next hops. A sample output with explanation of entries follows:

```
EZZ7874I ROUTE EXPANSION 370
DESTINATION: 9.68.101.0
MASK:   255.255.255.0
ROUTE TYPE:  SPF
DISTANCE:  6
AGE:   1344
NEXT HOP(S): 9.167.100.17  (CTC2)
   9.168.100.4  (CTC1)
```

DESTINATION	Indicates the IP destination.
MASK	Indicates the IP destination subnet mask.
ROUTE TYPE	Indicates how the route was derived: SBNT: Indicates that the network is subnetted; such an entry is a placeholder only. DIR: Indicates a directly connected network, subnet, or host. RIP: Indicates a route that was learned through the RIP protocol. DEL: Indicates the route has been deleted. STAT: Indicates a statically configured route. SPF: Indicates that the route is an OSPF intra-area route. SPIA: Indicates that the route is an OSPF inter-area route. SPE1: Indicates OSPF external route - type 1. SPE2: Indicates OSPF external route - type 2. RNGE: Indicates a route type that is an active OSPF area address range and is not used in forwarding packets. An asterisk (*) after the route type indicates that the route has a directly connected backup. A percent sign (%) after the route type indicates that RIP updates are always accepted for this network/subnet.
DISTANCE	Indicates the route cost.
AGE	Indicates the time that has elapsed since the routing table entry was last refreshed.
NEXT HOP(S)	Indicates the IP address of the next router and the interface used to reach that router for each of the paths toward the destination host.

Using Route Table Commands

OMPRoute Route Table commands may be submitted to display Route Table configuration and state information.

Assisted Route Table Commands

The following commands are available using the assisted mode:

- **DISPLAY CPIP,<tcpipjobname>,OMPROUTE,RTTABLE**
  This command lists all of the routes in the OMPROUTE routing table
- DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RTTABLE,DEST=<ip-addr>
  This command provides information about a particular route.

To use the assisted Route Table commands, perform the following steps:

1. From the Commands main menu, click the Route Table hyperlink under Route Display Commands.
2. Click the down triangle to view a drop-down list of the available Route Table commands.
3. Select a command, for example,

   DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RTTABLE,DEST=<ip-addr>
4. If you are doing the DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RTTABLE,DEST=<ip-addr> you must enter the Destination Address parameter in the field provided. The address is appended to the end of the command. For example,
5. DISPLAY TCPIP,<tcpipjobname>,OMPROUTE,RTTABLE,DEST=1.2.3.4
6. Click Submit. The response to the command appears on the next screen.
7. Use your Web browser's commands to:
   - find a particular string in the output
   - obtain hardcopy of the output
   - return to the main menu by clicking the Back arrow

Using Route Diagnostic Commands

See these topics for information on commands used for diagnostic purposes:

- (IP) Using the Ping Command
- (IP) Using the Trace Route Command
- (HPR/EE) Using the D NET,APING Command
- Using the D NET,RTPS Command

(IP) Using the Ping Command

Ping is used to diagnose network problems dealing with availability and response time. The Ping command sends an echo request to a foreign node to determine if the computer is accessible. When the response to the Ping command is received, the elapsed time is displayed. The time does not include the time spent communicating between the user and the TCP/IP address space.

The following parameters are available for the Ping command:

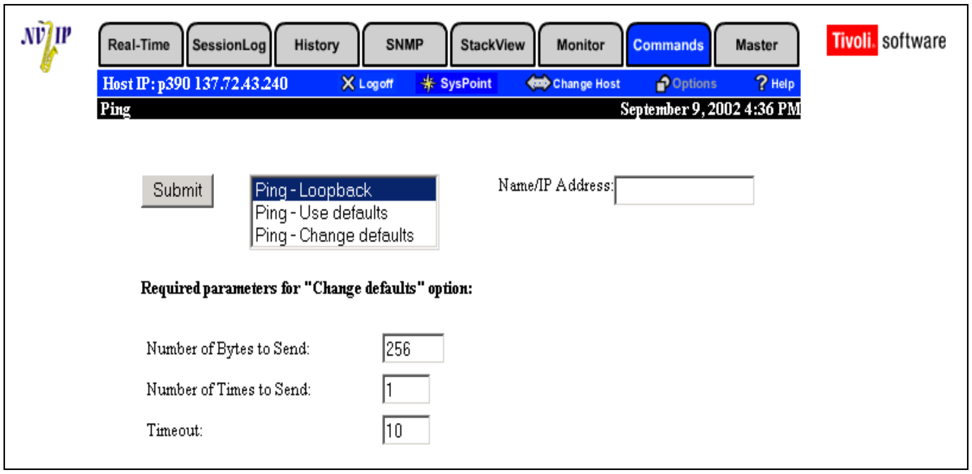
Address/Name	Local or remote host to which the echo request is sent. If you fail to enter a host name, the system prompts for one. Enter either the IP address or the character-string name for the host.
Bytes to Send	Default=256. Sets the number of bytes sent in the echo request. Valid values are a minimum of 8 and a maximum determined by the lrg_env_size value set in the PROFILE.TCPIP data set.
Times to Send	Valid values are 0 to 2,147,483,647. Sets the number of echo requests that are sent to the host. If the count is zero (0), PING continually sends requests. To stop the PING command, press PA1.
Timeout	Default=10 seconds. Sets the number of seconds that the PING command waits for a response. Valid values are 1 to 100.

The Commands module provides the following PING command formats:

PING – Use Defaults	Use the PING command with the defaults listed above.
PING – Change Parameters	Modify selected parameters from their default values.
PING Loopback - Verify Installation	Use the Loopback option to test the software installation of the TCP/IP system. The host you are running on is PINGed.

To use the PING command under the Expert-Assist Interface, perform the following steps:

1. From the Commands main menu, click the Ping hyperlink. The Ping Command screen displays:



Host IP: p390 137.72.43.240

Ping September 9, 2002 4:36 PM

Name/IP Address:

Required parameters for "Change defaults" option:

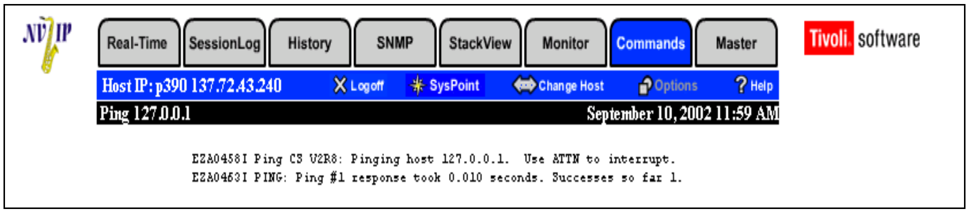
Number of Bytes to Send: 256

Number of Times to Send: 1

Timeout: 10

Figure 156. PING Command screen

2. From the Ping menu, select one of the command options described above.
3. If you entered a command other than Ping Loopback, enter the IP address or DNS name to Ping.
4. If you entered the Ping – Change Defaults command option, change the default parameters as desired.
5. Click Submit to proceed. The Ping Results screen appears:



Host IP: p390 137.72.43.240

Ping 127.0.0.1 September 10, 2002 11:59 AM

```
EZA0458I Ping CS V2R8: Pinging host 127.0.0.1.  Use ATTN to interrupt.
EZA0463I PING: Ping #1 response took 0.010 seconds. Successes so far 1.
```

Figure 157. Ping Results screen

6. Do one of the following:
   - To enter another Ping command, click the Back button on the browser.
   - To return to the main menu for Commands, click the Commands navigation tab.
   - To return to the SysPoint Home Page, click SysPoint on the main menu bar.

(IP) Using the Trace Route Command

The TraceRte command sends UDP requests with varying Time to Live (TTL) values. It waits for the routers between the local and remote hosts to send TTL exceeded messages. Use it to monitor response time from hop-to-hop (response time from host to each hop) and to diagnose network problems. The following parameters are available for the TraceRte command:

Address/Name	Local or remote host to which the echo request is sent. If you fail to enter a host name, the system prompts for one. Enter either the IP address or the character-string name for the host.
MAX	Default=30. Specifies maximum Time to Live value. Valid values=1 to 255.
TRY	Default=3. Number of attempts before the command aborts. Valid values=1 to 255.
PORT	Default=4096. Specifies the starting port number. Valid values=4096-60000.
WAIT	Default=5 seconds. Specifies how long to wait for a response before re-attempting the command or, if the TRYs value has been reached, halting the command. Valid Values=1 to 255.

The Commands module provides the following TraceRte command formats:

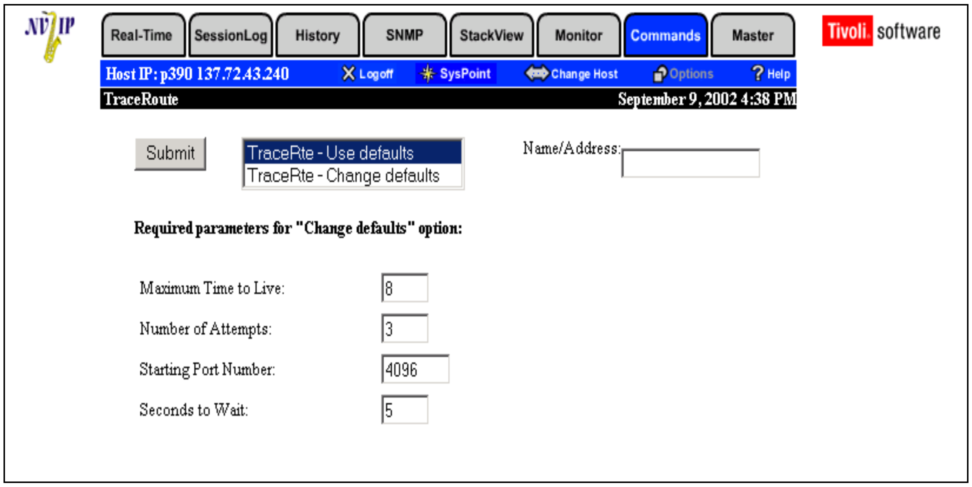
PING – Use Defaults	Use the PING command with the defaults listed above.
PING – Change Parameters	Modify selected parameters from their default values.

Trace Route Options

Trace Route provides two command options: Use Defaults and Change Parameters. The Use Defaults option submits the commands with the pre-set default values, as listed above. The Change Parameters option is used to modify any one of the parameters listed above before submitting the command for processing.

To use the TraceRte command, perform the following steps:

1. From the Commands main menu, click the TraceRoute hyperlink. The TraceRoute Command screen appears:



Host IP: p390 137.72.43.240

TraceRoute September 9, 2002 4:38 PM

Name/Address:

Required parameters for "Change defaults" option:

Maximum Time to Live: 8

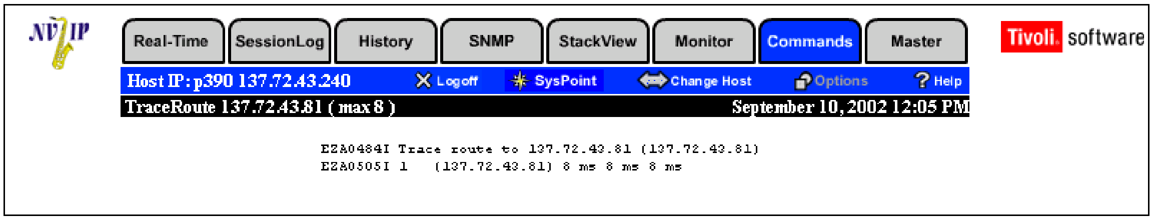
Number of Attempts: 3

Starting Port Number: 4096

Seconds to Wait: 5

Figure 158. TraceRoute Command screen

2. From the TraceRoute menu, select one of the TraceRte commands.
3. Enter the IP address or DNS name to Ping.
4. To change the defaults, use the TraceRte - Change Parameters option to change the default parameters as desired.
5. Click Submit to proceed. The TraceRoute Results screen appears:



Host IP: p390 137.72.43.240

TraceRoute 137.72.43.81 (max 8) September 10, 2002 12:05 PM

```
EZA0484I Trace route to 137.72.43.81 (137.72.43.81)
EZA0505I 1   (137.72.43.81) 8 ms 8 ms 8 ms
```

Figure 159. TraceRoute Results Screen

6. Do one of the following:
   - To enter another Ping command, click the Back button on the browser.
   - To return to the main menu for Expert Commands, click the Commands navigation tab.
   - To return to the SysPoint Home Page, click SysPoint on the main menu bar.

(HPR/EE) Using the D NET,APING Command

D NET,APING performs a VTAM-based Advanced Peer to Peer Networking (APPN) Ping test from the originating host to the remote host. The D NET,APING command is the VTAM-based equivalent of the TCP/IP Ping command. D NET,APING is used to diagnose APPN availability and response time issues for a specific APPN Transmission Group (TG) that may be defined between two APPN endpoints, or to test network connectivity of Enterprise Extender links.

D NET,APING also has the capability to designate a specific logon mode table (LOGMODE) that is used to test network connectivity of Enterprise Extender (EE) links. Because each defined EE UDP port has an associated priority assigned to it, D NET,APING tests a specific UDP port relative to that port's TOS (Types of Service) priority assignment. This test can be extremely useful to verify and compare newer High Performance Routing/Enterpise Extender (HPR/EE) connections from the perspective of APPN as well as from TCP/IP. To test connectivity as well as network reponse time, you must first specify a destination Control Point (CP) or host for the resource name ID parameter, and then choose to either use the defaults or specify one or more of six optional D NET,APING parameters before submitting the command.

Once the D NET,APING command has been submitted, it sends an 'echo' request to the foreign node or CP to determine if the remote host or resource is accessible. If a response to the D NET,APING command is received, information is provided regarding the LOGMODE and Class of Service (COS) used as well as TG information. It then returns D NET,APING test iteration response data as well as summaries of the minimum, average, and maximum response times in milliseconds for the specified test period.

The standard syntax for issuing the D NET,APING command via VTAM is:

```
D NET,APING,ID=SSCP2X,SIZE=100,LOGMODE=#INTER,ITER=2,CONSEC=1,
TP=APINGD,ECHO=YES
```

The following parameters are available for the D NET,APING command:

CP or Resource Name	The destination Control Point or Resource Name ID to which the D NET,APING request will be sent. You can enter up to 8 characters for a Resource Name. You must enter a CP or Resource Name in this field.
Packet Size for Each Send	Default=100. The size in bytes for each test packet. Valid values are 1 to 32,763.
Logon Mode Name	Default=#INTER. The Logon Mode Name must be taken from the default logon mode table (ISTINCLM), but cannot be the names CPSVCMG, CPSVRMGR, OR SNASVCMG.

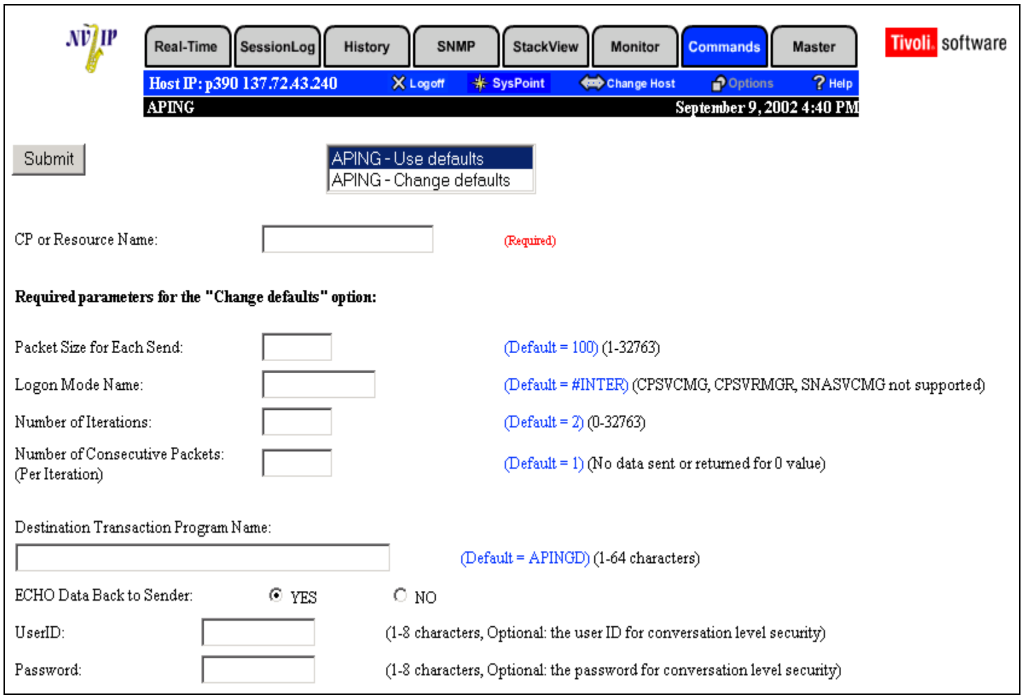
Number of Iterations	Default=2. The number of 'send and receive' iteration tests to be performed before the test ends. Valid values are 0 to 32,763. Specifying a value of 0 will perform a transaction program version exchange only.
Number of Consecutive Packets (Per Iteration)	Default=1. The number per iteration of consecutive packets as defined by the size parameter. Valid values are 0 to 32,763. Specifying a value of 0 will perform a transaction program version exchange only.
Destination Transaction Program Name	Default=APINGD. The Destination Transaction Program (TP) Name for data to be sent to for acknowledgment, and optionally to return. You can enter up to 64 characters. The default name is available in most VTAM environments. If unavailable, specify another TP Name.
ECHO Data Back to Sender	Default=YES. Indicates that you want to data to be returned to the sending transaction (if the remote TP supports ECHO).
User ID	Optional field. Use for conversation level security. You must also specify a Password. You can enter up to 8 characters.
Password	Optional field. Use with your User ID for conversation level security. The password you enter will not display for security purposes. You can enter up to 8 characters.

The Commands module provides the following D NET,APING command formats:

APING – Use Defaults	Use the D NET,APING command with the defaults listed above.
APING – Change Parameters	Modify selected parameters from their default values.

To use the D NET,APING command under the Expert-Assist Interface, perform the following steps:

1. From the Commands main screen, click the D NET,APING hyperlink under Route Diagnostic Commands. The APING Command screen displays:



Host IP: p390 137.72.43.240

APING September 9, 2002 4:40 PM

CP or Resource Name: (Required)

Required parameters for the "Change defaults" option:

Packet Size for Each Send: (Default = 100) (1-32763)

Logon Mode Name: (Default = #INTER) (CPSVCMG, CPSVRMGR, SNASVCMG not supported)

Number of Iterations: (Default = 2) (0-32763)

Number of Consecutive Packets: (Per Iteration) (Default = 1) (No data sent or returned for 0 value)

Destination Transaction Program Name: (Default = APINGD) (1-64 characters)

ECHO Data Back to Sender: ● YES ○ NO

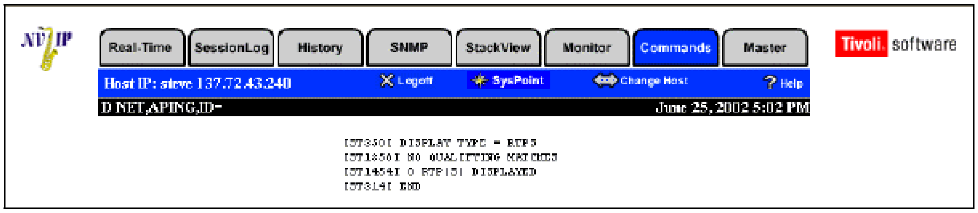
UserID: (1-8 characters, Optional: the user ID for conversation level security)

Password: (1-8 characters, Optional: the password for conversation level security)

Figure 160. APING Command screen

2. From the APING menu, select either APING – Use Defaults or APING – Change Parameters.
3. Enter the CP or Resource Name. This is a required field.
4. Do one of the following:
   - For **APING – Use Defaults** click the Submit button.
   - For **APING – Change Defaults** change the default values in the appropriate fields and click the Submit button.

   The D NET,APING Command Results screen displays:



Host IP: steve 137.72.43.240

D NET,APING,ID= June 25, 2002 5:02 PM

```
IST350I DISPLAY TYPE = RTPS
IST1856I NO QUALIFYING MATCHES
IST1454I 0 RTP(S) DISPLAYED
IST314I END
```

Figure 161. D NET,APING Results screen

5. Do one of the following:
   - To enter another D NET,APING command, click the Back button on the browser.
   - To return to the main menu for Commands, click the Commands navigation tab.
   - To return to the SysPoint Home Page, click SysPoint on the main menu bar.

Using the D NET,RTPS Command

The D NET,RTPS command provides the ability to quickly perform a VTAM-based RTP (Rapid Transport Protocol) Route Test across the 'HPR or RTPS pipe' for any Enterprise Extender (EE) connection to a specific RTP endpoint. In most EE environments this endpoint will usually be the same destination as the previously defined VTAM Cross Domain (CDRM) and associated Control Point (CP). The new RTP data transport, however, uses UDP and IP between both endpoints instead of SNA.

The D NET,RTPS command syntax for z/OS V.1.2 systems is:

```
D NET,RTPS,TEST=YES,ID=punm4rtp
```

where 'punm4rtp' is the specific RTP PU name you want to test

The D NET,RTPS hyperlink command syntax on pre-z/OS V.1.2 systems is:

```
D NET,RTPS
```

The following examples show how a user would manually determine the currently defined RTP PUs on their system and subsequently perform an RTP Route Test. Alternatively, it shows the results of a pre-z/OS V.1.2 display of all RTPS.

Displaying the rapid transport protocol (RTP) major node:

```
D NET,ID=ISTRTPMN,SCOPE=ALL

IST097I DISPLAY ACCEPTED
IST075I NAME = ISTRTPMN, TYPE = RTP MAJOR NODE
IST486I STATUS= ACTIV, DESIRED STATE= ACTIV
IST1486I   RTP NAME   STATE      DESTINATION      CP    MNPS TYPE
IST1487I   CNR00004   CONNECTED  NETA.SSCP2A      NO    LULU
IST1487I   CNR00003   CONNECTED  NETA.SSCP2A      NO    RSTP
IST1487I   CNR00002   CONNECTED  NETA.SSCP2A      NO    CPCP
IST1487I   CNR00001   CONNECTED  NETA.SSCP2A      NO    CPCP
IST314I END
```

Performing the RTP Route Test for CNR00003:

```
D NET,RTPS,TEST=YES,ID=CNR00003
```

```
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = RTPS
IST1695I PU NAME CP NAME COS NAME SWITCH CONGEST SESSIONS
IST1696I CNR00003 NETA.SSCPA SNASVCMG NO NO 1
IST1786I HPR ROUTE TEST INITIATED FOR RTP PU
IST1454I 1 RTP(S) DISPLAYED
IST314I END
```

```
IST1787I HPR ROUTE TEST RESULTS FOR RTP PU CNR00003
IST1788I NODE CP NAME  TG NUMBER PARTNER CP NAME INTERNODAL TIME
IST1789I                         (MILLISECONDS)
IST1790I NETA.SSCP2A   21   NETA.SSCP1A           3
IST1790I NETA.SSCP1A   21   NETA.SSCPAA          13
IST1790I NETA.SSCPAA   21   NETA.SSCPBA           1
IST1790I NETA.SSCPBA   21   NETA.SSCPCA           1
IST1792I TOTAL RTP TRANSVERSAL TIME 18 MILLISECONDS
IST314I END
```

Displaying RTPS pipe information:

```
D NET,RTPS
```

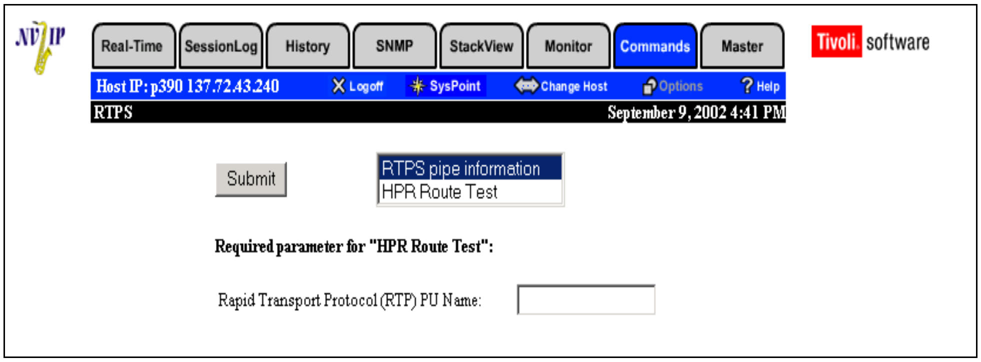
```
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = RTPS
IST1695I PU NAME CP NAME  COS NAME SWITCH CONGEST SESSIONS
IST1696I CNR00004 NETA.SSCP2A #INTER  NO    NO    5
IST1696I CNR00003 NETA.SSCP2A RSETUP  NO    NO    0
IST1696I CNR00002 NETA.SSCP2A CPSVCMG  NO    NO    1
IST1696I CNR00001 NETA.SSCP2A CPSVCMG  NO    NO    1
IST1454I 4 RTP(S) DISPLAYED
IST314I END
```

Note: The D NET,RTPS command remains valid on any z/OS system as well.

To use the D NET,RTPS command under the Expert-Assist Interface, perform the following steps:

1. From the Commands main menu, click the D Net,RTPS hyperlink.

   The RTPS screen displays:



Required parameter for "HPR Route Test":

Rapid Transport Protocol (RTP) PU Name:

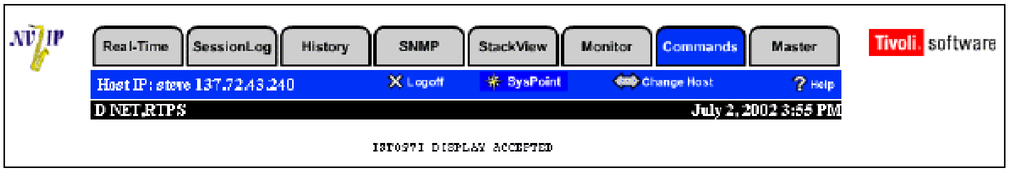
Figure 162. RTPS screen

2. From the menu in the RTPS screen, select either RTPS Pipe Information or HPR Route Test.

3. Do one of the following:

   - For **RTPS Pipe Information** proceed to Step 4.
   - For **HPR Route Test** enter a Rapid Transport Protocol PU Name (required) in the field provided and proceed to Step 4.
   - Click the Submit button.

   The D NET,RTPS Route Results screen appears:



```
IST097I DISPLAY ACCEPTED
```

Figure 163. D NET,RTPS Results screen

5. Do one of the following:

   - To enter another Route Test command, click the Back button on the browser.
   - To return to the main menu for Commands, click the Commands navigation tab.
   - To return to the SysPoint Home Page, click SysPoint on the main menu bar.

Using the USS Command

D OMVS is a UNIX System Services command used to display and diagnose current OMVS-based settings and associated processes. After you specify the desired display option and the required parameters, submit the command through the target TCP/IP for the MVS host to which you are connected. The D OMVS command is sent directly to MVS to be issued. To view detailed information and explanations for each D OMVS Command, please refer to the IBM MVS System Commands for the appropriate z/OS release.

Using the D OMVS Command)

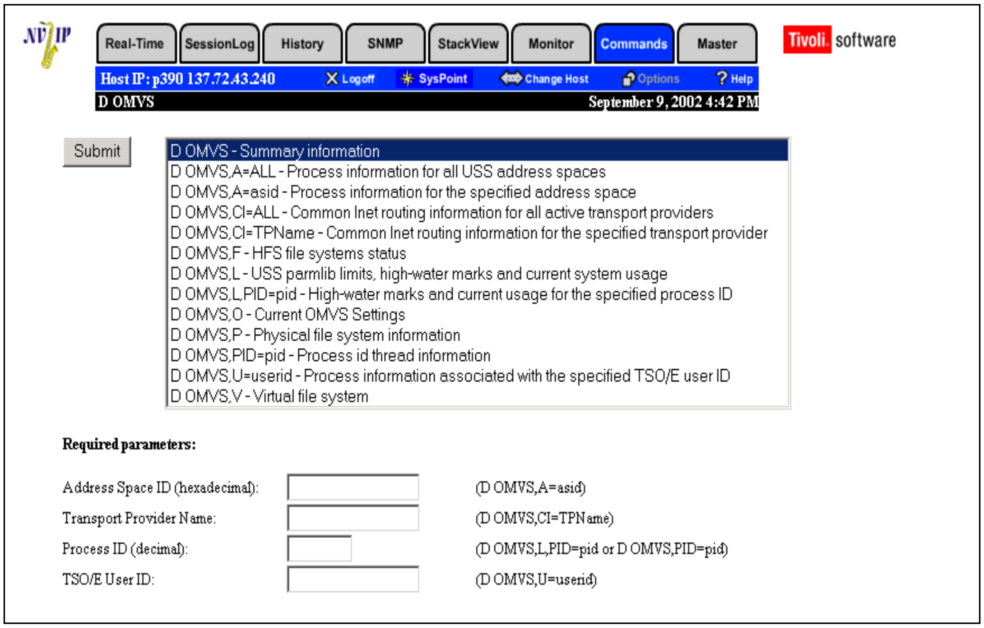
In the current release the pre-formatted D OMVS options available through the Commands menu are:

(Blank), S or Summary	Summary status information for all UNIX-based file systems, processes, servers and current parmlib settings.
ASID or A	Displays detailed information for the specific Address Space ID (ASID) or ALL ASIDs, depending on the parameter value specified. The ASID parameter is a required parameter. It can either be ALL or a specific ASID hexadecimal number, usually determined with an MVS D A command. This parameter is required.
CINET or CI	Displays the current Common Inet (CINET) Routing status information. The CINET Pre-Router process is used to link with TCP/IP for data transport over network routes. The CI parameter is a required parameter. It can either be ALL or a specific 'tpname' (transport provider name) as determined by values specified in the BPXPRMxx profile or by the SETOMVS command.
FILE or F	Displays a current list of Hierarchical File Structure (HFS) systems in use by USS as well as their current status.
LIMITS or L	Displays all the current system-wide USS parmlib value settings in place. This includes current system usage and high-water mark values.
L,PID	Provides current LIMIT values only for the specific active Process ID (PID). This includes current system usage and high-water mark values. A specific Process ID number must be entered for the PID field. This is a required value.
OPTIONS or O	Displays all current option settings as specified either during OMVS initialization using the BPXPRMxx parmlib member and/or settings that may have been dynamically altered via a SETOMVS command.

PID	Provides detailed thread information and current status for the Process ID (PID) specified by the required decimal value. A specific Process ID number must be entered for the PID field. This is a required value.
PFS or P	Displays information about all the currently configured USS Physical File System(s), either as an internal function of USS, as specified during OMVS initialization using the BPXPRMxx parmlib member, and/or as settings that have been recently altered via a SETOMVS command. This is not restricted to commonly recognized File Systems, such as HFS, but will also include application support processes, such as UNIX Affinity (local-based) sockets process, and the INET Affinity (network or remote server-based) sockets process. In the resulting display, these application support processes are labeled as PFS Types of UDS and TCP, respectively. There are some critical socket usage values you should watch carefully for these two important PFS types, including the MAXSOCK, OPNSOCK and HIGHUSED values.
VSERVER or V	Displays process details on all defined servers that utilize the Virtual File System (VFS) callable API services. Typically this could include BPXOINIT itself, or other defined servers, including web-based servers.
U	Lists process information for any active processes owned by the specified TSO/E user ID. This display might be utilized to determine which processes may have to be canceled when a user is reporting USS task processing problems. You should be aware that subsequent MVS cancellation of the TSO/E user ID may also be necessary in those situations. A specific TSO/E User ID must be entered for the U field. This is a required field.

To use the D OMVS command under the Expert-Assist Interface, complete these steps:

1. From the Commands main menu, click the D OMVS hyperlink under USS Command.
2. The D OMVS Command screen appears:



D OMVS - Summary information
D OMVS,A=ALL - Process information for all USS address spaces
D OMVS,A=asid - Process information for the specified address space
D OMVS,CI=ALL - Common Inet routing information for all active transport providers
D OMVS,CI=TPName - Common Inet routing information for the specified transport provider
D OMVS,F - HFS file systems status
D OMVS,L - USS parmlib limits, high-water marks and current system usage
D OMVS,L,PID=pid - High-water marks and current usage for the specified process ID
D OMVS,O - Current OMVS Settings
D OMVS,P - Physical file system information
D OMVS,PID=pid - Process id thread information
D OMVS,U=userid - Process information associated with the specified TSO/E user ID
D OMVS,V - Virtual file system

Required parameters:

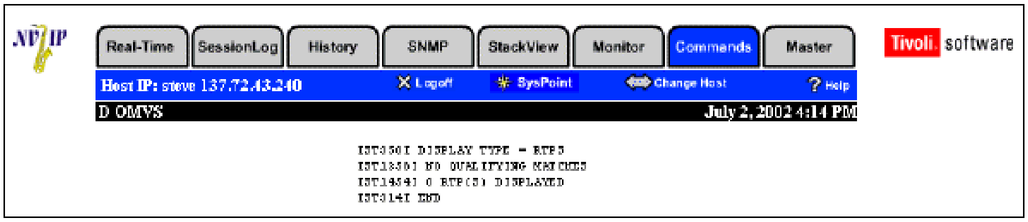
Address Space ID (hexadecimal): (D OMVS,A=asid)
Transport Provider Name: (D OMVS,CI=TPName)
Process ID (decimal): (D OMVS,L,PID=pid or D OMVS,PID=pid)
TSO/E User ID: (D OMVS,U=userid)

Figure 164. D OMVS Command screen

3. From the D OMVS menu, select one of the D OMVS commands. Some D OMVS commands require additional parameters. These commands are:

D OMVS,A=ALL or **D OMVS,A=asid**	The Address Space ID field is required. You can only specify a hexadecimal Address Space ID (ASID).
D OMVS,CI=ALL or **D OMVS,CI=TPname**	The Transporter Provider Name is required. You can specify either ALL or a specific active 'tpname' (transport name provider).
DOMVS,LPID=pid	The Process ID is required You must specify the decimal PID value assigned for a currently active Process ID (PID) in order to accurately display all the current limits for that Process ID.
D OMVS,PID=pid	The Process ID is required. You must specify the decimal PID value assigned for a currently active Process ID (PID) in order to accurately display all the current thread information for the Process ID.
D OMVS,U=userid	The TSO/E User ID is required. You must specify a currently active TSO/E user ID name or value in order to accurately display the current status of all USS processes associated with that TSO/E user ID.

4. When you are ready, click Submit to issue the command. The D OMVS Results screen appears. The D OMVS Results screen below displays if the user selected the DOMVS Summary Information command:



```
IST350I DISPLAY TYPE = RTPS
IST1350I NO QUALIFYING MATCHES
IST1454I 0 RTP(S) DISPLAYED
IST314I END
```

Figure 165. D OMVS,L Results Screen

5. Do one of the following:
   - Click the Back button on the browser to enter another D OMVS command.
   - Click the Commands navigation tab to return to the main Commands menu.
   - Click SysPoint on the main menu mar to return to the SysPoint Home Page.

Using Communication Server Commands

Communication Servers Commands cover:

- Using the Netstat Command
- Using Storage Commands
- Using VTAM Commands

Using the Netstat Command

The Netstat command is used to diagnose network problems and control network activity. Once you have selected the options desired and set up any necessary filters, submit the command to the TCP/IP on the MVS host you designated. To view detailed information on each Netstat Command, please refer to the IBM IP User Guide for the appropriate OS/390 release. The pre-formatted Netstat options available through the Commands module are:

All	Detailed information about TCP/IP connections (TCP/IP address space). Filter: User ID field.
AllConn	All connection information including TIME-WAIT and CLOSED connections. Filter: User ID field.
ARP	Query ARP cache for a selected address. Offload devices keep their own ARP cache, which you cannot retrieve with NETSTAT ARP.
ARP All	Queries the ARP cache for all addresses. Offload devices keep their own ARP cache, which you cannot retrieve with NETSTAT ARP.
Byteinfo	Provides connection display information: client ID, bytes sent/received on the connection, local port, foreign port, and state.
Byteinfo Idletime	Provides connection display information with the addition of the idle time for this connection in hours:minutes:seconds.

Cachinfo	Displays information about Fast Response Cache Accelerator (Cache Accelerator) statistics. For each listening socket configured for Cache Accelerator support, the following information is displayed: • Client socket • Maximum cache size • Current cache size • Maximum number of objects in cache • Current objects in cache • Number of connections with cache support • Number of connections processed • Number of connections deferred • Number of times the connection timer has expired • Number of requests processed • Number of incomplete requests • Number of cache hits • Number of cache misses • Number of unproductive cache hits
Clients	Provides Current clients information: client ID, authorization, notes handled by client, elapsed time for last used and last forced off, as well as VMCF error count.
Config	Displays the following information about the TCP/IP address space for each client: • Client ID (User ID) • Configured IP information • Configured TCP/IP information • Configured UDP information • SMF parameters • TCP/IP statistics • Data trace settings
Conn	Active TCP connections.
Devlinks	Lists information for the devices and defined links in the TCP/IP address space: device, type, status, address, queue size, link, type, bytes transmitted/received, net number, BSD parameters, packet trace settings, and ATM specific information.
Drop	Drops a connection.
Gate	Lists current known gateways: network address, first hop address, link name used by first hop, packet size used by first hop, and subnet mask/value.

Gate Detail

Provides the following information about each gateway:

- Address of the network
- First hop address
- Link name used by first hop
- Packet size used by first hop
- Subnet mask and subnet value
- Maximum retransmit time
- Minimum retransmit time
- Round trip gain
- Variance gain
- Variance multiplier

Help

Help on the Netstat command

Home

Home address list

Portlist

Displays the port reservation list with the following information:

- Port number
- Protocol
- Username
- Flags
    - A Autolog
    - D DelayAcks
- Optimize MSS
    - R Port is reserved by range
    - S Share port
- Range: This field is significant only for port entry reserved by range (flag R in the Flags field)

Route

Displays the following network routing information:

- Gateway used in forwarding packets
- Flags indicating the route state:
    - D Dynamically created route using a redirect
    - G Gateway route
    - H Host route rather than a network
    - U Route is up
- Reference count indicating the current number of active users
- Interface is the route's link name

SLAP

Displays all of the service policy definitions (policy rules, policy profiles, and service classes) and policy statistics data

Sockets

Clients using socket interface

TCP Details about the TCP/IP address space if the TCP/IP address spaces and NETSTAT are the same version.

Telnet Displays the status of the internal Telnet server. A connection in the listen state is always available for an incoming open request. The following fields are shown:

- Connection ID
- IP address - foreign port
- Status
- Bytes in
- Bytes out
- SNA application
- SNA Luname

Telnet Detail Displays further status detail than the Telnet option of the internal Telnet server. In addition to the fields displayed with the Telnet option, the following three additional fields display:

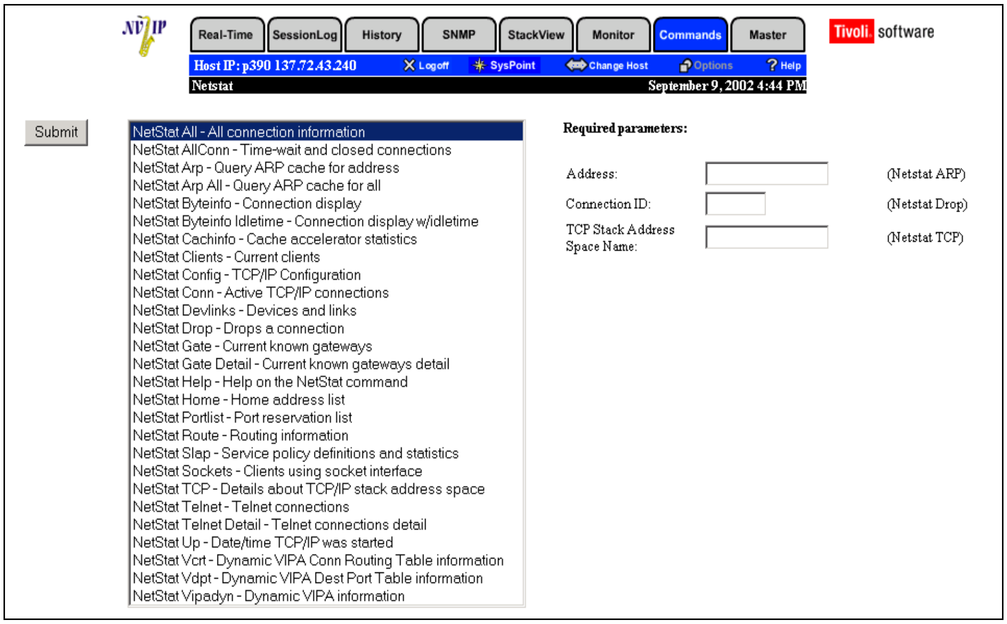
- SNA modename
- TN protocol
- TN User ID

UP Date and time TCP/IP was started.

Vipadyn Displays the current dynamic VIPA information for a local host.

To use the Netstat command under the Expert-Assist Interface, complete these steps:

1. From the Commands main menu, click the Netstat hyperlink under Communication Server Commands. The Netstat Command screen appears.



Host IP: p390 137.72.43.240

Netstat September 9, 2002 4:44 PM

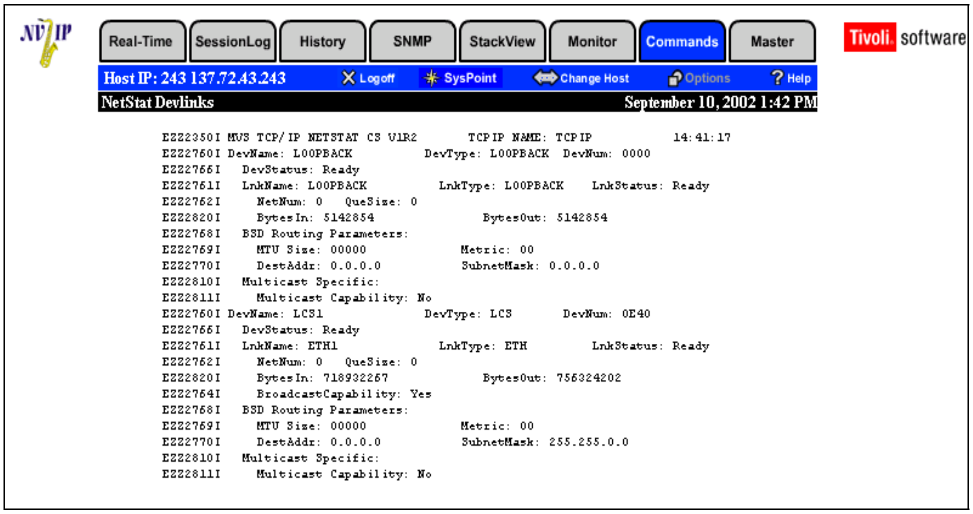
NetStat All - All connection information
NetStat AllConn - Time-wait and closed connections
NetStat Arp - Query ARP cache for address
NetStat Arp All - Query ARP cache for all
NetStat Byteinfo - Connection display
NetStat Byteinfo Idletime - Connection display w/idletime
NetStat Cachinfo - Cache accelerator statistics
NetStat Clients - Current clients
NetStat Config - TCP/IP Configuration
NetStat Conn - Active TCP/IP connections
NetStat Devlinks - Devices and links
NetStat Drop - Drops a connection
NetStat Gate - Current known gateways
NetStat Gate Detail - Current known gateways detail
NetStat Help - Help on the NetStat command
NetStat Home - Home address list
NetStat Portlist - Port reservation list
NetStat Route - Routing information
NetStat Slap - Service policy definitions and statistics
NetStat Sockets - Clients using socket interface
NetStat TCP - Details about TCP/IP stack address space
NetStat Telnet - Telnet connections
NetStat Telnet Detail - Telnet connections detail
NetStat Up - Date/time TCP/IP was started
NetStat Vcrt - Dynamic VIPA Conn Routing Table information
NetStat Vdpt - Dynamic VIPA Dest Port Table information
NetStat Vipadyn - Dynamic VIPA information

Required parameters:

Address: (Netstat ARP)
Connection ID: (Netstat Drop)
TCP Stack Address Space Name: (Netstat TCP)

Figure 166. NETSTAT Command Screen

2. From the Netstat menu, select one of the Netstat commands. Additional data may be required for certain commands.
3. Click Submit to proceed. The NETSTAT output screen appears.



```
EZZ2350I MVS TCP/IP NETSTAT CS V1R2       TCPIP NAME: TCPIP           14:41:17
EZZ2760I DevName: LOOPBACK          DevType: LOOPBACK  DevNum: 0000
EZZ2766I   DevStatus: Ready
EZZ2761I   LnkName: LOOPBACK          LnkType: LOOPBACK    LnkStatus: Ready
EZZ2762I     NetNum: 0   QueSize: 0
EZZ2820I     BytesIn: 5142854               BytesOut: 5142854
EZZ2768I   BSD Routing Parameters:
EZZ2769I     MTU Size: 00000             Metric: 00
EZZ2770I     DestAddr: 0.0.0.0           SubnetMask: 0.0.0.0
EZZ2810I   Multicast Specific:
EZZ2811I     Multicast Capability: No
EZZ2760I DevName: LCS1              DevType: LCS       DevNum: 0E40
EZZ2766I   DevStatus: Ready
EZZ2761I   LnkName: ETH1              LnkType: ETH         LnkStatus: Ready
EZZ2762I     NetNum: 0   QueSize: 0
EZZ2820I     BytesIn: 718932267             BytesOut: 756324202
EZZ2764I     BroadcastCapability: Yes
EZZ2768I   BSD Routing Parameters:
EZZ2769I     MTU Size: 00000             Metric: 00
EZZ2770I     DestAddr: 0.0.0.0           SubnetMask: 255.255.0.0
EZZ2810I   Multicast Specific:
EZZ2811I     Multicast Capability: No
```

Figure 167. NETSTAT DevLinks Output Screen

Some additional fields may be required for specific commands:

Address	The IP address for the resource. Required for the Netstat ARP command.
Connection ID	Required for the Netstat Drop command. The Drop command and the associated connection ID fields may not be visible if you do not have the appropriate level of user authority.
Address Space Name	Required for the Netstat TCP command.

4. Do one of the following:
   - To enter another Netstat command, click the Back button on the browser.
   - To return to the main Commands menu, click the Commands navigation tab.
   - To return to the SysPoint Home Page, click SysPoint on the main menu bar.

Using Storage Commands

Storage commands may be submitted to display shared storage, such as CSM or VTAM buffer pools. The following commands are available:

D NET,CSM,OWNERID=All	Display CSM usage for all owners
D NET,CSM	Display CSM allocations/max used
D NET,BFRUSE	Display VTAM buffer pools

To use the storage commands, perform the following steps:

1. From the Commands main menu, click the Storage hyperlink from under Communication Server Commands. The Shared Storage Commands screen appears.
2. Select a command from the list of available commands, for example,

   D NET,CSM – Display resource.
3. Click Submit. The response to the command appears on the next screen.
4. Use your Web browser's commands to:
   - find a particular string in the output,
   - obtain hardcopy of the output, or
   - return to the main menu by clicking the back button.

You may wish to view more information on CSM or VTAM buffer pools.

Communications Storage Manager (CSM)

The Communications Storage Manager (CSM) is a component of VTAM that allows authorized host applications to share data with VTAM and other CSM users without having to physically copy the data. CSM is provided as part of the HPDT family of services. HPDT optimizes system performance for the transfer of bulk data. By providing a means for authorized applications to share buffers, CSM improves system performance during the transfer of bulk data by reducing the processing required for data movement. As a result, CPU resources (CPU cycles, memory bus, and cache) are conserved.

Application Use of CSM

CSM includes an application programming interface (API) that allows users to obtain and return CSM buffers, change ownership of buffers, copy buffers, and perform other functions related to CSM buffer arrangement. Applications must be authorized to use CSM. The storage key for CSM buffers is key 6, fetch protected. Users set up access data that resides in the CSM buffers. These buffers are obtained from buffer pools that are identified by their buffer size and storage type as follows:

Storage Types	Buffer Sizes (in KB)				
Data space	4	16	32	60	180
ECSA	4	16	32	60	180

Data space storage is a common area data space. It is associated with the master scheduler address space, which results in a data space that persists for the life of the system. When an application obtains buffers from CSM, it is considered the owner of those buffers. CSM can associate buffer responsibility with an address space or a task within an address space, based on application specifications. Applications using CSM are responsible for returning owned buffers so that they are available for others. If ownership is transferred to another user, the new owner is responsible for the return of the buffers. CSM manages buffer reclamation during termination at the task/address space level based on ownership.

View CSM Command

The DISPLAY CSM command allows you to monitor the use of storage managed by the Communications Storage Manager (CSM). It determines how much CSM storage is in use for ECSA and data space storage pools and to get information about specific applications that are using CSM managed storage pools. Since it is routed to CSM, VTAM does not have to be operational when you execute this command.

The resulting VTAM display shows the following, with storage amounts displayed in units of K (kilobytes) or M (megabytes):

- the size of a buffer residing in a data space
- the size of a buffer residing in ECSA
- if OWNERID is specified, the amount of storage allocated to the owner
- if OWNERID is not specified, storage usage information for each buffer pool
- the maximum current values for fixed and ECSA storage

VTAM Buffers

VTAM uses buffer pools to control the handling of data: VTAM control blocks, I/O buffers, and channel programs that control the transmission of data. Each buffer pool handles storage for a different VTAM service, therefore, the needs of your network determine which buffer pools are used the most. After you determine which buffer pools are the most important to your system, you may want to change the size of some of them.

When you set a buffer pool size, you are reserving storage for use only by that buffer pool. If you specify buffer pools that are larger than necessary, you are setting aside storage that is not being used. In effect, the storage is being wasted when it could be used in other areas.

When you set a buffer pool size that is too small, VTAM reaches buffer pool limit and dynamically allocates more space in the buffer pool. When the current need is satisfied, VTAM dynamically de-allocates space in the buffer pool. Specifying small buffer pools conserves storage, but causes frequent CPU use for expansion and contraction.

Types of Buffer Pools

All buffer pools are allocated in extended CSA subpool 231 with KEY=6.

APBUF	Used to provide fixed common storage if VTAM fails to obtain other storage from the operating system. For buffers not related to I/O.
BSBUF	Used to maintain session information for peripheral nodes for which VTAM performs boundary function. One buffer is required for each boundary LU session (SSCP-PU, SSCP-LU, LU-LU).
CRA4	Used for scheduling and error recovery.
CRA8	Used for scheduling and error recovery.
CRPLBUF	RPL-copy pool. One buffer is required for each VTAM application program request until the operation is complete.
IOBUF	Used for input/output data. Every PIU that enters or leaves VTAM resides in an I/O buffer. This pool is 31-bit addressable.
LFBUF	One buffer is required for each active application program with an EAS value (on APPL definition statement) less than 30. If the EAS value is greater than 30, this information is contained in SFBUF. One buffer is required for each TSO user who is logged on.
LPBUF	Used for scheduling and audit trail (error recovery). One buffer is required for each active VTAM process.
SFBUF	Used to contain application program information and LU blocks. One buffer is required for each active application program with an EAS value (on APPL definition statement) greater than or equal to 30.
SPBUF	Used for large message (LMPEO) requests. One buffer is required per concurrent LMPEO send request.

TIBUF	Used to perform input/output operations for CSM-capable protocols. This pool is in 31-bit storage.
XDBUF	Used for physical I/O to VTAM peripheral nodes for connection activation (for example, XID exchange processing). This pool is 31-bit addressable.

The buffer pool types specifically used by TCP/IP are: IOBUF, LFBUF, CRPLBUF, TIBUF, and CRA4.

Display VTAM Buffer Pools

The DISPLAY BFRUSE (buffer use) command displays information about VTAM buffer use. It also displays storage usage summary information for VTAM modules. The command displays all buffer pools and information along with the following:

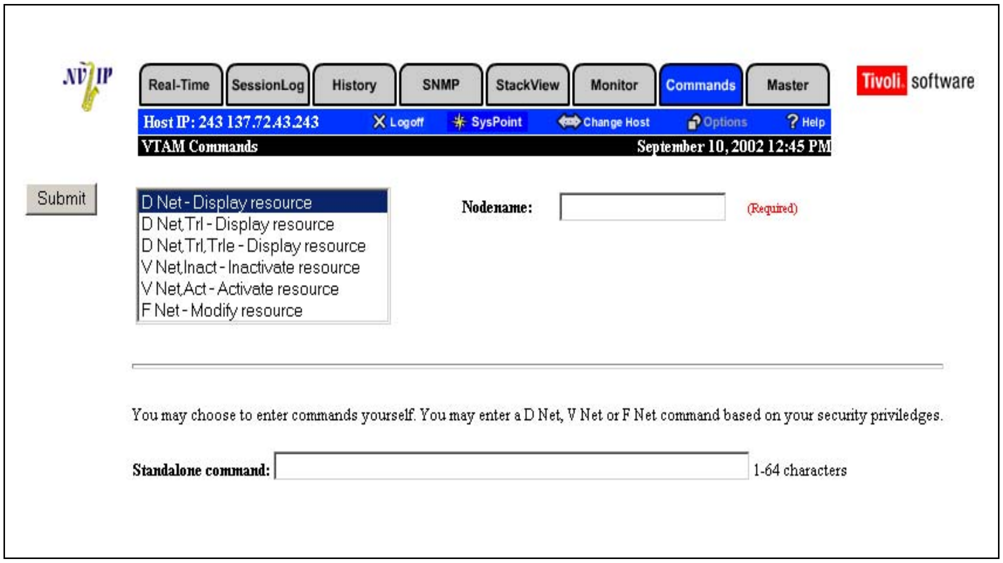
- common service area (CSA) usage for buffers
- intermediate routing node buffer usage limit (IRNLIMIT)
- VTAM private storage usage for buffers
- common service area (CSA) usage for modules
- VTAM private storage usage for modules

Using VTAM Commands

VTAM commands may be submitted by completing the required fields using the assisted mode, or by typing in the explicit command using the standalone option.

To access the VTAM Commands main page, perform the following steps:

1. From the Commands main menu, click the VTAM hyperlink under the Communication Server Commands. The VTAM Commands main screen appears.



Host IP: 243 137.72.43.243

VTAM Commands September 10, 2002 12:45 PM

D Net - Display resource
D Net,Trl - Display resource
D Net,Trl,Trle - Display resource
V Net,Inact - Inactivate resource
V Net,Act - Activate resource
F Net - Modify resource

Nodename: (Required)

You may choose to enter commands yourself. You may enter a D Net, V Net or F Net command based on your security priviledges.

Standalone command: 1-64 characters

Figure 168. VTAM Commands Main Screen

Assisted VTAM Commands

VTAM commands may be submitted to diagnose network problems for resources. You may execute Display (D Net), Vary Active (V Net,Act), Vary Inactive (V Net,Inact), or Modify (F Net) commands. The Display command is available to all users. The other commands require security authorization. Only authorized commands will appear.

The following VTAM command types are available using the assisted mode:

D NET ...	Display status of a resource in VTAM. A display with the extended attribute is shown.
V NET,INACT ...	Inactivate a resource in VTAM.
V NET,ACT ...	Activate a resource in VTAM.
F NET ...	Modify a resource in VTAM.

To use the assisted VTAM commands, perform the following steps:

1. Click on the Commands tab. The Commands main page appears.
2. Select a command from VTAM Command menu, for example, D NET - Display resource.

3. Enter the nodename of the device to be displayed in the Nodename field.
4. If you are doing a Modify command (F NET) and there are additional parameters to be entered, enter them in the field provided. The additional parameters are appended to the end of the command. For example, given the command "F NET,myNodename,myParms", myNodename is entered in the Nodename field and ",myParms" is entered in the additional parameters field.
5. Click Submit. The response to the command appears on the next screen.
6. Use your Web browser's commands to:
   - find a particular string in the output,
   - obtain hardcopy of the output, or
   - return to the main menu by clicking the Back arrow.

Entering Standalone Commands

You may enter commands by explicitly typing in the command yourself. This is the standalone command option. All commands must be prefaced by "D NET", "V NET", or "F NET". The commands are sent to VTAM. To use the standalone command option, simply enter the command in the space provided and press Submit. The response to the command appears on the following screen.

Appendix A: TCP Connect States

The following information is taken from RFC793 and explains the TCP/IP connect states. A connection progresses through a series of states during its lifetime. The states are listed in the table below. Note that CLOSED is a fictional state because it represents the state when there is no TCB, and therefore, no connection.

LISTEN	represents waiting for a connection request from any remote TCP and port.
SYN-SENT	represents waiting for a matching connection request after having sent a connection request.
SYN-RECEIVED	represents waiting for a confirming connection request acknowledgment after having both received and sent a connection request.
ESTABLISHED	represents an open connection, data received can be delivered to the user. The normal state for the data transfer phase of the connection.
FIN-WAIT-1	represents waiting for a connection termination request from the remote TCP, or an acknowledgment of the previous connection termination request.
FIN-WAIT-2	represents waiting for a connection termination request from the remote TCP.
CLOSE-WAIT	represents waiting for a connection termination request from the local user.
CLOSING	represents waiting for a connection termination request acknowledgment from the remote TCP.
LAST-ACK	represents waiting for an acknowledgment of the connection termination request previously sent to the remote TCP (which includes an acknowledgment of its connection termination request).
TIME-WAIT	represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request.
CLOSED	represents no connection state at all.

A TCP connection progresses from one state to another in response to events. The events are:

- the user calls: OPEN, SEND, RECEIVE, CLOSE, ABORT, and STATUS
- the incoming segments, particularly those containing the SYN, ACK, RST and FIN flags, and timeouts.

(This page intentionally left blank.)

Appendix B: FTP Replies

All FTP replies consist of three-digit numbers with an optional text message following the number. Each of the three-digit numbers has special significance.

The NV4IP FTP Error Log displays all reply codes where 250 = UNTRUE.

There are five values for the first digit of the reply code. "1-3" in the first digit indicates the three function groupings of Positive replies. "4-5" in the first digit indicates the two groupings of Negative replies (errors).

The value for the first digit in the reply code (1-5) indicates the following:

1	Positive Preliminary Reply. The requested action is being initiated and you should expect another reply before proceeding with a new command.
2	Positive Completion Reply. The requested action has been successfully completed and you can enter a new command. The command has been accepted, but the requested action is being held in abeyance pending receipt of further information. You should send another command specifying this information.
3	Positive Intermediate Reply.
4	Transient Negative Completion Reply. This is a temporary error condition. You should attempt to enter the command again.
5	Permanent Negative Completion Reply. The command was neither accepted nor executed. You should not attempt to enter the same command again (in the same sequence).

The value for the second digit in the reply code (0-5) indicates the following:

0	Syntax
1	Information
2	Connections
3	Authentication and Accounting
4	An unspecified value
5	File System

The value for the third digit in the reply code provides a finer gradation of meaning in each of the function categories specified by the second digit.

The following list displays typical error codes in numeric order, with message strings following each number. The message string associated with each reply may be server-dependent, so it is likely to vary for each reply code. The reply code itself, however, must strictly follow the specifications described in this section.

Error Code	Message String
110	Restart marker reply. In this case, the text is exact and not left to the particular implementation; it must read: MARK yyyy = mmmm Where yyyy is User-process data stream marker, and mmmm server's equivalent marker (note the spaces between markers and "=").
120	Service ready in nnn minutes.
125	Data connection already open; transfer starting.
150	File status okay; about to open data connection.
200	Command okay.
202	Command not implemented, superfluous at this site.
211	System status, or system help reply.
212	Directory status.
213	File status.
214	Help message On how to use the server or the meaning of a particular non-standard command. This reply is useful only to the human user.
215	NAME system type. where NAME is an official system name from the list in the Assigned Numbers document.
220	Service ready for new user.
221	Service closing control connection.
225	Data connection open; no transfer in progress.
226	Closing data connection.
227	Entering passive Mode (h1, h2, h3, h4, pl, p2).
230	User logged in, proceed.
250	Requested file action okay, completed.
257	"PATHNAME" created.
331	User name okay, need password.
332	Need account for login.
350	Requested file action pending further information.

Error Code	Message String
421	Service not available, closing control connection. This may be a reply to any command if the service knows it must shut down.
425	Can't open data connection.
426	Connection closed; transfer aborted.
450	Requested file action not taken. File unavailable (e.g., file busy).
451	Requested action aborted: local error in processing.
452	Requested action not taken. Insufficient storage space in system.
500	Syntax error, command unrecognized. This may include errors such as command line too long.
501	Syntax error in parameters or arguments.
502	Command not implemented.
503	Bad sequence of commands.
504	Command not implemented for that parameter.
530	Not logged in.
532	Need account for storing files.
550	Requested action not taken.
551	Requested action aborted: page type unknown.
552	Requested file action aborted. Exceeded storage allocation (for current directory or dataset).
553	Requested action not taken. File name not allowed.

(This page intentionally left blank.)

Appendix C: Sample Member BCONF00

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

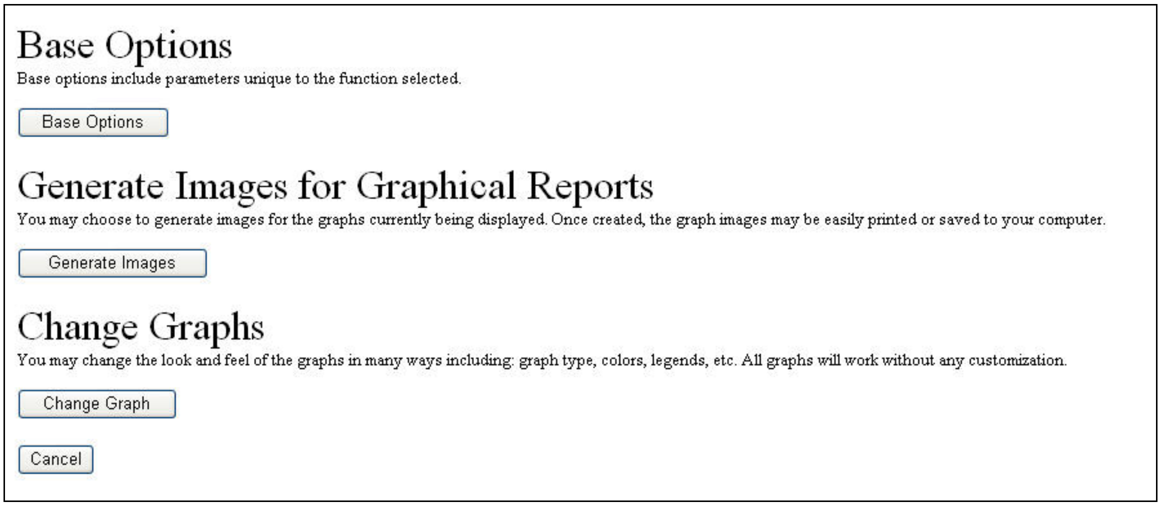
```
//AESTBPRM DD DISP=SHR,
//   DSN=AES.NPMTST13.SAEDSLIB(BCONF00)
```

Figure 169. AESTBPRM DD Statement

```
*
*  NPM/IP BATCHPR CONFIGURATION PARAMETERS
*
*  EACH STATEMENT HAS THE FOLLOWING SYNTAX:
*
*    <KEYWORD> = <VALUE>
*
*  > AN ASTERISK BEGINS A COMMENT.
*
****************
*************************************************
*                                               *
* 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. *
*                                               *
*****************************************************************
*
*  KEYWORD    PARAMETERS
*  ========
========================================================
*
*  COMPNAME   COMPANY NAME OR OTHER EQUIVALENT DESCRIPTION TO
BE
*           PUT INTO THE REPORT
*
*           E.G., COMPNAME=Acme Computer Services
*
*COMPNAME=Your Company Name
```

Appendix D : Options Button

The Options button appears in the menu bar below the navigation tabs on each reporting screen where charts may be shown. The Option button allows you to set Base Options (AutoRefresh and Refresh Interval) and/or set Change Graph options (change the look and feel of graphs), depending upon the function you are using. When both of these options are available, the Options main page appears.



Base Options

Base options include parameters unique to the function selected.

Generate Images for Graphical Reports

You may choose to generate images for the graphs currently being displayed. Once created, the graph images may be easily printed or saved to your computer.

Change Graphs

You may change the look and feel of the graphs in many ways including: graph type, colors, legends, etc. All graphs will work without any customization.

Figure 170. Options Main Page

Do one of the following from the Options main page:

- Click Base Options to set AutoRefresh/Refresh Interval options or filter data displayed for some types of reports.
- Click Generate Images to print or save a graph image.
- Click Change Graph to change the look and feel of the graphs in various ways, including: graph type, colors, titles, or legends.
- Click Cancel to return to the previous screen without making any changes.

Base Options

When you select Base Options from the Options main page, you can set AutoRefresh parameters and save them as the default, or cancel.

When you use Base Options from StackView, you can also select which ports you would like to monitor (those for predefined address spaces or those currently in use).

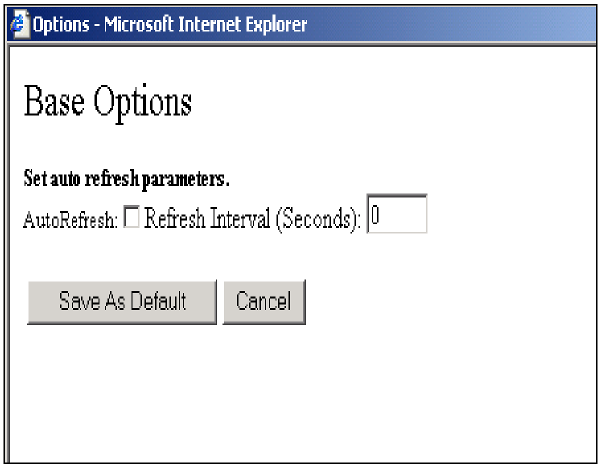
When you use Base Options from the Top Clients History Report, the Base Option buttons allows you to eliminate the viewing of the Loopback (127.0.01) and UDP (255.255.255.255) addresses from the reports.

When you use Base Options from the SNMB MIP Browser screen, you can specify a timeout value to use for the response time threshold. The default is 30 seconds.

Using Base Options

When you select Base Options from the Options main page, the Base Option main page appears. From the Base Option main page you can select AutoRefresh parameters and save them as the default, or cancel.

Note: If you do not set AutoRefresh parameters, you can manually refresh the screen at any time by clicking the Refresh link on the screen. Avoid setting a local interval value less than the Host Monitor interval value.



Set auto refresh parameters.

AutoRefresh: ☐ Refresh Interval (Seconds): 0

Figure 171. Base Options

When you use Base Options from StackView, you can also select which ports you would like to monitor (those for predefined address spaces or those currently in use).

When you use Base Options from the Top Clients History Report, the Base Option buttons allows you to eliminate the viewing of the Loopback (127.0.01) and UDP (255.255.255.255) addresses from the reports.

Generating a Graph Image

To generate an image of a graph:

1. From the Show Graph Options screen, click Generate Image.

   The graph appears in a graphical format in your browser.

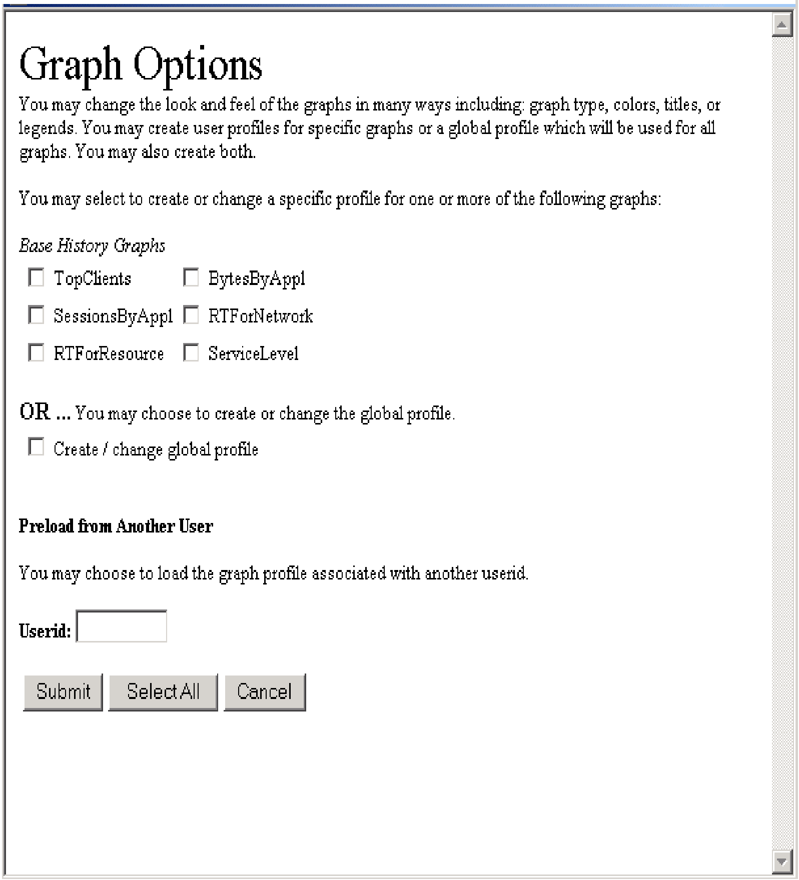
2. Right click the image.
3. Make a selection from the menu. Here you can save or print the image.

Graph Options

When you select Change Graphs from the Options main page, you can change the look and feel of the graphs in various ways, including: graph type, colors, titles, or legends. You can create user profiles for specific graphs, a global profile which will be used for all graphs, or both. If you create both specific graph profiles and a global profile, the specific profile will be used. If no specific profile exists, the global profile will be used. If no global profile exists, the defaults shipped with the product will be used. You may also choose to load the graph profile associated with another User ID. You may do this for either a particular graph or for the global profile.

Using Graph Options

When you select Change Graphs from the Options main page (accessed by clicking the Options link under the navigation bar), the Graph Options page appears.



Graph Options

You may change the look and feel of the graphs in many ways including: graph type, colors, titles, or legends. You may create user profiles for specific graphs or a global profile which will be used for all graphs. You may also create both.

You may select to create or change a specific profile for one or more of the following graphs:

Base History Graphs

☐ TopClients ☐ BytesByAppl
☐ SessionsByAppl ☐ RTForNetwork
☐ RTForResource ☐ ServiceLevel

OR ... You may choose to create or change the global profile.

☐ Create / change global profile

Preload from Another User

You may choose to load the graph profile associated with another userid.

Userid:

Figure 172. Show Graph Options

From this page you may change the look and feel of the graphs in various ways, including: graph type, colors, titles, or legends. You may create user profiles for specific graphs, a global profile which will be used for all graphs, or both. If you create both specific graph profiles and a global profile, the specific profile will be used. If no specific profile exists, the global profile will be used. If no global profile exists, the defaults shipped with the product will be used. You can also choose to load the graph profile associated with another User ID. You can do this for either a particular graph or for the global profile.

Do one of the following:

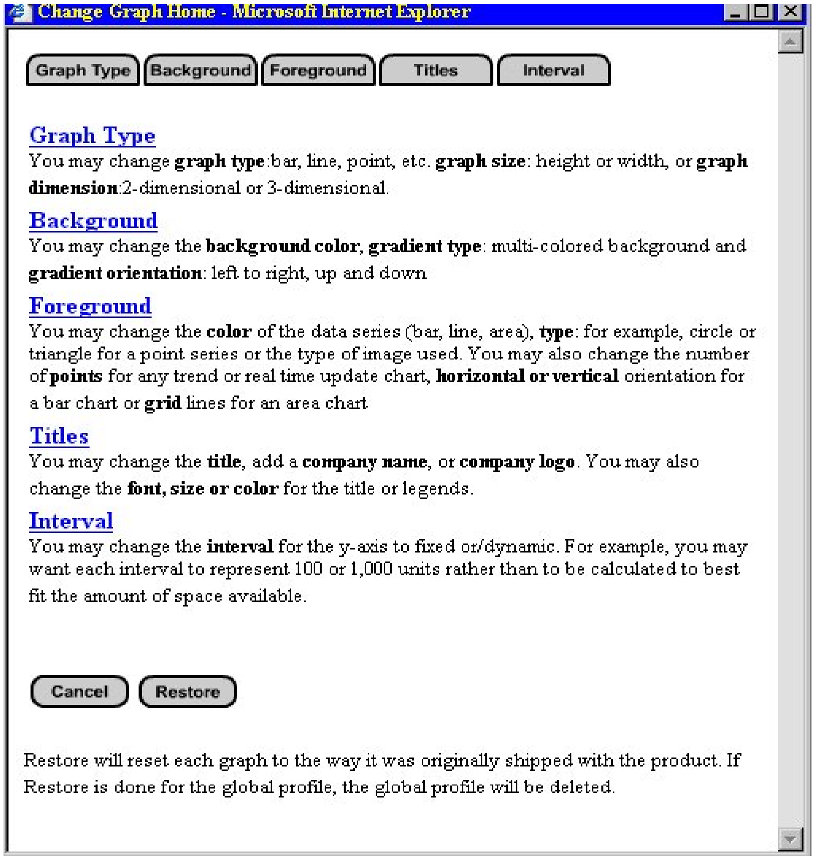
- Select an option and click Submit.
- Click Select All and click Submit.
- Click Cancel to return to the previous screen without making any changes.

Setting Up the Graph Format

The critical resources monitored, the packet size, and the frequency are determined by the Master component of the Performance Manager. The Performance Manager is used to filter what information is displayed and how.

You may customize this display in many ways. You may select from 6 graph types, which may be seen in 2 or 3 dimensions. Once you have selected the type of graph, use the background, foreground, titles, and interval functions to manipulate the graph's appearance to produce the kind of chart you need.

To customize the graphs, use the Options button that appears on each reporting screen where charts may be shown. It is in the menu bar below the navigation tabs. The Option button may allow you to do Base Options or Change Graph, depending on the function you are using. This section concentrates on the Change Graph function.



Graph Type

You may change **graph type**:bar, line, point, etc. **graph size**: height or width, or **graph dimension**:2-dimensional or 3-dimensional.

Background

You may change the **background color**, **gradient type**: multi-colored background and **gradient orientation**: left to right, up and down

Foreground

You may change the **color** of the data series (bar, line, area), **type**: for example, circle or triangle for a point series or the type of image used. You may also change the number of **points** for any trend or real time update chart, **horizontal or vertical** orientation for a bar chart or **grid** lines for an area chart

Titles

You may change the **title**, add a **company name**, or **company logo**. You may also change the **font, size or color** for the title or legends.

Interval

You may change the **interval** for the y-axis to fixed or/dynamic. For example, you may want each interval to represent 100 or 1,000 units rather than to be calculated to best fit the amount of space available.

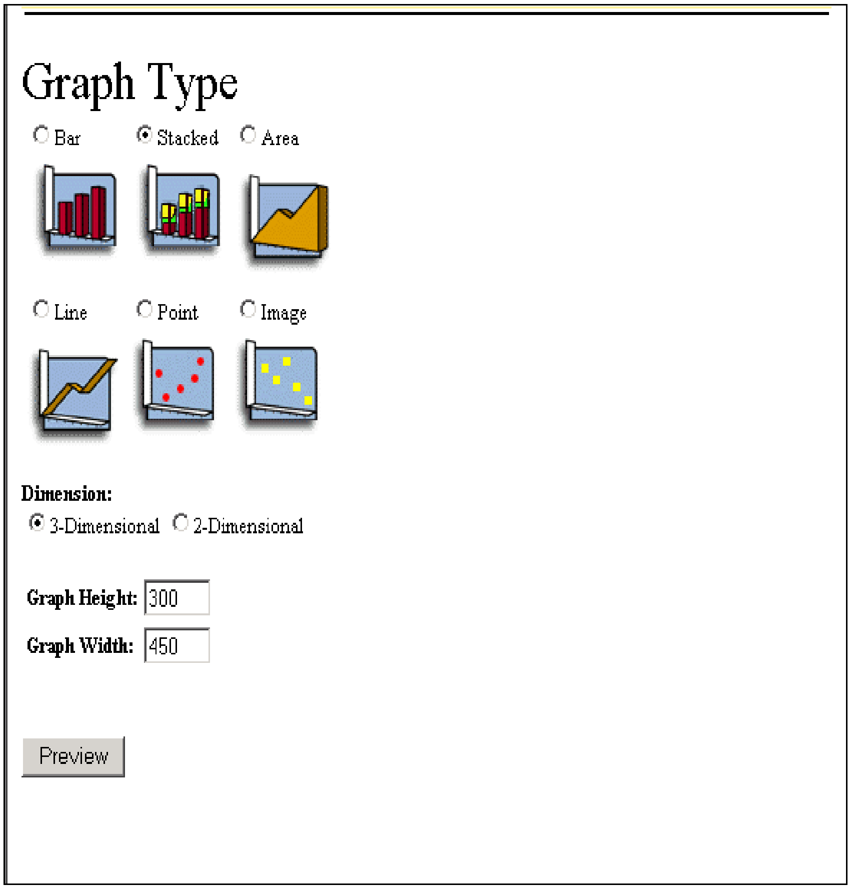
Restore will reset each graph to the way it was originally shipped with the product. If Restore is done for the global profile, the global profile will be deleted.

Figure 173. Change Graph Home

Using Change Graph Type

NV4IP provides data for (6) chart types. These types are:

- ***Area*** – shows the relative importance of values over a period of time.
- ***Bar*** – the most commonly used chart. It shows variation over a period of time.
- ***Stacked*** – this chart displays the same information as the bar chart but the bars are displayed in a stacked format instead of side-by-side
- ***Line*** – shows trends or changes in data over a period of time.
- ***Point*** – similar to the Line chart. It plots only the points or data markers.
- ***Image*** - similar to the Point chart except that an image may be used in place of points or line markers.



Graph Type

○ Bar ● Stacked ○ Area

○ Line ○ Point ○ Image

Dimension:

● 3-Dimensional ○ 2-Dimensional

Graph Height: 300

Graph Width: 450

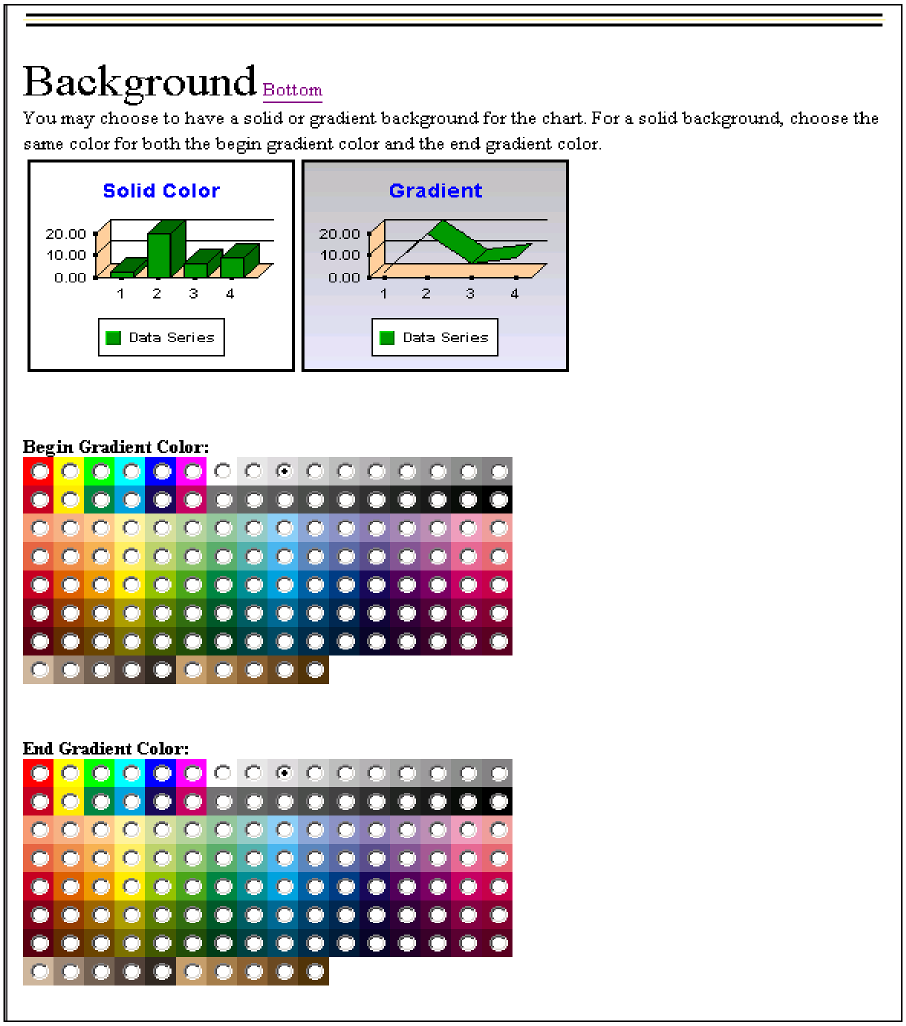
Figure 174. Change Graph Type

You may also change the following parameters:

- ***Dimension*** – shows graph in selected format, either three-dimensional or two-dimensional.
- ***Graph Height*** – assigns height of the graph in pixels.
- ***Graph Width*** – assigns width of the graph in pixels.

Using Change Graph Background

- ***Begin Gradient Color*** – assigns the beginning color in a fading gradient background.
- ***Ending Gradient Color*** – assigns the ending color in a fading gradient background.
- ***Gradient Orientation*** – determines direction of gradient fade.
- ***Grid Lines*** – shows grid lines on background.



Background Bottom

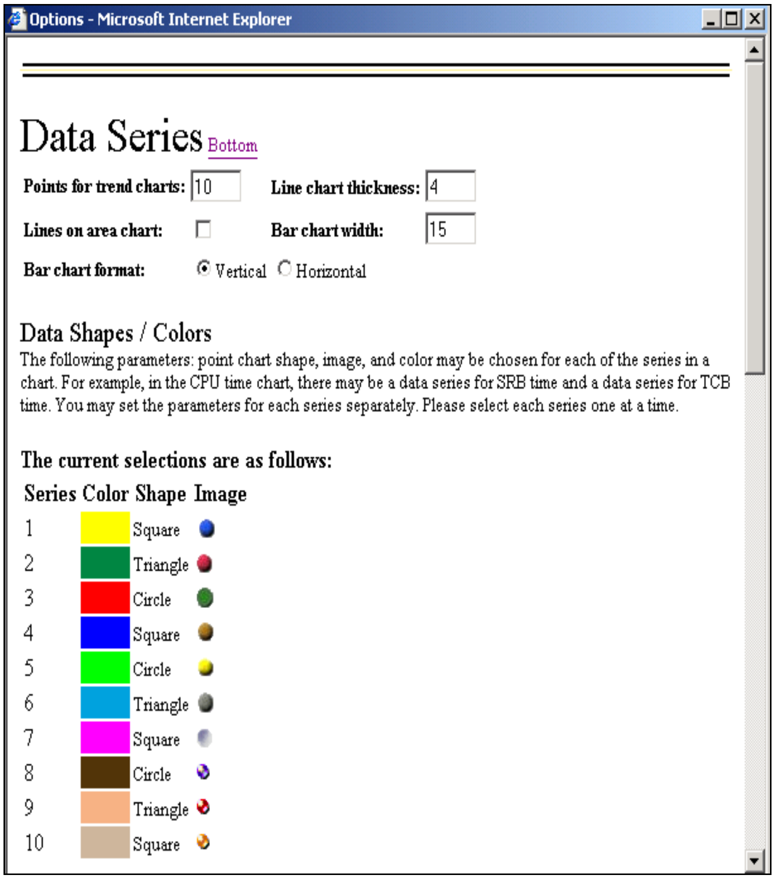
You may choose to have a solid or gradient background for the chart. For a solid background, choose the same color for both the begin gradient color and the end gradient color.

Figure 175. Change Graph Background

Using Change Graph Foreground

- ***Points For Trend Charts*** – defines the number of points used in trend charts.
- ***Line Chart Thickness*** – displays line charts with specified width. This applies to 2-dimensional charts only.
- ***Lines On Area Chart*** – shows lines on area chart.
- ***Bar Chart Width*** – assigns width of bars on bar charts.
- ***Bar Chart Format*** – determines orientation of bars on bar charts.

- ***Select Series Parameters*** – applies options to the chosen series. The user can select various options on the chosen series independent from the other series.
- ***Point chart shapes*** – selects shape type for point charts.
- ***Image chart selection*** – selects image for image charts. (Note: User can input their own images by replacing the default images.)
- ***Series color*** – changes colors of the chosen series.
- ***3D Color*** – changes the 3D perspective color of the chosen series.



Data Series Bottom

Points for trend charts: 10 **Line chart thickness:** 4

Lines on area chart: ☐ **Bar chart width:** 15

Bar chart format: ● Vertical ○ Horizontal

Data Shapes / Colors

The following parameters: point chart shape, image, and color may be chosen for each of the series in a chart. For example, in the CPU time chart, there may be a data series for SRB time and a data series for TCB time. You may set the parameters for each series separately. Please select each series one at a time.

The current selections are as follows:

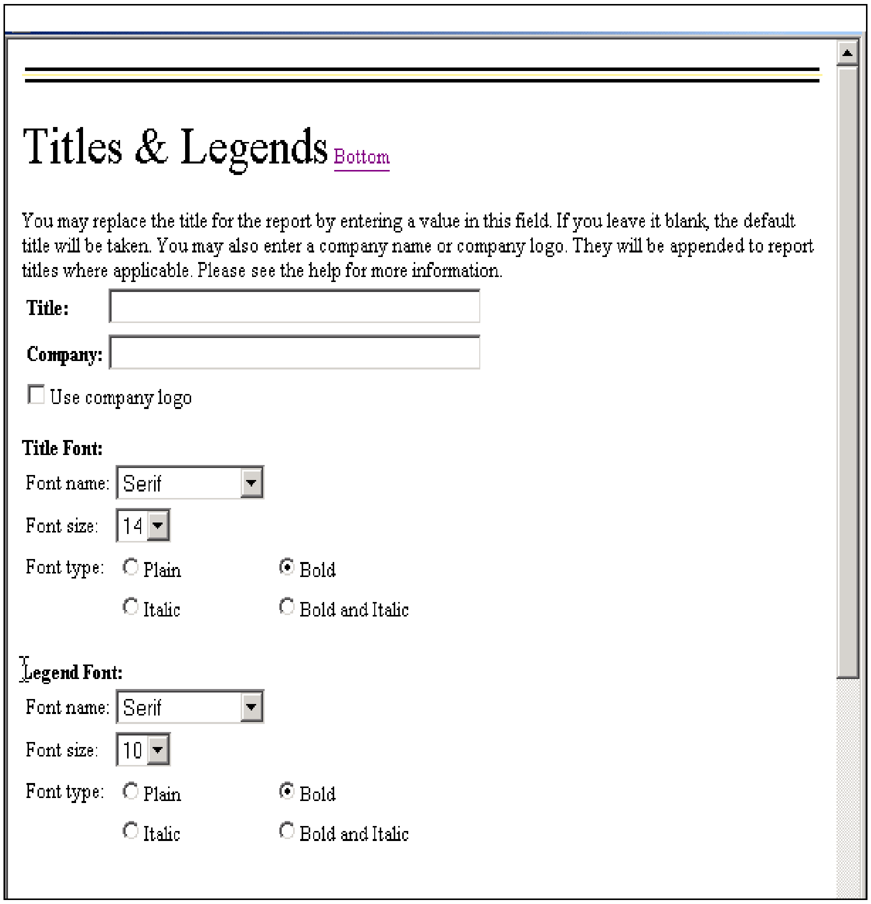
Series	Color	Shape	Image
1	🟨	Square	●
2	🟩	Triangle	●
3	🟥	Circle	●
4	🟦	Square	●
5	🟩	Circle	●
6	🟦	Triangle	●
7	🟪	Square	●
8	🟫	Circle	●
9	🟧	Triangle	●
10	🟫	Square	●

Figure 176. Change Graph Foreground

Using Change Graph Titles

- ***Title/Company*** – allows for input of graph titles as well as a company name.
- ***Company Logo*** –shows a company logo in a title bar above graphs. The image must be called "mycompany.gif" and placed in the \images directory where other product images are stored. For more assistance, please view the Web server documentation in the product installation guide.
- ***Title Font*** – changes various font attributes for the title.

- ***Legend Font*** – changes various font attributes for the legend.
- ***Legend Color*** – changes font colors for the legend.



Titles & Legends

You may replace the title for the report by entering a value in this field. If you leave it blank, the default title will be taken. You may also enter a company name or company logo. They will be appended to report titles where applicable. Please see the help for more information.

Title:

Company:

☐ Use company logo

Title Font:

Font name: Serif

Font size: 14

Font type: ○ Plain ● Bold ○ Italic ○ Bold and Italic

Legend Font:

Font name: Serif

Font size: 10

Font type: ○ Plain ● Bold ○ Italic ○ Bold and Italic

Figure 177. Change Graph Titles

Change Graph Intervals Option

- ***Calculate Automatically*** – automatically adjusts range increments of graphs.
- ***Range Increment*** – allows user to specify incremental marks on the Y-axis. (Note: "Calculate automatically" must be unchecked.)
- ***Minimum Value*** - sets the lowest value on the Y-axis. (Note: "Calculate automatically" must be unchecked.)

Index