

TR No. AMSEL-IE-TI 02/046



**DEPARTMENT OF THE ARMY  
UNITED STATES ARMY INFORMATION  
SYSTEMS ENGINEERING COMMAND  
FORT HUACHUCA, ARIZONA 85613-5300**



**END2END  
EVALUATION REPORT**

**BY**

**MERLIN TEAM**

**TECHNOLOGY INTEGRATION CENTER**

**AUGUST 2002**

**DISTRIBUTION A**

**Approved for public release; distribution is unlimited.**

### **DISCLAIMER**

**The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.**

### **CHANGES**

**Refer requests for all changes that affect this document to: USAISEC, ATTN: AMSEL-IE-TI, Fort Huachuca, AZ 85613-5300.**

### **DISPOSITION INSTRUCTIONS**

**Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements.**

## END2END EVALUATION REPORT

BY  
JAMES JOHNSON

AUGUST 2002

U.S. ARMY INFORMATION SYSTEMS ENGINEERING COMMAND  
TECHNOLOGY INTEGRATION CENTER

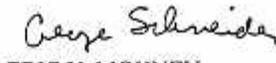
**Distribution Statement A**

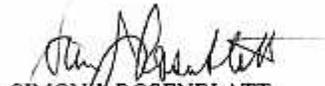
Approved for public release; distribution is unlimited.

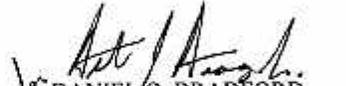
**Product Certification**

Signatures below indicate that this product does not develop a design or require a formal architectural review and complies with all USAISEC standards.

  
JAMES H. JOHNSON  
Electronics Engineer  
MERLIN Team

  
for ERIC V. MOHNEY  
MAJ, AC  
MERLIN Team Leader

  
SIMON J. ROSENBLATT  
Group Leader  
Technology Management Group

  
for DANIEL Q. BRADFORD  
Director  
Technology Integration Center

## EXECUTIVE SUMMARY

This report is a product review of NetIQ's End2End Network Monitoring Software Suite Version 4.2. It contains recommendations, results, and test procedures of an evaluation conducted at the U.S. Army Information Systems Engineering Command (USAISEC) Technology Integration Center (TIC) on a 30-day trial version of the product. The focus of this evaluation is to determine how useful this software would be to a network administrator.

This software is designed to be used by network administrators to monitor the health of their networked environment. It does this by using software agents installed on existing personal computers (PCs) located throughout a network. These agents, called performance endpoints, collect data from the user's perspective by generating emulated application network traffic to the designated target site. They can provide network throughput statistics, monitor applications activity and hardware performance based on user configurable parameters.

The result of the evaluation shows that the End2End software suite has the tools necessary to help network administrators make informed performance decisions about their network infrastructure. It provides easy navigation through its web interface and presents the results in easy to interpret reports. In addition, NetIQ's technical support was courteous, knowledgeable, and responsive.

Overall, this application was well planned and would be a welcomed addition to any network administrator's toolbox.

## TABLE OF CONTENTS

	<b>Page</b>
Executive Summary .....	v
1.0 INTRODUCTION .....	1
2.0 OBJECTIVES .....	1
3.0 METHODS .....	1
3.1. End2End Description.....	1
3.2. Configuration and Setup.....	2
4.0 RESULTS .....	8
4.1 Application .....	8
4.2 Network .....	8
4.3 Services.....	9
4.4 System .....	10
4.5 Additional Modules .....	11
5.0 CONCLUSIONS .....	13
6.0 RECOMMENDATIONS.....	13

### Tables

Table 1. Evaluation Equipment .....	3
-------------------------------------	---

### Figures

Figure 1. Network Configuration .....	2
Figure 2. Application Configuration .....	4
Figure 3. Network Configuration .....	6
Figure 4. Service Configuration .....	6
Figure 5. Web Post Translator Screen .....	7
Figure 6. Endpoint Configuration.....	7
Figure 7. Application Monitor Results .....	8
Figure 8. Network Monitor Results .....	9
Figure 9. Event Monitor .....	9
Figure 10. Services Monitor Results .....	10
Figure 11. System Monitor Results .....	10
Figure 12. Graphical Output.....	11
Figure 13. Tabular Output .....	11
Figure 14. Expert Analysis Screen .....	12
Figure 15. Diagnostic on Demand Screen .....	12

### Appendices

Appendix A. End2end System Requirements .....	A-1
Glossary. Acronyms and Abbreviations .....	Glossary-1

**This page is intentionally left blank**

## END2END EVALUATION REPORT

### 1.0 INTRODUCTION

With the integration of the network and Internet into the overall business process, users have needed a tool that allows network administrators to monitor their enterprise performance (network and personal computer (PC)) as a whole. With this information an administrator can develop performance trends, determine which network or PCs need to be upgraded, or how best to distribute the servers across the enterprise based on their installation's usage patterns. This report is a product review of NetIQ's End2End Performance Monitor Suite Version 4.2. It contains recommendations, results, and test procedures of an evaluation conducted at the U.S. Army Information Systems Engineering Command (USAISEC) Technology Integration Center (TIC) on a 30-day trial version of the product. The focus of this evaluation is to determine how useful this software would be to a network administrator.

### 2.0 OBJECTIVES

This report verifies NetIQ's claims of the main capabilities of End2End Performance Monitor Suite Version 4.2. This evaluation focuses on answering the following questions:

- Does this tool monitor network performance?
- Does this tool monitor applications usage and PC performance on a network?
- Does the product cause any performance problems on the network or host PC?
- Is the software easy to use and would it be a useful tool to a network administrator?

### 3.0 METHODS

#### 3.1. End2End Description

The End2End performance suite is composed of two parts, a server running the main End2End software and a remote software agent called a performance endpoint (PE). These agents are installed on the target PCs located throughout your network. The endpoints can collect four types of information:

- Network throughput as measured from the user's PC.
- Application response time measured from the user's perspective.
- Service response time from the user's PC to a particular site, not necessarily controlled by the administrator.
- The user's PC performance data (central processing unit (CPU), input/output (I/O) and memory usage).

Network traffic is generated from scripts that are running on these target PCs. The scripts emulate the actual packet traffic that an application would generate. This is accomplished by using the library of scripts that come with End2End or by creating your own unique scripts using their capture tools. The scripts that come with End2End emulate common applications (i.e. Exchange, Domain Name Service (DNS), etc.) found on a typical network. The endpoints run as background programs or services, communicating with the Application Programming Interfaces (API) connected to the network protocol stack.

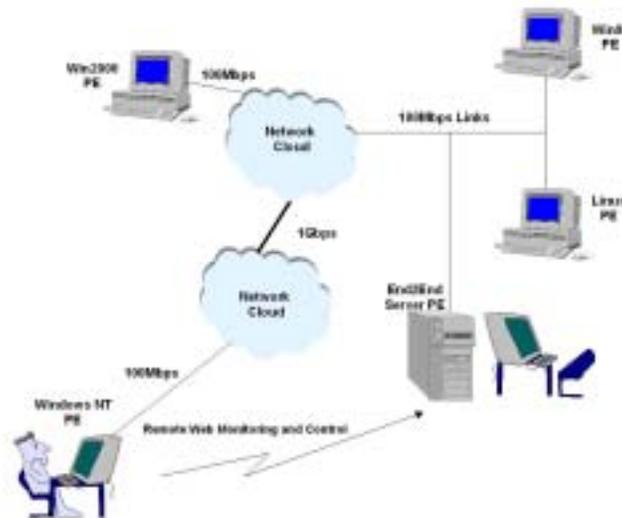
The application module, passively monitors the application's activity by sampling the network traffic generated by the host PC's port. Placement of these endpoints should focus on the key areas of the network (i.e., server farm, key network links).

The service module allows the operator to monitor the performance by sending queries from the user's PC to the designated target server. The scripts used in this module do not require the use of an endpoint at the distant end. This provides the flexibility to test response time to sites that are not under the control of the operator.

The PC performance data is collected by the endpoint and stored on the PC until requested by the server running the End2End program (here after referred to as the End2End server). By default the End2End server pulls down information every 30 minutes for the network and services data and 60 minutes for application and system data. There is an accelerated data flow option that comes up on the initial install. This sets the polling cycle to every 5 minutes for the network and services modules and 15 minutes for system and application. Evaluators used the optional configuration to conduct this evaluation.

### 3.2. Configuration and Setup

The target PCs needed separate endpoints loaded for each of the four operating systems (NT, Win98, Win2000 and Linux). For a listing of the supported operating systems, see [Appendix A](#). Figure 1 displays the network configuration for this evaluation.



**Figure 1. Network Configuration**

Each PC used in this evaluation, to include the End2End server, had an endpoint loaded on it. Loading the endpoint on the End2End server is not required for the software to function. However, for this evaluation the engineers loaded an endpoint on the server to see what effect it would have on the system. For the installation of the End2End software program, NetIQ recommends a dedicated server for best performance. [Appendix A](#) lists the hardware and software requirements for the End2End server. When loading the End2End software, the installation wizard checked to make sure the system met all the requirements before proceeding with the installation. If it determined that the system didn't have all the installed components, it stopped at a prompt that described the problem and contained a link to the required software. In addition to the software key, that was required to install the software, NetIQ attached an evaluation guide to the email. This had many helpful tips on the operation of their product, such as how the different modules (Network, Application, Services, and System) function. It explains the different types of scripts and how to use

them. All configuration and monitoring is accomplished via a web server, set up on the End2End server. The operator must do the initial setup from the End2End server. Once this is finished, the End2End program allows remote monitoring by default. This flexibility allows the administrator to monitor the tests from alternate locations and not become tied down to the console directly connected to the End2End server. To allow for remote configuration, the operator must download a small executable from the End2End server to a remote station. The operator's ability to use this option will depend on the organization's security policy. The software will not allow two operators to configure the system at the same time. It brings up a selection screen to show the operators their options (disconnect other user now, disconnect with warning, do not disconnect). Table 1 lists the equipment used to conduct this evaluation.

**Table 1. Evaluation Equipment**

Computer Description	Software/Hardware
Linux PC	Redhat Version 7.0 PII 933 MHz 128 MB RAM (1) 20 GB Hard drive
Windows 98 PC	Second Edition with Explorer 6.0 PII 266 MHz 64 MB RAM (1) 6.4 GB Hard drive
Windows NT PC	Version 4.0 SP5 Micron Client Pro PII 450 MHz 128 MB RAM (1) 2 GB (1) 10 GB Hard drive
Windows 2000 PC	2000Professional Dell Latitude PIII 600 MHz 256 MB RAM (1) 20 GB Hard drive

**Note:** GB – gigabyte    MB – megabyte    MHz – megahertz    RAM – random access memory

The Linux endpoints only monitor network performance. The Linux version did not support application, services, or system monitoring, which was only available with the Windows-based endpoints. The evaluators asked End2End technical support if they would support these services in the future. Their answer was that they currently did not know of any effort to incorporate these features in a future release. But they did recognize the need for such an upgrade citing the continued growth of Linux in the server market.

Once the evaluators installed the End2End software program and it discovered the endpoints, the monitoring of performance could begin. The End2End software program

performs the discovery process by sending a User Datagram Protocol (UDP) packet to all the devices on the network. Since this discovery process could potentially disrupt network traffic, the End2End software program provides the ability to search by subnet or at scheduled times. It also allows the user to define endpoints if the End2End server cannot discover them. This situation could occur if the endpoint is on the other side of a firewall, because the firewall would block the UDP packet query.

### 3.2.1 Application

To start testing the application monitoring function, the operator must enable the application of interest from the default list provided by the End2End program. The operator can modify or add to this list to meet their organization’s requirements. Evaluators chose Exchange and Web activity applications for this part of the evaluation. Figure 2 displays the list of default applications.

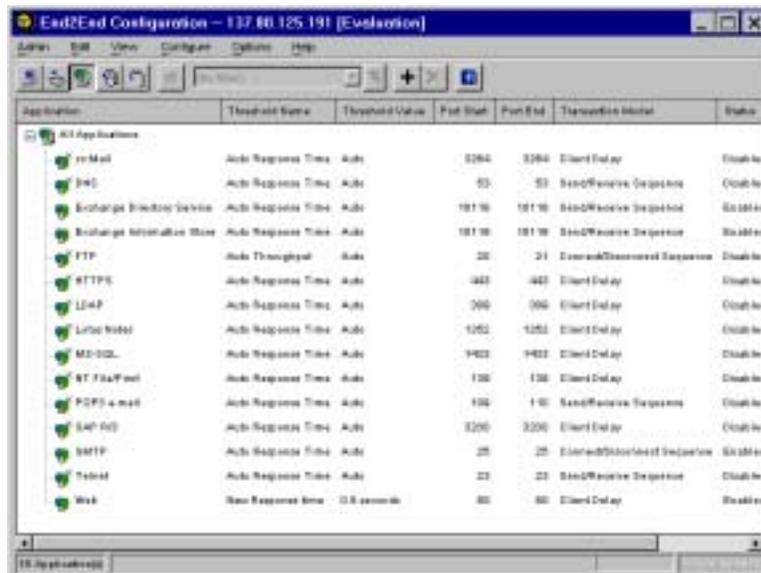


Figure 2. Application Configuration

The screen shot from Figure 2, also displays the different configuration options available to the operator: threshold levels, port numbers, and transaction mode. The End2End program has two built in auto threshold levels, one for response time and one for throughput. These dynamic mode settings adjust their values based on the historical data for that particular connection. This automated threshold level provides a quick way to gather performance statistics from the PC. The End2End program also allows the operator to add static response time thresholds. To add a static response time, evaluators made a copy of the auto response time threshold and saved it to a new name. They selected a static response time value of 0.5 seconds and applied it to the Web application (last entry in Figure 2). This had the effect of changing all the endpoints monitoring web activity to have the same static threshold of 0.5 seconds. Port numbers can be changed as well, but evaluators did not change these settings for this evaluation. The transaction model column contains a brief description describing how the End2End program will measure a transaction. A transaction is any function that can be performed by a user (i.e., logging on to a system, opening a web page etc.). The length of time required to complete a transaction is called a measured interval. End2End program supports three types of transaction models: Connect/Disconnect Sequence, Send/Receive Sequence, and Client Delay. The Connect/Disconnect Sequence measures the

time it takes from the completion of a connect request by the client to the start of a disconnect request generated by the same client. This model can include multiple sends and receives. The Send/Receive Sequence measures each send/receive sequence. The third model is similar to the Send/Receive except a delay (in milliseconds) can be set. The transaction will not be complete until the delay time threshold has been met or exceeded. This measure interval could include several send and receive pairs. For this evaluation, evaluators used the default transaction settings for each of the applications.

### **3.2.2 Network**

This module is designed to test the performance of the installation's infrastructure. To monitor network performance, evaluators used the recommended response time and throughput scripts. NetIQ recommends using the response time and throughput scripts to create a baseline measurement for the link. By using their default response time script, one can collect the best response time (measured in seconds) that the link can achieve. They do this by sending a very small (100 byte) file between the two endpoints. The End2End program uses the throughput scripts to measure the highest throughput (measured in kilobits per second (kbps)) that the link is capable of. This initial size is set to measure the throughput on a 10-megabits per second (Mbps) link. Their goal is to take a quick measurement by sending a small file (100 kilobyte (kB)) that would not interfere with the traffic on the existing network. For faster gigabit links or slower links like a T1, users should increase or decrease the file size accordingly. NetIQ recommends not using more than one-tenth of the capacity of the network to do this measurement, to limit its effect on the performance of the network. This would mean to test a 1-gigabits per second (Gbps) link, evaluators should modify the throughput script to send a 10-MB file. This is just a suggestion and can be modified to meet the user's requirements. NetIQ allows the user the ability to modify scripts to allow for as much flexibility as possible. To test this functionality, evaluators modified a copy of their File Transfer Protocol (FTP) script to send a 256-kB file. Evaluators added this script, plus a generic web request, and a long connection query to the mix. Then they chose one of their default schedules ("Mon-Fri, 0-24, every 15 minutes") to complete the configuration. The scheduler settings can range from having the endpoint collect data every minute to every 999 hours. Users can only make a test schedule by selecting a range of days and not by selecting a range of dates. The user cannot set up a test to run from 5-7 January, but would need to know the days (Sat, Sun, and Mon). The End2End program includes a calendar to help the operator with this setup. Figure 3 shows a screen shot of the network configuration screen listing the different clients installed on the test network.

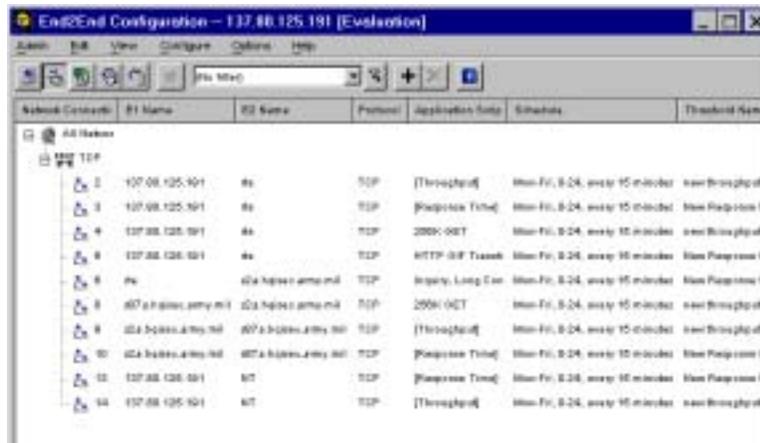


Figure 3. Network Configuration

### 3.2.3 Services

The service module allows the user to run an application on a scheduled basis. This is not the same as the application module, which is just passively monitoring the port activity of its host PC. Just as in the application module, users can modify all the settings or add new applications. The End2End program  up several of the endpoints to query a web site on an hourly basis. The web site does not need to have an endpoint installed on it. NetIQ provided an example in the evaluation guide, on how to best use this feature. They recommended using the main data server for the user's business as the target for this module. Evaluators used the Command's web site (www.hqisec.army.mil) as the target for this service connection. Figure 4 shows this configuration screen for this module.

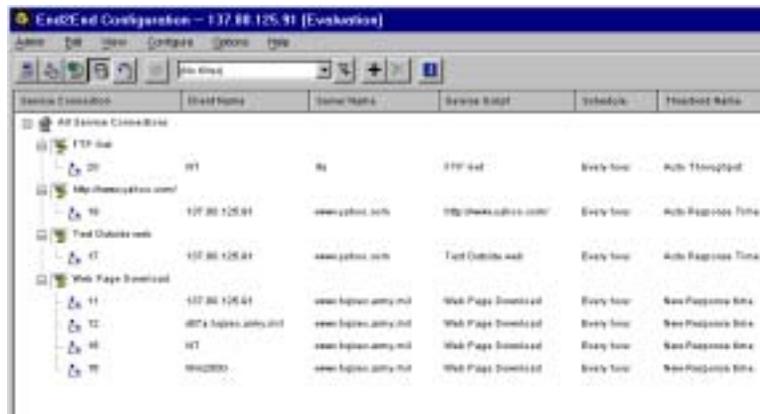


Figure 4. Service Configuration

In addition to the basic queries, evaluators used a customized service script using the Web Transaction Recorder application. With this tool the operators can create their own web queries to meet their specific needs. To test this feature, evaluators captured a session to the yahoo web site. This application also has a playback feature that allows one to test the newly created script. The finished script can then be imported into the service module, and scheduled to run. Figure 5 shows the screen of this capture tool.



Figure 5. Web Post Translator Screen

### 3.2.4 System/Endpoint

The operator can use the endpoint configuration screen to enable/disable application, system and service monitoring for endpoints that support that function. Endpoints allow the use of filters so users can only monitor traffic of interest. This prevents unwanted information from entering the End2End database. Figure 6 shows the endpoint configuration screen.

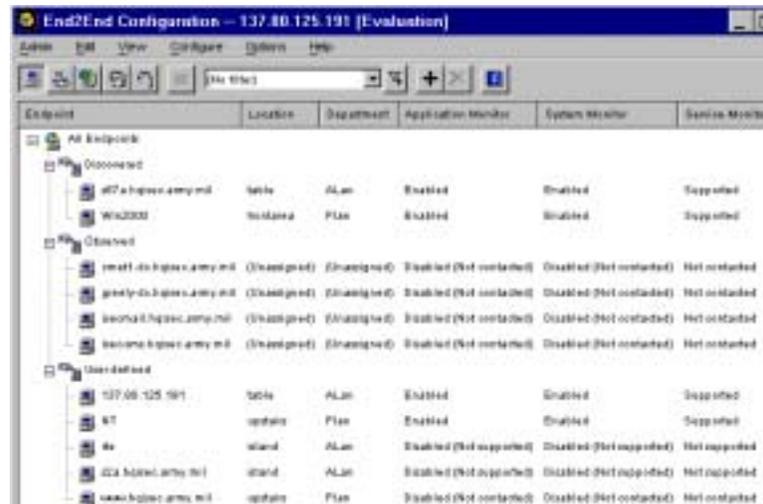


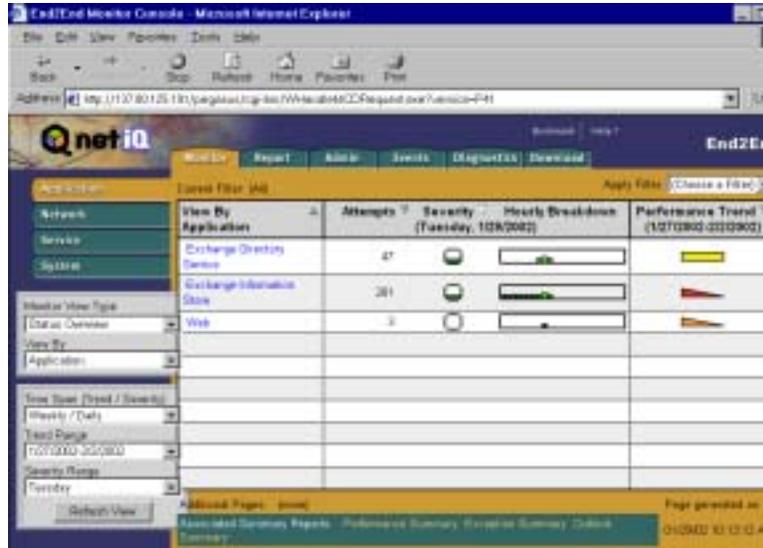
Figure 6. Endpoint Configuration

The endpoint configuration screen lists each endpoint/server and each module it supports. This screen also provides the status of each module. Note the observed section in Figure 6, displays all the servers that the application and service modules had accessed. These servers do not have the endpoints installed on them. They were only accessed by an endpoint. This provides the operator a way to monitor what sites are being accessed.

## 4.0 RESULTS

### 4.1 Application

To view the results, the operator accesses the monitor screen of the End2End program. Figure 7 displays the End2End program status screen showing the results up to that moment. The monitor screen provides the users with a visual representation of their performance based on the thresholds they configured. The screen shows a number of different categories relating to the performance of the connection. This includes the following: the name of the application, number of attempts, the severity level of the connection, the hourly status and the performance trend for the link.

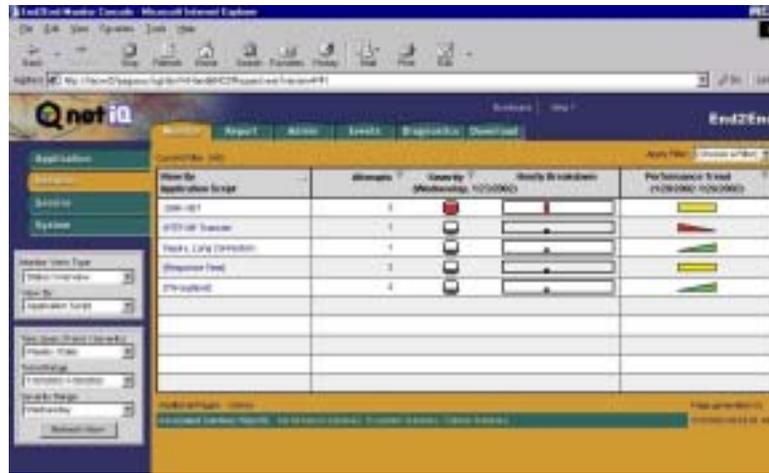


**Figure 7. Application Monitor Results**

The colors on the severity icon correspond to operator set alarm thresholds. The colors range from dark green, light green, to yellow, to orange, and then to red. The screen also displays a bar that records the history of that connection. The time they represent changes depending on the time scale selected. If users selected (monthly/weekly) settings, each bar would represent a day's activity, instead of the hourly results shown in Figure 7. The last column contains the performance trend data based on latest measurements. The severity and performance trend icons support "fly-over" functionality. This allows the user to place the cursor over the icon that will then display additional information for the color. In addition, the user can double-click and select both icons (severity and performance trend) to show more detailed information (exact value of each data point). The monitor screen provides selection fields on the left-hand side to allow the users to search for specific information that best fits their needs.

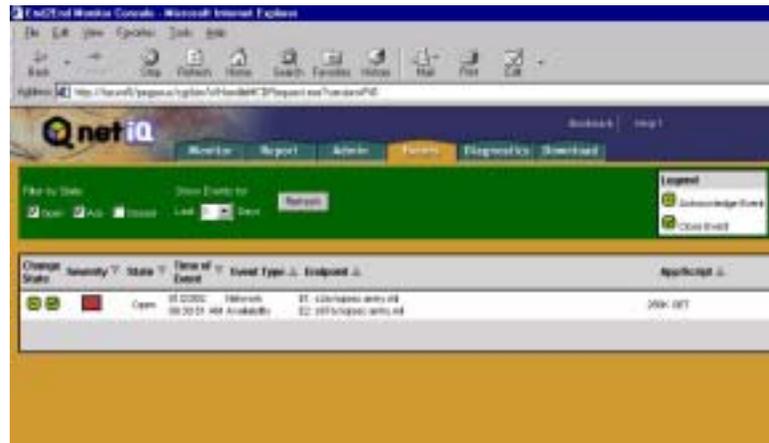
### 4.2 Network

Figure 8 shows the Network Monitor screen showing the five different application scripts and their results.



**Figure 8. Network Monitor Results**

The 256 GET request in Figure 8, has a red indication (very many exceptions). The evaluator purposely caused this event by the shutting down the endpoint on that server. This resulted in a logged event that generated a Simple Network Management Protocol (SNMP) trap. The evaluator configured the End2End program to send a trap for specified events to an Openview server. This ability to access information from different sources on the network, provides more flexibility to the operators. Figure 9 shows the event monitor screen for this event.



**Figure 9. Event Monitor**

### 4.3 Services

Figure 10 displays the results from the service configuration test. The results are displayed by service connection. The default setting is to display results by service script. The first two rows show that the End2End server is receiving an unacceptable response time to the www.yahoo.com web site. This is based on a 0.5-sec static response time threshold. This result did not correspond to the manual operation of this transaction. NetIQ’s answer to this issue was that the yahoo site must have had background pop-up advertisements running that skewed the results. Currently, they do not handle pop-up advertisements very well, but this should not be an issue with a transaction-processing site used in an organization. This module would also be helpful in monitoring Service Level Agreements (SLA).



Figure 10. Services Monitor Results

#### 4.4 System

Figure 11 shows the results from the system screen. It shows the activity of the four PCs that had the system module enabled. The 137.80.125.91 endpoint was the End2End server, two of the PCs are on the production network, and the top entry is a facility PC.

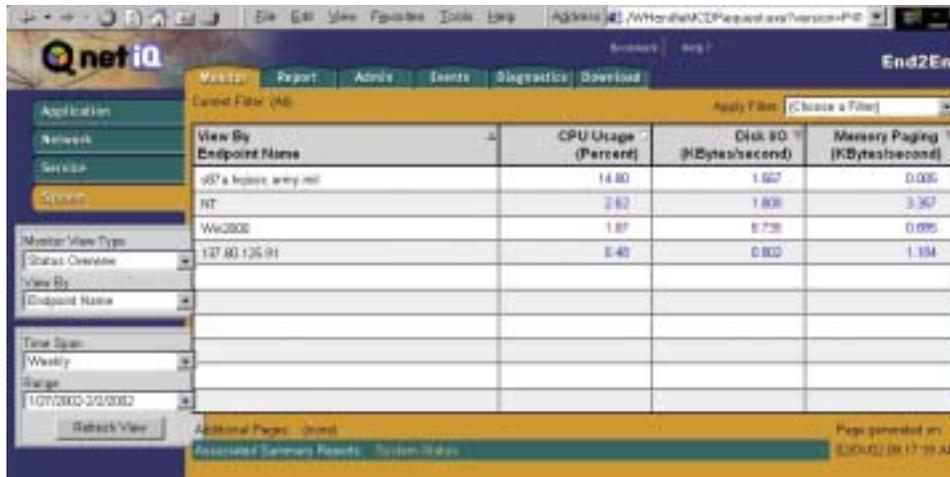


Figure 11. System Monitor Results

In addition to the default display from the monitor screens, the End2End program can display all the results in tabular and graphical format. See Figures 12 and 13.

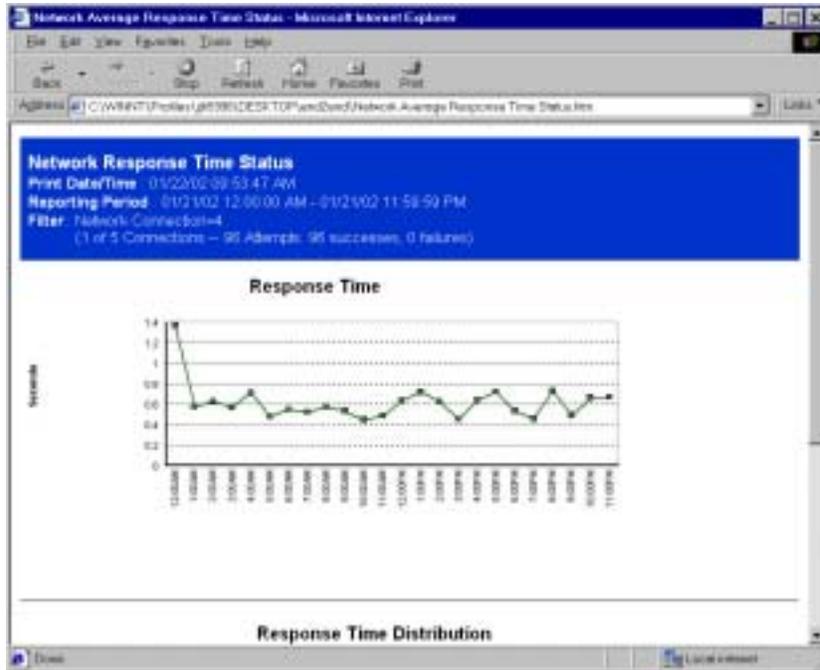


Figure 12. Graphical Output

The screenshot shows a web browser window titled 'Network Average Throughput Trend - Microsoft Internet Explorer'. The address bar contains a file path. The main content area has a blue header with the title 'Network Throughput Status'. Below the header, it displays 'Print Date/Time: 01/22/02 04:55:52 AM', 'Reporting Period: 01/21/02 12:00:00 AM - 01/21/02 11:59:59 PM', and 'Filter: Network Connection=4 (1 of 5 Connections - 96 Attempts, 0 failures)'. Below this is a section titled 'Throughput Details' containing a table with the following data:

Time	Sample	Bytes Received	Standard Deviation	90th Percentile	75th Percentile	50th Percentile
12:00:00AM	4	2,276,380	1,781,815	9,181,011	629,000	2,734,070
1:00:00AM	4	5,626,336	637,479	3,536,339	3,467,964	3,687,002
2:00:00AM	4	4,324,500	2,679,104	2,644,689	2,763,241	3,126,000
3:00:00AM	4	4,540,689	2,677,626	2,816,216	2,867,210	3,126,000
4:00:00AM	4	2,960,140	879,861	2,698,066	2,886,091	2,908,040
5:00:00AM	4	4,246,074	662,724	3,877,023	3,966,360	4,296,070
6:00:00AM	4	5,677,070	861,873	2,874,689	3,126,000	4,089,000
7:00:00AM	4	4,626,380	2,286,868	2,741,667	3,126,000	3,996,290
8:00:00AM	4	5,677,062	782,220	2,674,767	3,126,000	3,996,290
9:00:00AM	4	5,698,024	1,281,107	3,874,777	3,126,000	3,996,290
10:00:00AM	4	4,473,960	187,864	4,389,334	4,463,749	4,076,126
11:00:00AM	4	4,973,070	1,102,646	3,707,064	3,126,000	4,076,126

Figure 13. Tabular Output

In addition, users can export the results into Comma Separated Value (CSV) files, for use with a third party spread sheet application.

#### 4.5 Additional Modules

The evaluation copy came with two optional modules, Expert Analysis Module and Diagnostic on Demand. The Expert Analysis module displays more detailed information for problem events. It comes up as a separate screen invoked when you double-click on the severity icon listed with the problem event. It displays likely causes of the event and suggests operator actions to resolve the problem. Figure 14 shows an expert analysis screen

for a query that exceeded the 0.5-second response time for the web query (application module).

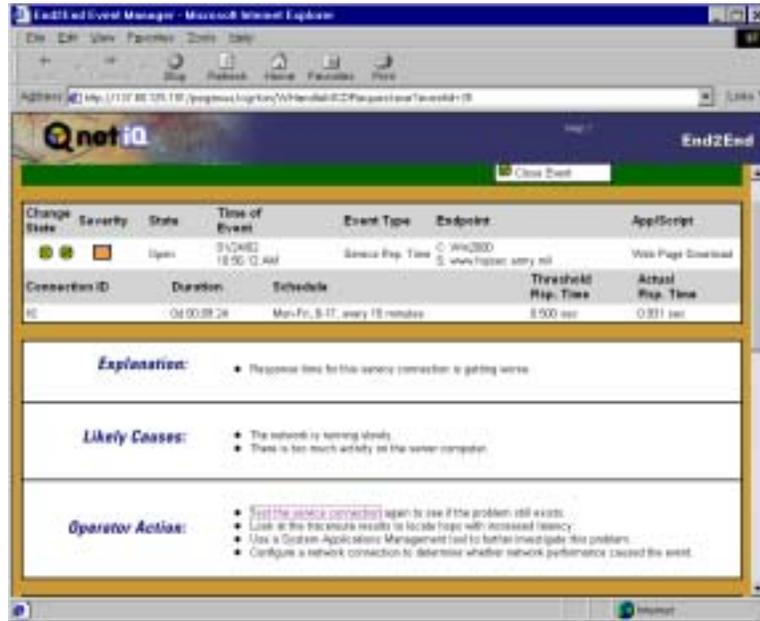


Figure 14. Expert Analysis Screen

The Diagnostic on Demand is displayed as a tab on the monitor screen. It allows the operator to perform real-time checks using the modules configured for that link. It was useful for double checking links that the operator had configured but had not yet been polled by the End2End server or confirming that a problem event was still present. In addition it has a quick test feature and traceroute capability. Figure 15 shows a capture of this screen.

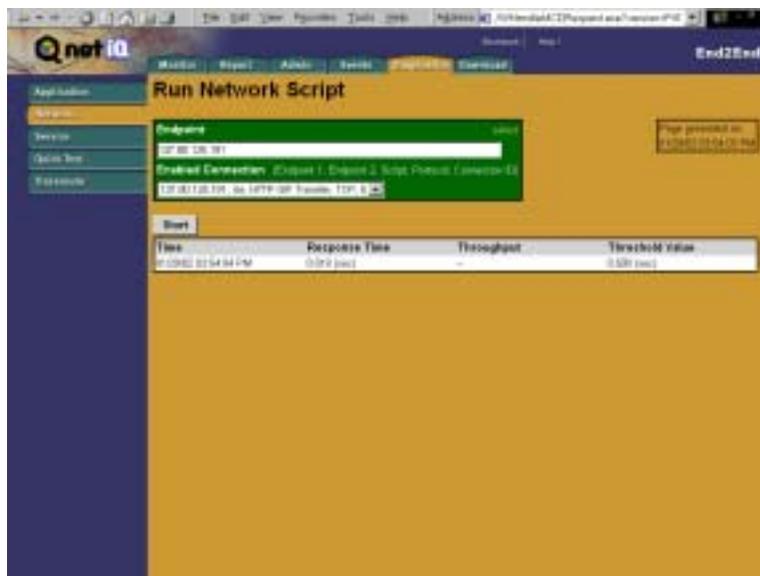


Figure 15. Diagnostic on Demand Screen

## 5.0 CONCLUSIONS

Based on the results collected and observations of the operation of the test network and PCs, the End2End program passed all the objectives of this evaluation. The results collected by the network module provide the operator throughput and response time statistics to monitor performance across the network. The service module allows the operator to examine service connection to specific sites. An administrator can use this module to set thresholds to determine if the network was providing adequate service. The application and system modules can monitor application activity on the selected PCs and determine if they are being over worked. Concerning the network and PC performance, the evaluator observed no discernable degradation in the performance of the test network or in the performance of any of the PCs running the endpoints. Overall, by combining all the information from the four modules (application, network, services, and system) an administrator would be able to understand their network performance from the user's perspective.

A network administrator would have no difficulty installing, configuring, and using this application. The product installed relatively quickly with the use of a setup wizard and the pre-loaded library of traffic generating scripts (Exchange, DNS queries, Active Directory updates, etc.). It had an extensive help section that was linked throughout the different screens. The product also had a list of default report formats and provided the ability to create or change them to meet the individual's needs. The technical support was knowledgeable, courteous, and responsive.

While documentation was not tested, it describes how to load the endpoints via Microsoft's Systems Management Server (SMS). This feature would be very useful in distributing the endpoints throughout the network.

Appendix [A](#) contains pricing information.

## 6.0 RECOMMENDATIONS

We recommend any system engineer or administrator, who is interested in knowing the performance of their network, download their own trial copy. This tool provides an objective way to measure the impact and/or improvement of a network or application upgrade within the Command's infrastructure.

**This page is intentionally left blank**

## APPENDIX A. END2END DETAILS

Endpoints create active emulated queries on the following network protocols; Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internetwork Packet Exchange (IPX), Sequenced Packet Exchange (SPX) and System Network Architecture (SNA) Application Program-to-Program Converter (APPC). Endpoints support the following operating systems;

- HP-UX
- IBM AIX
- IBM MVS
- Linux for Cobalt RaQ3
- Linux x86 (TAR)
- Linux x86 for RPM (Red Hat)
- Linux IA-64 (TurboLinux)
- Microsoft Windows 98/Me/NT/2000/XP
- Microsoft Windows XP 64-Bit
- Spirent Communications TeraMetrics
- Sun Solaris for SPARC
- Sun Solaris for x86

NetIQ recommends the following to install the End2End program on a server.

- Provide a dedicated server with at least 256 MB RAM
- Windows NT 4.0 with SP5 or SP6 or Windows 2000
- Install on a New Technology File System (NTFS) partition with at least 100 MB of free space. The partition does not have to be on the C drive.
- The Internet Information Server (IIS) is required to provide the web interface capability to the server. This allows for remote monitoring and configuration access.

NetIQ 12-point End2End program summary document.



"E2E 12 Point  
Summary.pdf"

Pricing Details



"1E2E GSA  
Pricing.xls"

**This page is intentionally left blank**

**GLOSSARY. ACRONYMS AND ABBREVIATIONS**

API	Application Programming Interfaces
APPC	Application Program-to-Program Converter
CPU	central processing unit
CSV	Comma Separated Value
DNS	Domain Name Service
FTP	File Transfer Protocol
GB	gigabyte
Gbps	gigabits per second
I/O	input/output
IIS	Internet Information Server
IPX	Internetwork Packet Exchange
kB	kilobyte
MB	megabyte
Mbps	megabits per second
MHz	megahertz
NTFS	New Technology File System
PC	personal computer
PE	performance endpoint
RAM	random access memory
SLA	Service Level Agreements
SMS	Systems Management Server
SNA	System Network Architecture
SNMP	Simple Network Management Protocol
SPX	Sequenced Packet Exchange
TCP	Transmission Control Protocol
TIC	Technology Integration Center
UDP	User Datagram Protocol
USAISEC	U.S. Army Information Systems Engineering Command