Performance Endpoints 5.1

Windows 2000, Windows XP, and Windows 2003 Server

April 2006

Legal Notice

Contents

About This Guide

This guide provides practical information about the free Performance Endpoint software NetIQ Corporation provides in association with its Systems Management products. It explains installation and configuration for all the endpoint platforms supported by NetIQ AppManager Networks Response Time and VoIP Quality modules, NetIQ Vivinet Assessor, and NetIQ Vivinet Diagnostics. You can also download individual endpoint guides in PDF format from the Internet at www.netiq.com/download/endpoints.

Intended Audience

This guide contains information about Performance Endpoint software for users of NetIQ AppManager, Vivinet Assessor, and Vivinet Diagnostics.

Using This Guide

Depending on your environment and your role as a user of the aforementioned NetIQ products, you may want to read portions of this guide selectively. It contains the following chapters:

- Chapter 1, "Introduction to Performance Endpoints," describes the software and hardware requirements and the supported functions of the Performance Endpoints, version 5.1.
- Chapter 2, "Endpoint Initialization File," discusses the functions of the endpoint initialization file, which is installed with each Performance Endpoint.

- Chapter 3, "Microsoft Windows 2000, Windows XP, and Windows Server 2003," explains the installation, configuration, and operation of the Performance Endpoint software for Microsoft Windows 2000, Windows XP, and Windows Server 2003.

In addition to these chapters, an index is provided for your reference.

Conventions Used in this Guide

The following conventions are used in this guide:

- `Fixed-width font` is used for source code, program names or output, file names, and commands that you enter at the command line.
- An *`italicized`* fixed-width font is used to indicate variables.
- **Bold text** is used to emphasize commands, buttons, or user interface text, and to introduce new terms.
- *Italics* are used for book titles.

Complementary NetIQ Products

NetIQ Corporation is a leading provider of intelligent, e-business management software solutions for all components of your corporate infrastructure. These components include servers, networks, directories, Web servers, and various applications.

NetIQ provides integrated products that simplify and unify directory, security, operations, and network performance management in your extended enterprise. NetIQ provides the following categories of products:

- **Systems Management** NetIQ Systems Management products provide control and automation for monitoring

the performance and availability of your critical servers, applications, and devices; tools for diagnosing and analyzing system operation; and extensive network monitoring capabilities to provide a complete, end-to-end management solution for the enterprise. These products enable you to pinpoint existing and potential server and network problems and resolve those problems quickly and effectively.

- **Security Management** NetIQ Security Management products enable you to administer, assess, enforce, and protect all aspects of security within your Windows environment. These products provide incident management and intrusion detection, vulnerability assessment, firewall reporting and analysis, and Windows security administration.
- **Smart Solutions for Windows Administration** NetIQ Smart Solutions for Windows Administration include tools for managing, migrating, administering and analyzing your Windows, Exchange, and SQL Server environments. These products include tools for setting and enforcing policies that govern user accounts, groups, resources, services, events, files, and folders, and products that automate time-consuming administration tasks.

Contacting NetIQ

Please contact us with your questions and comments. We look forward to hearing from you. For support around the world, please contact your local partner. For a complete list of our

partners, please see our Web site. If you cannot contact your partner, please contact our Technical Support team.

Telephone:	713-418-5678
Support:	support@netiq.com
Web site:	www.netiq.com/support

Chapter 1

Introduction to Performance Endpoints

This guide contains information about the Performance Endpoints, which are available for more than 15 different operating systems.

All the information you need to install, configure, and run the endpoints in your network is included here. In addition to topics discussing issues common to all the endpoints, this guide also contain information about each operating system, organized in separate chapters.

The following topics describe the software and hardware requirements and the supported functions of the Performance Endpoints, version 5.1.

- "Operating System and Protocol Stack Support" on page 2
- "Endpoint Capabilities" on page 2

The latest version of the endpoint software can always be downloaded free from the Internet. A single installable file is available for each supported operating system. Endpoints are available for downloading at www.netiq.com/download/endpoints.

You cannot run endpoint software from a CD-ROM; you must install it on a computer.

Operating System and Protocol Stack Support

The following table lists the software with which we have tested the Performance Endpoints for each operating system.

Endpoint	OS Version	TCP, UDP, RTP	IP Multicast Version
Cobalt RaQ3 (x86)	Kernel 2.0.32	Included	Kernel 2.0.32
HP-UX	HP-UX v10.10	Included	v10.10
IBM AIX	AIX v4.1.4	Included	v4.1.4
Linux (x86 and MIPS)	Kernel 2.0.32	Included	Kernel 2.0.32
Microsoft Windows Millennium Edition (Me)	Windows Me	Included	Included
Microsoft Windows 2000	Windows 2000	Included	Included
Microsoft Windows 2003 Server	Windows XP (32-bit)	Included	Included
Microsoft Windows XP	Windows XP (32-bit)	Included	Included
Sun Solaris for SPARC	Solaris v2.4	Included	v2.4
Sun Solaris for x86	Solaris v2.4	Included	v2.4

Endpoint Capabilities

The following table indicates which endpoints have been tested with and are supported by NetIQ products.

NetIQ Product	Vivinet Assessor	Vivinet Diagnostics	AppManager for Networks-RT	AppManager for VoIP Quality
Endpoint				
HP-UX	No	No	Yes	No
IBM AIX	No	No	Yes	No
Linux for Cobalt RaQ3 (x86)	Yes	Yes	Yes	Yes

NetIQ Product	Vivinet Assessor	Vivinet Diagnostics	AppManager for Networks-RT	AppManager for VoIP Quality
Endpoint				
Linux x86 (TAR)	Yes	Yes	Yes	Yes
Linux x86 (RPM)	Yes	Yes	Yes	Yes
Microsoft Windows Me/2000/XP/2003	Yes	Yes	Yes	Yes
Microsoft Windows Me/2000/XP/2003 (Web-Based)	Yes	No	No	No
Sun Solaris (SPARC)	Yes	Yes	Yes	Yes
Sun Solaris Endpoint (x86)	Yes	Yes	Yes	Yes

Chapter 2

Endpoint Initialization File

An endpoint initialization file is installed with each Performance Endpoint. With this file, you can do the following:

- Restrict the use of this endpoint to specific AppManager, Vivinet Diagnostics, or Vivinet Assessor Console.
- Control which access attempts are logged in an audit file.
- Change the filename of the audit file.
- Enable only particular protocols on this endpoint for setup connections.

On most operating systems, this file is named `endpoint.ini`. This file has the same format and structure on all the operating systems.

Here are the default contents of the endpoint initialization file. You can change these keywords and their parameters to tailor individual endpoints for your needs.

Keyword	Parameters
ALLOW	ALL
SECURITY_AUDITING	NONE
AUDIT_FILENAME	ENDPOINT.AUD
ENABLE_PROTOCOL	ALL

This file is an editable text file. There is a separate copy for each operating system. You might want to make changes to it once, before endpoint installation, which are then incorporated into all the installs for different sets of computers. You can modify this text file before installation by copying the endpoint installation directory for an

operating system to a hard drive (preferably a LAN drive), and then modifying the file before running the install from that drive.

We strongly recommend that you make any changes to your `endpoint.ini` files once, before you install any endpoints, as opposed to installing the endpoints and then going back to each of them and separately modifying each one.

ALLOW

This keyword determines which computers can run tests using this endpoint.

To allow any user to run tests on this endpoint, use the `ALL` parameter, which is the installation default:

```
ALLOW ALL
```

However, the default "**`ALLOW ALL`**" is ***not*** recommended. Although `ALLOW ALL` makes it easy to install an endpoint and see that it's running, it also lets any user who can reach the endpoint potentially use that endpoint as a traffic generator.

To allow only specific users to run tests with this endpoint, remove the `ALLOW ALL` line and identify one or more specific computers by their network addresses. You can specify more than one address per protocol. For example,

```
ALLOW TCP 192.86.77.120
ALLOW TCP 192.86.77.121
```

Specify a connection-oriented protocol (that is, TCP) as the first parameter and provide its corresponding network address as the second parameter. Endpoints listen only for incoming tests on connection-oriented protocols, such as TCP. Datagram tests are set up and results are returned using their "sister" connection-oriented protocol; thus, UDP tests are set up using TCP.

The network address in TCP/IP must be in dotted notation.

Endpoints do not respond to endpoint discovery requests unless the IP address of the computer is specifically allowed (or unless `ALLOW ALL` is specified). This prevents the user of a computer from finding endpoints to which it should not have access.

You cannot use the `ALLOW` parameter to restrict access from one endpoint to another endpoint. The `ALLOW` parameter can be used only to permit (or prevent) access from specific computers to the endpoint at which the parameter is defined.

If, for some reason, you need to restrict your endpoint to access only your own computer, specify your own IP network address rather than `127.0.0.1`. Specifying `127.0.0.1` (the equivalent of `localhost`) allows any other user who specifies `localhost` as Endpoint 1 to access your computer as Endpoint 2.

SECURITY_AUDITING

This keyword determines which access attempts the endpoint keeps track of in its audit file. Here are the possible parameters:

NONE	Writes nothing to the audit file
PASSED	Logs only access attempts that passed the ALLOW address check.
REJECTED	Logs only access attempts that failed the ALLOW address check.
ALL	Logs both passed and rejected access attempts.

If a test initialization fails for a reason other than address checking, no entry is made in the audit file.

AUDIT_FILENAME

This keyword specifies the filespec for the audit file. See "SECURITY_AUDITING" on page 7 to understand the types of events logged in its audit file. The default filename in `endpoint.ini` is `endpoint.aud`. If no drive or path is specified, the audit file uses the drive and path of the endpoint program.

This file contains at most two lines for each endpoint pair that is started on this endpoint. These two lines represent the start of an endpoint instance and the end of that instance.

Each line written to the audit file consists of a set of information about the endpoint instance and what it has been asked to do. The information is written in comma-separated form, so you can load the audit file into a spreadsheet or database. When the audit file is created, an initial header line explains the contents of the subsequent entries.

The following table shows the fields of each entry in the audit file:

Field	Description
Time	The date and time when the entry was created, in the local time zone.
Action	Whether an endpoint instance was "Started" or "Ended."
Endpoint	Whether the endpoint is in the role of Endpoint 1 or Endpoint 2.
Protocol of Console	The network protocol used to contact Endpoint 1.
Network Address of Console	The network address as seen by Endpoint 1. If you encounter problems setting up your `ALLOW` entries, use this value for the protocol address.
Security Result	Whether this `SECURITY_AUDITING` "passed" or was "rejected." If this is an entry for an "Ended" action, this field is reported as "n/a."
Endpoint Partner Protocol	The network protocol used to run the test with a partner endpoint.
Endpoint Partner Address	The network address of a partner endpoint.

ENABLE_PROTOCOL

This keyword lets you control which connection-oriented protocols an endpoint uses to listen for setup connections. This does not affect the network protocols, which can be used to run tests. Here are the possible parameters:

`ALL`

`TCP`

In general, you should use the `ALL` setting (the default). Specify protocols explicitly to reduce the overhead of listening on the other protocols or if you're encountering errors when listening on the other protocols.

See the discussion of the `ALLOW` keyword on page 6 for information about support of the datagram protocols, RTP, and UDP.

Configuring Endpoints for Large-Scale Customization

To customize features such as automatic upgrades, you must edit the `endpoint.ini` file for each endpoint. For obvious reasons, you may not want to undertake such a potentially lengthy procedure. You can extract the files located in `gsendw32.exe` if you need to perform a large-scale customization of endpoint.ini. In addition to WinZip, you'll need the WinZip command-line support add-on and WinZip Self-Extractor. Here's how to use it:

1. Open the file `gsendw32.exe` using WinZip. See "Using WinZip" on page 15 for more information.
2. Extract the files to a temporary directory.
3. Edit or replace the `endpoint.ini` that is now in the temporary directory.
4. Using WinZip, create a new archive that contains all the files in the temporary directory.
5. Using the WinZip Self-Extractor, create a self-extracting executable; for the command line to run, enter the following:

   ```
   SETUP.EXE replace_ini
   ```

Now, anyone who executes the new executable you've created will automatically have the endpoint installed using the `endpoint.ini` file that you've customized.

To create a file that silently self-installs with a custom endpoint.ini:

1. Open the file `gsendw32.exe` using WinZip. See "Using WinZip" on page 15 for more information.
2. Extract the files to a temporary directory.
3. Edit or replace the `endpoint.ini` that is now in the temporary directory.
4. Create a custom response file (say, `customer.iss`); enter

   ```
   i. SETUP -noinst -r -f1.\customer.iss
   ```

5. Using WinZip, create a new archive that contains all the files in the temporary directory.
6. Using the WinZip Self-Extractor, create a self-extracting executable; for the command line to run, enter the following:

   ```
   SETUP.EXE replace_ini -s -f1.\CUSTOMER.ISS
   ```

Now, anyone who executes the file you've created will automatically have the endpoint installed using `customer.iss` as the response file, and the `endpoint.ini` file installed will also be the customized version you created.

Chapter 3

Microsoft Windows 2000, Windows XP, and Windows Server 2003

This chapter explains the installation, configuration, and operation of the Performance Endpoint software for Microsoft Windows 2000, Windows XP, and Windows Server 2003. This endpoint is compatible with the 32- and 64-bit version of Windows XP.

- x86 computers are commonly known as "PCs"; they contain CPUs made by Intel, AMD, Cyrix, and others.
- Alpha computers contain CPUs made by Compaq Corporation (formerly Digital Equipment Corporation, or DEC).

The endpoint for the Windows Millennium Edition (Me) operating system is packaged with the endpoint for Windows 2000/XP/2003, but has slightly different code, hardware and software requirements, and installation instructions. Refer to "Microsoft Windows Me" on page 11 for more information about this operating system.

For details about installing, configuring, and using the Windows 2000/XP/2003 endpoint, see the following topics:

Installation Requirements for Windows 2000/XP/2003 Endpoints

Here's what you need to run the endpoint program with Windows 2000, Windows XP, or Windows Server 2003:

- A computer capable of running Windows 2000, Windows XP, or Windows Server 2003 well.

  For x86 computers, this implies a CPU such as an Intel 80486, a member of the Pentium family, or equivalent. A Pentium or better is recommended.

- 32 MBytes of random access memory (RAM).

  The total RAM requirement depends on the RAM usage of the underlying protocol stack and the number of concurrent connection pairs. For very large tests involving hundreds of connections through a single endpoint, additional memory may be required.

- A hard disk with at least 8 MBytes of space available.
- Microsoft Windows 2000, Windows XP, or Windows Server 2003.

  Both the Workstation and Server of these operating systems are supported.

  - for IP Multicast: Windows 2000 or Windows XP is required.
  - for IP QoS: Windows 2000 requires the QoS Packet Scheduler.

See the `README` file for this endpoint to see the latest Microsoft service packs with which we've tested.

You also need compatible network protocol software for RTP, TCP, and UDP. TCP/IP software is provided as part of the network support with Windows 2000, Windows XP, and Windows Server 2003. Quality of Service (QoS) support for TCP/IP is part of Microsoft Windows 2000, Windows XP, and Windows Server 2003.

We recommend that you get up-to-date with the latest Windows service levels. "Getting the Latest Fixes and Service Updates" on page 26 discusses where to get the latest software upgrades.

Installing the Endpoint

We recommend configuring your networking software — and ensuring that it is working correctly — before installing our software. See the Help for your networking software, and see "Configuring Windows Endpoints" on page 18 for more assistance.

Note Before installing the endpoint on Windows 2000, plan to close any other network applications. During the endpoint installation, Windows 2000 recycles the protocol stack, causing some client applications to lose connectivity to their servers. Some of these applications don't retry their connectivity before exiting and must be restarted.

The endpoint for Windows 2000, Windows XP, and Windows Server 2003 is installed and runs as a service. Only a user ID with Administrator authority is permitted to install services. To successfully install the endpoint, you must be logged in with Administrator authority. The permissions of the directory where the endpoint is installed must also be set to allow the `SYSTEM` (the operating system) full control access. Be sure to give the `System` "Full Control" permission on all files in the `NetIQ\Endpoint` directory or the directory where you've installed the endpoint, plus any relevant subdirectories.

The security implementation in Windows Server 2003 differs noticeably from that in earlier versions of Windows. Before you install the endpoint on Windows Server 2003, make sure your user account is running in "Install" mode and not in "Execute" mode. To change the mode so that you have the necessary installation privileges, run the following at a command prompt:

```
change user /install
```

The installation on Windows Server 2003 will fail with the message "`The InstallShield-generated file that allows uninstallation is missing`" if you're trying to install from the wrong mode.

Following are directions for installing the endpoint from a CD-ROM and from the Web.

- "Installing from a CD-ROM" on page 14

Installing from a CD-ROM

To install the endpoint from a CD-ROM:

1. Put the CD-ROM in your CD-ROM drive.
2. From a command prompt, go to the `WIN32` directory and enter the following:

   ```
   [drive:]\Endpoint\Win32\gsendw32.exe
   ```

3. Select the directory where the endpoint will be installed. We recommend installing it on a local hard disk of the computer you're using. If you install on a LAN drive, the additional network traffic may influence your performance results. The default directory is `\Program Files\NetIQ\Endpoint`, on your boot drive.
4. If you have a previous installation of the endpoint, you will be asked if you want it removed. If you select "**Yes**," the previous installation is removed, and the new installation continues. If you select "**No**," the install program exits with no changes to your existing installation because a new version cannot be added until the old version is removed. The installation program adds the endpoint program as a service.
5. The next dialog box contains two checkboxes.
   - The first check box lets you opt to install pre-built data files. We recommend that you clear this box. This feature is for Chariot users only.
   - Check the second box to start the endpoint installation. If you leave this box cleared, the endpoint starts when you restart the computer. No window is shown while the endpoint is running because it runs as a service.

   A Windows 2000, Windows XP, or Windows Server 2003 service is

controlled from the Services dialog inside the Control Panel. If you want to restart a service without restarting Windows, use the Services dialog box.

You can also manually start the endpoint after installation. See "Starting the Endpoint" on page 21 for instructions.

The installation is now complete; you can remove the CD-ROM from its drive.

To prevent the endpoint from running automatically on startup, see the section titled "Disabling Automatic Startup" on page 25.

When you've completed installation, refer to "Configuring Windows Endpoints" on page 18 to make sure your endpoint is ready for testing and monitoring.

Installing from the Web

To install an endpoint you've downloaded from the Web:

1. Save the `gsendw32.exe` file to a local directory.
2. Use Windows Explorer to navigate to the file and double-click to start the installation.
3. The first dialog box after the Setup dialog box lets you select the directory where the endpoint will be installed. We recommend installing it on a local hard disk of the computer you're using. If you install on a LAN drive, the additional network traffic may influence your performance results. The default directory is `\Program Files\NetIQ\Endpoint`, on your boot drive.
4. If you have a previous installation of the endpoint, you will be asked if you want it removed. If you select "**Yes**," the previous installation is removed, and the new installation continues. If you select "**No**," the install program exits with no changes to your existing installation because a new version cannot be added until the old version is removed. It then adds Endpoint (the endpoint program) as a service.

5 The next dialog box contains two checkboxes.

- The first check box lets you opt to install pre-built data files. We recommend that you clear this box. This feature is for Chariot users only.
- Check the second box to start the endpoint installation. If you leave this box cleared, the endpoint starts when you restart the computer. No window is shown while the endpoint is running because it runs as a service.

A Windows 2000, Windows XP, or Windows Server 2003 service is controlled from the Services dialog inside the Control Panel. If you want to restart a service without restarting Windows, use the Services dialog box.

You can also manually start the endpoint after installation. See "Starting the Endpoint" on page 21 for instructions.

To prevent the endpoint from running automatically on startup, see the section titled "Disabling Automatic Startup" on page 25. If you want to restore the setting later, you must do so manually.

When you've completed installation, refer to "Configuring Windows Endpoints" on page 18 to make sure your endpoint is ready for testing and monitoring.

Unattended Installation

Unattended installation (also called *silent installation*) is available for the endpoints for Windows. You install an endpoint once, by hand, while the install facility saves your input in an answer file. You can then install that same endpoint silently on other computers, that is, without providing input other than the answer file.

First, run `gsendw32.exe`. An answer file called `update.iss` is created in the `\Updates` subdirectory of the directory where you installed the endpoint.

To perform a silent installation, specify the "`-s`" option on `SETUP`. Make sure the answers documented in the answer file `update.iss` are

appropriate for the silent installation. If the `update.iss` file is not in the same directory as `setup.exe`, then specify the path and filename with the "`-f1`" option. For example, here's how to install using the `update.iss` file in the `\Program Files\NetIQ\Endpoint` directory on our `n:` LAN drive:

```
SETUP -s -f1n:\Program Files\NetIQ\Endpoint\update.iss
```

If you don't specify the path and filename with `-f1`, the default filename is `setup.iss`. Don't mix the `.iss` files among different Windows operating systems because their endpoint installations require slightly different input.

It's common to use unattended install from a LAN drive. Be sure you've copied all of the files for each type of endpoint into a single directory (rather than into separate diskette images), and you've created your initial `update.iss` file from that directory. Unattended install does not keep track of diskette label information, and will need user input if you install from separate disk images. You probably don't want your unattended install to ask you for `n:\disk1\`, `n:\disk2\`, and so on.

What Happens During Installation

Here's what happens during the installation steps. Let's say you install the endpoint into the directory `\Program Files\NetIQ\Endpoint`. A directory is created with the following contents:

- The executable programs
- The `README` file
- The directory `Cmpfiles`. This directory contains files with the `.CMP` file extension. These are files containing data of different types, such as typical text or binary data. These files are used by the endpoint as data on `SEND` commands. The different data types can be used to vary the data compression performance of your network hardware and software.
- The `endpoint.ini` file. See "Endpoint Initialization File" on page 5 for information about tailoring this file for individual endpoints.

The endpoint is installed as a service, which means there's nothing visible while it's running. During installation, the endpoint is configured to automatically start when the system reboots. A service can be controlled from the Services dialog box inside the Control Panel; this process is described in "Running Windows Endpoints" on page 21.

Removing the Endpoint Package

To remove the endpoint package from your hard disk, follow these steps:

1. Click **Start > Settings > Control Panel**.
2. Click **Add/Remove Programs**. The Add/Remove Programs Properties dialog box is displayed.
3. Highlight **NetIQ Endpoint** and click **Add/Remove**. The uninstallation program begins. After the program is completed, the endpoint should be uninstalled.

Removing the Endpoint Manually

If the uninstallation program is unable to uninstall the endpoint, you will need to manually uninstall it. For detailed instructions on manually removing the endpoints, see the Performance Endpoints FAQ page in the Knowledge Base on our Web site at www.netiq.com/support/pe/default.asp.

Configuring Windows Endpoints

The endpoint program uses the network application programming interfaces, such as Sockets, for all of its communications. The endpoint dynamically configures its own programs, so you do not have to update the configuration files for your communications software. However, your communications software must be configured and running correctly. The following steps guide you through this verification process.

1 Determine the network addresses of the computers to be used in tests.

2 Select a service quality.

3 Verify the network connections.

The following topics describe how to accomplish these steps:

- "Configuration for TCP/IP" on page 19
- "Determining the IP Address" on page 19
- "Testing the TCP/IP Connection" on page 20

Configuration for TCP/IP

The RTP, TCP, and UDP protocols use TCP/IP software for network communications. TCP/IP offers two forms of network addresses: IP addresses and domain names. An IP address is a 32-bit numeric address. It is represented in dotted notation as a set of four numbers separated by periods, such as `199.72.46.202`. An alternative, domain names are in a format that is easier to recognize and remember, such as www.netiq.com. To use domain names, you need either a Domain Name Server (DNS) set up in your network or an `/etc/hosts` file on each computer.

Determining the IP Address

To determine the local IP address for a Windows 2000, Windows XP, or Windows Server 2003 computer, enter the following command:

```
IPCONFIG
```

If your TCP/IP stack is configured correctly, your output will look like the following (this output is taken from Windows XP):

```
Windows IP Configuration
Ethernet adapter Local Area Connection:
IP Address. . . . . . . . . . : 10.10.44.3
Subnet Mask . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . : 10.10.44.254
```

Its local IP address is shown in the first row; here it's `10.10.44.3`.

You can also find your IP address using the graphical user interface. Open the Control Panel folder, and double-click on the **Network** icon. The installed network components are shown. Double-click **TCP/IP Protocol** in the list to get to the TCP/IP Configuration. Your IP address and subnet mask are shown.

To determine a the local hostname for a Windows 2000, Windows XP, or Windows Server 2003 computer, enter the following command:

```
HOSTNAME
```

The current hostname is shown in the first row.

From the graphical user interface, return to the TCP/IP Protocol configuration. Select **DNS** (Domain Name System) to see or change your domain name. If the DNS Configuration is empty, avoid using domain names as network addresses; use numeric IP addresses instead.

Testing the TCP/IP Connection

Ping is a simple utility program, included in all TCP/IP implementations. To check the connection from one computer to another, enter the following at a command prompt:

```
ping xx.xx.xx.xx
```

Replace the x's with the IP address of the target computer. If Ping returns a message that says "`Reply from xx.xx.xx.xx ...`," the Ping worked. If it says "`Request timed out`," the Ping failed, and you have a configuration problem.

Make sure that you can run Ping successfully from the AppManager, Vivinet Assessor, or Vivinet Diagnostics Console to each computer serving as Endpoint 1, and between each pair of endpoints involved in a test, before starting your testing with TCP/IP.

Running Windows Endpoints

The following topics describe starting and stopping an endpoint in the Windows 2000, Windows XP, or Windows Server 2003 operating systems, as well as some of the messages and information that become available during testing with this endpoint. The Windows endpoint is controlled from the Services dialog box: click **Start > Settings > Control Panel**, double-click **Administrative Tools**, and then double-click **Services**. The Services dialog box lets you start or stop the endpoint, listed as "NetIQ Endpoint."

Only a user ID with Administrator authority is permitted to start or stop Windows 2000, Windows XP, or Windows Server 2003 services.

Starting the Endpoint

By default, the endpoint service is configured to start automatically, which means that you will not see a window for the program when it is running. Because the endpoint runs as a service, you do not have to be logged into your workstation for the endpoint to run.

If you stop the endpoint service, you can restart it without restarting Windows. There are two ways to restart the endpoint service:

- At a command prompt, enter `net start netiqendpoint`
- In the Services dialog box, select **NetIQ Endpoint** and click **Start** (or **Play**). For example, to restart `endpoint.exe` in Windows XP, select **Performance and Maintenance** from the Control Panel. Click **Administrative Tools > Services**. In the Services dialog box, select the **NetIQ Endpoint** line, and click **Start the service** (or **Stop the**

service). The status changes to "started" when the service is successfully started.

Note A single running copy of the endpoint service handles one or multiple concurrent tests.

Stopping the Endpoint

There are two ways to stop the endpoint service:

- At a command prompt, enter the following:

  ```
  net stop netiqendpoint
  ```

- In the Services dialog box, click **NetIQ Endpoint** and click **Stop**. The status is blank when the endpoint program has stopped.

Disabling Your Screen Saver

Screen savers in Windows 2000 and Windows Server 2003 can significantly lower the throughput that's measured by an endpoint. We recommend disabling your screen saver at endpoint computers while running tests.

Using the SetAddr Utility

Endpoints for Windows operating systems now ship with a utility that helps you quickly create virtual IP addresses on Windows 2000, Windows XP (32-bit and 64-bit), and Windows Server 2003 endpoint computers. Virtual addresses are chiefly useful when you're testing hundreds or even thousands of endpoint pairs using only a few computers as endpoints. To all intents and purposes, the traffic on the network is identical, whether you're using "real" or virtual addresses.

When you install a Windows endpoint, `Setaddr.exe` for 32-bit Windows is automatically installed in the same directory. For 64-bit Windows, a 64-bit version of `Setaddr.exe` is installed. The two versions of `SetAddr` cannot be used across operating systems with different architectures.

The usage is as follows:

```
setaddr [-dr] -a N -f Addr -t Addr -i Addr -s Addr
| -l[a]
| -da
| -ds -f Addr -s Addr
```

(where "N" indicates the adapter number of the NIC card you're assigning virtual addresses to, and "Addr" indicates the virtual addresses or subnet mask you're assigning to it).

Options:

```
-l     List all network adapters
-la    List all network adapters and their IP addresses
-a     Adapter to modify (number given by -l options)
-dr    Delete a range of addresses
-da    Delete all addresses
-ds    Delete a single address
-f     From address
-t     To address
-i     Increment by
-s     Subnet Mask
```

The `-d` flags cannot be used to delete a computer's primary IP address.

The `-i` flag lets you determine how the range of addresses will be created. This is an optional field; by default, `SetAddr` increments the range by one in the final byte only. This "increment by" value is represented as "`0.0.0.1`". Enter a value (0-255) for each byte of the 4-byte IP address. A value of 1 specifies that the address values in that byte will be incremented by one when `SetAddr` creates the range. For example, enter

```
setaddr -f 10.40.1.1 -t 10.40.4.250 -i 0.0.1.1 -s 255.255.0.0
```

SetAddr creates 1000 virtual addresses.

Known Limitations:

- IPv4 only.
- Windows 2000, Windows XP, and Windows Server 2003 computers only.
- `SetAddr` only works on computers with fixed IP addresses. DHCP-enabled adapters can't be used.
- You must restart the computer to whose NIC you've assigned virtual IP addresses before you begin testing with that computer. `SetAddr` modifies some Windows Registry keys, and restarting is required for the changes to take effect.
- The number of virtual addresses you can assign to a single adapter depends on the protocol stack and the size of the Windows Registry. We benchmarked measurements using computers running up to 2500 virtual addresses, which is a recommended limit.
- No checking is done to ensure that thousands of addresses are not being created. Be careful! More TCP/IP stack resources are required to manage virtual addresses.
- You may only add Class A, B, and C virtual IP addresses. Loopback addresses and Class D and E IP addresses are invalid. Valid address ranges, then, are `1.x.x.x` to `233.x.x.x`, excluding `127.x.x.x`.
- When more than 2250 virtual address are defined on Windows 2000 computers, all the LAN adaptor icons disappear from the Network and Dial-up Connections dialog box in My Network Places. You can still see the adaptors by invoking `ipconfig` or setaddr from the command line, and the addresses are still reachable. Removing some virtual addresses so that fewer than 2250 were specified and restarting the computer solved the problem.

Disabling Automatic Startup

To disable the automatic starting of the endpoint, take the following steps:

1. Click **Start > Settings > Control Panel**, then **Administrative Tools**, then **Services**. The Services dialog box is displayed.
2. Double-click **NetIQ Endpoint**.
3. On the **Startup type** menu, click **Manual**.
4. Click **OK** to save the new setting and exit the dialog box. The endpoint will no longer start automatically when you restart the computer. However, you can manually start the endpoint.

How to Tell If a Windows Endpoint Is Active

The Status field in the Services dialog box shows whether the NetIQ Endpoint service has started.

Similarly, the Windows Performance Monitor program can be used to look at various aspects of the endpoint. Start Performance Monitor by double-clicking its icon in the **Administrative Tools** group. Click **Edit > Add to Chart**. Select the **Process** object and the **Endpoint** instance. Then add the counters you are interested in, such as thread count or % of processor time. In the Steady state (that is, no tests are active), Thread Count will show about 6 threads active for the endpoint; the answer depends on the number of protocols in use.

Logging and Messages

Although most error messages encountered on an endpoint are returned to the AppManager, Vivinet Assessor, or Vivinet Diagnostics Console, some may be logged to disk. Errors are saved in a file named `ENDPOINT.LOG`, in the directory where you installed the endpoint. To view an error log, use the command-line program named `FMTLOG.EXE`. The program `FMTLOG.EXE` reads from a binary log file, and writes its formatted output to `stdout`. Use the following `FMTLOG` command:

```
FMTLOG log_filename > output_file
```

This endpoint performs extensive internal cross-checking to catch unexpected conditions early. If an assertion failure occurs, the file `assert.err` is written to the directory where you installed the endpoint.

Getting the Latest Fixes and Service Updates

We've found that communications software is often fragile. Its developers are constantly working to make it more robust, as the software gets used in an ever-wider set of situations.

We therefore recommend working with the very latest software for the underlying operating system and communications software. Here are the best sources we've found for the Windows 2000, Windows XP, or Windows Server 2003 software used by the endpoint program.

Microsoft posts code and driver updates to the following Web site: www.microsoft.com/windows/downloads/.

Information about Service Pack 2 for Windows XP can be found at http://support.microsoft.com/default.aspx?pr=windowsxpsp2.

Index