

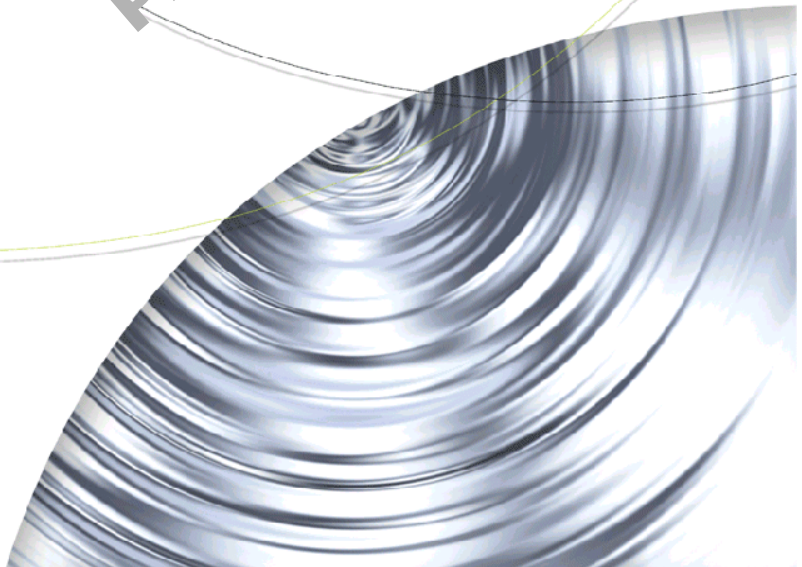


NVIDIA®

NVIDIA ForceWare Network Administrator's Guide

**Software Version 1.0
NVIDIA Corporation
January 2004**

Preliminary Edition



Published by
NVIDIA Corporation
2701 San Tomas Expressway
Santa Clara, CA 95050

Copyright © 2003 NVIDIA Corporation. All rights reserved.

This software may not, in whole or in part, be copied through any means, mechanical, electromechanical, or otherwise, without the express permission of NVIDIA Corporation.

Information furnished is believed to be accurate and reliable. However, NVIDIA assumes no responsibility for the consequences of use of such information nor for any infringement of patents or other rights of third parties, which may result from its use. No License is granted by implication or otherwise under any patent or patent rights of NVIDIA Corporation.

Specifications mentioned in the software are subject to change without notice.

NVIDIA Corporation products are not authorized for use as critical components in life support devices or systems without express written approval of NVIDIA Corporation.

NVIDIA, the NVIDIA logo, nForce, and ForceWare are registered trademarks or trademarks of NVIDIA Corporation in the United States and/or other countries.

Microsoft, Windows, Windows logo and/or other Microsoft products referenced in this guide are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries.

Other company and product names may be trademarks or registered trademarks of the respective owners with which they are associated.

Table of Contents

1. Introduction

Audience	7
Overview of ForceWare Network Access Manager7	
Command Line Interface (CLI)	8
Web Interface	9
Sample Web Pages.	9
WMI Script.	12
About Security	13
System Requirements	14
Hardware Requirements.	14
Software Requirements	14
General Requirements	14
Operating System Requirements.	15

2. Installation Guidelines

About the ForceWare Network Installer	16
Locating the ForceWare Network Installer.	17
Before You Run the ForceWare Network Installer.	17
Running the ForceWare Network Installer	18
Creating the Response File	18
Running Installation in Silent Mode.	18
Accessing the Network Access Manager Web Interface.	18
Configuration Deployment	18

3. ForceWare Personal Firewall: Basics Concepts

Types of Firewalls	21
Inbound vs. Outbound Packets.	22
About the TCP Protocol	22
About the UDP and ICMP Protocols	23
UDP	23
ICMP	23
Stateful vs. Stateless.	24
Stateful Filtering	24
Stateless Filtering	26

4. Configuring ForceWare Personal Firewall

Basic Configuration	29
Using the Wizard.	30
Advanced Configuration.	31
About Working With Tables	32
Configuration Dependencies	33

Recommendations	33
Firewall Statistics	34
Firewall Logging.	35

5. Administrative Tasks

Accessing the Administration Menu.	37
Application Access Control Page	38
Default Access Settings	39
Command Line Access	39
WMI Script	39
Local Web Access.	40
Remote Web Access	40
Additional Notes	40
Password.	41
IP Address and IP Address Mask (optional)	41
Restore Factory Default	41
Display Settings.	42
Backup/Restore	42
Backup Configuration	42
Restore User Configuration	43
Network Access Manager Software Version.	43

6. Using WMI Script

Before You Begin	44
Overview	44
Advanced Topics	45
NVIDIA Namespace.	45
WMI Provider	45
Synchronization	45
Examples	46

7. Using Command Line Interface (CLI) Access

Conventions Used	47
About Examples Used	47
Parameters	48
Modes of Operation.	48
Using Single Parameters.	49
Set (Expert Mode).	49
Example.	49
Set (Interactive Mode)	49
Example.	49
Get	50
Help	50
Example.	50

Using Table Parameters.	50		
Add Row.	50		
Example.	51		
Edit Row.	51		
Example.	51		
Delete Row.	52		
Example.	52		
Help.	52		
Example.	52		
Set Table.	52		
Example.	52		
Get Table.	53		
Example.	53		
About Expert Commands.	53		
Syntax.	53		
Example.	54		
About Other Table Commands.	54		
Syntax.	54		
Browse Parameter Structure.	54		
List.	54		
Example.	55		
Change Directory.	55		
Example 1.	55		
Example 2.	56		
Current Working Directory.	56		
Example.	56		
Context Sensitive Operations.	56		
Example.	56		
Text File Process.	57		
Export.	57		
Syntax.	57		
Example.	58		
Import.	58		
Syntax.	58		
Example.	58		
Selective Export.	59		
Syntax.	59		
Example.	59		
Context Export.	59		
Example.	59		
Glossary.	59		
 A. Ethernet Parameters: Reference			
Organization and Links.	61		
“Group: VLAN (Virtual LAN)” on page 80.	62		
“Group: Jumbo Frame” on page 82.	62		
“Group: Driver Optimization” on page 83.	62		
“Group: Ethernet Performance” on page 84.	62		
“Group: Factory Default” on page 103.	63		
		“Group: Alert Standard Format” on page 124.	64
		“Group: ASF Information” on page 127.	64
		“Group: System Fails to Boot Alert” on page 128.	64
		“Group: Fan Problem Alert” on page 129.	64
		“Group: ASF SMBus Error” on page 130.	64
		“Group: ASF WOL Alert” on page 131.	64
		“Group: ASF Heartbeat Alert” on page 132.	64
		“Group: ASF Operating System Hung Alert” on page 133.	65
		“Group: ASF Power Button Alert” on page 134.	65
		“Group: ASF System Hot Alert” on page 135.	65
		“Group: ASF CPU Overheated Alert” on page 136.	65
		“Group: ASF CPU Overheated Alert” on page 137.	65
		“Group: ASF Case Intrusion Alert” on page 138.	65
		Group: Remote Wakeup.	66
		Remote Wakeup.	66
		Remote Wakeup by Magic Packet.	67
		Remote Wakeup (Pattern Match).	68
		Remote Wakeup (Link State Change).	69
		Remote Wake Up from Hibernate or Shutdown.	70
		Group: Protocol Offload.	71
		Checksum Offload.	71
		IPv4 Transmit Checksum Offload.	72
		IPv4 Receive Checksum Offload.	73
		UDP Transmit Checksum Offload.	74
		UDP Receive Checksum Offload.	75
		TCP Transmit Checksum Offload.	76
		TCP Receive Checksum Offload.	77
		TCP Large Send Offload.	78
		Group: Microsoft Operating System VLAN (Virtual LAN).	79
		Microsoft Operating System VLAN.	79
		Group: VLAN (Virtual LAN).	80
		VLAN Support.	80
		VLAN ID.	81
		Group: Jumbo Frame.	82
		Jumbo Frame Payload Size.	82
		Group: Driver Optimization.	83
		Ethernet Driver Optimization.	83
		Group: Ethernet Performance.	84
		Number of Receive Buffers.	84
		Number of Receive Buffer Descriptors.	85
		Number of Transmit Buffer Descriptors.	86
		Maximum Transmit Frames Queued.	87

Number of Receive Packets to Process per Interrupt	88	Group: Alert Standard Format	124
Number of Transmit Packet to Process per Interrupt	89	ASF Support	124
Interrupt Interval	90	ASF Destination IP Address	125
Group: Traffic Prioritization	91	ASF Send Count.	126
IEEE 802.1p Support	91	Group: ASF Information	127
Group: Ethernet Speed/Duplex.	92	ASF Destination MAC Address	127
Configurable Ethernet Speed/Duplex Settings	92	Group: System Fails to Boot Alert	128
Group: Ethernet Information	93	System Fails to Boot Alert	128
Link Speed	93	Group: Fan Problem Alert	129
Maximum Link Speed	94	Fan Problem Alert	129
Duplex Setting	95	Group: ASF SMBus Error	130
Link Status.	96	ASF SMBus Error	130
Promiscuous Mode.	97	Group: ASF WOL Alert.	131
Permanent Ethernet Address	98	ASF WOL (Wake On Lan) Aler	131
Group: Ethernet Address	99	Group: ASF Heartbeat Alert	132
Current Ethernet Address	99	ASF Heartbeat Alert Interval	132
Group: Network Interface information	100	Group: ASF Operating System Hung Alert.	133
Computer (Machine) Name	100	ASF Operating System Hung Alert	133
IP Address	101	Group: ASF Power Button Alert.	134
IP Address Mask	102	ASF Power Button Alert	134
Group: Factory Default	103	Group: ASF System Hot Alert	135
Factory Default	103	ASF System Hot Alert.	135
Table: Multicast Address List	104	Group: ASF CPU Overheated Alert	136
Multicast Address List	104	ASF CPU Overheat Alert.	136
Multicast Addresses (Single Parameter)	105	Group: ASF CPU Overheated Alert.	137
Group: Ethernet Statistics.	106	ASF CPU Hot Alert	137
Frames Received with Alignment Error	106	Group: ASF Case Intrusion Alert	138
Frames Transmitted After One Collision.	107	ASF Case Intrusion Alert	138
Frames Transmitted After Two or More Collisions	108		
Frames Transmitted After Deferral	109		
Display Name Frames Exceed Maximum Collision	110		
Frames with Overrun Errors.	111		
Frames with Underrun Errors	112		
Frames with Heartbeat Failure	113		
Carrier Sense (CRS) Signal Lost.	114		
Late Collisions	115		
Group: General Networking Statistics	116		
Successfully Transmitted Frames	116		
Successfully Received Frames	117		
Transmit Failures	118		
Receive Failures	119		
No Receive Buffers.	120		
Direct Frames Received	121		
Multicast Frames Received	122		
Broadcast Frames Received	123		

B. ForceWare Personal Firewall

Parameters: Reference

Organization and Links.	139
Group: Configure Firewall Security Level	143
Configure Firewall Security Level	143
Continuation of Comments	144
Group: Configure Firewall Options	146
Disallow Promiscuous Mode	146
Disallow DHCP Server	147
Block Outbound Spoofed IP Packets	148
Block Spoofed ARP Packets	149
Block UDPv4 with No UDP Checksum.	150
Group: EtherType Default Rule	151
EtherType Default Rule	151
Group: IP Address/Mask Default Rule	152
IP Address/Mask Default Action	152
Group: Domain Name Default Rule.	153
Domain Name Default Rule	153
Group: IP Option Default Rule.	154
Inbound IP Option Default Rule	154

Outbound IP Option Default Rule	155	Table: Domain Names Rule	196
Group: IP Protocol Default Rule	156	Domain Name	197
IP Protocol Default Rule	156	Domain Action	198
Group: Port Number Default Rule	157	Table: IP Option Rules	199
Inbound Port Number Default Rule	157	IP Option Number	200
Outbound Port Number Default Rule	158	IP Option Name	201
Group: TCP Options Default Rule	159	IP Version	202
TCP Options Default Rule	159	Inbound Action	203
Group: ICMP Messages Default Rule	160	Outbound Action	204
Inbound ICMP Default Rule	160	Table: IP Protocol Rule	205
Outbound ICMP Default Rule	161	IP Protocol	206
Group: Clear Firewall Statistics	162	IP Protocol Name	207
Clear Firewall Statistics	162	IP Protocol Action	208
Group: Firewall Statistics	163	Table: TCP/UDP Port Rule	209
Allowed Inbound UDP Datagrams	163	TCP/UDP Port Outbound Action	210
Denied Inbound UDP Datagrams	164	Remote IP Address	211
Allowed Outbound UDP Datagrams	165	Remote IP Subnet Mask	212
Denied Outbound UDP Datagrams	166	Port Name	213
Denied Inbound UDP Connections	167	Beginning Port Number	214
Allowed Outbound UDP Connections	168	Ending Port Number	215
Denied Outbound UDP Connections	169	Port Protocol	216
Allowed Inbound TCP Segments	170	Table: TCP Options Rule	217
Denied Inbound TCP Segments	171	TCP Option Number	218
Allowed Outbound TCP Segments	172	TCP Option Name	219
Denied Outbound TCP Segments	173	TCP Option Action	220
Allowed Inbound TCP Connections	174	Table: ICMP Rules	221
Denied Inbound TCP Connections	175	Remote IP Address	222
Allowed Outbound TCP Connections	176	Remote IP Subnet Mask	223
Denied Outbound TCP Connections	177	ICMP Type	224
Allowed Inbound ICMP Packets	178	ICMP Code	225
Denied Inbound ICMP Packets	179	ICMP Name	226
Allowed Outbound ICMP Packets	180	ICMP Version	227
Denied Outbound ICMP Packets	181	Inbound Action	228
Other Allowed Inbound Packets	182	Outbound Action	229
Other Denied Inbound Packets	183		
Other Allowed Outbound Packets	184		
Other Denied Outbound Packets	185		
Group: Factory Default	186		
Factory Default	186		
Group: Flush DNS Cache	187		
Flush DNS Cache	187		
Table: EtherType Rules	188		
Ether Type	189		
EtherType Name	190		
EtherType Action	191		
Table: IP Address/Mask Rule	192		
Remote IP Address	193		
Remote IP Address Mask	194		
IP Action	195		

C. Glossary



List of Tables



Table 5.1 Default Access Settings for the ForceWare Network Access Manager 39

Preliminary Edition



List of Figures



Figure 1.1 NVIDIA ForceWare Network Access Manager Home Page 9

Figure 1.2 Sample Web Page Showing Ethernet Basic Information 10

Figure 1.3 Sample Web Page for ForceWare Personal Firewall Basic Configuration 10

Figure 1.4 Sample Web Page Showing ForceWare Personal Firewall Wizards 11

Figure 1.5 Sample Web Page Showing a Graphical Display of Packet Information. 12

Figure 5.1 Sample Application Access Control 38

Preliminary Edition

INTRODUCTION

This chapter contains the following major sections:

- “Audience” on page 7
- “Overview of ForceWare Network Access Manager” on page 7
- “About Security” on page 13
- “Software Requirements” on page 14
- “General Requirements” on page 14
- “Operating System Requirements” on page 15

Audience

This guide is intended for the system or network Administrator of an organization as a guide to install and use the NVIDIA[®] ForceWare[™] Network Access Manager application.

Note: All references to “you” in this guide assumes a reader with Administrator access privileges. Exceptions are noted, where applicable.

Overview of ForceWare Network Access Manager

Using the NVIDIA ForceWare Network Access Manager application, you can easily configure and control NVIDIA networking hardware and software, gather statistics, and monitor logs. NVIDIA ForceWare Network Access Manager gives you several choices in managing your networking hardware and software:

- “Command Line Interface (CLI)” on page 8

- “Web Interface” on page 9
- “WMI Script” on page 12

Command Line Interface (CLI)

The ForceWare Network Access Manager provides command line access through the **nCLI** program. The **nCLI** command can be run in either **expert** or **interactive** mode to configure and monitor NVIDIA networking components.

- **Expert mode** is suitable for deployment in an organization by running **nCLI** from a login script. To use **nCLI** in expert mode, you need to be familiar with the syntax and characteristics of configuration parameters.

For details and examples of using the **nCLI** command with various Ethernet and ForceWare Personal Firewall parameters, see “Ethernet Parameters: Reference” on page A-61 and “ForceWare Personal Firewall Parameters: Reference” on page B-139.

- **Interactive mode** runs in a shell environment and is suitable for Administrators who do not have access to the syntax and characteristics of the **nCLI** configuration parameters. **nCLI** provides navigation feature to assist these users.

Note: Extensive **nCLI** usage samples in batch file format are provided in the following *subdirectories**:

`samples\Eth` (for Ethernet)

`samples\Firewall` (for Firewall)

* under the *default* path of `c:\forceware\network access manager`, or your user-specified path.

You can cut and paste the appropriate command and use them in batch files or in command lines.

Also see “Using Command Line Interface (CLI) Access” on page 47.

Web Interface

The ForceWare Network Access Manager Web interface offers convenient access through

- **Wizards**
- **Profiles and status summaries**
- **Help.** Context-sensitive online Help is also available on a wide range of features.
- **Tool tips.** When your cursor hovers over a parameter name, its description is displayed in a popup text window, called a *tool tip*.

For additional details, see

- [Sample Web Pages](#) (below)
- “Accessing the Network Access Manager Web Interface” on page 18
- “Administrative Tasks” on page 37

Sample Web Pages

Figure 1.1 NVIDIA ForceWare Network Access Manager Home Page

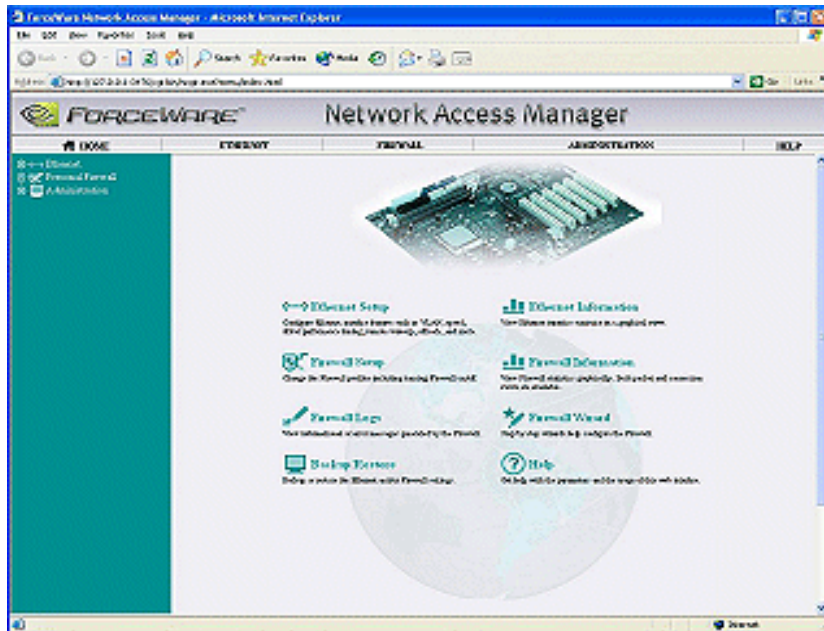


Figure 1.2 Sample Web Page Showing Ethernet Basic Information

The screenshot shows the ForceWare Network Access Manager web interface. The browser address bar displays <https://127.0.0.1:3476/cgi-bin/ncgr.exe?main/index.html>. The page has a navigation bar with tabs: HOME, ETHERNET, FIREWALL, ADMINISTRATION, and HELP. A left sidebar contains a tree view with 'Ethernet' selected, showing sub-items: Ethernet, Personal Firewall, and Administration. The main content area is titled 'Ethernet Basic Configuration' and contains the following settings:

Permanent Ethernet address	00:04:4b:19:23:00
Current Ethernet Address	<input type="text"/>
Speed/Duplex Settings	Full Autonegotiation (recommended)
Driver Optimization	CPU Utilization
ASF (Alert Standard Format)	Disable
Remote Wakeup	Enable
Checksum Offload	Enable
TCP Large Send Offload	Enable
Jumbo Frame	Only applicable for connections speeds of 1000Mbps and above.
802.1p (Prioritization)	Disable
802.1Q (VLAN)	Disable

An 'Apply' button is located at the bottom of the configuration box. At the bottom of the page, a copyright notice reads: © 2005-2004 by NVIDIA Corporation. All rights reserved. | Terms of Use Policy.

Figure 1.3 Sample Web Page for ForceWare Personal Firewall Basic Configuration

The screenshot shows the ForceWare Network Access Manager web interface. The browser address bar displays <https://127.0.0.1:3476/cgi-bin/ncgr.exe?main/index.html>. The page has a navigation bar with tabs: HOME, ETHERNET, FIREWALL, ADMINISTRATION, and HELP. A left sidebar contains a tree view with 'Personal Firewall' selected, showing sub-items: Basic Configuration, Wizards, Advanced Configuration, Log Information, Log Settings, and Administration. The main content area is titled 'Firewall Basic Configuration' and contains the following settings:

Security Profile	Medium (recommended)
------------------	----------------------

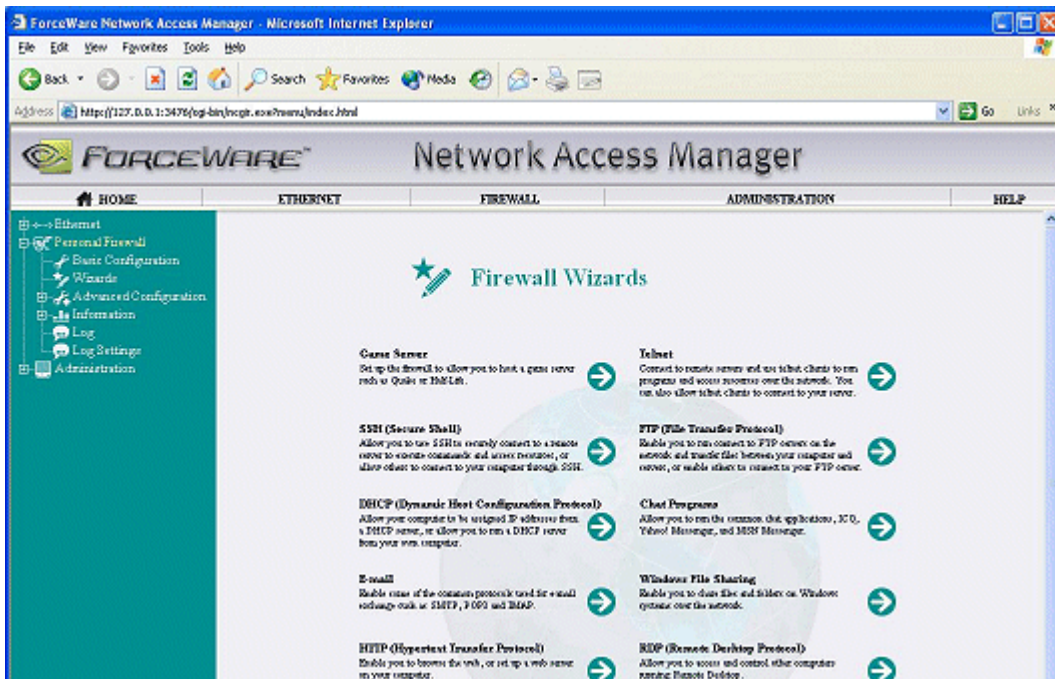
An 'Apply' button is located below the settings. Below the configuration box, there is a detailed explanation of the 'MEDIUM' setting:

MEDIUM will be the default setting when the firewall is first activated. MEDIUM does not have the "stealth" features associated with HIGH, therefore MEDIUM allows most (but not all) ICMP error messages to be sent and received. MEDIUM blocks most incoming connections, with the default action for unspecified TCP and UDP connections being "deny". In order to allow file transfers via MSN Messenger and Yahoo! Messenger, incoming connections to port 80 must be allowed (these applications will not work if the HIGH setting is chosen).

The MEDIUM setting will allow dynamic ports to be opened up from the inside only (default is: deny, default out: allow). Thus, MEDIUM will only support outgoing NetMeeting calls.

As in the HIGH setting, the MEDIUM setting allows VPNs based on both IPsec and on PPTP. Also, as in the HIGH setting, the MEDIUM setting restricts traffic by prohibiting IP and/or TCP options that might be misused, as well as by preventing the spoofing of IP source addresses (for both IPv4 and IPv6).

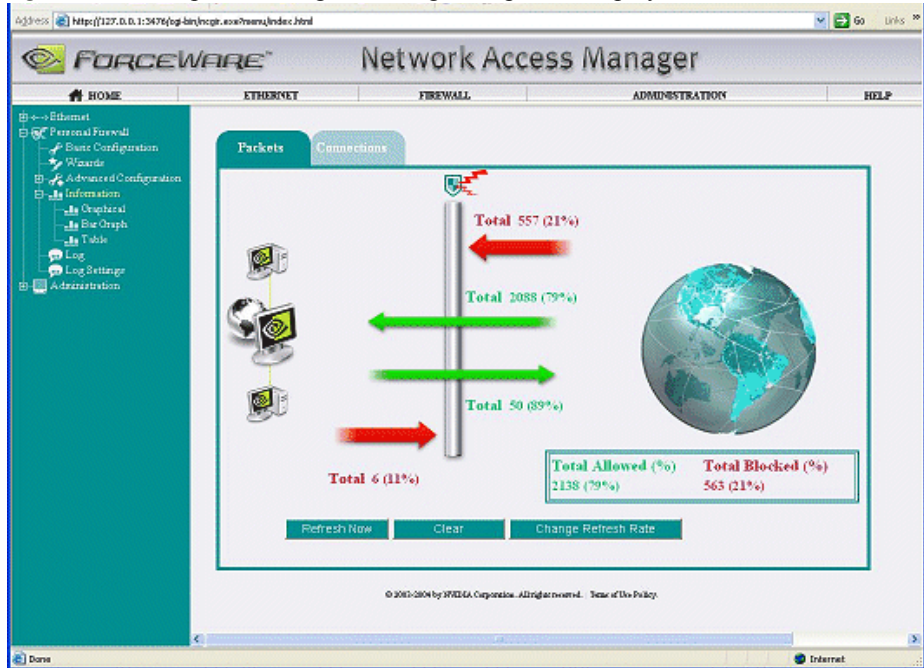
At the bottom of the page, a copyright notice reads: © 2005-2004 by NVIDIA Corporation. All rights reserved. | Terms of Use Policy.

Figure 1.4 Sample Web Page Showing ForceWare Personal Firewall Wizards

The ForceWare **Personal Firewall Wizards** page allows you to configure the firewall to allow certain applications to work. There are wizards for various types of applications including, Telnet, FTP, SSH, game servers, and so on.

These wizards will open the standard network ports that are used by these type of applications. If the particular application you are using needs non-standard ports to work, you can use the generic port wizards to allow these ports in the ForceWare Personal Firewall.

Note: Refer to your application documentation for information on the TCP/UDP ports that are used, if applicable.

Figure 1.5 Sample Web Page Showing a Graphical Display of Packet Information

WMI Script

You can use the Microsoft® **Windows Management Instrumentation (WMI)** script language to manage NVIDIA networking hardware and software.

Note: Using WMI script language is recommended *only* for Administrators who are already familiar with programming in WMI script.

WMI script programming is being used by the IT staff of larger corporations to carry out day to day maintenance work. Overall benefits of using WMI scripts include:

- Industry standard — can be implemented using languages such as VBScript and JScript.
- Ease of use
- Allows access to NVIDIA ForceWare Network Access Manager data through common scripts
- Flexibility. The WMI script user can code the script any way they want. For example, user can write code to scan for Yahoo Messenger on a computer and open the appropriate port if the user has sufficient rights.

Note: WMI script usage samples are provided in the following *subdirectories*:

- samples\Eth
 - samples\Firewall
- * under the *default* path of c:\forceware\network access manager, or your user-specified path.

You can cut and paste the appropriate command and use them in a batch file or the command line.

For further details, also see the following:

- WMI script can be run remotely and can be used for deployment in an organization. See [“Configuration Deployment” on page 18](#).
- [“Using WMI Script” on page 44](#).
- To use WMI scripting, you must be familiar with the syntax and characteristics of configuration parameters. See the [“Ethernet Parameters: Reference” on page A-61](#) and [“ForceWare Personal Firewall Parameters: Reference” on page B-139](#) for details.
- Refer to the Microsoft documentation on WMI scripting.

About Security

Access control is based on the type of application, the type of user (Administrator or not), and the type of access — i.e, local or remote.

The application access control allows you to configure non-Administrator access to the applications, which includes, nCLI, the command line interface, the WMI scripting interface, and the local and remote Web interfaces.

For all applications being accessed from the local computer, the access rights for the application depend on the current Windows login.

Note: A non-Administrator user on a computer cannot access the firewall parameters and modify the access control parameters.

For further details on security and access control, see [“Application Access Control Page” on page 38](#).

System Requirements

Hardware Requirements

To run the NVIDIA ForceWare Network Access Manager software, you must meet the following requirements:

- You need *one* of the following types of NVIDIA nForce computers:
 - nForce2 Gigabit MCP with NVIDIA Personal Firewall
 - or
 - nForce2 RAID MCP
- nForce Ethernet must be configured as a bridge device in the BIOS, which is the factory default.

Software Requirements

In order to run the NVIDIA ForceWare networking software, you need the following software:

- You need *one* of the following, depending on the type of nForce2 computer you are using:
 - Software loaded on the nForce2 Gigabit MCP computer
 - or
 - Software loaded on the nForce2 RAID MCP computer
- NVIDIA Network Access Manager software

General Requirements

- **WMI (Windows Management Instrumentation) service**

Note: WMI service is not started automatically on Windows 2000. The ForceWare Networking Installer needs to change this service to run automatically on Windows startup.

- **WMI MOF compiler (MOFCOMP)** must be available on your computer.

Operating System Requirements

Note: It is recommended that you install the NVIDIA ForceWare Network Access Manager application on an NTFS file system. If the software is installed on NTFS you will have additional access control for the files, registry, and the configuration information compared to installing the software on a FAT file system. *For further information on how to change file permission under NTFS, refer to the Windows online Help.*

The NVIDIA ForceWare Network Access Manager application supports the following operating systems:

- **Windows XP**
- **Windows 2000**

Preliminary Edition

CHAPTER

2

INSTALLATION GUIDELINES

This chapter contains the following main topics:

- “About the ForceWare Network Installer” on page 16
- “Running the ForceWare Network Installer” on page 18
- “Accessing the Network Access Manager Web Interface” on page 18
- “Configuration Deployment” on page 18

About the ForceWare Network Installer

The ForceWare Network Access Manager software supports the silent installation method, which means no user interaction is needed to install the software. The silent installation process uses a response (.iss) file that contains information similar to what you would enter as responses to dialog boxes when running a normal setup.

Below is a summary of the silent installation steps:

- 1 See “Before You Run the ForceWare Network Installer” on page 17.
- 2 Download/obtain the NVIDIA nForce Driver installer. See “Locating the ForceWare Network Installer” on page 17.
- 3 Run NVIDIA nForce Driver installer which will uncompress files.
- 4 Specify where to copy the nForce files.
- 5 Read the section “Locating the ForceWare Network Installer” on page 17.
- 6 Generate the response file, as explained in “Creating the Response File” on page 18.

- 7 At the target computer, install in silent mode using the three installation files and the response file. See [“Running Installation in Silent Mode” on page 18](#)

Locating the ForceWare Network Installer

The ForceWare Network Installer, setup.exe, and the Network Access Manager software are part of the basic nForce driver installation package, which can usually be obtained from the NVIDIA Web site or a partner OEM.

The nForce driver installer program uncompresses and saves the following ForceWare Network Installer (setup.exe) and the Network Access Manager software (listed below) in a user-specified directory:

- Setup.exe (located in *<name of uncompressed directory>\Ethernet\NRM*)
- Data1.cab
- NVIDIA ForceWare Network Manager.msi

Before You Run the ForceWare Network Installer

Before you run the ForceWare Network Installer (setup.exe) software, please note the following:

- The nForce Ethernet driver software must be installed and operational on your computer.
- You must have Administrator access rights to do the following:
 - Run the Setup installation program *and*
 - Uninstall and/or modify the NVIDIA Network Access Manager software, when needed.
- If you are using the **Network Access Manager** Web interface, note the following:
 - Microsoft Internet Explorer version 5 *or higher* must be running on your computer.
 - The NVIDIA **Network Access Manager Web** interface uses the NVIDIA registered port 3476.

Note: In case some other application on the computer is using this registered port, please change the port number for that application.

Running the ForceWare Network Installer

Creating the Response File

From the directory where the setup.exe program is located, run the following command and go through the installation dialog boxes as normal, selecting the options that will be used in subsequent silent installs. All choices are recorded in the response file (nvidia_net.iss).

```
setup.exe -a -r -fl"c:\nvidia_net.iss"
```

Note: You can change the path and name of the response file by replacing the c:

Running Installation in Silent Mode

```
setup.exe -s -a -s -fl"c:\nvidia_net.iss"
```

Accessing the Network Access Manager Web Interface

- 1 Using the instructions in the previous sections of this chapter, make sure you have the setup.exe installation program to install the ForceWare Network Access Manager software.
- 2 To launch the NVIDIA ForceWare Network Access Manager Web interface, you can do one of the following:
 - Double-click the NVIDIA Web Management icon on your desktop
 - or
 - Click **Start > Programs > NVIDIA Corporation > Network Access Manager > Web-based Interface**.

Configuration Deployment

Note: The Network Access Manager Web interface is not suitable for configuration deployment because an Administrator can only remotely access one computer at a time.

Configuration deployment means configuring multiple computers to use the same configuration through an “automated” procedure. There are several ways to achieve this:

- Run the nCLI command to change parameters during the login script.

- You can choose to run nCLI to configure one parameter at a time or use the `import` command for bulk configuration.

Note: Sample command line access scripts can be found in the `sample` directory, under the default path of `c:\forceware\network access manager`, or your user-specified path. See [“Using Command Line Interface \(CLI\) Access” on page 47](#) section for more information.

- Create and run WMI scripts to change parameter during login script execution.

Notes:

- WMI script usage samples are provided in the following subdirectories:
`samples\Eth`
`samples\Firewall`
 under the default path of `c:\forceware\network access manager`, or your user-specified path.
- You can cut and paste the appropriate command and use them in a batch file or the command line. For further details, see [“Using WMI Script” on page 44](#).
- To use WMI scripting, you must be familiar with the syntax and characteristics of configuration parameters. See the [“Ethernet Parameters: Reference” on page A-61](#) and [“ForceWare Personal Firewall Parameters: Reference” on page B-139](#) for details.
- For additional details, refer to the Microsoft documentation on WMI scripting.

Note: Many Ethernet parameters require restarting the network driver for script changes to take effect. When the network driver is restarted, network connections will terminate, which will terminate the login script. To get around the problem, you can utilize the `NV_DriverRestartFlag` to defer restarting the driver. Keep in mind that a driver restart is still required for script changes to take effect.

- **If you are using nCLI, run the following command:**

```
ncli set NV_DriverRestartFlag.RestartFlag DeferRestart
```

- **If you are using WMI scripting, run the following command:**

```
//Set NV_DriverRestartCmd ""
try
{
```

```
var NV_DriverRestartCmd = GetObject("winmgmts:root/
nvidia/NS_Eth").Get("NV_DriverRestartCmd=@");
NV_DriverRestartCmd.RestartCmd=1;
NV_DriverRestartCmd.Put_();
WScript.Echo("Success in Group Set");
}
catch(Exception)
{
    WScript.Echo("Error in Group Set: ",
Exception.description);
    WScript.Quit(1);
}
```

FORCEWARE PERSONAL FIREWALL: BASICS CONCEPTS

This chapter contains the following main topics:

- “Types of Firewalls” on page 21
- “Inbound vs. Outbound Packets” on page 22
- “Stateful vs. Stateless” on page 24
- “Stateful Filtering” on page 24
- “Stateless Filtering” on page 26

Types of Firewalls

The ForceWare Firewall is a type of firewall that is typically referred to as a "personal firewall" or a "desktop firewall." Another classification of firewalls is the "gateway firewall." The main difference is that while the gateway firewall monitors network traffic and controls access between two different networks or administrative domains, the personal firewall controls traffic generated or received by a single computer. Therefore, a gateway firewall is usually a dedicated computer, or a part of a network switch or router, with multiple interfaces through which certain traffic is allowed and other traffic is blocked. On the other hand, a personal firewall is usually software that is installed on the personal computer, or a combination of software and hardware that is integrated to the computer. In both types of firewalls, certain traffic is allowed and certain traffic is blocked according to the specific rules configured for the firewall.

Firewalls just discussed can be further classified as one of two types — “application layer” or “packet-based.” Packet-based firewalls can be divided into two main sub-types — “stateful” and “stateless” firewalls.

Note: The ForceWare Firewall is a *packet-based personal* firewall having both *stateful* and *stateless* features.

Inbound vs. Outbound Packets

In order to protect the computer from insecure and malicious traffic, but still allow secure and trusted traffic, firewall rules must be properly defined according to the direction of each type of network traffic. The meaning of direction differs between protocols, depending on whether or not the specific protocol relies on connections to exchange data.

For example, **TCP (Transmission Control Protocol)**, **UDP (User Datagram Protocol)**, and **ICMP (Internet Control Message Protocol)** each has a different definition for direction (or none at all) *and* for traffic that is **inbound** or **outbound**.

About the TCP Protocol

Some network protocols, such as **TCP**, require an explicit initialization process. Firewall rules that apply to TCP typically depend partially on the direction of the connection establishment. When referring to protocols that involve establishment of a connection:

- **Inbound** describes a connection attempt not originated by the current computer.
- **Outbound** describes a connection attempt that was originated by the current computer.

About the UDP and ICMP Protocols

Unlike TCP, other protocols, such as **UDP (User Datagram Protocol)** and **ICMP (Internet Control Message Protocol)**, do not have an explicit connection establishment process. A computer can use protocols such as UDP and ICMP to send data packets to any other computer at any time, but the receiving computer, or an intervening firewall, can reject or accept the data on a per-packet basis.

UDP

UDP is frequently used in a connection-like manner, but without the connection establishment process. In other words, UDP-based applications may rely on long-term computer-to-computer sessions, which re-use the same UDP ports.

However, the meaning of the “direction of the connection” in the UDP context is broader than in the TCP context.

- The direction of a packet is **inbound** if the initial packet matching this new set of **IP (Internet Protocol)** and UDP header field values was a *received* packet.
- Similarly, a UDP connection is considered to be **outbound** if the initial packet matching this new set of IP and UDP header field values was a *transmitted* packet.

Thus, firewall rules that apply to UDP typically also depend on the direction of the first packet of a new “connection.” UDP packets, like TCP packets, can be matched against a “connection table” by performing a hash function on certain fields in the packet to determine if there is a match in a table of hash values where there is at least one connection that corresponds to each hash value.

ICMP

ICMP is an example of a protocol with neither a connection establishment process nor any connection-like functionality.

Firewall rules relevant to these types of protocols are applied to every packet, and **inbound** and **outbound** respectively refer to packets (of one of these protocols) that are received and transmitted across any of the network interfaces that the firewall is protecting.

Stateful vs. Stateless

Stateful and **stateless** are adjectives that describe whether a computer or computer program is designed to note and remember one or more preceding events in a given sequence of interactions with a user, another computer or program, a device, or other outside element. **Stateful** and **stateless** are derived from the usage of *state* as a set of conditions at a moment in time.

Stateful means the computer or program keeps track of the state of interaction, usually by setting values in a storage field designated for that purpose.

Stateless means there is no record of previous interactions and each interaction request has to be handled based entirely on information that comes with it.

Stateful Filtering

Stateful filtering (also known as stateful inspection or dynamic packet filtering) provides enhanced security by monitoring network packets over the period of the connection for that particular traffic. Because stateful filtering can dynamically track each connection, compare packets against the connection's expected state, and drop the packets that don't conform to the protocol, it has replaced static filtering as the industry standard firewall solution for networks.

It is also the case that stateful filtering scales much better than stateless filtering because the firewall policy table is only consulted once per connection, instead of once per packet. This means that as the number of rules grows, the stateful firewall will use a lower percentage of CPU, because in a stateless design, each packet will have to be compared against half of the firewall rules, on average, until a matching rule is found that explicitly allows or denies the packet. However, an increase in the size of the firewall policy rule table does not impact the stateful firewall to such a large degree, since the majority of packets are not connection setup packets.

A stateful firewall amortizes the CPU cycles that were used to do the firewall policy rule table lookup over the massive per-packet CPU savings due to having only a simple per-packet hash to compute, to determine if the current packet is associated with a previously allowed connection.

In contrast, a stateless firewall must examine every packet against the complete firewall policy rule table, or until it finds a matching rule, so in essence, every packet is treated as a connection setup packet, incurring the associated processing penalty.

As a result of the differences in processing required for stateful vs. stateless firewall lookups, latency due to stateful firewall operations is very small and nearly constant on a per-packet basis, whereas latency in a stateless firewall

depends on the size of the firewall policy rule table, and is of a much larger magnitude.

Once a TCP or UDP connection is established, a stateful firewall ensures that data traffic for that connection can flow in either direction — even if the rules governing the firewall limit such traffic to be only associated with remotely generated (i.e., inbound), or locally-originated (i.e., outbound) connections.

When a stateful firewall has determined that a connection is being established by decoding each packet, it checks its policy table to find out whether the connection is allowed or denied.

- In TCP, the connection establishment packet is a specially marked TCP packet that the firewall can detect.
- A UDP connection is initiated by the first packet matching a set of identifying fields in the IP and UDP headers.

If the firewall allows the new connection, the firewall saves a set of five values related to that connection's establishment into its connection-tracking table during the lifetime of that connection.

Every inbound and every outbound packet associated with a given connection contains the same five values. This allows the stateful firewall to quickly check whether or not the packet belongs to a connection that was previously granted permission and then deny or allow the packet accordingly.

Note: Only TCP packets that match the connection-tracking table are allowed. UDP packets that do not match the table may represent a new “connection” and are compared with the firewall rules in order to determine whether or not to add an entry to the connection-tracking table for this new connection.

The five “connection identifying” values saved into the connection-tracking table are:

- **IP Source Address**
- **IP Destination Address**
- **IP Protocol**
- **TCP or UDP Source Port**
- **TCP or UDP Destination Port**

For TCP, in addition to the five items in the list, the firewall tracks the state of the TCP connection (for example, the current stage of the connection establishment process) in order to enforce legal state transitions in the TCP protocol.

The firewall also tracks the current TCP “sequence and acknowledgement” numbers and the most recent TCP window in order to determine whether to

drop packets that fall outside the current valid TCP window. This kind of scrutiny prevents potential attackers from sending spurious TCP “reset” packets to the local computer in that the firewall prevents these reset packets to reach the host if the TCP sequence number of the reset packet falls outside the current valid TCP receiving window.

Some TCP options can also be used by the stateful firewall in determining whether to allow or deny TCP packets because certain TCP options can only be used if their use was negotiated during the connection establishment process. If such TCP options were negotiated during the connection establishment phase, then the TCP state will reflect the successfully negotiated TCP options for that connection. The TCP policy table can still override the peers and prevent certain TCP options from being negotiated at all.

Note: Other TCP options are not pre-negotiated. Therefore, decisions about whether to allow or deny TCP packets with such options must be based on the **stateless** (see “[Stateful Filtering](#)”) configuration of the firewall.

Stateless Filtering

The main difference between **stateful filtering** and **stateless filtering** is that contrary to the quick lookup-and-decide process enabled by the connection state tracking table that drives the decision making process in stateful filtering, all of the stateless filtering rules must be examined in sequence, for each packet, until a rule is found that either explicitly allows or denies that packet.

Note: For protocols such as ICMP and other non-TCP and non-UDP protocols, and for any non-IP protocols, the firewall performs stateless filtering but no stateful tracking or filtering.

In **stateless filtering**, the firewall can be configured to “allow in” or “deny in” certain kinds of traffic (from a specific protocol, with a particular option, etc.) on a given network interface. Similarly, the firewall can be configured to “allow out,” “deny out,” “allow in and out,” or “deny in and out” on the same traffic. Note that “in” implies the receive direction and “out” implies the transmit direction.

On average, the firewall will need to search half of its rules list for any given packet in order to find an applicable rule. Therefore, in general, as the number of rules increases, the firewall consumes more time in determining the outcome of a given packet. On the other hand, the ForceWare Firewall has been optimized so that looking up certain commonly used parameters (for example, ICMP, TCP, and UDP in the IP protocol table) is much faster and independent of the table size.

The firewall can be configured to perform stateless filtering based on:

- EtherType values
- Specific IPv4 or IPv6 addresses or address prefixes
- Specific domain names contained within DNS name resolution queries or responses
- Specific IP options
- Specific TCP options
- Specific ICMP (Type, Code) pairs
- Other relevant parameters

In all cases, stateless filtering rules are specified in the appropriate firewall table in the ForceWare Network Access Manager Web-based interface.

For example, when filtering ICMP traffic, the filtering rule is based on both the first three items (IP Source Address, IP Destination Address, and IP Protocol) as listed in the section on [“Stateful Filtering” on page 24](#), as well as the particular ICMP (Type, Code) field values in each ICMP packet.

In ICMP filtering, the IP Protocol is implicitly required to have a value of “0x01,” which is the protocol value for ICMPv4. A similar requirement is placed on ICMPv6, with its own unique identifying number in the IPv6 headers (i.e., 0x3A).

In most situations involving stateless filtering, it is necessary to allow a given protocol to go both in and out on a given interface in order for the associated application to operate normally. However, it may also be the case that certain applications require that one type of traffic be allowed in, while another type is allowed out.

One example of the latter case is “ping” because in order for the application process to complete successfully, the firewall must be configured to allow *both* an outbound ICMP Echo packet (Type = 0x08, Code = 0x00) and an inbound ICMP Echo Reply packet (Type = 0x00, Code = 0x00). These settings will allow the local PC to “ping” remote computers but will not necessarily allow remote computers to “ping” the local computer because inbound ICMP Echo packets and outbound ICMP Echo Reply packets are not necessarily allowed.

Note: Based on the above values, note that the ICMP (Type, Code) pair values for ICMP Echo and Echo Reply are, in fact, different.

CONFIGURING FORCEWARE PERSONAL FIREWALL

This chapter contains the following main topics:

- “Basic Configuration” on page 29
- “Using the Wizard” on page 30
- “Advanced Configuration” on page 31
- “About Working With Tables” on page 32
- “Configuration Dependencies” on page 33
- “Firewall Statistics” on page 34
- “Firewall Logging” on page 35

Basic Configuration

- 1 Open the **ForceWare Network Access Manager** Web menu.
- 2 From the **Personal Firewall** menu, click the **Basic Configuration** submenu to open the Firewall Basic Configuration page.
- 3 Click the **Security Profiles** list to view the “profiles” (sets of table rules).
The following five pre-defined profiles are *not editable*.
 - **Lockdown** – drops all traffic packets, except **Alert Standard Format (ASF)** packets.
 - **High** is meant to be extremely secure, but due to its stringent filtering rules, many applications may not work as expected, or at all.

- **Medium** (the *default* profile *after* installation) is intended to be a good balance between usability and security, with an emphasis on security.
- **Low** is the least secure profile, which allows the most applications to work, but is probably not very secure.
- **Off** – turns off the firewall, allowing all traffic.

Note: There are also three other **Custom** profiles that allow you to define the table rules, as explained in the “[Advanced Configuration](#)” on page 31 section.

- 4 To enable a specific profile, click the **Security profiles** list and select the profile you want.
- 5 Click **Apply**.
- 6 To view the actual rules associated with a profile, repeat step 4 above.
- 7 Open the appropriate table sub-menu under the **Personal Firewall Advanced Configuration** menu.

This menu lets you see whether the settings are appropriate for your required applications at the desired level of protection.

Note: Unlike the custom profiles, you cannot edit the basic pre-defined profiles.

Using the Wizard

Another way to configure rules in your custom profile is through the **Personal Firewall Wizards** page ([Figure 1.4](#)), which is accessible from the **Personal Firewall > Wizards** menu. Using a questionnaire format, the wizards provide a simple, step-by-step method to configure the tables and, for convenience, are separated into different categories of commonly-used applications.

The wizards also allow you to configure the firewall to allow certain applications to work. There are wizards for various types of applications including, Telnet, FTP, SSH, game servers, etc. These wizards will open the standard network ports that are used by these type of applications.

If the particular application you are using needs other non-specific network ports, you can use the Generic Port wizard to add those ports for the application to work.

Advanced Configuration

If you to generate a customized configuration (set of rules), any of the basic **Lockdown**, **High**, **Medium**, **Low**, and **Off** profiles discussed in “[Basic Configuration](#)” on page 29 may be used as a starting point.

Note: Up to three independent custom profiles can be defined.

To create or choose a custom profile:

- 1 Open the **ForceWare Network Access Manager** Web menu.
- 2 From the **Personal Firewall** menu, click the **Basic Configuration** submenu to open the **Firewall Basic Configuration** page.
- 3 Click the **Security Profiles** list to view the “profiles” (sets of table rules).
- 4 Then select on of the three **Custom** profiles.
- 5 Specify a new name for each custom profile you select in step 4 in the **Rename...** edit box.

Note: You will probably choose to generate a custom profile based on one of the pre-defined profiles, i.e., Lockdown, High, Low, etc.

To edit the associated table rules, select the appropriate *table* sub-menu under the **Advanced Configuration** menu to perform any of the following actions:

- To add a rule or purge all rules in a table, use the **Add Rule** or **Purge Table** buttons in the corresponding table's page.
- To change only the “action” of an existing rule (from **Allow** to **Deny**, or vice-versa):
 - a Click the drop-down menu in the corresponding table row under one of the “action” columns
 - b Click **Apply**.

Multiple “actions” may be modified before clicking **Apply**, which accepts all changes at once.
- To edit any other parameter of an existing rule, or to delete a rule, click the icon in the corresponding row under the **Edit** column to open the **Rule editing** page.

Note: For brief descriptions of each table parameter, click the **Help** button on the upper-right corner of either the **Table** page or the **Rule editing** page. For more detailed descriptions of each table parameter, refer to “[ForceWare Personal Firewall Parameters: Reference](#)” on page B-139 in this guide.

The ForceWare **Personal Firewall > Advanced Configuration > Options** page also allows you to toggle the firewall's more advanced security features, which you can examine by accessing the online Help.

About Working With Tables

Note that after adding a rule to a table, the new rule appears at the bottom of the table so that it can be easily verified as having been added. When the table is viewed again (after navigating away to another page within the Web browser), the rules are sorted normally, which is by the most distinguishing numerical value. For example, the "UDP/TCP Port" rules are sorted by the "Starting port number", the "ICMP" rules are sorted by the "ICMP Type" and "ICMP Code," etc.

Note: You can always sort any table based on the contents of any column by simply clicking either the **up** or **down** arrows adjacent to the column name in the header at the top of each column.

Each table has an associated "default action" which may be set to **Allow** or **Deny**. Depending on the nature of the default action, a given individual rule may or may not have any effect.

For example, if the TCP default action is to **Allow** packets associated with outbound connections and to **Deny** packets associated with inbound connections, then having a rule to allow outbound HTTP (i.e., TCP port 80) connections would be redundant, because that traffic would already have been allowed by the "default action."

The "default action" defines the action that will be performed when no other specific rules in that particular table applies to a given type of packet.

- In general, if the "default action" of a table is to **Deny**, then most rules should be set to **Allow** specific exceptions.
- Similarly, if the "default action" is to **Allow**, then most rules should be to **Deny** specific exceptions.

Note: It is generally agreed that it is safer to discard traffic unless you specifically need to allow it, so a "default action" of **Deny** is likely to be more secure (or at least more convenient) than a "default action" of **Allow**.

The firewall will compare each packet to the firewall tables in the following order, from the lower, more fundamental parameters to the higher, more complex parameters.

Note: Packets of a specific protocol, such as TCP, will not be processed by the table of an unrelated protocol, such as ICMP.

- 1 EtherType table
- 2 IP Address table
- 3 IP Option table
- 4 IP Protocol table
- 5 TCP Option table
- 6 UDP/TCP Port table
- 7 ICMP table
- 8 Domain Name table

Configuration Dependencies

Preliminary Edition

Under certain configurations, the firewall might not function as expected even though its functionality is still consistent with the actual rules that were configured. In particular, it is possible to provide the firewall with conflicting configuration directives, yet it might not be obvious that this is the case. This situation may arise because of the many ways in which traffic can be allowed or denied and the overlapping scopes of the various firewall tables.

For example, suppose that you had configured the firewall to allow certain types of ICMPv4 traffic but had also configured it to block all IPv4 packets. If you had forgotten that the latter was the case, you might wonder why the allowed ICMPv4 traffic was not getting through. In this case, you would have to realize that you cannot expect ICMPv4 traffic to flow unless you allow at least IP Protocol number 0x01 and EtherType 0x0800 for IPv4.

Other less obvious cases are also possible. For example, if all inbound packets with IP options are blocked, then IGMP Reports will not be received by the stack, since all IGMP Reports have an IP Router Alert option included in the packet.

Recommendations

Note: There are many ways to configure different parameters, which could cause *unintended* and *troublesome* consequences.

Therefore, it is best to work step-by-step through a configuration, building up one layer of rules at a time. Once a given configuration is known to be effective, then it is possible to amend the configuration slightly and re-verify the old configuration, while verifying the new configuration as well. Ultimately, the configuration will converge on a set of rules that meets the stated requirements.

Note: Attempting to set up the final configuration in a single big step can sometimes enable interdependencies that prevents things from working as intended and result in difficult troubleshooting.

Firewall Statistics

All packets generate statistics when passing through the firewall, whether they are allowed or denied.

Each packet increments one of these packet counts—UDP, TCP, ICMP, or Other—as well as one of the TCP and UDP connection counts if it is a connection-initiating packet.

The firewall statistics allow you to:

- Get an idea of the kind of traffic your computer is exchanging
- Get an idea of the amount of the traffic being allowed or denied
- Enable verification of whether a recently changed firewall rule is operating as intended

For example, suppose that you wanted to add a rule to deny TCP packets to any port between 1002 and 1009. To do so you can use the ForceWare Network Access Manager Web interface and follow these steps:

- 1 Access the **Bar Graph** or the **Table** page by selecting a sub-menu under the **Personal Firewall > Information** menu.
- 2 After noting the current TCP statistics, you can add a **TCP Port Rule** to block the 1002 to 1009 range.
- 3 Then you can send some test packets to verify that such packets were indeed blocked.

In order to send TCP traffic to a particular port, you can open a command prompt window and type:

```
telnet foo.example.com 1003
```

where

foo.example.com is any valid domain name or IP address that will normally let a packet be sent through the firewall.

1003 is actually any number between 1002 and 1009 that should be blocked.

The Telnet program will attempt to connect and the expected result (if the rule has been set up properly) is that the Telnet connection attempt should eventually time out because the packets associated with that connection have been blocked.

- 4 After performing the above test, you can again access the **Bar graph** or the **Table** page to verify whether the “Outbound TCP connections denied” count or the “Outbound TCP packets denied” count has increased by an amount consistent with the tests that were performed.

Firewall Logging

In addition to statistics, the firewall generates log entries whenever a packet is dropped, and for all other significant events. When a packet is dropped by the firewall, the log message saved by the firewall corresponds to the first table or rule that denied the packet, as described in the “[Advanced Configuration](#)” on [page 31](#) section.

For example, if the firewall generates a “Blocked IP option” message because a TCP packet has a disallowed IP option, the dropped packet might not have passed the TCP rules, but since it was blocked by the IP option table first, “Blocked IP option” is the message saved by the firewall.

In the example in the “[Firewall Statistics](#)” on [page 34](#) section above, the telnet packet that was generated also causes a “Blocked port” message for port 1003 — unless another table blocks it first, in which case a log message for that table will be generated. In the latter case, the timestamps in the log messages can be used to correlate those log entries that were created during the test.

Other events that generate log entries include changing to a different profile, packets dropped by an advanced firewall security option, enabling and disabling an NVIDIA network interface, and any other changes to the firewall configuration.

Note: Log entries are saved in batches so that the most recent logs may take a short time to appear in the ForceWare Network Access Manager Web interface.

- 1 To view the log page, select the **Log** menu and use the links at the bottom of the page (**First**, **Previous**, **Next**, and **Last**) to navigate.
- 2 If you feel that too many log entries are being generated, click **Clear All Logs**, or consider changing the log “filter” setting under the **Log Settings** menu.

Preliminary Edition

ADMINISTRATIVE TASKS

This chapter contains the following topics:

- “Accessing the Administration Menu” on page 37
- “Application Access Control Page” on page 38
- “Restore Factory Default” on page 41
- “Display Settings” on page 42
- “Backup/Restore” on page 42
- “Network Access Manager Software Version” on page 43

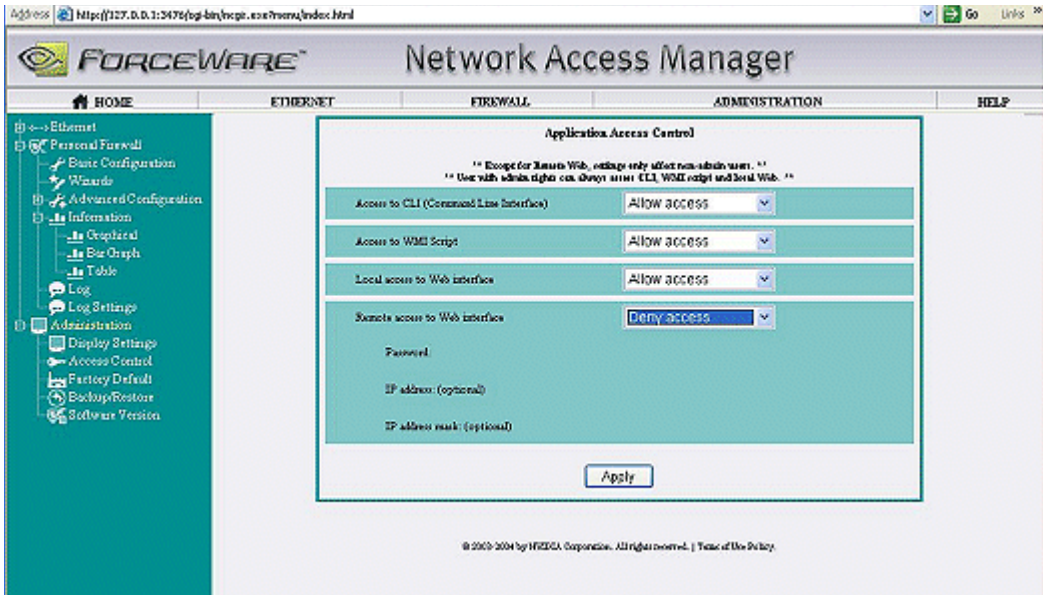
Accessing the Administration Menu

- 1 Open the **ForceWare Network Access Manager** Web menu.
- 2 Click the **Administration** menu on the left of the window to expand it so that you can see the various menu choices.
- 3 Click the menu item to display its associated page on the right.

Application Access Control Page

From the Administration menu, click **Access Control** to display the **Application Access Control** page (Figure 5.1).

Figure 5.1 Sample Application Access Control



This Application Access Control page lets you configure the application access permissions. Note the following about these permissions:

- Can only be configured from the local computer by an Administrator.

An administrator on a local computer has access to all applications and configuration information — i.e., WMI scripts, the command line, and the Web interfaces, provided they are installed on the computer. The access control settings do not affect the Administrator.

- Cannot be viewed, accessed, or configured *remotely*, even by an Administrator.
- Apply only to non-Administrator users and remote users.

Note: Most of the access control in place will work only if the applications are installed on the NTFS file system. Though the application would function if installed on a FAT file system, it is recommended that you use NTFS.

Default Access Settings

Table 5.1 shows the *default* access settings of the NVIDIA ForceWare Network Access Manager software.

Note: You can also control access by using nCLI parameters such as `AccessCLI`, `AccessWMIScript`, etc.

Table 5.1 Default Access Settings for the ForceWare Network Access Manager

Feature	nCLI Access	WMI Script Access	Web Local Access	Web Remote Access
Ethernet	Any user	Any user	Any user	Administrator only
Firewall	Administrator only	Administrator only	Administrator only	Administrator only
Change access settings	Administrator only	Administrator only	Administrator only	None

Command Line Access

Note: The **Access to CLI** parameter is displayed only if the nCLI program is installed on the computer.

Default: Allow access

This field lets you specify whether to **Allow** or **Deny** command line access to the non-Administrator users.

If local command line access is denied, non-Administrator users cannot access the Network Access Manager. However, Administrator users can always access the Command Line interface.

WMI Script

Default: Allow access.

This field lets you specify whether to **Allow** or **Deny** WMI scripting access to the non-Administrator users.

If disabled, no instances of WMI classes, which are part of the NVIDIA namespace, will be available through WMI script or other third party WMI application.

Administrator users can always access WMI using scripts.

Local Web Access

Default: Local Web access is **Allow**.

This options allows or denies access to the Web interface from the local computer.

If local Web access is denied, non-Administrator users cannot access the Network Access Manager. However, Administrator users can always access the Web interface.

Remote Web Access

Default: Remote Web access is **Deny**.

Note: Enabling remote access is a security risk, since the configuration information is passed over the network in the clear (it is not encrypted).

When connecting to the Web interface from a remote computer using the following command:

```
http://<computer name>:3476
```

type **admin** as the user name and the password, as shown below:

```
username: admin
```

```
password: admin
```

Note: The password for this account can be changed.

The username and the password are sent over the network in the clear (it is not encrypted). The remote user then obtains Administrator access rights.

Additional Notes

- Remote access to Network Access Manager is most suitable from a home environment.
- Remote access to Network Access Manager provides limited access to the IP address/mask and can also be restricted based on the IP address or subnet address.
- Remote access to the Network Access Manager's Web-based interface is unencrypted and can be sniffed easily. It is highly recommended that you connect to this interface from the local network or a secure channel like VPN.

Password

Default: By default there is no password — that is, the password string is empty.

When you enable remote Web access, you can set a password.

Note: The user name for remote access is “admin.”

IP Address and IP Address Mask (optional)

Default: By default there is no IP address or mask.

An IP address or a subnet (specified as a combination of an IP address and an IP address mask) can be used to restrict remote access to the computer. So users from any computer are allowed remote access.

Note: To restrict access to only one computer, you can specify an IP address and no IP address mask. Specifying an IP address mask *without* an IP address is *invalid*.

Restore Factory Default

Note: Only Administrator users can restore factory default values to the firewall.

- 1 Click **Ethernet** or **Firewall** to enable one of these options:
 - Click **Ethernet** to restore factory default values to all the Ethernet-related parameters.
 - Click **Firewall** to restore factory default values to all the Firewall-related parameters.
- 2 After you select either **Ethernet** or **Firewall**, click **Start Restore** to restore the Ethernet or Firewall factory default values.

An alert appears asking you to confirm whether you want to wipe out your current settings and replace them with the default values.
- 3 To proceed click **OK**. To cancel the operation, click **Cancel**.

Display Settings

The **Display Settings** page allows you to configure the font size for the pages and the refresh rate for the statistics pages.

- **Statistics refresh rate (Min 1, Max 65535)** controls the refresh rate of all the statistics pages in the Web interface.
 - **Range of values:** 1 to 65535 seconds
 - **Default:** 10 seconds
- **Font size** controls the font size used in the Web interface. The options are:
 - **Default font**
 - **Small font**

Click **Apply** for the changes to take effect.

Backup/Restore

The Backup/Restore page allows you to backup your configuration to a file or restore your configuration from a file you specify.

- Click **Backup** to launch the “[Backup Configuration](#)” page described below, which will allow you to backup your configuration to a file.
- Click **Restore** to launch the “[Restore User Configuration](#)” page described below, which will allow you to restore the configuration you have backed up in a file.

Backup Configuration

The **Backup Configuration** page will allow you to export the current configuration into a file. You can select the filename and also provide a brief description to be added to the top of the file. Once the backup is completed, a link to the file will be provided. You can right click on the link and save the file to any folder you want.

Note: Only Administrator users can backup the firewall configuration.

- **Backup filename** is the filename of the backup file created.

Note: The *default* file name is `export.txt`

- **Description.** You can enter a short description of the configuration you are backing up. This description will be added to the top of the file along with the date and time of the backup.

- **Configuration.** You can choose either the **Ethernet** or the **Firewall** component to backup.
Note: If you don't choose one of the components, you will get an empty backup file.
- **Backup.** Click **Backup** to start backing up the configuration settings for the selected components.

Restore User Configuration

Note: Only an Administrator users can restore the firewall configurations.

This **Restore User Configuration** page lets you restore or import the configuration settings from a backup file, which will replace all your current configuration with the values is the file.

- **Configuration File to Upload.** Browse the folders in your computer and choose the backup file with the configuration you want to restore.
Note: If you don't specify a file, the last configuration you exported will be restored.
- **Restore.** Click this button to restore configuration values contained in the specified file.
Note: A warning will be displayed indicating that the network interface might have to be restarted for these settings to take effect. You might lose connection to the server and that you will be able to get back to the page by clicking the browser **Refresh** button once the changes are applied. To proceed click **OK**. To cancel the operation, click **Cancel**.

At the end of the restore operation, a log appears, indicating any errors in the restore operation. You can restore the previous settings by clicking the **Restore Backup** button.

Network Access Manager Software Version

From the main ForceWare Network Access Manager menu, click **Administration - Software Version** to display the **Network Access Manager Software Version** page.

This page displays the version information for all the NVIDIA ForceWare Network Access Manager files you have installed on this computer.

Note: The version information is useful when you contact the computer manufacturer for technical support.

CHAPTER

6

USING WMI SCRIPT

This chapter contains the following topics:

- “Before You Begin” on page 44
- “Overview” on page 44
- “Advanced Topics” on page 45
- “Examples” on page 46

Before You Begin

This chapter is intended for those Administrators who are familiar with using Microsoft WMI scripting language.

Overview

WMI technology is Microsoft Windows’s implementation of **Web-Based Enterprise Management (WBEM)**, an industry standard for management infrastructure that supports **Common Information Model (CIM)**, **Managed Object Format (MOF)**, and a common programming interface.

The WMI technology also provides support for third-party custom Providers. **Custom Providers** can be used to service requests related to managed objects that are environment-specific.

Providers typically do the following:

- Use the **MOF** language to define and create classes.
- Use the **WMI API** to

- access the **CIM Object Manager (CIMOM)** object repository
- respond to CIMOM requests made initially by applications.

WMI consists of a management infrastructure (CIM object manager) and WMI custom Providers that communicate with each other through a common programming interface using **Component Object Model (COM)**.

The NVIDIA ForceWare Network Access Manager solutions supports

- **CIM** extension schemas
- **Custom Providers**.

For further details, see the following Web site:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwm/html/wmiscript.asp>

Advanced Topics

NVIDIA Namespace

NVIDIA ForceWare Network Access Manager classes are located under `root/NVIDIA` namespace in the WMI repository.

Note: It is strongly recommended that you do not modify anything in the NVIDIA namespace; for example., do not add or remove classes, or update their qualifiers. Modifying these items can prevent the proper functioning of the ForceWare Network Access Manager software.

WMI Provider

NVIDIA implements an extensible instance provider to manage the NVIDIA-specific objects. It is a COM in-proc server.

Synchronization

NVIDIA management framework ensures that only one Web, nCLI, or WMI script user interface is running at any given time. This feature is implemented to avoid data synchronization problems and improve the user experience.

Note: Within the WMI script, you can execute more than one script at any given time. However, doing so can potentially introduce data inconsistency. NVIDIA recommends that you run only one script at a time.

Examples

NVIDIA provide examples of all common parameters.

Sample script files can be found under the “sample” subdirectory, under the default path of `c:\forceware\network access manager`, or your user-specified path.

For example, Firewall WMI script examples are in: `sample\Firewall\PerFireWMIScriptExamples.js`

USING COMMAND LINE INTERFACE (CLI) ACCESS

This chapter contains the following major sections:

- “Conventions Used” on page 47
- “Parameters” on page 48
- “Modes of Operation” on page 48
- “Using Single Parameters” on page 49
- “Using Table Parameters” on page 50
- “Browse Parameter Structure” on page 54
- “Text File Process” on page 57

Conventions Used

Text in “code” font (`this is code font`) means it is text that is displayed on your screen. Text in bold “code” font (**bold code font**) indicates text you type on your computer.

About Examples Used

Examples are used to show how to use the nCLI command and parameters in “Expert” mode (not Interactive mode) to configure some of the MCP networking features of the NVIDIA ForceWare Network Access Manager application. You can simplify the example to suit your needs.

Note: Examples are also provided in the `samples` subdirectory, under the default path of `c:\forceware\network access manager`, or your user-specified path.

Parameters

The nCLI command accepts three classes of parameters — single, namespace, and table.

- **Single** parameters contain a single value of some type.
- **Table** parameters contain data grouped in rows. Each row follows a fixed structure. You can only perform row operations on tables.
- **Namespace** parameters are a collection of tables and other parameters. Namespace is a way to group parameters. You can only browse into a namespace. No Set or Get commands are allowed on namespace parameters.

Modes of Operation

You can run nCLI in either **expert mode** or **interactive mode**. nCLI also supports import/export functions and expert commands grouped in batch files.

The key difference between expert mode vs. interactive mode is whether the control is switched back to command prompt when a command has completed.

- **Expert mode:** In expert mode, the control is switched back to the command prompt after a command has completed executing.
From the command prompt, if you type `ncli` followed by a parameter, you exit to the command prompt after the command has completed.
- **Interactive Mode:** In interactive mode, the control remains in nCLI until you type `quit` to exit nCLI. You remain in the nCLI shell during interactive operations.

You can enter interactive mode in two ways,

First Method

- a From the command prompt, type `ncli` and press Enter.

The nCLI command prompt (`nCLI>`) appears to indicate nCLI is ready to accept a command.

- b You can now type commands in the nCLI mode without having to prefix the keyword `ncli`.

Second Method

- a Enter an incomplete command from the command prompt. For example:

```
ncli set ASFSupport
```


nCLI automatically enters interactive mode. When this command completes, it remains in nCLI mode with the prompt, `nCLI>`. You have to type `quit` to exit nCLI and switch control to the command prompt.

Using Single Parameters

Get and Set are the two most frequently used nCLI operations.

- Get is used to retrieve the setting of a parameter and can be invoked on single, group, and table parameters.
- Set is used to change or update the current setting of a parameter. Set can be used in an “expert” mode, where the command is done in one line, or it can be used in “interactive” mode. Single parameter Get and Set operations are discussed with examples in the sections that follow.

Set (Expert Mode)

Using the Set command in expert mode is intended for expert users to set a single parameter on a single computer. Using expert set requires knowing the correct (error-free) format or selection for the parameter and therefore requires familiarity with the distinguished name of the single parameter

Some frequently set parameters, such as `ASFSupport enable` or `ASFSupport disable`, are usually set using expert mode.

Note: These commands can also be included in script or batch files.

Example

```
C:\NVIDIA\NetMgmt\bin>ncli set ASFSupport enable
```

Set (Interactive Mode)

Using interactive set doesn't require too much prior knowledge of the parameter. In the following case, the parameter to be set, `ASFSupport`, is a selection, so the two choices are shown to help you select a value.

Example

```
C:\NVIDIA\NetMgmt\bin>ncli set ASFSupport
```

```
NVIDIA ForceWare Network Access Manager Framework Version
01.00
ASFSupport:
1 Disable
2 Enable
choose one(Enable) : 1
```

Get

```
C:\NVIDIA\NetMgmt\bin>ncli get ASFSupport
NVIDIA ForceWare Network Access Manager Framework Version
01.00
ASFSupport enable
```

Help

Example

```
C:\NVIDIA\NetMgmt\bin>ncli help ASFSupport
NVIDIA ForceWare Network Access Manager Framework Version 01.00
Enable or disable ASF (Alert Standard Format). ASF is an industry
specification that defines alerting capability in both OS-present
and OS-absent environments.
```

Using Table Parameters

A table is a collection of groups (rows) that share the same fields (columns). Tables are frequently used to store the settings for firewall rules, filters, and statistics. Each row inside the table is uniquely identified by a **key**. A key is composed of one or more of fields of a row.

Note: Only *expert users* need to know the key format and composition.

nCLI supports both interactive and expert operations on tables.

- **Interactive** mode is recommended for average users.
- **Expert** operations on tables are usually executed through batch files. Expert users can also use the `export/import` method and text file to set up tables quickly.

Add Row

The following example shows how to add three rows to an empty table (NV_FireEtherType), edit the table, and then delete one row.

The following example shows how to add rows, edit rows, and delete rows in the NV_FwlEtherType table.

Example

```
C:\NVIDIA\NetMgmt\bin>ncli addrow nv_fireethertype
NVIDIA ForceWare Network Access Manager Framework Version
01.00
EtherType:2048
EtherTypeName:IP
EtherTypeRule
1 Deny
2 Allow
choose one: 2
C:\NVIDIA\NetMgmt\bin>ncli addrow nv_fireethertype
NVIDIA ForceWare Network Access Manager Framework Version
01.00
EtherType:2054
EtherTypeName:ARP
EtherTypeRule
1 Deny
2 Allow
choose one: 2
C:\NVIDIA\NetMgmt\bin>ncli addrow nv_fireethertype
NVIDIA ForceWare Network Access Manager Framework Version 01.00
EtherType:32923
EtherTypeName:AppleTalk
EtherTypeRule
1 Deny
2 Allow
choose one: 1
```

Edit Row

Example

```
C:\NVIDIA\NetMgmt\bin>ncli editrow nv_fireethertype
NVIDIA ForceWare Network Access Manager Framework Version 01.00
```

#	EtherType	EtherTypeName	EtherTypeRule
1	2048	IP	Allow
2	2054	ARP	Allow
3	32923	AppleTalk	Deny

```
Select a row to edit: 3
EtherType(32923)=2056
EtherTypeName(AppleTalk)=Frame Relay ARP / Inverse ARP
EtherTypeRule:
1 Deny
2 Allow
choose one(Deny): 2
```

Delete Row

Example

```
C:\NVIDIA\NetMgmt\bin>ncli delrow nv_fireethertype
```

```
NVIDIA ForceWare Network Access Manager Framework Version
01.00
```

#	EtherType	EtherTypeName	EtherTypeRule
1	2048	IP	Allow
2	2054	ARP	Allow
3	2056	Frame Relay A..	Allow

```
Select a row to delete: 3
Are you sure? (y/n): Y
```

Help

Example

```
C:\NVIDIA\NetMgmt\bin>ncli help nv_fireethertype
```

```
NVIDIA ForceWare Network Access Manager Framework Version 01.00
Firewall rules for different Data Link Layer protocols
Firewall rules for different Data Link Layer protocols (identified
by Ethernet type) including IP, IPX, NetBEUI, AppleTalk and other
protocols.
```

Set Table

Invoking the nCLI set command on table parameters guides you through different operations that can be performed on a table. In the following example, a row is added to the table, then edited, and finally deleted.

Note: Set table does not require your to know addRow, delRow, and editRow command names.

Example

```
C:\NVIDIA\NetMgmt\bin>ncli set nv_fireethertype
```

```
NVIDIA ForceWare Network Access Manager Framework Version
01.00
```

```
Select an option: AddRow(A), EditRow(E), Purge(P), DeleteRow(D), Quit(Q):A
```

```
EtherType:32923
```

```
EtherTypeName:AppleTalk
```

```
EtherTypeRule
```

```
1 Deny
```

```
2 Allow
```

choose one: **1**

```
C:\NVIDIA\NetMgmt\bin>ncli set nv_fireethertype
NVIDIA ForceWare Network Access Manager Framework Version
01.00
Select an option: AddRow(A), EditRow(E), Purge(P), DeleteRow(D), Quit(Q):E
EtherType(32923)=33079
EtherTypeName(AppleTalk)=IPX
EtherTypeRule:
1 Deny
2 Allow
choose one(Deny): 2
```

```
C:\NVIDIA\NetMgmt\bin>ncli set nv_fireethertype
NVIDIA ForceWare Network Access Manager Framework Version
01.00
Select an option: AddRow(A), EditRow(E), Purge(P), DeleteRow(D), Quit(Q):D
```

#	EtherType	EtherTypeName	EtherTypeRule
1	2048	IP	Allow
2	2054	ARP	Allow
3	33079	IPX	Allow

```
Select a row to delete: 3
Are you sure? (y/n): y
```

Get Table

Example

```
C:\NVIDIA\NetMgmt\bin>ncli get nv_fireethertype
NVIDIA ForceWare Network Access Manager Framework Version
01.00
```

#	EtherType	EtherTypeName	EtherTypeRule
1	2048	IP	Allow
2	2054	ARP	Allow

About Expert Commands

Due to the inherent complexity, expert commands are not as intuitive as interactive commands. The syntax of an expert command is shown below. Examples are also provided in the `samples` subdirectory, under the default path of `c:\forceware\network access manager`, or your user-specified path.

Syntax

```
ncli addrow <tablename>
<column1>=<column1value>,<column2>=<column2value>,...i
```

```
ncli editrow i\<tablename>.<key1>=<key1value>,<key2>=<key2value>,...i
<column1>=<column1value>,<column2>=<column2value>,...i
ncli delrow i\<tablename>.<key1>=<key1value>,<key2>=<key2value>,...i
```

In the following example:

- A new row for IPv6 EtherType is added and initially set to Allow.
- The table is then edited with the IPv6 Ethertype rule set to Deny.
- Finally, the entire row is deleted.

Example

```
C:\NVIDIA\NetMgmt\bin>ncli addrow nv_fireethertype
"EtherType=34525,EtherTypeName=IPv6,EtherTypeRule=Allow"
C:\NVIDIA\NetMgmt\bin>ncli editrow
iNV_FireEtherType.EtherType=34525"
"EtherType=34525,EtherTypeName=IPv6,EtherTypeRule=Deny"
C:\NVIDIA\NetMgmt\bin>ncli delrow
iNV_FireEtherType.EtherType=34525i
```

About Other Table Commands

The `purge` command is used to delete all the rows in the table; i.e., the entire table.

Note: Please use this command cautiously.

Syntax

```
purge <tablename>
```

Note: If the table has read-only access, the `purge` action will fail.

Browse Parameter Structure

The MCP networking parameters are organized in a tree structure. You can explore the tree structure. The browsing capability of nCLI is a powerful tool for non-expert use as one does not have to know the parameter's distinguished name before using the command.

List

The `ls` or `dir` command lists the children of the current parameter, as illustrated in the next example.

Example

```
C:\NVIDIA\NetMgmt\bin>ncli
NVIDIA ForceWare Network Access Manager Framework Version
01.00
ncli>ls
NS_Eth
NS_NvConfig
NS_Firewall
NS_UserLog
NS_Security
ncli>ls ns_eth
NS_EthStat
NS_EthConfig
NS_ASF
NV_DriverRestartCmd
NV_DriverRestartFlag
ncli>
```

Change Directory

The `cd` command lets you browse through the parameter tree structure.

Example 1

```
C:\NVIDIA\NetMgmt\bin>ncli
NVIDIA ForceWare Network Access Manager Framework Version
01.00
ncli>ls
NS_Eth
NS_NvConfig
NS_Firewall
NS_UserLog
NS_Security
ncli>cd NS_Eth
ncli>ls
NS_EthStat
NS_EthConfig
NS_ASF
NV_DriverRestartCmd
NV_DriverRestartFlag
ncli>cd ns_ethstat
ncli>ls
NV_NetworkGenStat
NV_EthStat
ncli>
```


Example 2

Note: Invoking the `cd` command by itself will bring you to the root level, as shown in the following example.

```
C:\NVIDIA\NetMgmt\bin>ncli
NVIDIA ForceWare Network Access Manager Framework Version
01.00
ncli>cd ns_eth
ncli>cd ns_ethstat
ncli>cd
ncli>
```

Since each parameter under management will have a unique name, you do not need the complete path to get to a single parameter. The example below shows how this can help you get to a parameter quickly.

```
C:\NVIDIA\NetMgmt\bin>ncli
NVIDIA ForceWare Network Access Manager Framework Version 01.00
ncli>cd ASFSupport
ncli>pwd
<root>/NS_Eth/NS_ASF/NV_ASF/ASFSupport
ncli>
```

Current Working Directory

The `pwd` command is used to display the path to the current parameter.

Example

```
C:\NVIDIA\NetMgmt\bin>ncli
NVIDIA ForceWare Network Access Manager Framework Version 01.00
ncli>cd ns_ethstat
ncli>pwd
<root>/NS_Eth/NS_EthStat
ncli>cd
ncli>pwd
<root>
ncli>
```

Context Sensitive Operations

`ls`, `cd`, and `pwd` commands allow you to browse through the parameters. `nCLI` always remembers that parameter you are currently in so that all the operations you invoke will be in the context of the parameter.

Example

```
C:\NVIDIA\NetMgmt\bin>ncli
NVIDIA ForceWare Network Access Manager Framework Version 01.00
ncli>cd nv_fireethertype
ncli>get
```

#	EtherType	EtherTypeName	EtherTypeRule
1	2048	IP	Allow
2	2054	ARP	Allow

```
ncli>help
Firewall rules for different Data Link Layer protocols
Firewall rules for different Data Link Layer protocols (identified
by Ethernet type) including IP, IPX, NetBEUI, AppleTalk and other
protocols.
ncli>addrow
EtherType:2056
EtherTypeName:FrameRelay ARP/Inverse IP
EtherTypeRule
1 Deny
2 Allow
choose one: 2
```

```
ncli>get
```

#	EtherType	EtherTypeName	EtherTypeRule
1	2048	IP	Allow
2	2054	ARP	Allow
3	2056	FrameRelay AR..	Allow

```
ncli>
```

Text File Process

Text file processing is intended for expert users to quickly update complex parameters and perform large configurations.

For example, you can use the nCLI command line to perform interactive settings *only* on tables. Text file processing offers an alternative to the Get and Set parameter values in a flat text format.

Export

Export files follow a standard format that will make it compatible with Web-based management. That is, export files from nCLI can be imported using the Web-based management and export files from Web-based management can be imported using nCLI.

Syntax

```
export /f<filename> <parameter name>
```

Note that either one or both of /f<filename> and <parameter name> may be omitted.

- If /f<filename> is omitted, the output of the export will be stored in frontend\backup\cliexport.txt under the directory where NVIDIA ForceWare Network Access Manager software is installed.
- If <parameter name> is omitted, the current parameter and its children will be exported. An example is shown below.

Example

```
C:\NVIDIA\NetMgmt\bin>ncli
NVIDIA ForceWare Network Access Manager Framework Version
01.00
ncli>export
.....
.....Finished
ncli>
```

Import

Before importing new parameter settings, old parameter settings are backed up to prevent any problems during import that could throw the system into an unknown state. The backup file can be used to restore the system to the previous state.

Note: If nCLI encounters problems in importing parameters, it will abort and instruct you to restore to the previous state. Use the `restore` command for recovery.

Syntax

```
import /f<filename>
```

If /f<filename> is omitted, the default file frontend\backup\cliexport.txt under the directory where NVIDIA ForceWare Network Access Manager software will be read and imported.

Example

```
C:\NVIDIA\NetMgmt\bin>ncli
NVIDIA ForceWare Network Access Manager Framework Version 01.00
ncli>import
Reading text and importing
.....
.....Backing up to clibackup.txt in case of failure
.....
.....Finished Import.
ncli>
```

Selective Export

Selective export allows you to export only the parameter branch specified.

Syntax

```
export /f<file name> <parameter name>
```

Example

To export only the NS_XXXX namespace, the following command can be used.

```
ncli export /fc:\xxxx_export.txt ns_XXXX
```

```
NVIDIA ForceWare Network Access Manager Framework Version  
01.00
```

```
..Finished
```

Context Export

nCLI lets you browse into a parameter branch and export it.

Example

```
C:\NVIDIA\NetMgmt\bin>ncli  
NVIDIA ForceWare Network Access Manager Framework Version 01.00  
ncli>cd ns_eth  
ncli>export  
ncli>
```

As a result, only the NS_Eth branch is exported.

Glossary

See [“Glossary” on page C-231](#).

Preliminary Edition



ETHERNET PARAMETERS: REFERENCE

Organization and Links

“Group: Remote Wakeup” on page 66

Single Parameter: “Remote Wakeup” on page A-66

Single Parameter: “Remote Wakeup by Magic Packet” on page A-67

Single Parameter: “Remote Wakeup (Pattern Match)” on page A-68

Single Parameter: “Remote Wakeup (Link State Change)” on page 69

Single Parameter: “Remote Wake Up from Hibernate or Shutdown” on page 70

“Group: Protocol Offload” on page 71

Single Parameter: “Checksum Offload” on page 71

Single Parameter: “IPv4 Transmit Checksum Offload” on page 72

Single Parameter: “IPv4 Receive Checksum Offload” on page 73

Single Parameter: “UDP Transmit Checksum Offload” on page 74

Single Parameter: “UDP Receive Checksum Offload” on page 75

Single Parameter: “TCP Transmit Checksum Offload” on page 76

Single Parameter: “TCP Receive Checksum Offload” on page 77

Single Parameter: “TCP Large Send Offload” on page 78

“Group: Microsoft Operating System VLAN (Virtual LAN)” on page 79

“Microsoft Operating System VLAN” on page 79

“Group: VLAN (Virtual LAN)” on page 80

“VLAN Support” on page 80

“VLAN ID” on page 81

“Group: Jumbo Frame” on page 82

Single Parameter: “Jumbo Frame Payload Size” on page 82

“Group: Driver Optimization” on page 83

Single Parameter: “Ethernet Driver Optimization” on page 83

“Group: Ethernet Performance” on page 84

Single Parameter: “Number of Receive Buffers” on page 84

Single Parameter: “Number of Receive Buffer Descriptors” on page 85

Single Parameter: “Number of Transmit Buffer Descriptors” on page 86

Single Parameter: “Maximum Transmit Frames Queued” on page 87

Single Parameter: “Number of Receive Packets to Process per Interrupt” on page 88

Single Parameter: “Number of Transmit Packet to Process per Interrupt” on page 89

Single Parameter: “Interrupt Interval” on page 90

“Group: Traffic Prioritization” on page 91

Single Parameter: “IEEE 802.1p Support” on page 91

“Group: Ethernet Speed/Duplex” on page 92

Single Parameter: “Configurable Ethernet Speed/Duplex Settings” on page 92

“Group: Ethernet Information” on page 93

Single Parameter: “Configurable Ethernet Speed/Duplex Settings” on page 92

Single Parameter: “Link Speed” on page 93

Single Parameter: “Maximum Link Speed” on page 94

Single Parameter: “Duplex Setting” on page 95

- Single Parameter: “Link Status” on page 96
- Single Parameter: “Promiscuous Mode” on page 97
- Single Parameter: “Permanent Ethernet Address” on page 98
- “Group: Ethernet Address” on page 99
 - Single Parameter: “Current Ethernet Address” on page 99
- “Group: Network Interface information” on page 100
 - Single Parameter: “Computer (Machine) Name” on page 100
 - Single Parameter: “IP Address ” on page 101
 - Single Parameter: “IP Address Mask” on page 102
- “Group: Factory Default” on page 103
 - Single Parameter: “Factory Default” on page 103
- “Table: Multicast Address List” on page 104
 - Single Parameter: “Multicast Addresses (Single Parameter)” on page 105
- “Group: Ethernet Statistics” on page 106
 - Single Parameter: “Frames Received with Alignment Error” on page 106
 - Single Parameter: “Frames Transmitted After One Collision” on page 107
 - Single Parameter: “Frames Transmitted After Two or More Collisions” on page 108
 - Single Parameter: “Frames Transmitted After Deferral” on page 109
 - Single Parameter: “Display Name Frames Exceed Maximum Collision” on page 110
 - Single Parameter: “Frames with Overrun Errors” on page 111
 - Single Parameter: “Frames with Underrun Errors” on page 112
 - Single Parameter: “Frames with Heartbeat Failure” on page 113
 - Single Parameter: “Carrier Sense (CRS) Signal Lost” on page 114
 - Single Parameter: “Late Collisions” on page 115
- “Group: General Networking Statistics” on page 116
 - Single Parameter: “Successfully Transmitted Frames” on page 116
 - Single Parameter: “Successfully Received Frames” on page 117
 - Single Parameter: “Transmit Failures” on page 118
 - Single Parameter: “Receive Failures” on page 119

- Single Parameter: “No Receive Buffers” on page 120
- Single Parameter: “Direct Frames Received” on page 121
- Single Parameter: “Multicast Frames Received” on page 122
- Single Parameter: “Broadcast Frames Received” on page 123
- “Group: Alert Standard Format” on page 124
 - Single Parameter: “ASF Support” on page 124
 - Single Parameter: “ASF Support” on page 124
 - Single Parameter: “No Receive Buffers” on page 120
 - Single Parameter: “Direct Frames Received” on page 121
 - Single Parameter: “Multicast Frames Received” on page 122
 - Single Parameter: “Broadcast Frames Received” on page 123
- “Group: Alert Standard Format” on page 124
 - Single Parameter: “ASF Support” on page 124
 - Single Parameter: “ASF Destination IP Address” on page 125
 - Single Parameter: “ASF Send Count” on page 126
- “Group: ASF Information” on page 127
 - Single Parameter: “ASF Destination MAC Address” on page 127
- “Group: System Fails to Boot Alert” on page 128
 - Single Parameter: “System Fails to Boot Alert” on page 128
- “Group: Fan Problem Alert” on page 129
 - Single Parameter: “Fan Problem Alert” on page 129
- “Group: ASF SMBus Error” on page 130
 - Single Parameter: “ASF SMBus Error” on page 130
- “Group: ASF WOL Alert” on page 131
 - Single Parameter: “ASF WOL (Wake On Lan) Aler” on page 131
- “Group: ASF Heartbeat Alert” on page 132
 - Single Parameter: “ASF Heartbeat Alert Interval” on page 132

“Group: ASF Operating System Hung Alert” on page 133

Single Parameter: “ASF Operating System Hung Alert” on page 133

“Group: ASF Power Button Alert” on page 134

Single Parameter: “ASF Power Button Alert” on page 134

“Group: ASF System Hot Alert” on page 135

Single Parameter: “ASF System Hot Alert” on page 135

“Group: ASF CPU Overheated Alert ” on page 136

Single Parameter: “ASF CPU Overheat Alert” on page 136

“Group: ASF CPU Overheated Alert” on page 137

Single Parameter: “ASF CPU Hot Alert” on page 137

“Group: ASF Case Intrusion Alert” on page 138

Single Parameter: “ASF Case Intrusion Alert ” on page 138

Group: Remote Wakeup

Remote Wakeup

Parameter	WakeUp
Description	Enables or disables Ethernet remote wake up capability. When enabled, the user can remotely turn on the power of systems across the network. For example, a network administrator can use Remote Wake Up to perform after-hours maintenance from a remote location without requiring a technician to be physically present.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_EthConfig</div> <div> <div>Group: NV_EthWakeUp</div> <div> <div>Single: WakeUp</div> </div> </div> </div> </div>
Usage example:	nCLI Set "WakeUp" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Remote Wakeup by Magic Packet

Parameter	WakeUpMagic
Description	Enables or disables the magic packet wake-up feature. When this feature is enabled, networked computers that are in a low power state receive the “magic packet” to wake up
Comment	If WakeUp is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_EthWakeUp </div> <div> Single: WakeUpMagic </div> </div>
Usage example:	nCLI Set "WakeUpMagic" "Enable"
Access	ReadWrite
Restart network connection:	Restart required
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Remote Wakeup (Pattern Match)

Parameter	WakeUpPattern
Description	Enables or disables the pattern match remote wakeup feature. When this feature is enabled, networked computers that are in a low power state receive a packet that contains a pattern specified by the operating system's network protocol to wake up.
Comment	If WakeUp is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_EthWakeUp </div> <div> Single: WakeUpPattern </div> </div>
Usage example:	nCLI Set "WakeUpPattern" "Enable"
Access	ReadWrite
Restart network connection:	Restart required
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Remote Wakeup (Link State Change)

Parameter:	WakeUpLink
Description	Enables or disables the WakeUpLink feature. Change in the link state refers to the connection or disconnection of the Ethernet network cable. When a networked computer is in a low power state, a change in the link state wakes up the computer.
Comment	If WakeUp is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_EthWakeUp </div> <div> Single: WakeUpLink </div> </div>
Usage example:	nCLI Set "WakeUpLink" "Enable"
Access	ReadWrite
Restart network connection:	Restart is required
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Remote Wake Up from Hibernate or Shutdown

Parameter	WakeUpS4S5
Description	Enables or disables the Remote Wake Up from Hibernate or Shutdown feature. Hibernate means that all devices in a networked computer are turned off. This state is saved to the computer's hard disk and is then used for a fast startup. Shutdown means that the operating system will shut down and the BIOS will be re-initialized during wake up.
Comment	If WakeUp is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_EthWakeUp </div> <div> Single: WakeUpS4S5 </div> </div>
Usage example:	nCLI Set "WakeUpS4S5" "Enable"
Access	ReadWrite
Restart network connection:	Restart is required.
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Group: Protocol Offload

Checksum Offload

Parameter	EthOffloadChkSum
Description	Enables or disables the Ethernet checksum offload feature. Offloads increase the system performance by offloading TCP/IP CPU-intensive tasks to hardware.
Comment	This feature is not supported by WMI scripting.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_Eth_Offload </div> <div> Single: EthOffloadChkSum </div> </div>
Usage example:	nCLI Set "EthOffloadChkSum" "Enable"
Access	ReadWrite
Restart network connection:	Restart is required.
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

IPv4 Transmit Checksum Offload

Parameter	EthOffloadIPv4TxChkSum
Description	Enables or disables the IPv4 Transmit Checksum Offload feature. When this feature is enabled, the operating system passes the task of calculating IP (Internet Protocol) checksums for transmitted packets to the Ethernet hardware.
Comment	This parameter is not supported by WMI scripting. If EthOffloadChkSum is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_Eth_Offload </div> <div> Single: EthOffloadIPv4TxChkSum </div> </div>
Usage example:	nCLI Set "EthOffloadIPv4TxChkSum" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

IPv4 Receive Checksum Offload

Parameter:	EthOffloadIPv4RxChkSum
Description	Enables or disables the IPv4 Receive Checksum Offload feature. When this feature is enabled, the operating system passes the task of calculating IP checksums for received packets to the Ethernet hardware.
Comment	This parameter is not supported by WMI scripting. If EthOffloadChkSum is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_Eth_Offload </div> <div> Single: EthOffloadIPv4RxChkSum </div> </div>
Usage example:	nCLI Set "EthOffloadIPv4RxChkSum" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

UDP Transmit Checksum Offload

Parameter	EthOffloadUDPTxChkSum
Description	Enables or disables the UDP (User Datagram Protocol) Transmit Checksum Offload feature. When this feature is enabled, the operating system can use the Ethernet hardware to calculate UDP checksums for transmitted packets.
Comment	This parameter is not supported by WMI scripting. If EthOffloadChkSum is set to Disable, this parameter value is ignored.
Hierarchy	<div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_Eth_Offload </div> <div> Single: EthOffloadUDPTxChkSum </div>
Usage example:	nCLI Set "EthOffloadUDPTxChkSum" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

UDP Receive Checksum Offload

Parameter	EthOffloadUDPRxChkSum
Description	Enables or disables the UDP Receive Checksum Offload feature. When the feature is enabled, the operating system can use the Ethernet hardware to calculate UDP checksums for received packets.
Comment	This parameter is not supported by WMI scripting. If EthOffloadChkSum is set to Disable, this parameter value is ignored.
Hierarchy	<div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_Eth_Offload </div> <div> Single: EthOffloadUDPRxChkSum </div>
Usage example:	nCLI Set "EthOffloadUDPRxChkSum" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

TCP Transmit Checksum Offload

Parameter	EthOffloadTCPTxChkSum
Description	Enables or disables the TCP Transmit Checksum Offload feature. When the feature is enabled, the operating system can use the Ethernet hardware to calculate TCP checksums for transmitted packets.
Comment	This parameter is not supported by WMI scripting. If EthOffloadChkSum is set to Disable, this parameter value is ignored.
Hierarchy	<div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_Eth_Offload </div> <div> Single: EthOffloadTCPTxChkSum </div>
Usage example:	nCLI Set "EthOffloadTCPTxChkSum" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

TCP Receive Checksum Offload

Parameter	EthOffloadTCPRxChkSum
Description	Enables or disables the TCP Receive Checksum Offload feature. When the feature is enabled, the operating system can use the Ethernet hardware to calculate TCP checksums for transmitted packets.
Comment	This parameter is not supported by WMI scripting. Note: If EthOffloadChkSum is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_Eth_Offload </div> <div> Single: EthOffloadTCP RxChkSum </div> </div>
Usage example:	nCLI Set "EthOffloadTCPRxChkSum" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

TCP Large Send Offload

Parameter	EthOffloadTxLargeSend
Description	Enables or disables the TCP Large Send Offload feature. When the feature is enabled, the operating system can utilize the Ethernet hardware capabilities to segment large TCP packets into smaller packets. Note: This feature applies to packet transmissions only.
Hierarchy	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Namespace: NS_Eth </div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px; margin-left: 100px;"> Namespace: NS_EthConfig </div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px; margin-left: 200px;"> Group: NV_Eth_Offload </div> <div style="border: 1px solid black; padding: 5px; margin-left: 300px;"> Single: EthOffloadTxLargeSend </div>
Usage example:	nCLI Set "EthOffloadTxLargeSend" "Enable"
Access	ReadWrite
Restart network connection:	Restart is required.
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Group: Microsoft Operating System VLAN (Virtual LAN)

Microsoft Operating System VLAN

Parameter	EthMSVLAN
Description	Specifies the Virtual LAN (VLAN) ID returned by the Microsoft operating system. The VLAN ID is an identifier used by a networked computer to determine its associated VLAN. VLAN allows a set of networked computers to function as if they were not connected to the same wire even though they may be physically connected to the same segments of a Local Area Network (LAN).
Comment	The Microsoft VLAN ID overrides the NVIDIA EthVLAN and EthVLANID settings. When the Microsoft VLAN ID is 0 (zero), the NVIDIA EthVLAN and EthVLANID are used.
Hierarchy	<div style="margin-left: 40px;"> Namespace: NS_Eth </div> <div style="margin-left: 100px;"> Namespace: NS_EthConfig </div> <div style="margin-left: 160px;"> Group: NV_Eth_MS VLAN </div> <div style="margin-left: 220px;"> Single: EthMSVLAN </div>
Usage example:	nCLI Get "EthMSVLAN"
Access	Read
Data type	Number (32 bit)
Maximum Value	4095
Minimum Value	0

Group: VLAN (Virtual LAN)

VLAN Support

Parameter	EthVLAN
Description	Enables or disables VLAN support. VLAN allows a network of computers to function as if they are not connected to the same wire even though they may be physically located on different segments of a LAN.
Comment	The Microsoft VLAN ID overrides the NVIDIA EthVLAN and EthVLANID values. When the Microsoft VLAN ID is 0 (zero), the NVIDIA EthVLAN and EthVLANID are used.
Hierarchy	<div style="display: flex; flex-direction: column; align-items: center;"> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Namespace: NS_Eth </div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Namespace: NS_EthConfig </div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Group: NV_Eth_VLAN_Setting </div> <div style="border: 1px solid black; padding: 5px;"> Single: EthVLAN </div> </div>
Usage example:	nCLI Set "EthVLAN" "Disable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

VLAN ID

Parameter	EthVLANID
Description	The VLAN ID is an identifier used by a computer to determine its associated VLAN. A value of 0 (zero) means VLAN is disabled. VLAN allows a set of networked computers to function as if they were not connected to the same wire even though they may be physically connected to same segments of a LAN.
Comment	The Microsoft VLAN ID overrides the NVIDIA EthVLAN and EthVLANID values. When the Microsoft VLAN ID is 0 (zero), the NVIDIA EthVLAN and EthVLANID are used.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_Eth_VLAN_Setting </div> <div> Single: EthVLANID </div> </div>
Usage example:	nCLI Set "EthVLANID" "0"
Access	ReadWrite
Data type	Number (32 bit)
Maximum Value	4095
Minimum Value	0

Group: Jumbo Frame

Jumbo Frame Payload Size

Parameter	EthJumboSize
Description	Specify the Ethernet jumbo frame payload size. Jumbo frame supports larger Ethernet packet sizes to reduce server overhead and increase throughput. Payload size of 1,500 means Jumbo Frame is disabled.
Comment	Jumbo frame is supported only when the connection speed is 1000 Mbps.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_EthConfig</div> <div> <div>Group: NV_Eth_Jumbo</div> <div> <div>Single: EthJumboSize</div> </div> </div> </div> </div>
Usage example:	nCLI Set "EthJumboSize" "1500"
Access	ReadWrite
Restart network connection:	Restart required
Data type	Selection
User selection	<ul style="list-style-type: none"> • 1500 • 2500 • 4500 • 9000

Group: Driver Optimization

Ethernet Driver Optimization

Parameter	EthOptimization
Description	Allows Ethernet driver optimization by adjusting Ethernet driver operating parameters to suit different needs.
Comment	This driver optimization profile feature is not supported by WMI scripting. WMI script users must configure parameters within the Ethernet Performance group individually. Profiles are listed and described in the User selection section below.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_EthConfig</div> <div> <div>Group: NV_Eth_Optimization</div> <div> <div>Single: EthOptimization</div> </div> </div> </div> </div>
Usage example:	nCLI Set "EthOptimization" "CPU"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Throughput maximizes the amount of network traffic sent and received. • CPU Utilization optimizes to lower the amount of time CPU spent in processing network traffic. • Multimedia reduces the time spent per network interrupt to allow time-critical media devices to be serviced. • CPU Utilization is the recommended and <i>default</i> setting.

Group: Ethernet Performance

Number of Receive Buffers

Parameter	EthNoOfRxBuff
Description	Specifies the number of receive buffers allocated by the NVIDIA Ethernet driver. Receive buffers are memory blocks used to store packets received from the network.
Comment	For optimal performance, the number of receive buffers need to be at least TWICE the number of receive descriptors.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_EthConfig</div> <div> <div>Group: NV_Eth_Performance</div> <div> <div>Single: EthNoOfRxBuff</div> </div> </div> </div> </div>
Usage example:	nCLI Set "EthNoOfRxBuff" "512"
Access	ReadWrite
Restart network connection:	Restart is required.
Data type	Selection
User selection	<ul style="list-style-type: none"> • 2 • 4 • 8 • 16 • 32 • 64 • 128 • 256 • 512

Number of Receive Buffer Descriptors

Parameter	EthNoOfRxDesc
Description	Number of receive buffer descriptors available to the Ethernet hardware. This value determines the number of receive buffers that may be queued for the hardware.
Comment	For optimal performance, the number of receive buffers need to be set to at least <i>twice</i> the number of receive descriptors.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_Eth_Performance </div> <div> Single: EthNoOfRxDesc </div> </div>
Usage example:	nCLI Set "EthNoOfRxDesc" "64"
Access	ReadWrite
Restart network connection:	Restart required
Data type	Selection
User selection	2, 4, 8, 16 , 32 , 64, 128, 256

Number of Transmit Buffer Descriptors

Parameter	EthNoOfTxDesc
Description	Specifies the number of transmit buffer descriptors available to the Ethernet hardware. This value determines the number of transmit buffers that may be queued for the hardware.
Hierarchy	<div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_Eth_Performance </div> <div> Single: EthNoOfTxDesc </div>
Usage example:	nCLI Set "EthNoOfTxDesc" "256"
Access	ReadWrite
Restart network connection:	Restart is required.
Data type	Selection
User selection	<ul style="list-style-type: none"> • 2 • 4 • 8 • 16 • 32 • 64 • 128 • 256 • 512 • 1024

Maximum Transmit Frames Queued

Parameter	EthMaxTxPktQueue
Description	Specifies the maximum number of frames which may be queued by the Ethernet driver.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthConfig</div><div>Group: NV_Eth_Performance</div><div>Single: EthMaxTxPktQueue</div></div>
Usage example:	nCLI Set "EthMaxTxPktQueue" "1024"
Access	Read Write
Restart network connection:	Restart is required.
Data type	Selection
User selection	<ul style="list-style-type: none">• 2• 4• 8• 16• 32• 64• 128• 256• 512• 1024



Number of Receive Packets to Process per Interrupt

Parameter	EthNoOfRxPktToProcessEachTime
Description	Specifies the number of receive packet to process per interrupt.
Hierarchy	<div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_Eth_Performance </div> <div> Single: EthNoOfRxPktToProcessEachTime </div>
Usage example:	nCLI Set "EthNoOfRxPktToProcessEachTime" "1280"
Access	ReadWrite
Restart network connection:	Restart is required.
Data type	Selection
User selection	<ul style="list-style-type: none"> • 10 • 20 • 40 • 80 • 160 • 320 • 640 • 1280

Number of Transmit Packet to Process per Interrupt

Parameter	EthNoOfTxPktToProcessEachTime
Description	Specifies the number of transmit packet to process per interrupt.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Group: NV_Eth_Performance </div> <div> Single: EthNoOfTxPktToProcessEachTime </div> </div>
Usage example:	nCLI Set "EthNoOfTxPktToProcessEachTime" "1280"
Access	ReadWrite
Restart network connection:	Restart is required.
Data type	Selection
User selection	5 10 20 40 80 160 320 640 1280

Prelim

Interrupt Interval

Parameter	EthPollingInterval
Description	Specifies the time (in milliseconds) between hardware interrupts in the hardware polling mode.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_EthConfig</div> <div> <div>Group: NV_Eth_Performance</div> <div>Single: EthPollingInterval</div> </div> </div> </div>
Usage example:	nCLI Set "EthPollingInterval" "425"
Access	ReadWrite
Restart network connection:	Restart is required.
Data type	Selection
User selection	0, 425

Group: Traffic Prioritization

IEEE 802.1p Support

Parameter	Eth8021p
Description	Enables or disables Ethernet IEEE 802.1p support. IEEE 802.1p allows frames to be grouped into priority classes.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_EthConfig</div> <div> <div>Group: NV_Eth_8021p</div> <div> <div>Single: Eth8021p</div> </div> </div> </div> </div>
Usage example:	nCLI Set "Eth8021p" "Disable"
Access	ReadWrite
Restart network connection:	Restart is required.
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Group: Ethernet Speed/Duplex

Configurable Ethernet Speed/Duplex Settings

Parameter	EthSpeed	
Description	Specifies the configurable Ethernet speed/duplex settings.	
Comment	For systems equipped with Gigabit Ethernet PHY (physical layer transceivers), the “Autonegotiate for 1000 Mbps” selection is available. Otherwise, only the 100/10 Mbps selections are available.	
Hierarchy	<div style="display: flex; flex-direction: column; align-items: center; gap: 20px;"> <div style="border: 1px solid black; padding: 5px; text-align: center;"> Namespace: NS_Eth </div> <div style="border: 1px solid black; padding: 5px; text-align: center;"> Namespace: NS_EthConfig </div> <div style="border: 1px solid black; padding: 5px; text-align: center;"> Group: NV_Eth_Speed </div> <div style="border: 1px solid black; padding: 5px; text-align: center;"> Single: EthSpeed </div> </div>	
Usage example:	nCLI Set "EthSpeed" "Full"	
Access	ReadWrite	
Restart network connection:	Restart is required.	
Data type	Selection	
User selection	<ul style="list-style-type: none"> - Full Autonegotiation - Autonegotiate for 1000 mbps Full Duplex - Autonegotiate for 100 mbps Full Duplex - Autonegotiate for 100 mbps Half Duplex - Autonegotiate for 10 mbps Full Duplex 	<ul style="list-style-type: none"> - Autonegotiate for 10 mbps Half Duplex - Force 100 mbps Full Duplex - Force 100 mbps Half Duplex - Force 10 mbps Full Duplex - Force 10 mbps Half Duplex

Group: Ethernet Information

Link Speed

Parameter	EthLinkSpeed
Description	Specifies the current speed (in Mbps) of the Ethernet device.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthConfig</div><div>Group: NV_EthInfo</div><div>Single: EthLinkSpeed</div></div>
Usage example:	nCLI Get "EthLinkSpeed"
Access	Read
Data type	Number (32 bit)
Maximum Value	10000
Minimum Value	0

Pr

Maximum Link Speed

Parameter	EthLinkMaxSpeed
Description	Specifies the maximum speed (in Mbps) at which the Ethernet interface can operate.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthConfig</div><div>Group: NV_EthInfo</div><div>Single: EthLinkMaxSpeed</div></div>
Usage example:	nCLI Get "EthLinkMaxSpeed"
Access	Read
Data type	Number (32 bit)
Maximum Value	10000
Minimum Value	0



Duplex Setting

Parameter	EthDuplex
Description	Specifies the current Ethernet interface duplex setting. Full duplex means th the Ethernet interface on both ends of a link can receive and transmit data simultaneously over the cable. Half duplex means that either the transmit or receive operation can occur at a given time.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div>Namespace: NS_EthConfig</div> <div>Group: NV_EthInfo</div> <div>Single: EthDuplex</div> </div>
Usage example:	nCLI Get "EthDuplex"
Access	Read
Data type	Selection
User selection	<ul style="list-style-type: none"> • Half Duplex • Full Duplex

Pre

Link Status

Parameter	EthConnectStatus
Description	Displays the current Ethernet link status. When the Ethernet link is disconnected, the remote configuration tool will not function.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_EthConfig</div> <div> <div>Group: NV_EthInfo</div> <div> <div>Single: EthConnectStatus</div> </div> </div> </div> </div>
Usage example:	nCLI Get "EthConnectStatus"
Access	Read
Data type	Selection
User selection	<ul style="list-style-type: none"> Connected Disconnected

Pre

Promiscuous Mode

Parameter	EthPromiscuous
Description	When this parameter is enabled, all packets (including frames addressed other stations) that arrive at this Ethernet interface are received.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthConfig</div><div>Group: NV_EthInfo</div><div>Single: EthPromiscuous</div></div>
Usage example:	nCLI Get "EthPromiscuous"
Access	Read
Data type	Selection
User selection	<ul style="list-style-type: none">• Disable• Enable

Preli

Permanent Ethernet Address

Parameter	EthAddressPermanent
Description	Specifies the fixed Ethernet address encoded in the hardware.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_EthConfig</div> <div> <div>Group: NV_EthInfo</div> <div> <div>Single: EthAddressPermanent</div> </div> </div> </div> </div>
Usage example:	nCLI Get "EthAddressPermanent"
Access	Read
Data type	MAC Address

Prelim

Group: Ethernet Address

Current Ethernet Address

Parameter	EthAddressCurrent
Description	Specifies the Ethernet address currently being used. The Ethernet interface then uses the Current Ethernet Address in place of the Permanent Ethernet Address.
Comment	Format of Ethernet Address must be XX:XX:XX:XX:XX:XX
Hierarchy	<div style="display: flex; flex-direction: column; align-items: center;"> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Namespace: NS_Eth </div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Namespace: NS_EthConfig </div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Group: NV_Eth_Address </div> <div style="border: 1px solid black; padding: 5px;"> Single: EthAddressCurrent </div> </div>
Usage example:	nCLI Set "EthAddressCurrent" "0C:12:34:56:78:9A"
Access	ReadWrite
Restart network connection:	Restart is required.
Data type	MAC Address

Group: Network Interface information

Computer (Machine) Name

Parameter	MachineName
Description	Specifies the unique name that is used to identify a computer on the network domain. The computer (machine) name is specified through the operating system and must be unique within a network domain.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthConfig</div><div>Group: NV_InterfaceInfo</div><div>Single: MachineName</div></div>
Usage example:	nCLI Get "MachineName"
Access	Read
Data type	String
Maximum Length	64

IP Address

Parameter	IPAddress
Description	Specifies the IP address of the current Ethernet interface.
Comment	If an interface has multiple IP addresses and masks, only the first set returned by the operating system is shown.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthConfig</div><div>Group: NV_InterfaceInfo</div><div>Single: IPAddress</div></div>
Usage example:	nCLI Get "IPAddress"
Access	Read
Data type	String
Maximum Length	64

Preli

IP Address Mask

Single Parameter	IPAddressMask
Description	Specifies the IP address mask of the current Ethernet interface.
Comment	If an interface has multiple IP addresses and masks, only the first set returned by the operating system is shown.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_EthConfig</div> <div> <div>Group: NV_InterfaceInfo</div> <div>Single: IPAddressMask</div> </div> </div> </div>
Usage example:	nCLI Get "IPAddressMask"
Access	Read
Data type	String
Maximum Length	64



Group: Factory Default

Factory Default

Parameter	EthDefault
Description	Restores the Ethernet factory default settings.
Comment	Restore factory default feature is not available through WMI scripting.
Hierarchy	<div style="margin-left: 40px;"> <div style="border: 1px solid black; padding: 5px; display: inline-block;"> Namespace: NS_Eth </div> <div style="margin-left: 100px;"> <div style="border: 1px solid black; padding: 5px; display: inline-block;"> Namespace: NS_EthConfig </div> <div style="margin-left: 100px;"> <div style="border: 1px solid black; padding: 5px; display: inline-block;"> Group: NV_Eth_FactoryDefault </div> <div style="margin-left: 100px;"> <div style="border: 1px solid black; padding: 5px; display: inline-block;"> Single: EthDefault </div> </div> </div> </div> </div>
Usage example:	nCLI Set "EthDefault" "Restore"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • NoRestore • Restore

Table: Multicast Address List

Multicast Address List

Table Parameter	NV_Eth_MulticastAddress
Description	Specifies a list of multicast addresses from which the Ethernet interface will receive frames. The Ethernet multicast packet refers to packets addressed to a group of recipients.
Hierarchy	<div> Namespace: NS_Eth </div> <div> Namespace: NS_EthConfig </div> <div> Table: NV_Eth_MulticastAddress </div>
Usage example:	nCLI Get "NV_Eth_MulticastAddress"
Access	Read
Single parameter	EthMulticast (See the next section for details on the EthMulticast parameter.)

Prelim

Multicast Addresses (Single Parameter)

Parameter	EthMulticast
Description	The Ethernet multicast packet refers to packets addressed to a group of recipients.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthConfig</div><div>Table: NV_Eth_MulticastAddress</div><div>Row:</div><div>Single: EthMulticast</div></div>
Access	Read
Table key	This parameter is a key to the table
Data type	MAC Address

Prelim

Group: Ethernet Statistics

Frames Received with Alignment Error

Parameter	EthReceiveErrorAlign
Description	Specifies the number of received frames with alignment errors.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_EthStat</div><div>Single: EthReceiveErrorAlign</div></div>
Usage example:	nCLI Get "EthReceiveErrorAlign"
Access	Read
Data type	Number (64 bit)

Preliminary

Frames Transmitted After One Collision

Parameter	EthTransmitOneCollision
Description	Specifies the number of frames that successfully transmitted after encountering one collision.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_EthStat</div><div>Single: EthTransmitOneCollision</div></div>
Usage example:	nCLI Get "EthTransmitOneCollision"
Access	Read
Data type	Number (64 bit)

Prelimin

Frames Transmitted After Two or More Collisions

Parameter	EthTransmitMoreCollision
Description	Specifies the number of frames that successfully transmitted after encountering two or more collisions.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_EthStat</div><div>Single: EthTransmitMoreCollision</div></div>
Usage example:	nCLI Get "EthTransmitMoreCollision"
Access	Read
Data type	Number (64 bit)

Prelim

Frames Transmitted After Deferral

Parameter	EthTransmitDeferred
Description	Specifies the number of frames that successfully transmitted after the Ethernet hardware defers transmission at least once.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_EthStat</div><div>Single: EthTransmitDeferred</div></div>
Usage example:	nCLI Get "EthTransmitDeferred"
Access	Read
Data type	Number (64 bit)

Preliminary

Display Name Frames Exceed Maximum Collision

Parameter	EthTransmitMaxCollision
Description	Specifies the number of frames not transmitted because of excessive collisions.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_EthStat</div><div>Single: EthTransmitMaxCollision</div></div>
Usage example:	nCLI Get "EthTransmitMaxCollision"
Access	Read
Data type	Number (64 bit)

Prelim

Frames with Overrun Errors

Parameter	EthReceiveOverrun
Description	Specifies the number of frames not received because of overrun errors. An overrun error occurs when the Ethernet hardware receives more data than it can process.
Hierarchy	<div> Namespace: NS_Eth </div> <div> Namespace: NS_EthStat </div> <div> Group: NV_EthStat </div> <div> Single: EthReceiveOverrun </div>
Usage example:	nCLI Get "EthReceiveOverrun"
Access	Read
Data type	Number (64 bit)

Prelimi

Frames with Underrun Errors

Parameter	EthTransmitUnderrun
Description	Specifies the number of frames not transmitted because of underrun errors. An underrun error occurs when the Ethernet hardware cannot transmit frames because the data is not available within the expected time.
Hierarchy	<div><div>Namespace : NS_Eth</div><div>Namespace : NS_EthStat</div><div>Group: NV_EthStat</div><div>Single: EthTransmi tUnderrun</div></div>
Usage example:	nCLI Get "EthTransmitUnderrun"
Access	Read
Data type	Number (64 bit)

Preli

Frames with Heartbeat Failure

Parameter	EthTransmitHeartbeatFail
Description	Specifies the number of frames transmitted without detection of the collision-detect heartbeat.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_EthStat</div><div>Single: EthTransmitHeartbeatFail</div></div>
Usage example:	nCLI Get "EthTransmitHeartbeatFail"
Access	Read
Data type	Number (64 bit)

Prelim

Carrier Sense (CRS) Signal Lost

Parameter	EthTransmitTimesCRSLost
Description	Specifies the number of times the CRS signal has been lost during packet transmission.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_EthStat</div><div>Single: EthTransmitTimesCRSLost</div></div>
Usage example:	nCLI Get "EthTransmitTimesCRSLost"
Access	Read
Data type	Number (64 bit)

Prelim

Late Collisions

Parameter	EthTransmitLateCollisions
Description	The number of collisions detected after the normal detection period.
Hierarchy	<div>Namespace: NS_Eth</div> <div>Namespace: NS_EthStat</div> <div>Group: NV_EthStat</div> <div>Single: EthTransmitLateCollisions</div>
Usage example:	nCLI Get "EthTransmitLateCollisions"
Access	Read
Data type	Number (64 bit)

Preliminary

Group: General Networking Statistics

Successfully Transmitted Frames

Parameter	TransmitOK
Description	Specifies the number of frames transmitted without errors.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_NetworkGenStat</div><div>Single: TransmitOK</div></div>
Usage example:	nCLI Get "TransmitOK"
Access	Read
Data type	Number (64 bit)

Prel

Successfully Received Frames

Parameter	ReceiveOK
Description	Specifies the number of frames that the network card has received without errors.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_NetworkGenStat</div><div>Single: ReceiveOK</div></div>
Usage example:	nCLI Get "ReceiveOK"
Access	Read
Data type	Number (64 bit)

Prelimin:

Transmit Failures

Parameter	TransmitError
Description	Specifies the number of frames that failed to transmit.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_NetworkGenStat</div><div>Single: TransmitError</div></div>
Usage example:	nCLI Get "TransmitError"
Access	Read
Data type	Number (64 bit)

Prelimi

Receive Failures

Parameter	ReceiveError
Description	Specifies the number of frames that are received but not passed to the operating system because of errors.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_NetworkGenStat</div><div>Single: ReceiveError</div></div>
Usage example:	nCLI Get "ReceiveError"
Access	Read
Data type	Number (64 bit)

Prelim

No Receive Buffers

Parameter	ReceiveNoBuffer
Description	Specifies the number of frames that are dropped because of lack of space receive buffers.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_NetworkGenStat</div><div>Single: ReceiveNoBuffer</div></div>
Usage example:	nCLI Get "ReceiveNoBuffer"
Access	Read
Data type	Number (64 bit)

Prelin

Direct Frames Received

Parameter	ReceiveFramesDirect
Description	The number of packets received without errors and addressed to the local Ethernet address.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_NetworkGenStat</div><div>Single: ReceiveFramesDirect</div></div>
Usage example:	nCLI Get "ReceiveFramesDirect"
Access	Read
Data type	Number (64 bit)

Prelimi

Multicast Frames Received

Parameter	ReceivedFramesMulticast
Description	Specifies the number of multicast frames received without errors.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_NetworkGenStat</div><div>Single: ReceiveFramesMulticast</div></div>
Usage example:	nCLI Get "ReceiveFramesMulticast"
Access	Read
Data type	Number (64 bit)

Preliminary

Broadcast Frames Received

Parameter	ReceiveFramesBroadcast
Description	Specifies the number of broadcast frames received without errors.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_EthStat</div><div>Group: NV_NetworkGenStat</div><div>Single: ReceiveFramesBroadcast</div></div>
Usage example:	nCLI Get "ReceiveFramesBroadcast"
Access	Read
Data type	Number (64 bit)

Prelimina

Group: Alert Standard Format

ASF Support

Parameter	ASFSupport
Description	Enables or disables the ASF (Alert Standard Format) feature. ASF is a industry specification that defines alerting capability in both operating system-present and operating system-absent environments.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_ASF </div> <div> Group: NV_ASF </div> <div> Single: ASFSupport </div> </div>
Usage example:	nCLI Set "ASFSupport" "Disable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

ASF Destination IP Address

Parameter	ASFDestIPAddr
Description	Specifies the IP address of the managing station computer that is receiving the ASF alert frames. For ASF to be functional, the destination IP address must be specified.
External Comment	Only the IPv4 (not IPv6) address is supported. Note: If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_ASF</div><div>Group: NV_ASF</div><div>Single: ASFDestIPAddr</div></div>
Usage example:	nCLI Set "ASFDestIPAddr" ""
Access	ReadWrite
Data type	String
Maximum length	15

ASF Send Count

Parameter	ASFSendCount
Description	Specifies the number of times an ASF alert will be sent out for a given event. If the value is more than one, the alert is sent at an interval of approximately 1 second. This is a global setting applied across all events.
External Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_ASF </div> <div> Group: NV_ASF </div> <div> Single: ASFSendCount </div> </div>
Usage example:	nCLI Set "ASFSendCount" "1"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • 0 • 1 • 2 • 3

Group: ASF Information

ASF Destination MAC Address

Parameter	ASFDestMACAddr
Description	Displays the MAC address of the managing station computer that is receiving the ASF alert frames.
Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_ASF</div><div>Group: NV_ASFInfo</div><div>Single: ASFDestMACAddr</div></div>
Usage example:	nCLI Get "ASFDestMACAddr"
Access	Read
Data type	MAC Address

Pre

Group: System Fails to Boot Alert

System Fails to Boot Alert

Parameter	ASFEventBootFailure
Description	This ASF alert is triggered when the operating system fails to start up.
External Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_ASF</div> <div> <div>Group: NV_ASFEventBootFailure</div> <div> <div>Single: ASFEventBootFailure</div> </div> </div> </div> </div>
Usage example:	nCLI Set "ASFEventBootFailure" "Disable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Group: Fan Problem Alert

Fan Problem Alert

Parameter	ASFEventFanProblem
Description	This alert is triggered if the CPU fan is running at a low speed or has stopped, which can cause the CPU or system temperature to increase.
Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_ASF </div> <div> Group: NV_ASFEventFanProblem </div> <div> Single: ASFEventFanProblem </div> </div>
Usage example:	nCLI Set "ASFEventFanProblem" "Disable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Group: ASF SMBus Error

ASF SMBus Error

Parameter	ASFEventSMBusError
Description	This alert packet is sent when there is a SMBus (System Management Bus) error. The SMBus is a two-wire interface through which the system can communicate with simple power-related chips.
Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_ASF </div> <div> Group: NV_ASFEventSMBusError </div> <div> Single: ASFEventSMBusError </div> </div>
Usage example:	nCLI Set "ASFEventSMBusError" "Disable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Group: ASF WOL Alert

ASF WOL (Wake On Lan) Aler

Parameter	ASFEventWOL
Description	This alert is triggered when the system is wakened through the wake on LAN feature.
Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> Namespace: NS_Eth </div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px; margin-left: 100px;"> Namespace: NS_ASF </div> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px; margin-left: 150px;"> Group: NV_ASFEventWOL </div> <div style="border: 1px solid black; padding: 5px; margin-left: 200px;"> Single: ASFEventWOL </div>
Usage example:	nCLI Set "ASFEventWOL" "Disable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Pro

Group: ASF Heartbeat Alert

ASF Heartbeat Alert Interval

Parameter	ASFHeartbeatInterval
Description	Set the interval (in seconds) between ASF heartbeat alerts.
Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_ASF</div> <div> <div>Group: NV_ASFEventHeartbeat</div> <div> <div>Single: ASFHeartbeatInterval</div> </div> </div> </div> </div>
Usage example:	nCLI Set "ASFHeartbeatInterval" "10"
Access	Read Write
Data type	Selection
User selection	<ul style="list-style-type: none"> • 10 seconds • 20 seconds • 30 seconds • 45 seconds • 1 minute • 2 minutes • 3 minutes • 5 minutes • 7.5 minutes • 10 minutes

Group: ASF Operating System Hung Alert

ASF Operating System Hung Alert

Parameter	ASFEventOSHung
Description	This alert is triggered when the operating system is hung and the driver software or the operating system is not servicing the interrupts generated by the network interfaces.
Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_ASF</div> <div> <div>Group: NV_ASFEventOSHung</div> <div> <div>Single: ASFEventOSHung</div> </div> </div> </div> </div>
Usage example:	nCLI Set "ASFEventOSHung" "Enable"
Access	ReadWrite
Data type	Selection
User Selection	<ul style="list-style-type: none"> • Disable • Enable

Group: ASF Power Button Alert

ASF Power Button Alert

Parameter	ASFEventPowerButton
Description	Enables or disables the power button alert. This alert is triggered each time the user presses the power button for shutting down or turning on the computer.
Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div> Namespace: NS_Eth </div> <div> Namespace: NS_ASF </div> <div> Group: NV_ASFEventPowerButton </div> <div> Single: ASFEventPowerButton </div>
Usage example:	nCLI Set "ASFEventPowerButton" "Enable"
Access	ReadWrite
Data type	Selection
User Selection	<ul style="list-style-type: none"> • Disable • Enable

Group: ASF System Hot Alert

ASF System Hot Alert

Parameter	ASFEventSystemHot
Description	This alert is triggered when the temperature in the computer has exceeded a threshold limit.
Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_ASF</div> <div> <div>Group: NV_ASFEventSystemHot</div> <div> <div>Single: ASFEventSystemHot</div> </div> </div> </div> </div>
Usage example:	nCLI Set "ASFEventSystemHot" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable



Group: ASF CPU Overheated Alert

ASF CPU Overheat Alert

Parameter	ASFEventCPUOverheated
Description	This alert is triggered when the temperature of the CPU exceeds a threshold.
Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div> Namespace: NS_Eth </div> <div> Namespace: NS_ASF </div> <div> Group: NV_ASFEventCPUOverheated </div> <div> Single: ASFEventCPUOverheated </div> </div>
Usage example:	nCLI Set "ASFEventCPUOverheated" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Group: ASF CPU Overheated Alert

ASF CPU Hot Alert

Parameter	ASFEventCPUHot
Description	This alert is triggered when the fan in the CPU is not functioning or the temperature is increasing.
Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div><div>Namespace: NS_Eth</div><div>Namespace: NS_ASF</div><div>Group: NV_ASFEventCPUHot</div><div>Single: ASFEventCPUHot</div></div>
Usage example:	nCLI Set "ASFEventCPUHot" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none">• Disable• Enable



Group: ASF Case Intrusion Alert

ASF Case Intrusion Alert

Parameter	ASFEventCaseIntrusion
Description	This alert is triggered when the computer's case is opened.
Comment	If ASFSupport is set to Disable, this parameter value is ignored.
Hierarchy	<div> <div>Namespace: NS_Eth</div> <div> <div>Namespace: NS_ASF</div> <div> <div>Group: NV_ASFEventCaseIntrusion</div> <div> <div>Single: ASFEventCaseIntrusion</div> </div> </div> </div> </div>
Usage example:	nCLI Set "ASFEventCaseIntrusion" "Disable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

B

FORCEWARE PERSONAL FIREWALL PARAMETERS: REFERENCE

Organization and Links

“Group: Configure Firewall Security Level” on page B-143

Single Parameter: “Configure Firewall Security Level” on page B-143

“Group: Configure Firewall Options” on page B-146

Single Parameter: “Disallow Promiscuous Mode” on page B-146

Single Parameter: “Disallow DHCP Server” on page B-147

Single Parameter: “Block Outbound Spoofed IP Packets” on page B-148

Single Parameter: “Block Spoofed ARP Packets” on page B-149

Single Parameter: “Block UDPv4 with No UDP Checksum” on page B-150

“Group: EtherType Default Rule” on page B-151

Single Parameter: “EtherType Default Rule” on page B-151

“Group: IP Address/Mask Default Rule” on page B-152

Single Parameter: “IP Address/Mask Default Action” on page B-152

“Group: Domain Name Default Rule” on page B-153

Single Parameter: “Domain Name Default Rule” on page B-153

“Group: IP Option Default Rule” on page B-154

Single Parameter: “Inbound IP Option Default Rule” on page B-154

Single Parameter: “Outbound IP Option Default Rule” on page B-155

“Group: IP Protocol Default Rule” on page B-156

Single Parameter: “IP Protocol Default Rule” on page B-156

“Group: Port Number Default Rule” on page B-157

Single Parameter: “Inbound Port Number Default Rule” on page B-157

Single Parameter: “Outbound Port Number Default Rule” on page B-158

“Group: TCP Options Default Rule” on page B-159

Single Parameter: “TCP Options Default Rule” on page B-159

“Group: ICMP Messages Default Rule” on page B-160

Single Parameter: “Inbound ICMP Default Rule” on page B-160

Single Parameter: “Outbound ICMP Default Rule” on page B-161

“Group: Clear Firewall Statistics” on page B-162

Single Parameter: “Clear Firewall Statistics” on page B-162

“Group: Firewall Statistics” on page B-163

Single Parameter: “Allowed Inbound UDP Datagrams” on page B-163

Single Parameter: “Denied Inbound UDP Datagrams I” on page B-164

Single Parameter: “Allowed Outbound UDP Datagrams” on page B-165

Single Parameter: “Denied Outbound UDP Datagrams” on page B-166

Single Parameter: “Denied Inbound UDP Connections” on page B-167

Single Parameter: “Denied Outbound UDP Connections” on page B-169

Single Parameter: “Allowed Inbound TCP Segments” on page B-170

Single Parameter: “Allowed Outbound TCP Connections” on page B-176

Single Parameter: “Denied Outbound TCP Connections” on page B-177

Single Parameter: “Allowed Inbound ICMP Packets” on page B-178

Single Parameter: “Denied Inbound ICMP Packets” on page B-179

Single Parameter: “Allowed Outbound ICMP Packets” on page B-180

- Single Parameter: “Denied Outbound ICMP Packets” on page B-181
- Single Parameter: “Other Allowed Inbound Packets” on page B-182
- Single Parameter: “Other Denied Inbound Packets” on page B-183
- Single Parameter: “Other Allowed Outbound Packets” on page B-184
- Single Parameter: “Other Denied Outbound Packets” on page B-185
- “Group: Factory Default” on page B-186
 - Single Parameter: “Factory Default” on page B-186
- “Group: Flush DNS Cache” on page B-187
 - Single Parameter: “Flush DNS Cache” on page B-187
- “Table: EtherType Rules” on page B-188
 - Single Parameter: “Ether Type” on page B-189
 - Single Parameter: “EtherType Name” on page B-190
 - Single Parameter: “EtherType Action” on page B-191
- “ITable: IP Address/Mask Rule” on page B-192
 - Single Parameter: “Remote IP Address” on page B-193
 - Single Parameter: “Remote IP Address Mask” on page B-194
- “Table: Domain Names Rule” on page B-196
 - Single Parameter: “Remote IP Address” on page B-193
 - Single Parameter: “Remote IP Address Mask” on page B-194
 - Single Parameter: “IP Action” on page B-195
- “Table: Domain Names Rule” on page B-196
 - Single Parameter: “Domain Name” on page B-197
 - Single Parameter: “Domain Action” on page B-198
- “Table: IP Option Rules” on page B-199
 - Single Parameter: “Domain Name” on page B-197
 - Single Parameter: “Domain Action” on page B-198
- “Table: IP Protocol Rule” on page B-205
 - Single Parameter: “Domain Name” on page B-197
 - Single Parameter: “Domain Action” on page B-198
- “Table: TCP/UDP Port Rule” on page B-209

Single Parameter: “Domain Name” on page B-197

Single Parameter: “Domain Action” on page B-198

“Table: TCP Options Rule” on page B-217

Single Parameter: “Domain Name” on page B-197

Single Parameter: “Domain Action” on page B-198

“Table: ICMP Rules” on page B-221

Single Parameter: “Domain Name” on page B-197

Single Parameter: “Domain Action” on page B-198

“Table: ICMP Rules” on page B-221

Single Parameter: “Domain Name” on page B-197

Single Parameter: “Domain Action” on page B-198

Group: Configure Firewall Security Level

Configure Firewall Security Level

Parameter	FwlProfiles
Description	Selects a default security level or configure a custom security level, which is a set of rules that determines the policy that the firewall follows.
Comment	This parameter is not supported through WMI script. For CLI user who wants to customize the firewall settings and not use a pre-defined profile, change the firewall security level to one of the custom levels. Note: For further details, see the next page.
Hierarchy	<div> <div>Namespace: NS_Firewall</div> <div> <div>Group: NV_FwlProfiles</div> <div> <div>Single: FwlProfiles</div> </div> </div> </div>
Usage example:	nCLI Set "FwlProfiles" "Medium"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Off • Low • Medium • High • Lockdown • Custom1 • Custom2 • Custom3

Continuation of Comments

This parameter is not supported through WMI script. For CLI user who wants to customize the firewall settings and not used a pre-defined profile, change the firewall security level to one of the custom levels described below. Lockdown blocks all traffic, both in and out.

- **High.** The High setting contains the following features and functionality:
 - Allows the least traffic through.
 - Only outbound connections may be established. Inbound connections are not allowed. Inbound traffic is allowed only if it is in response to an outbound packet that was seen previously on a valid connection.
 - Encompasses what was formerly known as “stealth mode” in which the station cannot be “pinged” and is not permitted to generate any ICMP error messages, except where necessary to permit normal operation.
 - Allows VPNs, including those based on IPsec (requiring AH, ESP, L2TP, IKE, i.e., UDP port 500), as well as those that rely on PPTP (which uses GRE).
 - Restricts traffic by prohibiting IP and/or TCP options that might be misused, as well as by preventing the spoofing of IP source addresses (for both IPv4 and IPv6).
- **Medium.** The Medium setting contains the following features and functionality:
 - Medium is expected to be the default setting when the firewall is enabled.
 - Does not have the “stealth” features associated with the High setting and therefore allows most (but not all) ICMP error messages to be sent and received.
 - Blocks most incoming connections with the default action being *Deny*. In order to allow file transfers via MSN Messenger and Yahoo! Messenger, incoming connections to port 80 must be allowed. Note that these applications will not work if the HIGH setting is chosen.
 - Allows dynamic ports to be opened up from the inside only. (Default in: *Deny*; Default out: *Allow*)
 - Supports outgoing NetMeeting calls.
 - As in the High setting, the Medium setting allows VPNs based on both IPsec and on PPTP.
 - Restricts traffic by prohibiting IP and/or TCP options that might be misused, as well as by preventing the spoofing of IP source addresses (for both IPv4 and IPv6).

LOW allows “safe” incoming connections, denying those that are known to be dangerous, defaulting to "allow" TCP or UDP connections for which a rule has not been specified.

- LOW allows pretty much all ICMP traffic, except for not sending router-oriented (e.g., router advertisement) or deprecated (e.g., source quench) type/code pairs.
- The LOW setting will allow bi-directional dynamic ports to be opened (*default in*: allow, *default out*: allow). Thus, LOW will support NetMeeting in either direction.
- As in the HIGH and MEDIUM settings, the LOW setting also allows VPNs, based on both IPsec and on PPTP.
- As in the HIGH and MEDIUM settings, the LOW setting also restricts traffic by prohibiting IP and/or TCP options that might be misused, as well as by preventing the spoofing of IP source addresses (for both IPv4 and IPv6). Off setting is the most permissive, in that it allows all traffic, both in and out.

Group: Configure Firewall Options

Disallow Promiscuous Mode

Parameter	FwlPromiscuous
Description	When this parameter is enabled, the firewall prevents applications from setting the NVIDIA network interface to promiscuous mode. Promiscuous mode is primarily used by packet sniffing software.
Hierarchy	<div> <div>Namespace: NS_Firewall</div> <div> <div>Group: NV_FwlOptions</div> <div>Single: FwlPromiscuous</div> </div> </div>
Usage example:	nCLI Set "FwlPromiscuous" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Enable • Disable

Pre

Disallow DHCP Server

Parameter	FwldHCPServer
Description	When this option is enabled, the firewall prevents a DHCP (Dynamic Host Configuration Protocol) server process in the computer from using the NVIDIA network interface to communicate using the DHCP protocol. The DHCP server is used to assign IP addresses to client computers.
Hierarchy	<div> <div>Namespace: NS_Firewall</div> <div> <div>Group: NV_FwlOptions</div> <div> <div>Single: FwldHCPServer</div> </div> </div> </div>
Usage example:	nCLI Set "FwldHCPServer" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Prelim

Block Outbound Spoofed IP Packets

Parameter	FwlAntiIPspoofing
Description	When this parameter is enabled, the firewall blocks any application on the NVIDIA network interface from sending network traffic using an IP address different than the one assigned to the interface. Such network packets are called spoofed IP packets, and this feature, also known as “anti-IP-spoofing,” is intended to prevent the NVIDIA network interface from participating in distributed denial of service attacks.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlOptions </div> <div> Single: FwlAntiIPspoofing </div>
Usage example:	nCLI Set "FwlAntiIPspoofing" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Pre

Block Spoofed ARP Packets

Parameter	FwlAntiARPSpoofing
Description	When this parameter is enabled, the firewall filters out any ARP packets sent by an offending computer (i.e, a computer that pretends to be another computer by altering the local ARP cache). Such network packets are called spoofed ARP packets and this feature is also known as “anti-ARP-spoofing”.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlOptions </div> <div> Single: FwlAntiARPSpoofing </div>
Usage example:	nCLI Set "FwlAntiARPSpoofing" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable

Pre

Block UDPv4 with No UDP Checksum

Parameter	FwlChecksumUDP
Description	When this parameter is enabled, the firewall drops any UDP datagram that has no UDP checksum if it is inside an IPv4 packet (UDP checksums are optional when used over IPv4, but are mandatory when used over IPv6).
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Group: NV_FwlOptions</div> <div>Single: FwlChecksumUDP</div>
Usage example:	nCLI Set "FwlChecksumUDP" "Enable"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Disable • Enable



Group: EtherType Default Rule

EtherType Default Rule

Parameter	FwLEtherTypeDefault
Description	This rule is applied when a packet contains an EtherType that does not match any rule in the EtherType rule table.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwLEtherTypeDefault </div> <div> Single: FwLEtherTypeDefault </div>
Usage example:	nCLI Set "FwLEtherTypeDefault" "Deny"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Preli

Group: IP Address/Mask Default Rule

IP Address/Mask Default Action

Parameter	FwlIPDefault
Description	This action is applied when a packet contains an IP address/mask that does not match any rule in the IP rule table.
Hierarchy	<div> <div>Namespace: NS_Firewall</div> <div> <div>Group: NV_FwlIPDefault</div> <div> <div>Single: FwlIPDefault</div> </div> </div> </div>
Usage example:	nCLI Set "FwlIPDefault" "Allow"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Group: Domain Name Default Rule

Domain Name Default Rule

Parameter	FwlDomainDefault
Description	This rule is applied when a DNS packet contains a domain name that does not match any rule in the domain name rule table.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Group: NV_FwlDomainDefault</div><div>Single: FwlDomainDefault</div></div>
Usage example:	nCLI Set "FwlDomainDefault" "Allow"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none">• Deny• Allow

Pre

Group: IP Option Default Rule

Inbound IP Option Default Rule

Parameter	FwlIPOptionDefaultIn
Description	This rule is applied when an inbound packet contains an IP option that does not match any rule in the IP option rule table.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlIPOptionDefault </div> <div> Single: FwlIPOptionDefaultIn </div>
Usage example:	nCLI Set "FwlIPOptionDefaultIn" "Deny"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Pr

Outbound IP Option Default Rule

Parameter	FwlIPOptionDefaultOut
Description	This rule is applied when an outbound packet contains an IP option that does not match any rule in the IP option rule table.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Group: NV_FwlIPOptionDefault</div> <div>Single: FwlIPOptionDefaultOut</div>
Usage example:	nCLI Set "FwlIPOptionDefaultOut" "Deny"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none">• Deny• Allow

Preliminary

Group: IP Protocol Default Rule

IP Protocol Default Rule

Parameter	FwlIPProtocolDefault
Description	This rule is applied when a packet contains an IP protocol that does not match any rule in the IP protocol rule table
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlIPProtocolDefault </div> <div> Single: FwlIPProtocolDefault </div>
Usage example:	nCLI Set "FwlIPProtocolDefault" "Deny"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Pre

Group: Port Number Default Rule

Inbound Port Number Default Rule

Parameter	FwlPortDefaultIn
Description	This rule is applied when an inbound packet contains a UDP or TCP port that does not match any rule in the Port rule table.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlPortDefault </div> <div> Single: FwlPortDefaultIn </div>
Usage example:	<code>nCLI Set "FwlPortDefaultIn" "Deny"</code>
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Prelim

Outbound Port Number Default Rule

Parameter	FwlPortDefaultOut
Description	This rule is applied when an outbound packet contains a UDP or TCP port that does not match any rule in the Port rule table.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlPortDefault </div> <div> Single: FwlPortDefaultOut </div>
Usage example:	nCLI Set "FwlPortDefaultOut" "Allow"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Prelim

Group: TCP Options Default Rule

TCP Options Default Rule

Parameter	FwlTCPOptionDefault
Description	This rule is applied when a packet contains a TCP option that does not match any rule in the TCP option rule table.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlTCPOptionDefault </div> <div> Single: FwlTCPOptionDefault </div>
Usage example:	
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Prelin

Group: ICMP Messages Default Rule

Inbound ICMP Default Rule

Parameter	FwIcmpDefaultIn
Description	This rule is applied when an inbound packet contains an ICMP type/code pair that does not match any rule in the ICMP rule table.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwIcmpDefault </div> <div> Single: FwIcmpDefaultIn </div>
Usage example:	nCLI Set "FwIcmpDefaultIn" "Deny"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Pr

Outbound ICMP Default Rule

Parameter	FwIICMPDefaultOut
Description	This rule is applied when an outbound packet contains an ICMP type/code pair that does not match any rule in the ICMP rule table.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwIICMPDefault </div> <div> Single: FwIICMPDefaultOut </div>
Usage example:	nCLI Set "FwIICMPDefaultOut" "Deny"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Prelin

Group: Clear Firewall Statistics

Clear Firewall Statistics

Parameter	FwlStatClearAll
Description	Clears all firewall statistics.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlStatClear </div> <div> Single: FwlStatClearAll </div>
Usage example:	
Access	ReadWrite
Data type	Selection
User selection	Clear

Pr

Group: Firewall Statistics

Allowed Inbound UDP Datagrams

Parameter	FwlStatUDPInPktsAllowed
Description	Specifies the number of inbound UDP datagrams allowed by the firewall.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Group: NV_FwlStat</div><div>Single: FwlStatUDPInPktsAllowed</div></div>
Usage example:	nCLI Get "FwlStatUDPInPktsAllowed"
Access	Read
Data type	Number (64 bit)

Prelimin

Denied Inbound UDP Datagrams I

Parameter	FwlStatUDPInPktsDenied
Description	Number of inbound UDP datagrams denied by the firewall.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Group: NV_FwlStat</div><div>Single: FwlStatUDPInPktsDenied</div></div>
Usage example:	nCLI Get "FwlStatUDPInPktsDenied"
Access	Read
Data type	Number (64 bit)

Preliminary

Allowed Outbound UDP Datagrams

Parameter	FwLStatUDPOutPktsAllowed
Description	Number of outbound UDP datagrams allowed by the firewall.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Group: NV_FwLStat</div><div>Single: FwLStatUDPOutPktsAllowed</div></div>
Usage example:	nCLI Get "FwLStatUDPOutPktsAllowed"
Access	Read
Data type	Number (64 bit)

Preliminary I

Denied Outbound UDP Datagrams

Parameter	FwlStatUDPOutPktsDenied
Description	Number of outbound UDP datagrams denied by the firewall.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlStat </div> <div> Single: FwlStatUDPOutPktsDenied </div>
Usage example:	nCLI Get "FwlStatUDPOutPktsDenied"
Access	Read
Data type	Number (64 bit)

Preliminar

Denied Inbound UDP Connections

Parameter	FwlStatUDPInConnectionsDenied
Description	Number of inbound UDP connections denied by the firewall.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Group: NV_FwlStat</div> <div>Single: FwlStatUDPInConnectionsDenied</div>
Usage example:	nCLI Get "FwlStatUDPInConnectionsDenied"
Access	Read
Data type	Number (64 bit)

Preliminary

Allowed Outbound UDP Connections

Parameter	FwlStatUDPOutConnectionsAllowed
Description	Number of outbound UDP connections allowed by the firewall.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlStat </div> <div> Single: FwlStatUDPOutConnectionsAllowed </div>
Usage example:	nCLI Get "FwlStatUDPOutConnectionsAllowed"
Access	Read
Data type	Number (64 bit)

Preliminary

Denied Outbound UDP Connections

Parameter	FwlStatUDPOutConnectionsDenied
Description	Number of outbound UDP connections denied by the firewall.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Group: NV_FwlStat</div> <div>Single: FwlStatUDPOutConnectionsDenied</div>
Usage example:	nCLI Get "FwlStatUDPOutConnectionsDenied"
Access	Read
Data type	Number (64 bit)

Preliminary

Allowed Inbound TCP Segments

Parameter	FwlStatTCPInPktsAllowed
Description	Number of inbound TCP segments allowed by the firewall.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Group: NV_FwlStat</div><div>Single: FwlStatTCPInPktsAllowed</div></div>
Usage example:	nCLI Get "FwlStatTCPInPktsAllowed"
Access	Read
Data type	Number (64 bit)

Preliminary

Denied Inbound TCP Segments

Parameter	FwlStatTCPInPktsDenied
Description	Number of inbound TCP segments denied by the firewall.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Group: NV_FwlStat</div> <div>Single: FwlStatTCPInPktsDenied</div>
Usage example:	nCLI Get "FwlStatTCPInPktsDenied"
Access	Read
Data type	Number (64 bit)

Prelim

Allowed Outbound TCP Segments

Parameter	FwlStatTCPOutPktsAllowed
Description	Number of outbound TCP segments allowed by the firewall.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlStat </div> <div> Single: FwlStatTCPOutPktsAllowed </div>
Usage example:	nCLI Get "FwlStatTCPOutPktsAllowed"
Access	Read
Data type	Number (64 bit)

Prelimi

Denied Outbound TCP Segments

Parameter	FwlStatTCPOutPktsDenied
Description	Number of outbound TCP segments denied by the firewall.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Group: NV_FwlStat</div> <div>Single: FwlStatTCPOutPktsDenied</div>
Usage example:	nCLI Get "FwlStatTCPOutPktsDenied"
Access	Read
Data type	Number (64 bit)

Preliminary

Allowed Inbound TCP Connections

Parameter	FwlStatTCPInConnectionsAllowed
Description	Number of inbound TCP connections allowed by the firewall.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlStat </div> <div> Single: FwlStatTCPInConnectionsAllowed </div>
Usage example:	nCLI Get "FwlStatTCPInConnectionsAllowed"
Access	Read
Data type	Number (64 bit)

Preliminary

Denied Inbound TCP Connections

Parameter	FwlStatTCPInConnectionsDenied
Description	Number of inbound TCP connections denied by the firewall.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Group: NV_FwlStat</div> <div>Single: FwlStatTCPInConnectionsDenied</div>
Usage example:	nCLI Get "FwlStatTCPInConnectionsDenied"
Access	Read
Data type	Number (64 bit)

Preliminary

Allowed Outbound TCP Connections

Parameter	FwlStatTCPOutConnectionsAllowed
Description	Number of outbound TCP connections allowed by the firewall.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlStat </div> <div> Single: FwlStatTCPOutConnectionsAllowed </div>
Usage example:	nCLI Get "FwlStatTCPOutConnectionsAllowed"
Access	Read
Data type	Number (64 bit)

Prelimina

Denied Outbound TCP Connections

Parameter	FwlStatTCPOutConnectionsDenied
Description	Number of outbound TCP connections denied by the firewall.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Group: NV_FwlStat</div> <div>Single: FwlStatTCPOutConnectionsDenied</div>
Usage example:	nCLI Get "FwlStatTCPOutConnectionsDenied"
Access	Read
Data type	Number (64 bit)

Preliminary E

Allowed Inbound ICMP Packets

Parameter	FwlStatICMPInPktsAllowed
Description	Number of inbound ICMP packets allowed by the firewall.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Group: NV_FwlStat</div> <div>Single: FwlStatICMPInPktsAllowed</div>
Usage example:	nCLI Get "FwlStatICMPInPktsAllowed"
Access	Read
Data type	Number (64 bit)

Preliminary

Denied Inbound ICMP Packets

Parameter	FwIStatICMPInPktsDenied
Description	Number of inbound ICMP packets denied by the firewall.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Group: NV_FwIStat</div> <div>Single: FwIStatICMPInPktsDenied</div>
Usage example:	nCLI Get "FwIStatICMPInPktsDenied"
Access	Read
Data type	Number (64 bit)

Preliminary E

Allowed Outbound ICMP Packets

Parameter	FwlStatICMPOutPktsAllowed
Description	Number of outbound ICMP packets allowed by the firewall.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlStat </div> <div> Single: FwlStatICMPOutPktsAllowed </div>
Usage example:	nCLI Get "FwlStatICMPOutPktsAllowed"
Access	Read
Data type	Number (64 bit)

Preliminar

Denied Outbound ICMP Packets

Parameter	FwlStatICMPOutPktsDenied
Description	Specifies the number of outbound ICMP packets denied by the firewall.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlStat </div> <div> Single: FwlStatICMPOutPktsDenied </div>
Usage example:	nCLI Get "FwlStatICMPOutPktsDenied"
Access	Read
Data type	Number (64 bit)

Preliminary

Other Allowed Inbound Packets

Parameter	FwlStatOtherInPktsAllowed
Description	Specifies the number of inbound packets allowed by the firewall that are not UDP, TCP, or ICMP.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlStat </div> <div> Single: FwlStatOtherInPktsAllowed </div>
Usage example:	nCLI Get "FwlStatOtherInPktsAllowed"
Access	Read
Data type	Number (64 bit)

Prelimina

Other Denied Inbound Packets

Parameter	FwlStatOtherInPktsDenied
Description	Number of inbound packets denied by the firewall that are not UDP, TCP, or ICMP.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Group: NV_FwlStat</div> <div>Single: FwlStatOtherInPktsDenied</div>
Usage example:	nCLI Get "FwlStatOtherInPktsDenied"
Access	Read
Data type	Number (64 bit)

Preliminary

Other Allowed Outbound Packets

Parameter	FwlStatOtherOutPktsAllowed
Description	Number of outbound packets allowed by the firewall that are not UDP, TCP, or ICMP.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_FwlStat </div> <div> Single: FwlStatOtherOutPktsAllowed </div>
Usage example:	nCLI Get "FwlStatOtherOutPktsAllowed"
Access	Read
Data type	Number (64 bit)

Preliminary

Other Denied Outbound Packets

Parameter	FwlStatOtherOutPktsDenied
Description	Specifies the number of outbound packets denied by the firewall that are not UDP, TCP, or ICMP.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Group: NV_FwlStat</div> <div>Single: FwlStatOtherOutPktsDenied</div>
Usage example:	nCLI Get "FwlStatOtherOutPktsDenied"
Access	Read
Data type	Number (64 bit)

Preliminary

Group: Factory Default

Factory Default

Parameter	FwlDefault
Description	Specifies to restore all firewall settings to the factory default.
Comment	This parameter is not supported through WMI scripting.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Group: NV_Fwl_Default </div> <div> Single: FwlDefault </div>
Usage example:	nCLI Set "FwlDefault" "NoRestore"
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • NoRestore • Restore

Pre

Group: Flush DNS Cache

Flush DNS Cache

Parameter	FwIFlushDNS
Description	Specifies to flush the operating system DNS cache.
Comment	DNS cache needs to be flushed when Firewall Domain Name configuration is changed.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Group: NV_FwIFlushDNS</div><div>Single: FwIFlushDNS</div></div>
Usage example:	nCLI Set "FwIFlushDNS" "Clear"
Access	ReadWrite
Data type	Selection
User selection	Clear

Prelir

Table: EtherType Rules

Table	EtherType Rules Table
Name	NV_FwlEtherType
Description	Specifies table to configure EtherType firewall rules. As part of the Ethernet header, the EtherType is used to identify the type of Ethernet payload. Example payloads include IPv4, AppleTalk, IPX, and NetBEUI.
Comment	For EtherType that does not match any rule in the table, default setting in FwlEtherTypeDefault will be used.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Table: NV_FwlEtherType</div>
Usage example:	<ul style="list-style-type: none"> • <code>nCLI AddRow "NV_FwlEtherType" "EtherType=2048,EtherTypeName=Internet Protocol version 4 (IPv4) (RFC 791),EtherTypeAction=Allow"</code> • <code>nCLI EditRow "NV_FwlEtherType.EtherType=2048" "EtherTypeName=Address Resolution Protocol (ARP) (RFC 826),EtherTypeAction=Allow"</code> • <code>nCLI DelRow "NV_FwlEtherType.EtherType=2048"</code>
Access	ReadWrite
Single Parameter	<ul style="list-style-type: none"> • EtherType • EtherTypeName • EtherTypeAction

Ether Type

Parameter	EtherType
Description	The EtherType identifies the type of Ethernet payload. Some examples and their hexadecimal values include IPv4 (0x0800), AppleTalk (0x809B), IPX (0x8137) and NetBEUI (0x8191).
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Table: NV_FwlEtherType </div> <div> Row:: </div> <div> Single: EtherType </div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	Number (32 bit)
Maximum Value	65535
Minimum Value	1501

Pre

EtherType Name

Parameter	EtherTypeName
Description	Name associated with the EtherType.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlEtherType</div><div>Row::</div><div>Single: EtherTypeName</div></div>
Access	ReadWrite
Data type	String
Maximum Length	60

Prelimi

EtherType Action

Parameter	EtherTypeAction
Description	Specifies action for the EtherType.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlEtherType</div><div>Row::</div><div>Single: EtherTypeAction</div></div>
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none">• Deny• Allow

Preliminary

Table: IP Address/Mask Rule

Table parameter	NV_FwlIP
Description	Specifies table to configure firewall rules based on IP addresses/masks.
Comment	For IP address/mask pair that does not match any rule in the table, default setting in FwlIPDefault will be used.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Table: NV_FwlIP</div>
Usage example:	<ul style="list-style-type: none"> nCLI AddRow "NV_FwlIP" "IPRemoteIP=0000:0000:0000:0000:0000:FFFF:000:0000,IPRemoteIPMask=32,IPAction=Allow" nCLI DelRow "NV_FwlIP.IPRemoteIP='0000:0000:0000:0000:000:FFFF:0000:0000',IPRemoteIPMask='32'"
Access	ReadWrite
Single Parameter	<ul style="list-style-type: none"> IPRemoteIP IPRemoteIPMask IPLocalIP IPLocalIPMask IPAction

Pi

Remote IP Address

Parameter	IPRemoteIP
Description	IP address of the remote machine or subnet.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlIP</div><div>Row:.</div><div>Single: IPRemoteIP</div></div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	IP Address

Preliminary

Remote IP Address Mask

Parameter	IPRemoteIPMask
Description	IP address mask of the remote machine or subnet.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlIP</div><div>Row::</div><div>Single: IPRemoteIPMask</div></div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	IP Mask Length

Prelim

IP Action

Parameter	IPAction
Description	Specifies the action for network traffic.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Table: NV_FwlIP </div> <div> Row:: </div> <div> Single: IPAction </div>
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Prelim

Table: Domain Names Rule

Table parameter:	NV_FwlDomain
Description	Specifies the table to configure domain name rules. Domain name is a user-friendly name used to identify a Web site; for example, www.nvidia.com . The firewall blocks DNS lookups of domain names. You can bypass this filter by directly entering an IP address (if the IP address is known) instead of a domain name to access a Web site.
Comment	CLI users need to flush DNS cache for domain name rules to take effect. To flush DNS cache, set FwFlushDNS. For a given domain name that does not match any rule in the table, the default setting in FwDomainDefault will be used.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Table: NV_FwlDomain</div>
Usage example:	<ul style="list-style-type: none"> nCLI AddRow "NV_FwlDomain" "DomainName=www.dummy.com,DomainAction=Deny" nCLI EditRow "NV_FwlDomain.DomainName='www.dummy.com' " "DomainAction=Deny" nCLI DelRow "NV_FwlDomain.DomainName='www.dummy.com' "
Access	ReadWrite
Single Parameter	<ul style="list-style-type: none"> DomainName DomainAction DomainLocalIP DomainLocalIPMask

Domain Name

Parameter	DomainName
Description	Domain name of the computer or Web site
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_Fwldomain</div><div>Row::</div><div>Single: DomainName</div></div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	String
Maximum Length	127

Prelimin

Domain Action

Parameter	DomainAction
Description	Specifies action for network traffic.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlDomain</div><div>Row::</div><div>Single: DomainAction</div></div>
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none">• Deny• Allow

Preli

Table: IP Option Rules

Table parameter	NV_FwIPOption
Description	Specifies the table to configure IP option rules. IPv4 options are added to the basic IPv4 header to provide additional features beyond those that are supported by the standard IPv4 packet's header. The standard 20-byte IPv4 header can be expanded to have up to 40 bytes of options. IPv6 options have no fixed size, are otherwise similar to IPv4 options and provide for many of the same features.
Comment	For an IP option that does not match any rule in the table, the default setting FwIPOptionDefault will be used.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Table: NV_FwIPOption </div>
Usage example:	<ul style="list-style-type: none"> nCLI AddRow "NV_FwIPOption" "IPOptionNumber=0,IPOptionName=End of Option List,IPOptionVersion=IPv4,IPOptionActionIn=Allow,IPOptionActionOut=Allow" nCLI EditRow "NV_FwIPOption.IPOptionNumber=0,IPOptionVersion=4" "IPOptionName=Pad-1 (i.e., one octet of padding),IPOptionActionIn=Allow,IPOptionActionOut=Allow" nCLI DelRow "NV_FwIPOption.IPOptionNumber=0,IPOptionVersion=4"
Access	ReadWrite
Single Parameter	<ul style="list-style-type: none"> IPOptionNumber IPOptionName IPOptionVersion IPOptionActionIn IPOptionActionOut

IP Option Number

Parameter	IPOptionNumber
Description	IP option number. IPv4 options are added to the basic IPv4 header to provide additional features beyond those that are supported by the standard IPv4 packet's header. The standard 20-byte IPv4 header can be expanded to have up to 40 bytes of options. IPv6 options have no fixed size, but are otherwise similar to IPv4 options and provide for many of the same features.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Table: NV_FwlIPOption </div> <div> Row:: </div> <div> Single: IPOptionNumber </div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	Number (32 bit)
Maximum Value	255
Minimum Value	0

IP Option Name

Parameter	IPOptionName
Description	Specifies name associated with the IP option number.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlIPOption</div><div>Row::</div><div>Single: IPOptionName</div></div>
Access	ReadWrite
Data type	String
Maximum Length	60

Prelimina

IP Version

Parameter	IPOptionVersion
Description	Specifies whether rule is for IPv4 or IPv6.
Hierarchy	<div> <div>Namespace: NS_Firewall</div> <div> <div>Table: NV_FwlIPOption</div> <div> <div>Row:</div> <div> Single: IPOptionVersion </div> </div> </div> </div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	Selection
User selection	<ul style="list-style-type: none"> • IPv4 • IPv6

Pi

Inbound Action

Parameter	IPOptionActionIn
Description	Specifies action for inbound network traffic.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlIPOption</div><div>Row::</div><div>Single: IPOptionAction In</div></div>
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none">• Allow• Deny

Preliminary

Outbound Action

Parameter	IPOptionActionOut
Description	Specifies action for outbound network traffic.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlIPOption</div><div>Row::</div><div>Single: IPOptionActionOut</div></div>
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none">• Allow• Deny

Prelimi

Table: IP Protocol Rule

Table parameter	NV_FwlIPProtocol
Description	Specifies table to configure IP protocol rules. IP protocol identifies the type of IP payload. ICMP, TCP and UDP are examples of common IP payloads.
Comment	For an IP protocol that does not match any rule in the table, the default setting in FwlIPProtocolDefault will be used.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Table: NV_FwlIPProtocol </div>
Usage example:	<ul style="list-style-type: none"> nCLI AddRow "NV_FwlIPProtocol" "IPProtocol=1,IPProtocolName=Internet Control Message Protocol for IPv4 (ICMP),IPProtocolAction=Allow" nCLI EditRow "NV_FwlIPProtocol.IPProtocol=1" "IPProtocolName=Internet Group Management Protocol for IPv4 (IGMP),IPProtocolAction=Allow" nCLI DelRow "NV_FwlIPProtocol.IPProtocol=1"
Access	ReadWrite
Single Parameters	<ul style="list-style-type: none"> IPProtocol IPProtocolName IPProtocolAction

IP Protocol

Parameter	IPProtocol
Description	Specifies the IP protocol number. IP protocol identifies the type of IP payload. Common protocols and their decimal values include ICMP (1), TCP (6), and UDP (17).
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Table: NV_FwlIPProtocol </div> <div> Row:: </div> <div> Single: IPProtocol </div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	Number (32 bit)
Maximum Value	255
Minimum Value	0

Pi

IP Protocol Name

Parameter	IPProtocolName
Description	Specifies a name for an IP protocol.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlIPProtocol</div><div>Row::</div><div>Single: IPProtocolName</div></div>
Access	ReadWrite
Data type	String
Maximum Length	60

Preliminary

IP Protocol Action

Parameter	IPProtocolAction
Description	Specifies the action for network traffic.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Table: NV_FwlIPProtocol </div> <div> Row:: </div> <div> Single: IPProtocolAction </div>
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Prelimi

Table: TCP/UDP Port Rule

Parameter name	NV_FwlPort
Description	Specifies the table to configure TCP or UDP port rules. Port numbers are used by TCP or UDP to identify sending and receiving applications. Some common ports include HTTP (80), TELNET (23) and SMTP (25).
Comment	For a TCP/UDP port that does not match any rule in the table, the default setting in FwlPortDefault will be used.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Table: NV_FwlPort</div>
Usage examples:	<ul style="list-style-type: none"> nCLI AddRow "NV_FwlPort" "PortActionIn=Deny,PortActionOut=Deny,PortRemoteIP=0000:0000:0000:0000:0000:FFFF:0000:0000,PortRemoteIPMask=32,PortName=Reserved,PortRangeBegin=0,PortRangeEnd=0,PortProtocol=Both" nCLI EditRow "NV_FwlPort.PortRemoteIP='0000:0000:0000:0000:0000:FFFF:0000:0000',PortRemoteIPMask='32',PortRangeBegin=0,PortRangeEnd=0,PortProtocol=0" "PortActionIn=Deny,PortActionOut=Allow,PortName=Time (RFC 868)" nCLI DelRow "NV_FwlPort.PortRemoteIP='0000:0000:0000:0000:0000:FFFF:0000:0000',PortRemoteIPMask='32',PortRangeBegin=0,PortRangeEnd=0,PortProtocol=0"
Access	ReadWrite
Single Parameter	<ul style="list-style-type: none"> PortActionIn PortActionOut PortRemoteIP PortRemoteIPMask PortLocalIP PortRangeBegin PortRangeEnd PortLocalIPMask PortName PortProtocol

TCP/UDP Port Outbound Action

Parameter	PortActionOut
Description	Specifies outbound action for the network connection.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlPort</div><div>Row::</div><div>Single: PortActionOut</div></div>
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none">• Deny• Allow

Prelin

Remote IP Address

Parameter	PortRemoteIP
Description	IP address of the remote machine or subnet.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlPort</div><div>Row::</div><div>Single: PortRemoteIP</div></div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	IP Address

Preliminary

Remote IP Subnet Mask

Parameter	PortRemoteIPMask
Description	Specifies the IP address mask of the remote machine or subnet.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Table: NV_FwlPort </div> <div> Row:: </div> <div> Single: PortRemoteIPMask </div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	IP Mask Length

Prelimin

Port Name

Parameter	PortName
Description	Specifies the name associated with the TCP or UDP port range.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Table: NV_FwlPort</div> <div>Row::</div> <div>Single: PortName</div>
Access	ReadWrite
Data type	String
Maximum Length	100

Prelim

Beginning Port Number

Parameter	PortRangeBegin
Description	Specifies the first UDP or TCP port in the range.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Table: NV_FwlPort </div> <div> Row:: </div> <div> Single: PortRangeBegin </div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	Number (32 bit)
Maximum Value	65535

Prelim

Ending Port Number

Parameter	PortRangeEnd
Description	Specifies the last UDP or TCP port in the range.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlPort</div><div>Row::</div><div>Single: PortRangeEnd</div></div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	Number (32 bit)
Maximum Value	65535

Prelimi

Port Protocol

Parameter	PortProtocol
Description	Specifies whether the port protocol is UDP, TCP, or both.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Table: NV_FwlPort</div> <div>Row::</div> <div>Single: PortProtocol</div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	Selection
User selection	<ul style="list-style-type: none"> • UDP • TCP

Pi

Table: TCP Options Rule

Table parameter	NV_FwlTCPOption
Description	Specifies the table to configure the TCP options rule. TCP options are added to the standard 20-byte TCP header to provide additional features that typically can only be used if they are negotiated at the beginning of a TCP connection.
Comment	For a given TCP option that does not match any rule in the table, the default setting in FwlTCPOptionDefault will be used.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Table: NV_FwlTCPOption</div>
Usage examples:	<ul style="list-style-type: none"> nCLI AddRow "NV_FwlTCPOption" "TCPOptionNumber=0,TCPOptionName=End of Option List (RFC 793),TCPOptionAction=Allow" nCLI EditRow "NV_FwlTCPOption.TCPOptionNumber=0 " "TCPOptionName=No Operation (RFC 793),TCPOptionAction=Allow" nCLI DelRow "NV_FwlTCPOption.TCPOptionNumber=0 "
Access	ReadWrite
Single Parameters	<ul style="list-style-type: none"> TCPOptionNumber TCPOptionName TCPOptionAction

TCP Option Number

Parameter	TCPOptionNumber
Description	Represents the TCP option number. TCP options are added to the standard 20-byte TCP header to provide additional features that typically can only be used if they are negotiated at the beginning of a TCP connection.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Table: NV_FwTCPOption </div> <div> Row:: </div> <div> Single: TCPOptionNumber </div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	Number (32 bit)
Maximum Value	255
Minimum Value	0

TCP Option Name I

Parameter	TCPOptionName
Description	Specifies a name associated with a TCP option number.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlTCPOption</div><div>Row::</div><div>Single: TCPOptionName</div></div>
Access	ReadWrite
Data type	String
Maximum Length	60

Preliminar

TCP Option Action

Parameter	TCPOptionAction
Description	Specifies the action for network traffic containing a given TCP option number.
Hierarchy	<div> <div>Namespace: NS_Firewall</div> <div> <div>Table: NV_FwTCPOption</div> <div> <div>Row::</div> <div> <div>Single: TCPOptionAction</div> </div> </div> </div> </div>
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Prel

Table: ICMP Rules

Table parameter	NV_FwICMP
Description	Specifies the table to configure ICMP message rules. ICMP communicates error, diagnostic and control messages. Examples of ICMP messages include echo (i.e., ping) and 'destination unreachable'.
Comment	For an ICMP message that does not match any rule in the table, the default setting in FwICMPDefault will be used.
Hierarchy	<div>Namespace: NS_Firewall</div> <div>Table: NV_FwICMP</div>
Usage examples:	<ul style="list-style-type: none"> nCLI AddRow "NV_FwICMP" "ICMPRemoteIP=0000:0000:0000:0000:0000:FFFF:0000:0000,ICMPRemoteIPMask=32,ICMPType=0,ICMPCode=0,ICMPName=Echo_reply(RFC792),ICMPVersion=ICMPv4,ICMPActionIn=Allow,ICMPActionOut=Allow" nCLI EditRow "NV_FwICMP.ICMPRemoteIP='0000:0000:0000:0000:0000:FFFF:0000:0000',ICMPRemoteIPMask='32',ICMPType=0,ICMPCode=0,ICMPVersion=4" "ICMPName=Not assigned,ICMPActionIn=Deny,ICMPActionOut=Deny" nCLI DelRow "NV_FwICMP.ICMPRemoteIP='0000:0000:0000:0000:0000:FFFF:0000:0000',ICMPRemoteIPMask='32',ICMPType=0,ICMPCode=0,ICMPVersion=4"
Access	ReadWrite
Single Parameters	<ul style="list-style-type: none"> ICMPRemoteIP ICMPRemoteIPMask ICMPLocalIP ICMPLocalIPMask ICMPType ICMPCode ICMPName ICMPVersion ICMPActionIn ICMPActionOut

Remote IP Address

Parameter	ICMPRemoteIP
Description	Specifies the IP address of the remote machine or subnet.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwICMP</div><div>Row::</div><div>Single: ICMPRemoteIP</div></div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	IP Address

Prelim

Remote IP Subnet Mask

Parameter	ICMPRemoteIPMask
Description	Specifies the IP address mask of the remote machine or subnet.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwICMP</div><div>Row::</div><div>Single: ICMPRemoteIPMask</div></div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	IP Mask Length

Preliminar

ICMP Type

Parameter	ICMPType
Description	Specifies the ICMP type
Hierarchy	<div> <div>Namespace: NS_Firewall</div> <div> <div>Table: NV_FwICMP</div> <div> <div>Row::</div> <div> <div>Single: ICMPType</div> </div> </div> </div> </div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	Number (32 bit)
Maximum Value	255
Minimum Value	0

—

ICMP Code

Parameter	ICMPCode
Description	Specifies the ICMP code.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Table: NV_FwICMP </div> <div> Row:: </div> <div> Single: ICMPCode </div>
Access	ReadWrite
Table key	This parameter is a key to the table
Data type	Number (32 bit)
Maximum Value	255
Minimum Value	0

Prelim

ICMP Name

Parameter	ICMPName
Description	Specifies a name for the ICMP type/code pair.
Hierarchy	<div> <div>Namespace: NS_Firewall</div> <div> <div>Table: NV_FwlICMP</div> <div> <div>Row::</div> <div> <div>Single: ICMPName</div> </div> </div> </div> </div>
Access	ReadWrite
Data type	String
Maximum Length	120

Prelim

ICMP Version

Parameter	ICMPVersion
Description	Specifies whether the rule is for ICMPv4 or ICMPv6.
Hierarchy	<div> <div>Namespace: NS_Firewall</div> <div> <div>Table: NV_FwICMP</div> <div> <div>Row:: </div> <div> <div>Single: ICMPVersion</div> </div> </div> </div> </div>
Access	ReadWrite
Factory default value	<ul style="list-style-type: none"> • ICMPv4 • ICMPv6
Table key	This parameter is a key to the table
Data type	Selection
User selection	<ul style="list-style-type: none"> • ICMPv4 • ICMPv6

Preliminary

Inbound Action

Parameter	ICMPActionIn
Description	Specifies the action for inbound network traffic.
Hierarchy	<div> Namespace: NS_Firewall </div> <div> Table: NV_FwlICMP </div> <div> Row:: </div> <div> Single: ICMPActionIn </div>
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none"> • Deny • Allow

Prelim

Outbound Action

Parameter	ICMPActionOut
Description	Specifies the action for outbound network traffic.
Hierarchy	<div><div>Namespace: NS_Firewall</div><div>Table: NV_FwlICMP</div><div>Row::</div><div>Single: ICMPActionOut</div></div>
Access	ReadWrite
Data type	Selection
User selection	<ul style="list-style-type: none">• Deny• Allow

Prelimin

Preliminary Edition

APPENDIX



GLOSSARY

- **distinguished name.** In reference to the ForceWare Network Access Manager application, a distinguished name is the name that uniquely identifies a parameter. Each parameter has a distinguished name.
- **group parameter.** In reference to the ForceWare Network Access Manager application, a group parameter is a collection of single parameters that belong to a functionality set.
- **ICMP (Internet Control Message Protocol)** is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.
- **IP (Internet Protocol).** The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive

in a different order than the order they were sent in. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order.

IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

The most widely used version of IP today is **Internet Protocol Version 4 (IPv4)**. However, IP Version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

- **namespace parameter.** In reference to the ForceWare Network Access Manager application, a namespace parameter is the largest container of parameters. A namespace parameter contains multiple group parameters and/or table parameters.
- **nCLI (NVIDIA command line interface).** In reference to the ForceWare Network Access Manager application, nCLI is a command line interface that can be used to configure and monitor NVIDIA networking components. nCLI can run in either export or interactive mode.
- **single parameter.** In reference to the ForceWare Network Access Manager application, a single parameter is the smallest parameter unit. It contains a name and value pair.
- **table parameter.** In reference to the ForceWare Network Access Manager application, a table parameter is a collection of group parameters (rows) that share the same fields (columns). Table parameters are frequently used as place holders for firewall rules, filters, and statistics. Each row inside the table is uniquely identified by a key. A key is composed of one or more of fields of a row.
- **TCP (Transmission Control Protocol)** is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

TCP is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or

messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

- **UDP (User Datagram Protocol)** is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

In the Open Systems Interconnection (OSI) communication model, UDP, like TCP, is in layer 4, the Transport Layer.