neoworx™

Information in this document is subject to change without notice.

NeoTrace is not public domain software, nor is it free software.

Thanks to Rick Grunwald for his contributions to the *Hunting Spammers* section.

License Agreement

Shareware License
FOR DISTRIBUTION OF SHAREWARE FILES, USER GROUPS, BBS's, ONLINE SERVICES, SHAREWARE VENDORS, and OTHERS

A limited license is granted to copy and distribute our shareware software only for the trial use of others, subject to the following limitations:

1) The software must be copied in unmodified form, complete with the file containing this license information.

2) The full machine-readable documentation must be included with each copy.

3) Our software may not be distributed in conjunction with any other product without a specific license to do so from NeoWorx inc.

4) Vending of our software products in retail stores (by "shareware rack vendors") is specifically prohibited without prior written authorization.

5) No fee, charge, or other compensation may be requested or accepted, except for a nominal disk duplication fee not to exceed two dollars.

License Agreement
NeoWorx inc. warrants that it is sole owner of the software and has full power and authority to grant this license herein without consent of any other party.

This software is licensed, not sold. The fee you pay entitles you to use the software, not to own it.

The software contained in this package (hereafter referred to as "the Software") is copyrighted material owned by NeoWorx inc. Payment of the single copy license fee authorizes one named person to use the Software on one computer provided this copyright is not violated and provided the rules outlined herein are observed.

One person may use the Software on any single computer. This license can not be transferred. You must pay for additional copies of the Software if more than one person uses it at one time, or if the Software is used on two or more computers. Neither concurrent use on two or more computers, nor use by more than a single individual on a network is permitted without authorization and payment of other license fees.

You may make copies of the software for backup purposes, as long as all such copies, along with the original, are kept in your possession or control.

You may not make any changes or modifications to the Software, including, but not limited to, de-compiling, disassembling, or otherwise reverse engineering it. You may not rent or lease it to others. You may not use it on a computer network if more than one user can use it on more than one computer during any one twenty-four hour span of time.

NeoWorx hereby disclaims all warranties relating to this software, whether express or implied, including without limitation any implied warranties of merchantability or fitness for a particular purpose. NeoWorx will not be liable for any special, incidental, consequential, indirect or similar damages due to loss of data or any other reason, even if NeoWorx or an agent of NeoWorx has been advised of the possibility of such damages. In no event shall NeoWorx's liability for any damages ever exceed the price paid for the license to use the software, regardless of the form of the claim. The person using the software bears all risk as to the quality and performance of the software.

U.S. GOVERNMENT RESTRICTED RIGHTS
Use, duplication, or disclosure by the Government is subject to standard shrink-wrapped software restrictions.

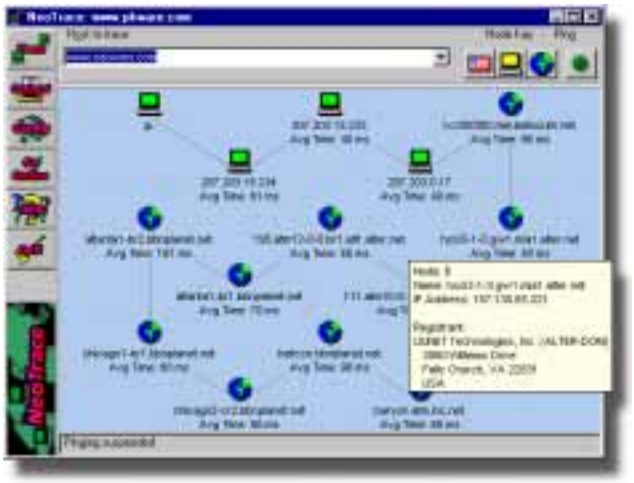
Disclaimer of Warranty
THIS SOFTWARE AND THE ACCOMPANYING FILES ARE SOLD "AS IS" AND WITHOUT WARRANTIES AS TO PERFORMANCE OR MERCHANTABILITY OR ANY OTHER WARRANTIES WHETHER EXPRESSED OR IMPLIED. NO WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE IS OFFERED.

Contents

Introduction

NeoTrace can help you:

- Discover why you can't reach a site due to a failure at your ISP or further into the internet.
- Determine the point of a network failure that is preventing you from reaching a web site.
- Track down the origin of unwanted email ('spam').
- Monitor performance.
- Uncover the owners of a site.
- Determine the type and quality of connection a site has to the net.
- Get detailed contact information on sites all over the world (when available).



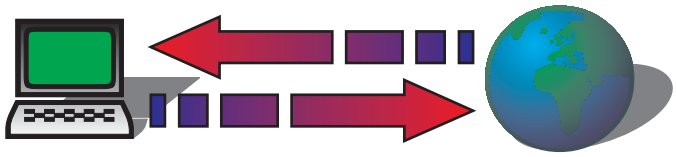
What is NeoTrace?

NeoTrace is an Internet utility used to trace the connections between computers on the Internet. At its heart is a super fast multi-threaded version of Traceroute. NeoTrace allows you to trace the connection from your computer to other sites on the Internet, and analyze this information.

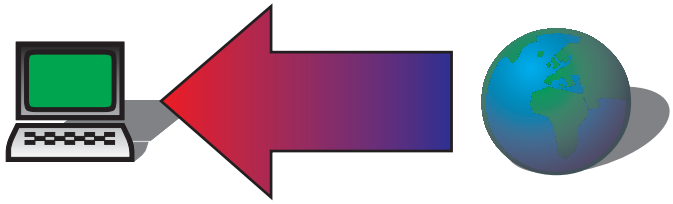
All traffic on the Internet is made up of packets of data that travel between multiple computers or *nodes* from their destination to their source. The path that these packets traverse is called the *route*.

The structure of the Internet has a long history and many aspects of it are a result of the evolution it has made from the original network into the global data infrastructure it is used as today. One of these aspects is that there is no single route between any two distantly spaced nodes. Another aspect is that you are at the mercy of the intervening route for the performance of your traffic.

Regardless of how fast your connection to 'the Internet' is, the slowest point in the route limits your overall connection to another site. The chain is only as strong as its weakest link.



Latency **is the time it takes for data to travel the route.**

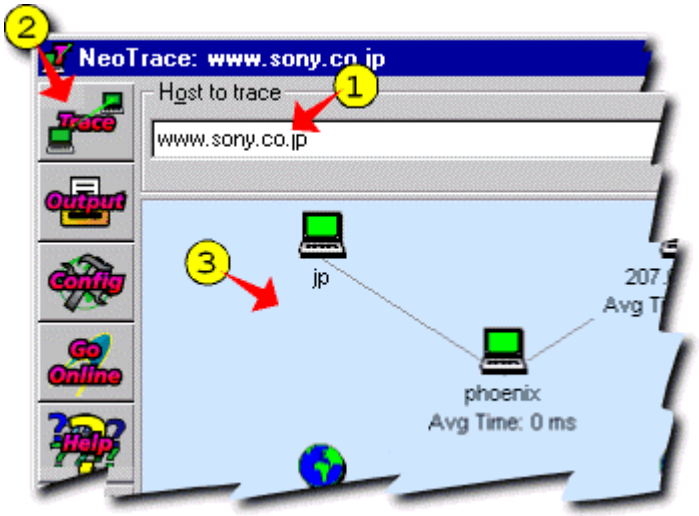


Bandwidth **is the amount of data that can travel through the connection in a given period of time.**

Getting Started

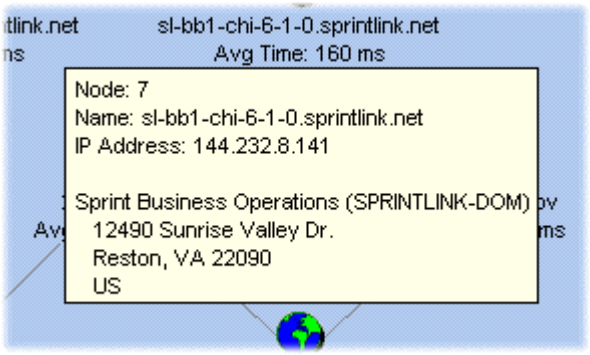
Basic Use

1. Enter the name or IP number you would like to trace to into the combo box labeled “Host to trace”.
2. Press the button at the top of the toolbar (trace).
3. View the results in the Trace Display



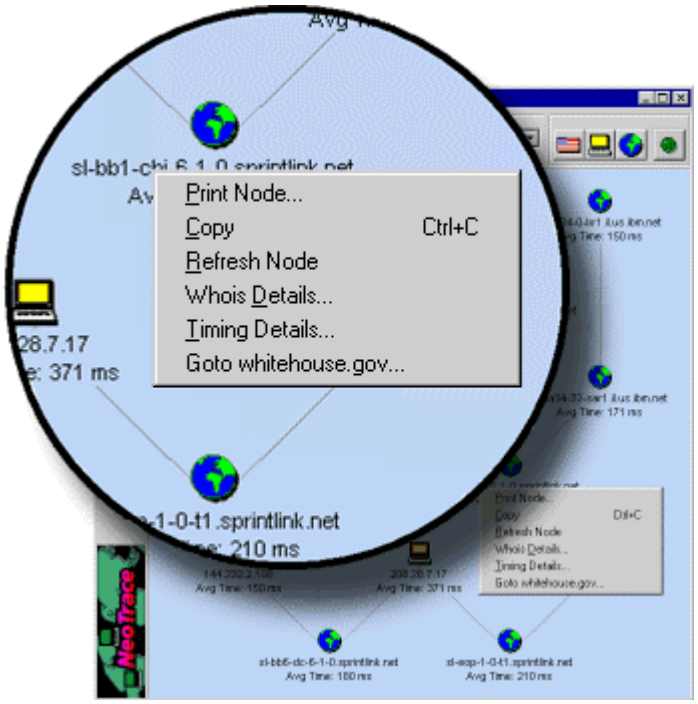
You can also pick a previously traced site to trace again by using the drop-down portion of the combo box.

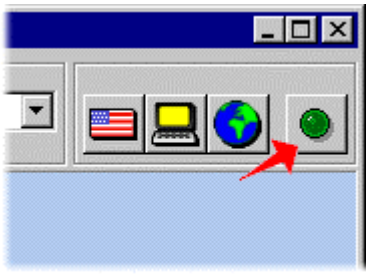
During the trace information is returned the trace display is updated. If you move your mouse over the nodes you will see pop-up windows that display further information about the nodes, including the name and address of the owner if available. If you wish to terminate a trace before it completes press the trace button again. Its appearance will indicate whether a trace is in progress.



At any time there are nodes on the screen you can view additional information about the nodes by moving the mouse cursor over the nodes and viewing the small windows that appear.

Once the trace is complete you can get additional information and options through a contextual menu. Move the mouse pointer to the node you are interested in and right-click to view this menu.





You can toggle re-ping of the destination node or the route with the button in the upper right corner

of the display. Ping settings are in the configuration dialog.

Go Online

The ‘Go Online’ button will open your default web browser to view a special page at the NeoWorx web site.

This page is customized for your version of NeoTrace and will display:

- The version of NeoTrace you are using
- Upgrade information when appropriate
- Additional help or FAQ information
- Ordering information

Please be sure to use this button occasionally to check for updated information.

Step by Step Procedures

Performing a Trace

Select the site you want to trace to. You may type in a new computer name, select one from the list of previous traces, or you can drag a link out of your web browser onto NeoTrace.

To trace to the site you are currently viewing in your web browser, grab the icon just to the left of the site URL in the navigation bar. The icon will vary depending upon the browser you are using, but they all work the same.

 Internet Explorer 4 or 5

 Netscape Navigator 4

 Internet Explorer 3

 Netscape Navigator 3

Drop it onto the NeoTrace window. The site name will appear in the Host to Trace window and the trace will begin. You cannot drop a link if there is a trace in progress.

The route from your computer to the target will start to form. Very quickly you will see the full path to the other computer. Initially each node in the path will be labeled with its IP address. As NeoTrace resolves the names for each node, the IP will be replaced with a 'human friendly' name.

If you move your mouse pointer over the nodes a small window will pop up displaying further details about the node, including the round trip (ping) time to the node and the address of the person or organization that owns the node if that information is available.

In some cases the address (*WhoIs* information) will not be available.

Checking WhoIs information

As the trace progresses and finishes NeoTrace will query for detailed 'WhoIs' information. This is a set of information about a site with the following format:

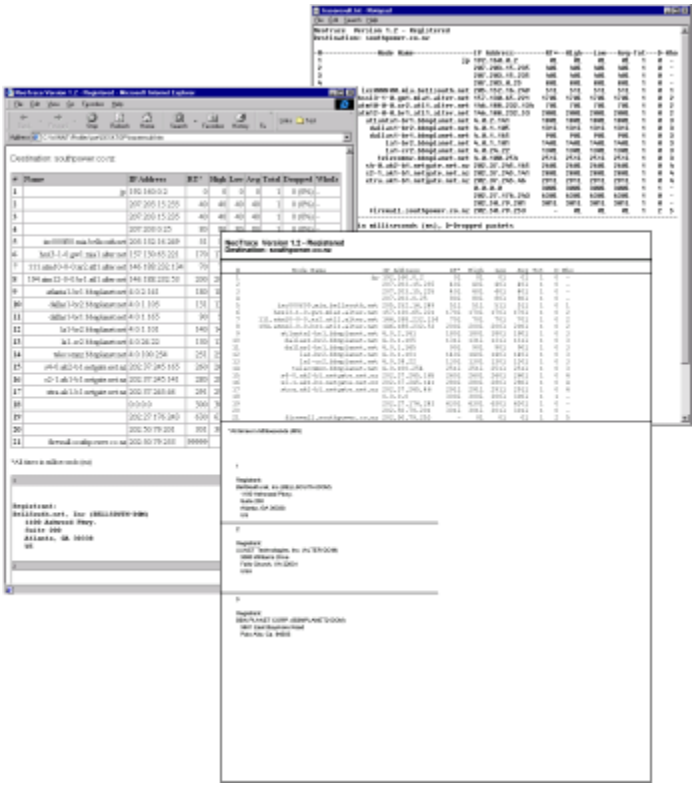
1. Company name and address
2. Domain name (i.e. neoworx.com)
3. Contact information for administrative, billing and technical needs
4. Date information on the creation and most recent update of this information
5. The servers which are responsible for providing the DNS info for this domain

The format for the information returned from international servers may be a bit different.

Unfortunately the majority of countries do not have WhoIs servers available. This makes retrieval of information on them impossible. Check the NeoWorx web site for up to date information on which domains can be queried.

Printing or Saving results

The results of a trace can be output to the printer, a text file or to simple HTML format. You have a choice of the degree of information included in the output as well.



Simple
Displays the node number, hostname, IP address and timing results (essentially the same as command line traceroute)

Standard
Also displays short WhoIs results (essentially the normal NeoTrace results)

Detailed
Includes detailed WhoIs results

The output consists of a table containing all the nodes and their current stats, followed by a table of WhoIs information when using the Standard or Detailed output options.

Configuration

Select the ‘Config’ button from the tool bar to access the configuration dialog. This dialog lets you set options for NeoTrace.

Speed Indicators

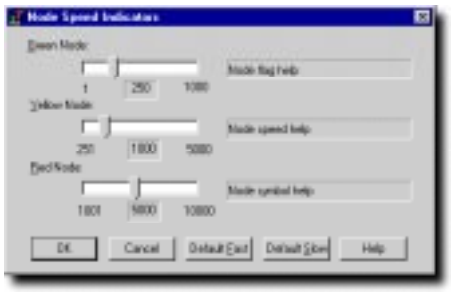
Because different response times are suitable for different applications and connection types, you may configure the node speed display.

Note: In this context ‘speed’ refers to latency, or the time it takes traffic to travel, not bandwidth, which is the quantity of traffic. All modems, regardless of bandwidth, are high-latency.

To change the speed ranges choose the Config button from the toolbar and then the ‘Adjust Speeds…’ button. This will display the ‘Speed Indicators’ dialog.

There are **default settings** available in this dialog for ‘Fast’ and ‘Slow’ connections.

Generally speaking you should choose the ‘**Slow’** default settings any time a **modem** is involved in your Internet connection. For example if you connect to the Internet by dialing in with your modem. In some office situations you may be connected via Ethernet to the rest of the network but the connection from your network into the Internet is through a modem or other relatively slow connection. In this case as well you should choose the slow defaults.



If your connection to the Internet is through an ISDN connection or through an office LAN with a high-speed connection such as a T1, T3 or partial T1 you should choose the ‘**Fast’** defaults.

Advanced users can customize the speed ranges to their particular needs. When you drag the sliders their behavior may seem a little confusing at first. This is because as you adjust the slider you are adjusting the upper limit for the range of that color, and by definition you are simultaneously adjusting the lower limit for the range above it.

Output options

The last two options affect the **output** of the trace when you pick the ‘Output’ button on the NeoTrace toolbar. You can choose to have the trace results sent to the printer, and HTML file or a text file. There are three different **styles** of output available as well.

Output to:

- Printer
- HTML
- Text file

Output style:
- Simple
- Standard
- Detailed

Press the output button to initiate saving or printing.

Cache

NeoTrace records the information it receives from the DNS (node name) and WhoIs (node owner) lookups. DNS and WhoIs information are treated as two separate caches. If you perform traces frequently this cache can grow large. Information may also change, and if it is only retrieved from the cache it will no longer be accurate. For this reason you may wish to configure your cache information to expire more frequently.

To clear the entire cache now simply press the ‘Clear DNS’ or ‘Clear WHOIS’ buttons.

Display Options

Each node is labeled with one or two lines of text and is colored to indicate its relative ‘speed’ or ping time.

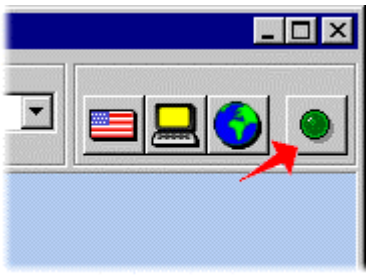
Select the information you would like displayed for each node from the list of available items in the ‘Top Line Text’ and ‘Bottom Line Text’ drop-down controls.

The available label items are:
- Domain Name
- Response Time
- Highest Response Time
- Average Response Time
- Lowest Response Time
- IP Address

If you want a single-line display select ‘None’ for the second line.

Continuous Pinging

To simplify investigation of the performance of a particular node or path you can turn on continuous pinging. This causes NeoTrace to ping either the destination node or every node on the route in turn upon completion of the trace.



Toggle pinging with this button

You can choose no pinging, pinging of just the **destination** node, or pinging of every node on the **route** with the radio buttons at the left.

The **update frequency** is how often the ping will be performed. The **time out** value is how long NeoTrace will wait for a response before giving up on the node responding.

Changing Fonts

You may alter the font used to display the node labels. When you select the font configuration button a standard font dialog will appear. You may choose any font that is installed on your system for the display.

Note that NeoTrace does not prevent you from picking fonts that look terrible, use your own discretion.

Node Meanings

The icons used to represent nodes have several meanings. They are intended to convey the type or location of node and the relative 'speed' or latency of traffic to that site.

The latency is indicated from better to worse by green, yellow, red and gray icons.
'Top level' domains, i.e. domains which are not contained within a two-letter country domain, are indicated by special icons which represent NET, COM, MIL, GOV and EDU. The flag of each country represents sites with names contained by a two-letter country domain.

Latency Indicators

The relative speed of nodes is indicated by color. This is an indication of how long it takes a packet (data) to make a round trip between your computer and that particular computer. Note that the time can vary between traces, and may vary a great deal at different times of the day due to traffic conditions on the Internet. The color ranges can be adjusted in the configuration dialog.

	Display	**Default Speed Ranges**	
Graphic	**Meaning**	**Fast**	**Slow**
	Fast Node	0-100ms	0-250ms
	Moderate Node	101-750	251-1000
	Slow Node	751-5000	1001-5000
	Very Slow or Unresponsive Node	>5 seconds	>5 seconds

Nodes indicated with flags use a bar of colored squares above them to indicate relative speed. The colors have identical meanings to the colors used in other nodes as indicated in the above table. The length of the color bar also relates to the relative speed and has no separate meaning.

US and Top Level Symbols

The function of a node is indicated by the symbol used to represent it. The currently supported types are:

Graphic	Type	
	Generic node	This is used for any node that does not fall into the other categories
	NET	These nodes are typically internet providers, international gateways, or part of the internet backbone.
	EDU	US Educational institutions
	MIL	US Military
	GOV	US Government

Country Abbreviations By Country Name (in English)

Source: ISO 3166 Maintenance Agency

CODE	Country
AF	AFGHANISTAN
AL	ALBANIA
DZ	ALGERIA
AS	*AMERICAN SAMOA
AD	ANDORRA
AO	ANGOLA
AI	*ANGUILLA
AQ	*ANTARCTICA
AG	ANTIGUA AND BARBUDA
AR	ARGENTINA
AM	ARMENIA
AW	*ARUBA
AU	AUSTRALIA
AT	AUSTRIA
AZ	AZERBAIJAN
BS	BAHAMAS
BH	BAHRAIN
BD	BANGLADESH
BB	BARBADOS
BY	BELARUS
BE	BELGIUM
BZ	BELIZE
BJ	BENIN
BM	*BERMUDA
BT	BHUTAN
BO	BOLIVIA
BA	BOSNIA AND HERZEGOWINA
BW	BOTSWANA
BV	*BOUVET ISLAND
BR	BRAZIL
IO	*BRITISH INDIAN OCEAN TERRITORY
BN	BRUNEI DARUSSALAM
BG	BULGARIA
BF	BURKINA FASO
BI	BURUNDI
KH	CAMBODIA
CM	CAMEROON
CA	CANADA
CV	CAPE VERDE
KY	*CAYMAN ISLANDS
CF	CENTRAL AFRICAN REPUBLIC
TD	CHAD
CL	CHILE
CN	CHINA
CX	CHRISTMAS ISLAND
CC	*COCOS (KEELING) ISLANDS
CO	COLOMBIA
KM	COMOROS
CG	CONGO
CD	*CONGO, THE DEMOCRATIC REPUBLIC OF THE
CK	*COOK ISLANDS
CR	COSTA RICA
CI	COTE D'IVOIRE
HR	CROATIA (local name: Hrvatska)
CU	CUBA
CY	CYPRUS
CZ	CZECH REPUBLIC
DK	DENMARK
DJ	DJIBOUTI
DM	DOMINICA
DO	DOMINICAN REPUBLIC
TP	*EAST TIMOR
EC	ECUADOR
EG	EGYPT
SV	EL SALVADOR
GQ	EQUATORIAL GUINEA
ER	ERITREA
EE	ESTONIA
ET	ETHIOPIA
FK	*FALKLAND ISLANDS (MALVINAS)
FO	*FAROE ISLANDS
FJ	FIJI
FI	FINLAND
FR	FRANCE
FX	*FRANCE, METROPOLITAN
GF	FRENCH GUIANA
PF	*FRENCH POLYNESIA
TF	*FRENCH SOUTHERN TERRITORIES
GA	GABON
GM	GAMBIA
GE	GEORGIA
DE	GERMANY
GH	GHANA
GI	*GIBRALTAR
GR	GREECE
GL	*GREENLAND
GD	GRENADA
GP	*GUADELOUPE
GU	*GUAM
GT	GUATEMALA
GN	GUINEA
GW	GUINEA-BISSAU
GY	*GUYANA
HT	HAITI
HM	*HEARD AND MC DONALD ISLANDS
VA	HOLY SEE (VATICAN CITY STATE)
HN	HONDURAS
HK	*HONG KONG
HU	HUNGARY
IS	ICELAND
IN	INDIA
ID	INDONESIA
IR	IRAN (ISLAMIC REPUBLIC OF)
IQ	IRAQ
IE	IRELAND
IL	ISRAEL
IT	ITALY
JM	JAMAICA
JP	JAPAN
JO	JORDAN
KZ	KAZAKHSTAN
KE	KENYA
KI	KIRIBATI
KP	KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF
KR	KOREA, REPUBLIC OF
KW	KUWAIT
KG	KYRGYZSTAN
LA	LAO PEOPLE'S DEMOCRATIC REPUBLIC
LV	LATVIA
LB	LEBANON
LS	LESOTHO
LR	LIBERIA
LY	LIBYAN ARAB JAMAHIRIYA

LI	LIECHTENSTEIN
LT	LITHUANIA
LU	LUXEMBOURG
MO	*MACAU
MK	MACEDONIA, THE FORMER YUGOSLAV REPUBLIC OF
MG	MADAGASCAR
MW	MALAWI
MY	MALAYSIA
MV	MALDIVES
ML	MALI
MT	MALTA
MH	MARSHALL ISLANDS
MQ	*MARTINIQUE
MR	MAURITANIA
MU	MAURITIUS
YT	*MAYOTTE
MX	MEXICO
FM	MICRONESIA, FEDERATED STATES OF
MD	MOLDOVA, REPUBLIC OF
MC	MONACO
MN	MONGOLIA
MS	*MONTSERRAT
MA	MOROCCO
MZ	MOZAMBIQUE
MM	MYANMAR
NA	NAMIBIA
NR	NAURU
NP	NEPAL
NL	NETHERLANDS
AN	*NETHERLANDS ANTILLES
NC	*NEW CALEDONIA
NZ	NEW ZEALAND
NI	NICARAGUA
NE	NIGER
NG	NIGERIA
NU	*NIUE
NF	*NORFOLK ISLAND
MP	*NORTHERN MARIANA ISLANDS
NO	NORWAY
OM	OMAN
PK	PAKISTAN
PW	*PALAU
PA	PANAMA
PG	PAPUA NEW GUINEA
PY	PARAGUAY
PE	PERU
PH	PHILIPPINES
PN	*PITCAIRN
PL	POLAND
PT	PORTUGAL
PR	*PUERTO RICO
QA	QATAR
RE	*REUNION
RO	ROMANIA
RU	RUSSIAN FEDERATION
RW	RWANDA
KN	SAINT KITTS AND NEVIS
LC	SAINT LUCIA
VC	SAINT VINCENT AND THE GRENADINES
WS	SAMOA
SM	SAN MARINO
ST	SAO TOME AND PRINCIPE
SA	SAUDI ARABIA
SN	SENEGAL
SC	SEYCHELLES
SL	SIERRA LEONE
SG	SINGAPORE
SK	SLOVAKIA (Slovak Republic)
SI	SLOVENIA
SB	SOLOMON ISLANDS
SO	SOMALIA
ZA	SOUTH AFRICA
GS	*SOUTH GEORGIA AND THE SOUTH SANDWICH ISLANDS
ES	SPAIN
LK	SRI LANKA
SH	*ST. HELENA
PM	*ST. PIERRE AND MIQUELON
SD	SUDAN
SR	SURINAME
SJ	*SVALBARD AND JAN MAYEN ISLANDS
SZ	SWAZILAND
SE	SWEDEN
CH	SWITZERLAND
SY	SYRIAN ARAB REPUBLIC
TW	TAIWAN, PROVINCE OF CHINA
TJ	TAJIKISTAN
TZ	TANZANIA, UNITED REPUBLIC OF
TH	THAILAND
TG	TOGO
TK	*TOKELAU
TO	TONGA
TT	TRINIDAD AND TOBAGO
TN	TUNISIA
TR	TURKEY
TM	TURKMENISTAN
TC	*TURKS AND CAICOS ISLANDS
TV	TUVALU
UG	UGANDA
UA	UKRAINE
AE	UNITED ARAB EMIRATES
GB	UNITED KINGDOM
US	UNITED STATES
UM	*UNITED STATES MINOR OUTLYING ISLANDS
UY	URUGUAY
UZ	UZBEKISTAN
VU	VANUATU
VE	VENEZUELA
VN	VIET NAM
VG	*VIRGIN ISLANDS (BRITISH)
VI	*VIRGIN ISLANDS (U.S.)
WF	WALLIS AND FUTUNA ISLANDS
EH	*WESTERN SAHARA
YE	YEMEN
YU	YUGOSLAVIA
ZR	ZAIRE
ZM	ZAMBIA
ZW	ZIMBABWE

* Indicates no flag implemented in current version of NeoTrace

Country Abbreviations and Flags By Code

Source: ISO 3166 Maintenance Agency

Code	Flag	Country
AD		ANDORRA
AF		AFGHANISTAN
AG		ANTIGUA AND BARBUDA
AI		*ANGUILLA
AL		ALBANIA
AM		ARMENIA
AN		*NETHERLANDS ANTILLES
AO		ANGOLA
AQ		*ANTARCTICA
AR		ARGENTINA
AS		*AMERICAN SAMOA
AT		AUSTRIA
AU		AUSTRALIA
AW		*ARUBA
AZ		AZERBAIJAN
BA		BOSNIA AND HERZEGOWINA
BB		BARBADOS
BD		BANGLADESH
BE		BELGIUM
BF		BURKINA FASO
BG		BULGARIA
BH		BAHRAIN
BI		BURUNDI
BJ		BENIN
BM		*BERMUDA
BN		BRUNEI DARUSSALAM
BO		BOLIVIA
BR		BRAZIL
BS		BAHAMAS
BT		BHUTAN
BV		*BOUVET ISLAND
BW		BOTSWANA
BY		BELARUS
BZ		BELIZE
CA		CANADA
CC		*COCOS (KEELING) ISLANDS
CD		*CONGO, THE DEMOCRATIC REPUBLIC OF THE
CF		CENTRAL AFRICAN REPUBLIC
CG		CONGO
CH		SWITZERLAND
CI		COTE D'IVOIRE
CK		*COOK ISLANDS
CL		CHILE
CM		CAMEROON
CN		CHINA
CO		COLOMBIA
CR		COSTA RICA

CU  CUBA

CV  CAPE VERDE

CX  CHRISTMAS ISLAND

CY  CYPRUS

CZ  CZECH REPUBLIC

DE  GERMANY

DJ  DJIBOUTI

DK  DENMARK

DM  DOMINICA

DO  DOMINICAN REPUBLIC

DZ  ALGERIA

EC  ECUADOR

EE  ESTONIA

EG  EGYPT

EH *WESTERN SAHARA

ER  ERITREA

ES  SPAIN

ET  ETHIOPIA

FI  FINLAND

FJ  FIJI

FK *FALKLAND ISLANDS (MALVINAS)

FM  MICRONESIA, FEDERATED STATES OF

FO *FAROE ISLANDS

FR  FRANCE

FX *FRANCE, METROPOLITAN

GA  GABON

GB  UNITED KINGDOM

GD  GRENADA

GE  GEORGIA

GF  FRENCH GUIANA

GH  GHANA

GI *GIBRALTAR

GL *GREENLAND

GM  GAMBIA

GN  GUINEA

GP *GUADELOUPE

GQ  EQUATORIAL GUINEA

GR  GREECE

GS *SOUTH GEORGIA AND THE SOUTH SANDWICH ISLANDS

GT  GUATEMALA

GU *GUAM

GW  GUINEA-BISSAU

GY *GUYANA

HK *HONG KONG

HM *HEARD AND MC DONALD ISLANDS

HN  HONDURAS

HR  CROATIA (local name: Hrvatska)

HT  HAITI

HU  HUNGARY

ID  INDONESIA

IE  IRELAND

IL		ISRAEL
IN		INDIA
IO		*BRITISH INDIAN OCEAN TERRITORY
IQ		IRAQ
IR		IRAN (ISLAMIC REPUBLIC OF)
IS		ICELAND
IT		ITALY
JM		JAMAICA
JO		JORDAN
JP		JAPAN
KE		KENYA
KG		KYRGYZSTAN
KH		CAMBODIA
KI		KIRIBATI
KM		COMOROS
KN		SAINT KITTS AND NEVIS
KP		KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF
KR		KOREA, REPUBLIC OF
KW		KUWAIT
KY		*CAYMAN ISLANDS
KZ		KAZAKHSTAN
LA		LAO PEOPLE'S DEMOCRATIC REPUBLIC
LB		LEBANON
LC		SAINT LUCIA
LI		LIECHTENSTEIN
LK		SRI LANKA
LR		LIBERIA
LS		LESOTHO
LT		LITHUANIA
LU		LUXEMBOURG
LV		LATVIA
LY		LIBYAN ARAB JAMAHIRIYA
MA		MOROCCO
MC		MONACO
MD		MOLDOVA, REPUBLIC OF
MG		MADAGASCAR
MH		MARSHALL ISLANDS
MK		MACEDONIA, THE FORMER YUGOSLAV REPUBLIC OF
ML		MALI
MM		MYANMAR
MN		MONGOLIA
MO		*MACAU
MP		*NORTHERN MARIANA ISLANDS
MQ		*MARTINIQUE
MR		MAURITANIA
MS		*MONTSERRAT
MT		MALTA
MU		MAURITIUS
MV		MALDIVES

MW MALAWI

MX MEXICO

MY MALAYSIA

MZ MOZAMBIQUE

NA NAMIBIA

NC *NEW CALEDONIA

NE NIGER

NF *NORFOLK ISLAND

NG NIGERIA

NI NICARAGUA

NL NETHERLANDS

NO NORWAY

NP NEPAL

NR NAURU

NU *NIUE

NZ NEW ZEALAND

OM OMAN

PA PANAMA

PE PERU

PF *FRENCH POLYNESIA

PG PAPUA NEW GUINEA

PH PHILIPPINES

PK PAKISTAN

PL POLAND

PM *ST. PIERRE AND MIQUELON

PN *PITCAIRN

PR *PUERTO RICO

PT PORTUGAL

PW *PALAU

PY PARAGUAY

QA QATAR

RE *REUNION

RO ROMANIA

RU RUSSIAN FEDERATION

RW RWANDA

SA SAUDI ARABIA

SB SOLOMON ISLANDS

SC SEYCHELLES

SD SUDAN

SE SWEDEN

SG SINGAPORE

SH *ST. HELENA

SI SLOVENIA

SJ *SVALBARD AND JAN MAYEN ISLANDS

SK SLOVAKIA (Slovak Republic)

SL SIERRA LEONE

SM SAN MARINO

SN SENEGAL

SO SOMALIA

SR SURINAME

ST SAO TOME AND PRINCIPE

SV EL SALVADOR

SY SYRIAN ARAB REPUBLIC

SZ SWAZILAND

TC *TURKS AND CAICOS ISLANDS

TD CHAD

TF *FRENCH SOUTHERN TERRITORIES

TG TOGO

TH THAILAND

TJ TAJIKISTAN

TK *TOKELAU

TM TURKMENISTAN

TN TUNISIA

TO TONGA

TP *EAST TIMOR

TR TURKEY

TT TRINIDAD AND TOBAGO

TV TUVALU

TW TAIWAN, PROVINCE OF CHINA

TZ TANZANIA, UNITED REPUBLIC OF

UA UKRAINE

UG UGANDA

UM *UNITED STATES MINOR OUTLYING ISLANDS

US UNITED STATES

UY URUGUAY

UZ UZBEKISTAN

VA HOLY SEE (VATICAN CITY STATE)

VC SAINT VINCENT AND THE GRENADINES

VE VENEZUELA

VG *VIRGIN ISLANDS (BRITISH)

VI *VIRGIN ISLANDS (U.S.)

VN VIET NAM

VU VANUATU

WF WALLIS AND FUTUNA ISLANDS

WS SAMOA

YE YEMEN

YT *MAYOTTE

YU YUGOSLAVIA

ZA SOUTH AFRICA

ZM ZAMBIA

ZR ZAIRE

ZW ZIMBABWE

* Indicates no flag implemented in current version of NeoTrace

Details

WhoIs

WhoIs information is a sort of 'white pages' for the internet provided by InterNIC and other domain registration authorities..

At the present time most international authorities have either no whois available or very poorly maintained servers or information. For this reason you will find that international whois information returned is spotty.

The address shown does not always indicate the location of a node. This is particularly true of nodes that are part of the Internet backbone. Every computer operated by a given domain owner will return the same WhoIs information. You can sometimes get an idea of where a computer is actually located by looking at the nodes on either side of it, or at the name of the node itself. Many backbone nodes have names that are related to the city or company they service.

If you are aware of a whois server we do not currently support in NeoTrace please let us know!

Unreachable Nodes and Networks

This usually indicates that the target machine is behind a firewall which blocks the traffic used to perform the trace. You will not be able to get an accurate trace to the target machine.

In some cases *you* may be the one behind a firewall which is not allowing your trace traffic out of the local network. Contact your system administrator to see if he can help you get around the problem.

How NeoTrace Works

NeoTrace works by exploiting a feature of the Internet Protocol called TTL, or Time To Live. Originally, this data field in an IP packet header was supposed to contain a value representing the actual amount of time a packet could be flying around the Internet before a router would simply discard it. This was designed to eliminate damaged packets which were endlessly looping around the network and therefore wasting bandwidth and router capability.

NeoTrace sends out a packet destined for the destination you specify. It sets the TTL field in the packet to 1. The first router in the path receives the packet, decrements the TTL value by 1, and if the resulting TTL value is 0, it discards the packet and sends a message back to the originating host to inform it that the packet has been discarded.

NeoTrace records the IP address and DNS name (if available) of that router, then sends out another packet with a TTL value of 2. This packet makes it through the first router, then times-out at the next router in the path. This second router also sends an error message back to the originating host. NeoTrace continues to do this, recording the IP address and name of each router until a packet finally reaches the target host, or until it decides that the host is unreachable. In the process, NeoTrace records the time it took for each packet to travel round trip to each router. Slow links are therefore pinpointed.

Using NeoTrace through a Firewall

It is possible to use NeoTrace through a firewall. If the firewall is not already configured to permit the use of PING or TRACERT through it (by use of ICMP packets) the firewall will need to be reconfigured.

In order for NeoTrace (or ping for that matter) to operate through a firewall two rules must be added to the firewall configuration. The first rule is to allow machines to send echo-requests. The second rule is to allow receipt of echo-replies. Depending on your particular firewall vendor the terminology used may be different but the principle holds true

NeoTrace makes use of ICMP (Internet Control Message Protocol) packets. ICMP packets are not associated with any particular port number.

Please note that changes to firewall configuration should only be made by a network administrator with an understanding of the characteristics of the firewall. Consult the documentation for your particular firewall for further information. Configuration changes that allow Ping to operate through the firewall will typically be documented, and these same procedures will allow use of NeoTrace.

Spam Hunting

We've all experienced 'spam'; those unwanted, unsolicited bulk emails that extol the benefits of everything from Multi Level Marketing to water softeners. Sadly there is a lot of porn arriving the same way. They often use bogus return addresses and generally try to hide their tracks by any means possible.

The Internet has always been a free place where anything goes. However these people are creating a situation where governments may start legislating if we don't police the situation ourselves.

Is it spam?

Before pursuing the source of a message be sure to determine if it really is spam. You may be receiving a message because you subscribed to a mailing list, asked to be notified of web site changes or product updates, etc.

Does the body of the message contain unsubscribe instructions? Email from a responsible organization will always contain unsubscribe instructions. If so follow them. Irresponsible organizations often include this as well, so consider carefully if this is mail related to something you asked for or not.

Did the sender attempt to obscure their identity? If so they are definitely email abusers of the worst kind.

What can you do?

First of all never buy anything from a bulk emailer. If they're not making a profit from bulk email, they'll stop sending it. Educate your friends and colleagues that they should not encourage this behavior either. (Also for the sanity of us all ask them not to mass-forward email appeals and chain letters.)

"Spamming" is an anathema to most Internet service providers. They will give a spammer one warning before closing the account. Sometimes they don't even give the first warning. With this knowledge and Neotrace you can hunt down these intruders.

Please take the moral high-ground when hunting spammers. Don't do anything improper, and always keep a pleasant tone when dealing with ISPs and agencies. After all they aren't the one's sending the spam.

Reading Headers

First lets find the header. Where the header information is available to you will vary depending on the email software you are using. If you're using MS Internet Explorer 4 (Outlook Express), you can right click on the message and choose "properties". In MS Outlook open the message then choose view/options from the menu. Some email programs show you all headers all the time (such as Eudora 3.0).

The email header consists of information related to the source and routing of the message. Most of the time this information is of no interest to people which is why your email software generally does not display all of it.

Here's a sample header

```
Return-Path: <we_deliver@mailexcite.com>
Received: from www.comune.collegno.to.it
(root@www.comune.collegno.to.it [158.102.48.66]) by lucky.innet.com
(8.8.7/8.8.7) with ESMTP id VAA03877 for <rgrun@innet.com>; Fri, 11 Sep
1998 21:07:03 -0400
From: we_deliver@mailexcite.com
Received: from www.comune.collegno.to.it (hil-dnppi-
053.oh.compuserve.net [206.175.98.53]) by www.comune.collegno.to.it
(8.8.6/8.8.6) with SMTP id DAA07201; Sat, 12 Sep 1998 03:06:23 +0200
Received: from we_deliver@mailexcite.com by we_deliver@mailexcite.com
(8.8.5/8.6.5) with SMTP id GAA05956 for <we_deliver@mailexcite.com>;
Fri, 11 Sep 1998 19:03:15 -0600 (EST)
Date: Fri, 11 Sep 98 19:03:15 EST
To: we_deliver@mailexcite.com
Subject: Do it for Yourself  or  We can Do it for You !
Message-ID: <Do It Yourself  or  We Can Do It For You>
Reply-To: we.deliver@mailexcite.com
X-PMFLAGS: 128 0
X-UIDL: 10000000000000000000000000000011
Comments: Authenticated sender is <we_deliver@mailexcite.com>
Status:
```

Notice the return path and the reply-to can be anything the sender chooses. In this case it's we_deliver@mailexcite.com.

Your key to locating the source of the email is the 'Received' header entries. Each of these entries indicates the message was passed from one email server to another one on the path from the originator to you.

Where did lucky.innet.com (the Internet provider for the email address in this example) get it? The next line holds the first clue; we_deliver@mailexcite.com who received it from www.comune.collegno.to.it Notice the IP address; They connect through compuserve with the IP of 206.175.98.53. Notice THEY received it from we_deliver@mailexcite.com.

Here's what happened

The spammer used his correct mail address in the reply field. He "bounced" the message from his mailexcite account through www.comune.collegno.to.it. They are probably unaware that the spammer used their server. This is done to hide his tracks.

The trick is to follow back the "received from" names and IP addresses until you get to the originating domain

Sniffing Clues with NEOTRACE

Look at the header again. You can copy a name, an IP address or everything to the right of "@" in an email address.

In Neotrace trace to the source domain, "mailexcite.com" in this case. When it finishes hold you cursor over the last item. It should show all the information of the Internet service provider. Right click and choose "copy". Now in your mail program FORWARD the spam.. Go to the bottom and PASTE the data from Neotrace. Next copy the header from the original spam and paste that on the bottom. Look in the data from Neotrace and you will see the domain's business addresses.

Copy them to the To: field. You may want to CC it to the addresses “Postmaster@<domain name>” and “abuse@<domain name>” One or both should be received by the Internet service provider. Write a quick and friendly note at the top of the letter and send it. The provider will be able to determine who sent the spam and usually close the account.

It is possible use an anonymous server to send spam. This strips the header and adds another. You won’t be able to trace this back. Be assured that a person with enough experience to run an anonymous server finds a million messages going through his server, he will be able to handle the abuser in some truly unpleasant ways.

That’s all there is to it. Follow the steps above. Neotrace makes it easy and fun.

The Price of Spam

Even aside from laws relating directly to unsolicited mass email, there are specific legal and contractual penalties that will apply to most spammers.

Loss of account or connection

All responsible ISPs reserve the right to cut off customers that abuse its spam policy. If you are able to notify the management of the ISP the spammer connects through you can get them shut down.

Mail Fraud

Many spammers are committing mail fraud without realizing it. The penalties for mail fraud are very serious. If convicted of mail fraud a spammer will very likely do prison time and be on probation at a minimum, often with restrictions placed on their Internet access.

Further Resources

Please visit our web site for a list of links to ‘spam hunting’ articles and anti-spam resources.
http://www.neoworx.com/neotrace/spam.asp

Diagnosing Connection Problems

In this section we make the assumption that you are attempting to view a web site and find that it is not working. If it is a site you have never visited before, attempt tracing to it first. In some cases you will find the site no longer exists. In dealing with sites you visit often, it is more likely a network or connection failure.

Due to the nature of the Internet there are a large number of points where a connection can fail. These possible failure points include:

- The connection from your computer to your ISP (typically a modem)
- The connection from your ISP to their provider or backbone
- Backbone segments
- Interconnection points
- The connection from the backbone to the ISP of the site you are trying to reach
- The connection from their ISP to the site

Power outages, equipment failures, severed cables or fiber, fire, earthquakes and more can cause failure.

Make a Baseline Trace

If you are not currently experiencing a connection problem as you read this, we suggest that you perform a trace to several sites you use frequently and print out or save the results. This will give you useful information when you have problems later.

Is it You?

Your first goal is to determine whether the connection failure is in your local loop (the connection from you to your ISP) or further along. Attempt to trace to your ISP's main domain address. This is typically your email server or the main web site of your ISP. If you are unable to reach it then there is a problem with your connection. You should attempt re-establishing your connection and check your hardware. If you are still unable to get a good connection contact your ISP.

If you can reach servers at the ISP the next step is to trace to the site you are trying to reach. If the trace reaches all the way to the target site and it does not appear as a 'gray' (no colors) icon then the target server is working. If you do not already have it on you can turn on continuous pinging. After a few pings right-click on the target node and view the *timing details*. The important information to look for here is the total responses and percentage of dropped packets. If there has been a response then traffic is getting through, if a high percentage of packets have been dropped then there is a connection problem.

If you see a packet loss of 30% or less then the connection is quite good enough for you to web browse, so if the site is not responding to your web browser there is another problem. Either you have a browser problem or the web server software on the target site is crashed. Determine if your browser is working properly by viewing other sites. If it is working well you should send email to the webmaster at the target site informing them that you checked their site and can reach it but not web browse and that their server may be crashed.

ISP Failure

If your trace to the target site gets no further than your ISP it is likely they have had a connection failure. Attempt tracing to several more sites and see if you can get any of them. If all the sites you attempt to trace to fail you can be confident your ISP is suffering a major outage. At this point you should attempt contacting technical support to make certain they are aware of the outage.

If you get a busy signal it's pretty obvious they are being inundated with calls already and are aware of the problem. Stop calling and let them concentrate on fixing the problem. If you get through the first thing you should ask is if they are aware of a network failure. If they are not you should explain to them what you have seen and tried. If they are aware of the problem politely ask if they have an estimate of when it will be fixed, thank them and hang up.

Backbone failures

If you find that you are able to reach some sites, but not others, or that there is a vast disparity in performance from what you normally see, then there is very likely a backbone failure. In the US you can be quite certain that in the case of a backbone failure there are already lots of people aware of the problem and working on it.

There is no way to 're-route' your personal traffic. The Internet is designed to route traffic where it can, and if you traffic does not get through it is because there is no place for it to go.

Common Questions and Problems

Are the times shown for each node round-trip to me or between nodes?

The time at each node is the round-trip (ping) time from your computer to that node. Times have no relationship to adjacent nodes.

Why then do you see nodes with higher times before nodes with lower times? Since the time measured is the total round-trip, it includes the time it takes for that computer to respond, not just the travel time. Many nodes, typically dedicated routers, are more efficient at passing traffic than they are at responding to our request. This causes higher times in the midst of otherwise fast routes.

I can't see WhoIs results

There are two times when you typically won't see WhoIs results (the detailed name and address info for a node).

The first and by far the most common is when the WhoIs servers are unavailable. This is beyond your control and ours.

If you are *never* able to get WhoIs information you may be blocked by your firewall or proxy. Port 43 needs to be enabled for TCP/IP traffic in order for it to work. Alert your system or network administrator if you think there is a problem.

Be certain to flush your WhoIs cache if you are experiencing this problem.

You must use Microsoft's TCP/IP Stack

The method of implementation of the ICMP calls in NeoTrace has been tested only with the tcp/ip stack provided by Microsoft. This stack is found on Windows 95 and Windows 98, as well as Windows NT 3.51 and up. NeoTrace will work properly in this situation.

There is a known problem that prevents NeoTrace from working with other stacks. At this point NeoTrace is known to not work with: Trumpet Winsock, Novell, and NetManage tcp/ip stacks.

Microsoft's WINSOCK doesn't support ICMP or RAW SOCKET's which are necessary for PING and Trace Route to work. Microsoft's incomplete WINSOCK doesn't work with these programs without some additional help files. Microsoft had to add ICMP.DLL to support these programs, PING and TRACEROUTE (tracert). These two programs call this ICMP.DLL. Due to how Microsoft added ICMP.DLL after the fact and not part of the Winsock, they don't use Winsock, therefore, these two applications won't work with other implementations of Winsock.

MS Winsock 2 fixes this problem, but because Winsock 2 has to be installed as an upgrade to the operating system we presently do not assume its existence. Non-upgraded MS tcp/ip stack users represent the vast majority of users at the present.

This is a legacy issue, which will be addressed, in a future version of NeoTrace.

Destination Nodes with Different Names

Sometimes you may perform a trace to a certain location, and when it gets there NeoTrace labels it with a different name. This is not an error, what you are seeing is the 'true' name of that computer.

A single physical computer can have many names and IP addresses assigned to it. While this is not normally the case, it does happen frequently with web servers. This allows a company to sell web space to many different organizations and have those organizations be able to have unique addresses, while serving all of them from a single machine or cluster of machines.

In some cases hundreds of separate domain URLs may resolve to a single machine.

You may also see a trace locate the destination machine, but the label never resolves back from being a numerical IP address. This means that the 'reverse DNS lookup' for that IP address failed. This is a DNS problem or reverse lookup of that IP address has been deliberately disabled.

Changing Routes

The Internets underlying structure evolved from a network that was originally created to handle military traffic. Part of its very nature is to be resistant to damage and to route around problems. For this reason traffic across the Internet is not guaranteed to follow any particular path between two given points. A stream of traffic is usually made of many separate packets. These packets can all travel different routes and may not even arrive in the same order that they left in.

At different times of the day as traffic flow varies you may see different routes to different sites. You can even see different routes taken on traces only seconds apart.

Error Messages

The Errors you may see are:

- No Response
- Network Unreachable
- Bad Destination

No Response

On some traces you may see nodes labeled 'No Response'. In some cases this indicates a computer that is not responding properly, and in other cases is a symptom of something else.

Large numbers of 'No Response' nodes generally indicates that the route you are tracing passes through a 'firewall'. This is a method of defense for a portion of the Internet against unauthorized access from other parts of the network. In order to provide added protection for computers behind that firewall it has been configured not to return information on the route that your data takes. You will see this most frequently when you attempt to trace to certain commercial sites such as MSN. Version 1.1 and higher recognize and eliminate bogus 'No Response' nodes from the trace.

Isolated 'No Response' nodes can be due to an incorrectly configured or deliberately mis-configured machine, and in some cases is due to a bug in the network code of that machine.

In some cases the target machine is returning datagrams with an incorrect TTL which causes it to appear that there are a great many more nodes in the route than there actually are.

In most cases there is no actual computer at the point where the 'No Response' message appears.

Bad Destination

When you see 'Bad Destination' appear it means that the address could not be resolved, or that the IP number is invalid. Basically you have entered an address which does not exist. In some cases it may be that you have a valid address, but at this exact point in time it doesn't exist as far as the Internet is concerned. This can occur if the domain name server information for that site is being reconfigured and is fairly rare. You may also see this problem occur (and constantly) if the domain name server your computer is using is not working correctly.

How to Purchase NeoTrace

NeoTrace is available to individual users as Shareware, and if you use it we encourage you to register it**. If you use it for commercial purposes you are required to register it.** Your registration ensures you that we will be able to continue to update the product and provide you with newer and better versions.

Site licenses for 5 or more users can be purchased inexpensively from NeoWorx or authorized resellers.

Always be sure you have the latest pricing and contact information by visiting our web site.

You may register online, by phone, fax or mail. Download order forms and view contact information, or use our online registration system, by visiting our home page:

http://www.neoworx.com

NeoWorx Inc.
251 W. Central Ave. #273
Springboro, OH 45066 USA

Order Form

Name			
Company			
Address			
City, State			
Country		**Postal Code**	
Fax		**Phone**	
Email			

Program	Price Each	Quantity	Total
NeoTrace Single User	$24.50		
NeoLite Executable Compressor (Intro pricing ends October 31, 1998)	$128 **Introductory Price: $98**		
NeoTrace/PKZIP Bundle	$53.50		
NeoTrace/PKZIP CLI Bundle	$39		
NeoTrace 5 User License	$78		
NeoTrace 10 User License	130		
NeoTrace 25 User License	$260		
NeoTrace 50 User License	$390		
NeoTrace 100 User License*	$650		
*Call for pricing on larger site licenses			
PKZIP for Windows 95/98/NT	$49		
PKZIP for Windows CLI Version	$29		
PKZIP for Unix (multiple platforms)	Call/Email		
Data Compression Library Win32	$350		
Data Compression Library Unix	$450		
PKLite Executable Compressor (16 bit)	$158		
Shipping and Handling Fees: US & Canda $6.00 per item, Outside US & Canada $12.00 per item, call or email for express shipping options			
Ohio Residents add 6% sales tax			
Total Enclosed			

Method of Payment

☐Check or Money Order ☐Visa ☐Mastercard ☐American Express

Please note that any check or money order must be in US Dollars drawn on a US bank.

Card Number	
Expiration Date	
Signature	

Thank you for your order. We appreciate your business.

Purchase orders over $80 are accepted from corporations and government agencies within the US & Canada. Please make payment to NeoWorx inc. Prices, terms and conditions are subject to change without notice.

http://www.neoworx.com Voice (561)712-0890 **Fax (561)683-3740**