Overview

The pingVs application is a simple GUI front end in .Net4.5+ for the common network utility and fault finding ping and tracert (Trace Route) command line functions.

It also provides various other IP related seaches and support requests such as DNS lookup etc depending on the operating environment and product version.

It allows users to quickly execute ping and trace requests for any supplied IP or host name and to set optional parameters such as ttl, hop limits etc. without recourse to the command line -xxx options hand typing.

As with the latest Windows command line versions both IP Version 4 and 6 Address formats are supported.

In addition, further support is added for automatic fall back of IP addressing formats if a selected format is not supported somewhere in the routes or end points along with reporting of any DNS redirection of targets.

Output from ping and trace can be easily cut and pasted into other applications (i.e. Mail Messages) using standard Windows copy and paste options and commands.

The application can be installed free of charge on as many PC's as your require making it suitable for use as a troubleshooting tool for single user internet connectivity, through small home or SOHO networks to corporate LAN/WAN systems, where user access to Command line utilities are neither desirable or permitted.

Advanced lookup, configuration and network installation options are available depending on the version and licencing options installed - Please visit our Desktop Software pages at http://asgnet.co.uk for details of out Network and utilities software options.

System Requirements

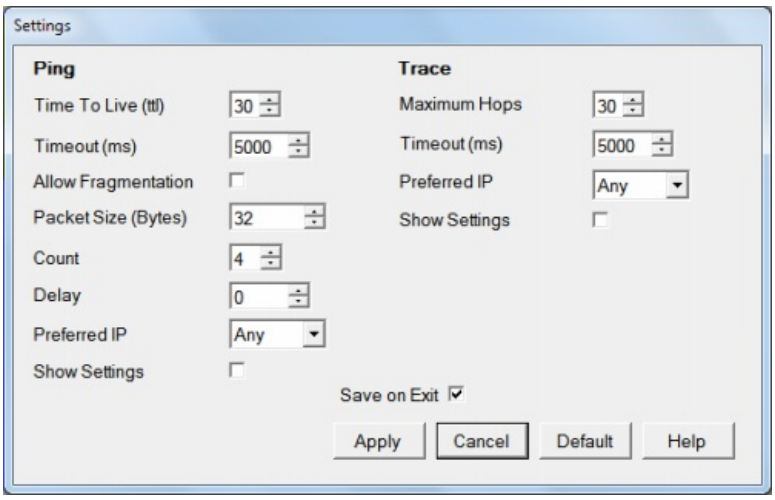
Windows Vista or above

Microsoft .NET Framework 4.5 or Above

600 x 800 VGA Monitor

Note: *Runs on both 32 and 64 Bit Windows*

Settings



Use the Settings menu option or tool to open the ping and trace settings editor.

By default changes made with the Apply Button are automatically saved and re-loaded the next time the application is run. To discard changes on the application close then uncheck the Save on Exit option.

When first used these settings replicate the default settings of the traditional Windows command line ping and tracert tools. You can use the Defauit button to reset back to these values.

Ping

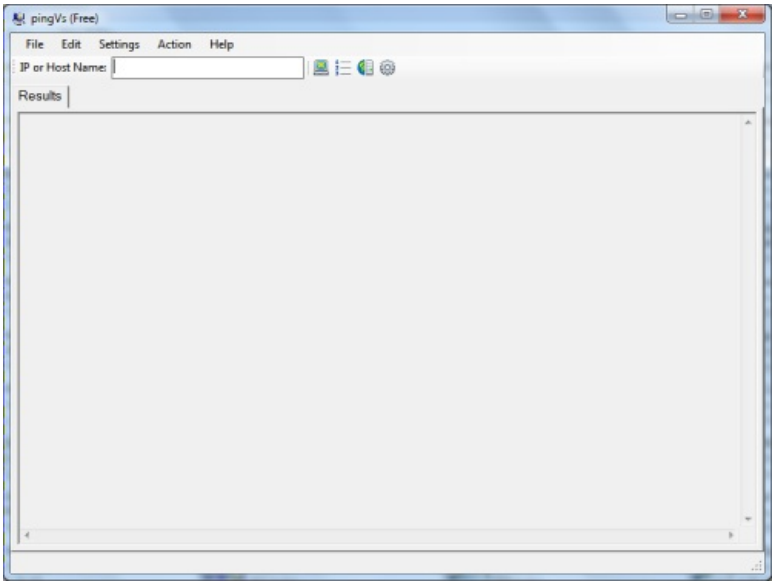
Setting	Description
ttl (Time to Live)	The number of routers/servers/networks the ping packet can pass through to try and reach its final destination (5-50)
Timeout (ms)	The maximum number of milliseconds that a ping packet can take between sending and a reply being received (500-10,000) = 0.5-10 Seconds
Allow Fragmentation	Not recommended for normal use but can be used if MTU sizes on large packets require fragmentation by any server/router in the route
Packet Size	The ping packet size in bytes to send (1 Byte to 16K Bytes). The actual successful packet size maximum is dependent on MTU and other system hardware and software settings
Count	The number of consecutive ping packets to send in a ping test (1-10)
Delay	The number of milliseconds (0-1000) to wait between each ping packet sent to a host (ignored if count is 1)
Preferred IP	The Prefered IP Address format to use for the request when a host name is used for the target. (Any, IPv4 or IPv6)
Show Settings	When checked outputs the settings along with the ping results in the results window.

Trace

Setting	Description
Maximun Hops	The maximum number of routers/servers/networks the trace packet can pass through to try and reach its final destination (5-50)
Timeout (ms)	The maximum number of milliseconds that a packet can take between sending and a reply being received by each server/router in the trace (500-10,000) = 0.5-10 Seconds
Preferred IP	The Prefered IP Address format to use for the request when a host name is used for the target. (Any, IPv4 or IPv6)
Show Settings	When checked outputs the settings along with the trace results in the results window.

Using pingVs

On launching the application the following window will open



Enter a Host Name or Version 4 or 6 IP address into the IP or Host field that you wish to test.

The host name can be any valid name, either global (www.microsoft.com) or local LAN name (i.e. MYLAPTOP), The IP Address can be either a version 4 (xxx.xxx.xxx.xxx) format or a Version 6 (xxxx::xxxx:xxxx:xxxx:xxxx)

Note: *If an IP address is specified then the preferred IP setting is ignored and the format entered is used for the test.*

Once a Host name or IP is entered use either the menu bar actions option or the Ping, TraceRT or DNS Lookup tools to perform the required test or enquiry.

When a test or enquiry is run the results are appended into the main results section of the window and can be copied and pasted as required. Use the menu bar File -> New option to clear any existing results from the results area.

Because a trace can be a lengthy process when the final destination is unreachable or has ICMP packets blocked (See troubleshooting) a mechanism is provided to replicate the command version keyboard interrupt ctl+C to stop the trace by displaying a Stop Button in the top right hand corner of the results area when running.

When the stop button is pressed the application will request the current trace to be stopped after completion of the current packet or DNS resolution request. As it waits for these processes to complete their internal processing the time lag between pressing stop and the trace actually halting and returning control back to the user can be up to 2 x the current timeout setting

Ping

Below is a typical output from a ping to a tablet on the local area network with default settings.

```
Ping Test Started at 15:49 on 31 July 2017

mytablet [fe80::d974:5c8c:4f84:aaba%13]

Reply [fe80::d974:5c8c:4f84:aaba] Success -      4ms  (32 Bytes)
Reply [fe80::d974:5c8c:4f84:aaba] Success -      6ms  (32 Bytes)
Reply [fe80::d974:5c8c:4f84:aaba] Success -      4ms  (32 Bytes)
Reply [fe80::d974:5c8c:4f84:aaba] Success -      7ms  (32 Bytes)

Minimum Round Trip Time = 4ms
Maximum Round Trip Time = 7ms
Average Round Trip Time = 5ms
```

And the same host but with preferred IP set to IPv4 in the settings

```
Ping Test Started at 16:04 on 31 July 2017

mytablet [192.168.0.16]

Reply [192.168.0.16] Success -     59ms  (32 Bytes)
Reply [192.168.0.16] Success -      9ms  (32 Bytes)
Reply [192.168.0.16] Success -     10ms  (32 Bytes)
Reply [192.168.0.16] Success -      4ms  (32 Bytes)

Minimum Round Trip Time = 4ms
Maximum Round Trip Time = 59ms
Average Round Trip Time = 20ms
```

Ping to external host with show settings checked and displaying a DNS host name redirection

```
Ping Test Started at 16:18 on 31 July 2017

bill.xyz [46.30.215.60]

ttl=30, Packet Size=32 Bytes, Don't Fragment=True, Timeout=5000ms

DNS Redirect bill.xyz to webserver109.web-ppd.xxy.com

Reply [46.30.215.60] Success -     42ms  (32 Bytes)
Reply [46.30.215.60] Success -     42ms  (32 Bytes)
Reply [46.30.215.60] Success -     42ms  (32 Bytes)
Reply [46.30.215.60] Success -     45ms  (32 Bytes)

Minimum Round Trip Time = 42ms
Maximum Round Trip Time = 45ms
Average Round Trip Time = 43ms
```

TraceRT

Below is a typical output from a trace to a tablet on the local area network with default settings.

```
TraceRT Started at 17:21 on 31 July 2017

mytablet [fe80::d974:5c8c:4f84:aaba%13]

  1:    40ms    14ms     5ms [fe80::d974:5c8c:4f84:aaba]

Done
```

And the same host but with preferred IP set to IPv4 and show settings checked in the settings options.

```
TraceRT Started at 17:22 on 31 July 2017

Max Hops=30, Timeout=5000ms, Preferred Ip Version: IPv4

mytablet [192.168.0.16]

  1:    94ms     7ms     7ms [192.168.0.16]

Done
```

Trace to external host with default settings and displaying a DNS host name redirection

```
TraceRT Started at 17:33 on 31 July 2017

asgdevnet.co.uk [185.43.2.1]

DNS name asgdevnet.co.uk Redirects to websrv991.pleskctlpanel.co.uk

  1:     9ms     8ms     9ms [192.168.0.1]
  2:     *       *       *   Request timed out.
  3:    22ms    16ms    17ms [62.255.109.137]   popl-core-2a-xe-312-0.network.virginmedia.net
  4:     *       *       *   Request timed out.
  5:     *       *       *   Request timed out.
  6:     *       *       *   Request timed out.
  7:     *       *       *   Request timed out.
  8:    19ms    25ms    22ms [195.66.224.84]    te-0-2-0-0.cr01.the-lon.pulsant.net
  9:    21ms    22ms    18ms [193.29.223.70]    te-0-0-0-0.cr01.dc1-mhd.pulsant.net
 10:    22ms    29ms    24ms [46.249.195.10]    te-0-1-0.cs01-1u.dc1-mhd.pulsant.net
 11:    23ms    19ms    18ms [185.43.2.1]       websrv991.pleskctlpanel.co.uk

Done
```

DNS Lookup

Below is a typical output from a DNS Lookup to the localhost.

```
DNS Lookup for localhost at 20:33 on 07 August 2017

Host      IP Address Alias
--------- ---------- -------------------
mylaptop1 ::1
          127.0.0.1  localhost_mylaptop1

Done
```

Note the multiple IP addresses and alias

And the reverse lookup of IP Address 127.0.0.1

```
DNS Lookup for 127.0.0.1 at 20:36 on 07 August 2017

Host for IP 127.0.0.1 Resolves to: localhost_mylaptop1

Done
```

Reverse DNS lookup support depends on the support provided by the DNS server(s) and hosts file your system uses for name resolution

Trouble Shooting

When attempting a ping or trace to the 127.0.0.1 (localhost) IP4 address the DNS resolves to an unexpected host name such as www.007guard.com

The probable cause is with running spybot or a similar anti-malware/anti-virus software that has modified the system hosts file to protect against attacks to the localhost. The redirect will point to the first valid entry in the hosts file for IP address 127.0.0.1, in the example below this is www.007guard.com

```
# localhost name resolution is handled within DNS itself.
# 127.0.0.1       localhost
# ::1             localhost
# Start of entries inserted by Spybot - Search & Destroy
127.0.0.1 www.007guard.com
```

One might assume simply uncommenting the existing 127.0.0.1 localhost entry will resolve this - ***DO NOT DO THIS***

The fix is to add an entry between the # ::1 and start of the spybot or other entries such as:

```
127.0.0.1    localhost_MYCOMPUTERNAME
```

where MYCOMPUTERNAME is the name of the local PC/Server.

This method protects the existing DNS localhost resolution anti attack mechanisms whilst providing a meaningful name resolution to the localhost/127.0.0.1 tests and reporting.

Ping resolves to a host name/IP but returns timeout on each test packet.

Possible causes are:

- ttl setting is too low.
- timeout setting is too low.
- your machine is disconnected from the LAN/Internet
- the target host/IP machine is in standby/hibernation or disconnected.
- The target host/IP is set to ignore or block ICMP ping requests.

Use the settings option to increase the ttl and/or timeout values, if possible check the physical connections and running state of the target PC/Server. If you have access to the target machine then check it is set to respond to ICMP ping packets.

TraceRT displays routing information but fails to complete returning unreachable or timeouts on final hop.

possible causes are:

- Hop count is too low
- Timeout is too low
- A router/server in the route is down/faulty/not responding.
- The final target host/IP machine is in standby/hibernation or disconnected.
- Final target host/IP is set to ignore or block ICMP ping packets.

Use the settings option to increase the hops and/or timeout values, if possible check the physical connections and running state of the target PC/Server and routers/servers in the route. If you have access to the target machine then check it is set to respond to ICMP ping packets.

A trace can be interrupted by the user (see Using pingVs)

Ping or TraceRT succeeds but you cannot access remote services such as Web server on the host

Check that the DNS or a hosts entry has not re-directed the target to a different host - if it has it will be reported as the final hop of a trace or detailed at the start of the ping or trace results. You can use the DNS lookup function to report any IP or host name aliases that the DNS holds.

Note: *A redirection of a host by the DNS is not always a fault with the DNS resolution as some servers such as a shared webserver can have different domain names assigned. i.e. abc.com may host 123.com and xyz.com. Pinging xyz.com may redirect to abc.com and the target host will be responsible for resolving the particular service associated with the original host.*
