/ping plotter tutorial

Last revision date: September 2, 2003

Click here for the Ping Plotter FAQ.

beating up on your ISP
long-term monitoring/working with historical data
ping plotter for the online gamer (though applicable to all)

/undocumented features and other tidbits

advanced whois server setup
automatic license key entry on installation
changing thread counts
changing timeline interval values

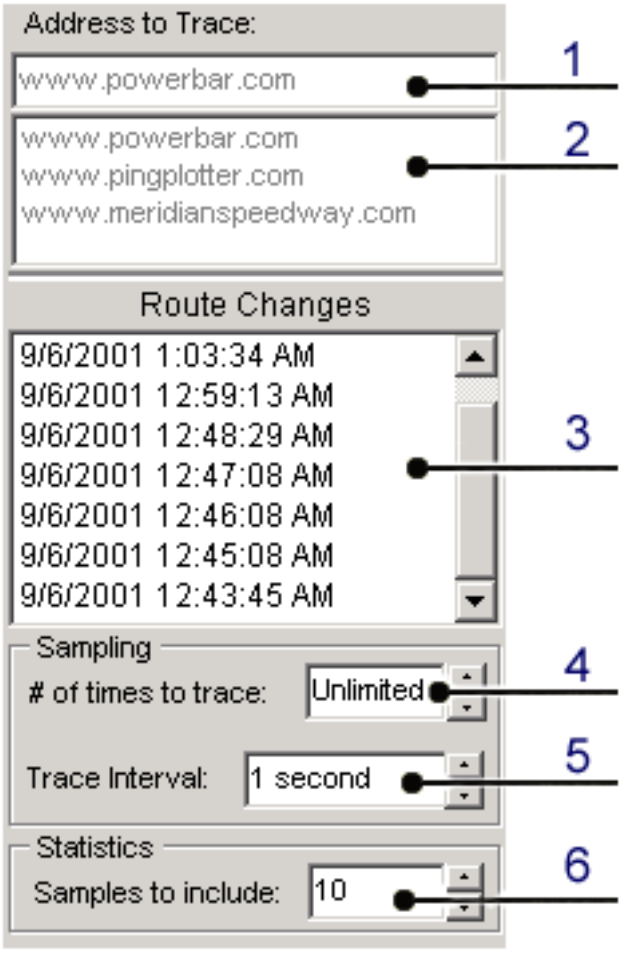
/related links

daryl's TCP/IP primer
navas cable modem/DSL tuning guide
broadband reports (your one stop shop for xDSL information)
808hi.com (tons of information for modem users)
speedguide.net (has equipment reviews, tweaks, etc.)

/other interesting stuff

some thoughts on speed of light latency
the ping page (links to lots of stuff related to ping)
internet backbones and router instability (dated but a good read anyway)
NetMon.org (lots of cool tools and links)
the story of PING
the museum of broken packets
traceroute (and Pirates)
when the CRC and TCP checksum disagree

/the interface - basic settings



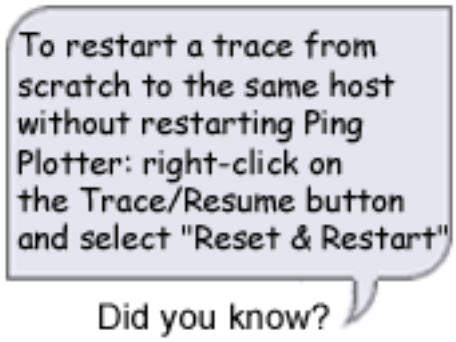
1. IP Address or DNS name of the destination you want to trace. If you enter an IP Address here Ping Plotter will start tracing immediately before the IP is resolved to a name. The name will show as "resolving" until the request is complete.

2. If the site you wish to trace is already listed, you can select it instead of typing it in. To delete a host, right-click it in the list and select “Delete”. Double-clicking on a site in this list starts a traceroute to that site.

3. The Route Change pane is used to show the history of route changes. Any time any hop in the route changes, Ping Plotter stores the old and new route data and adds the time of the change to this list box. Double-clicking on any time will show the route as of that time. This is the starting time for the change.
Double-clicking on the time-line graph (covered in the next section) will refocus the upper graph on the period you double-clicked on the lower time-line graph. The route window will also follow this - to show the route that was current at the time you selected.

4 . The # of times to trace allows you to stop tracing after a certain number of times. If you’re only interested in a set trace count, you can save some bandwidth by not allowing Ping Plotter to trace forever.

5. The Trace Interval is the amount of time Ping Plotter will wait between each sample set. If you’re doing a long term monitoring project, you may want to set it to be 1 minute (or more). If you’re doing a quick test, you might want to set this to something lower (5 seconds or 10 seconds). If the up/down arrow doesn’t have the amount of time you want, just type the time interval you want (e.g. 3.5 seconds).

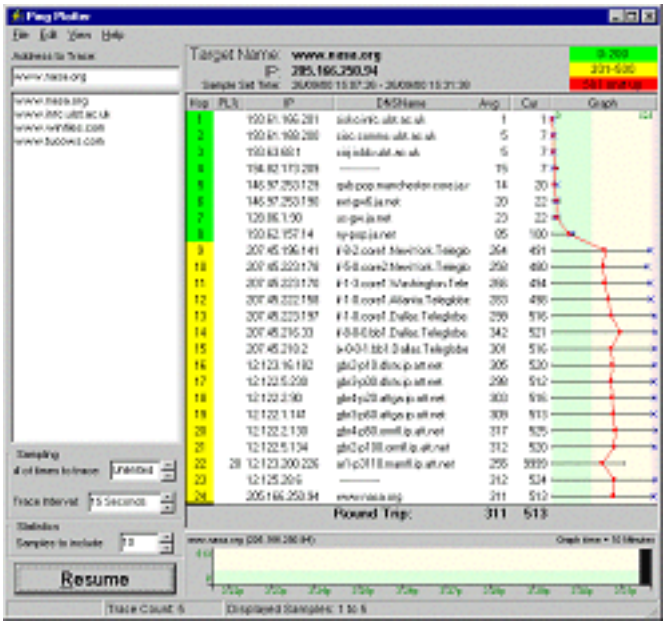


6. When running a trace, Ping Plotter can look at just the most current samples. This is great to watch "trending" (where the response changes over time). If

you include ALL samples (type 0 in this field for ALL), then after a lot of samples, new samples don't affect the graph very much. Setting this to something like 10 allows you to see how the response times are right now. All numbers in the trace (upper) graph are affected by this. When zooming in on the timeline graph, it's important to not have this set to "ALL".

/introduction

Ping Plotter is a utility for tracing IP packets through a network. It graphically illustrates the route that a request takes, and the IP address of each server along the route. Ping Plotter was born out of a need by it's author, who needed to find out why his broadband Internet connection was so erratic. Sometimes it was really fast, other times it was slow to the the point of being unusable and he had to use a dial-up. What he needed was a good way to prove the performance (or lack of performance) of his connection to his Internet service provider.



Ping Plotter is a trace route program on steriods. It uses the multithreading capabilities of Windows to check performance on all hops in the route at the same time. This has several advantages: 1) It's a lot faster. 2) All hops are tested at the same time, instead of seconds apart, so the comparison is better.

Another thing you can do with Ping Plotter is set it to continuous trace mode - in which it will test the same route over and over again (forever if you want). That way you can watch the performance over a period of time, without having to rerun the trace over and over again.

The graphing capabilities is where Ping Plotter really shines. Being able to see where problems are visually is invaluable. As they say, a picture is worth a thousand words (or if you're used to using the command line tracert...a whole bunch of text).

Take a look at the graph below. Look at the jump between hops seven and eight. There's a problem there, and it's easy to tell by looking at the graph.

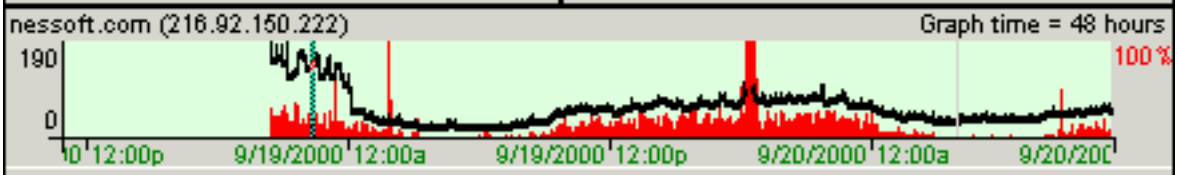
As one satisfied customer wrote once, "HMOs should reimburse for prescribing Ping Plotter to Internet-intense patients as a prophylactic against ulcers".

Target Name: **www.nessoft.com**
IP: **216.92.150.222**
20 Samples Timed: 9/18/2000 10:19:12 PM - 9/18/2000 10:20:47 PM

0 - 200
201 - 500
501 and up

Hop	PL%	IP	DNSName	Avg	Cur	Graph
5		24.218.188.78	pos0-1-0.akrnoh1-brt1.rr.com	35	8	
6		24.218.188.82	ser6-0-0.clmboh1-brt1.rr.com	87	63	
7		24.218.190.38	pos1-0.chcgil1-brt3.rr.com	94	67	
8		24.218.188.222	pos1-1.vinnva1-brt3.rr.com	203	182	
9	25	192.41.177.248	br1.tco1.alter.net	171	ERR	
10	10	192.41.177.248	br1.tco1.alter.net	174	163	
11	5	146.188.160.78	111.at-1-0-0.XR2.TCO1.ALTE	168	ERR	
[12]	10	146.188.160.121	292.ATM6-0.XR2.DCA1.ALTE	174	181	
13	5	146.188.162.85	192.ATM9-0-0.GW1.PIT1.AL1	179	156	
14	25	157.130.32.178	pairnetworks-gw.customer.AL	174	142	
15	15	192.168.1.5	----------	205	237	
16	25	216.92.150.222	nessoft.com	170	163	

Round Trip: 170 163



Data and Image generated by Ping Plotter 2.30 (http://www.pingplotter.com)

/how ping plotter works

At its heart, Ping Plotter is a trace route utility. It's souped up and on steroids, but the basic concept is the same as any other trace route utility.

A ping packet is an IP packet requesting that a copy of its contents be echoed back to the sender. When you "ping" a site, you send over an echo request and that site responds back that it received it. The amount of time it takes for the packet to get to that site, and then return to you, is the ping time, or latency. In general, the lower this is, the better your connection to the site. This time is usually specified in milliseconds (1/1000 of a second).

One of the parameters on a ping packet (and any packet, but we're only talking about ping here) is something called "Time to live" (TTL). TTL is an IP header field designed to keep packets from running in loops, essentially forever, throughout a network (this can happen when there is a route change, and the routers involved don't all know the same information as new information is being replicated out). Initially it's usually set to somewhere between 64 and 255, and is reduced by 1 every time it passes through a server.

If the TTL should ever reach zero, the packet has expired, and the router that it's passing through will send it back to the source. Again, this happens so that packets don't get caught in an endless loop.

Traceroute plays with this TTL number on outgoing packets. It first sends out a packet with a TTL of 1. The first router that sees this decrements it to 0, and then sends it back. It also sends back its own IP address with the packet, and DNS is used to do a lookup for an actual domain name.

Ok, so next, traceroute sends out a packet with a TTL of 2 so it can find out what the next computer in the route is. Then it sends out a packet with a TTL of 3. This process is repeated until the final destination is reached. At that point, you know the entire path the packet has traversed to reach the destination computer/router. Each server in this chain is called a hop.

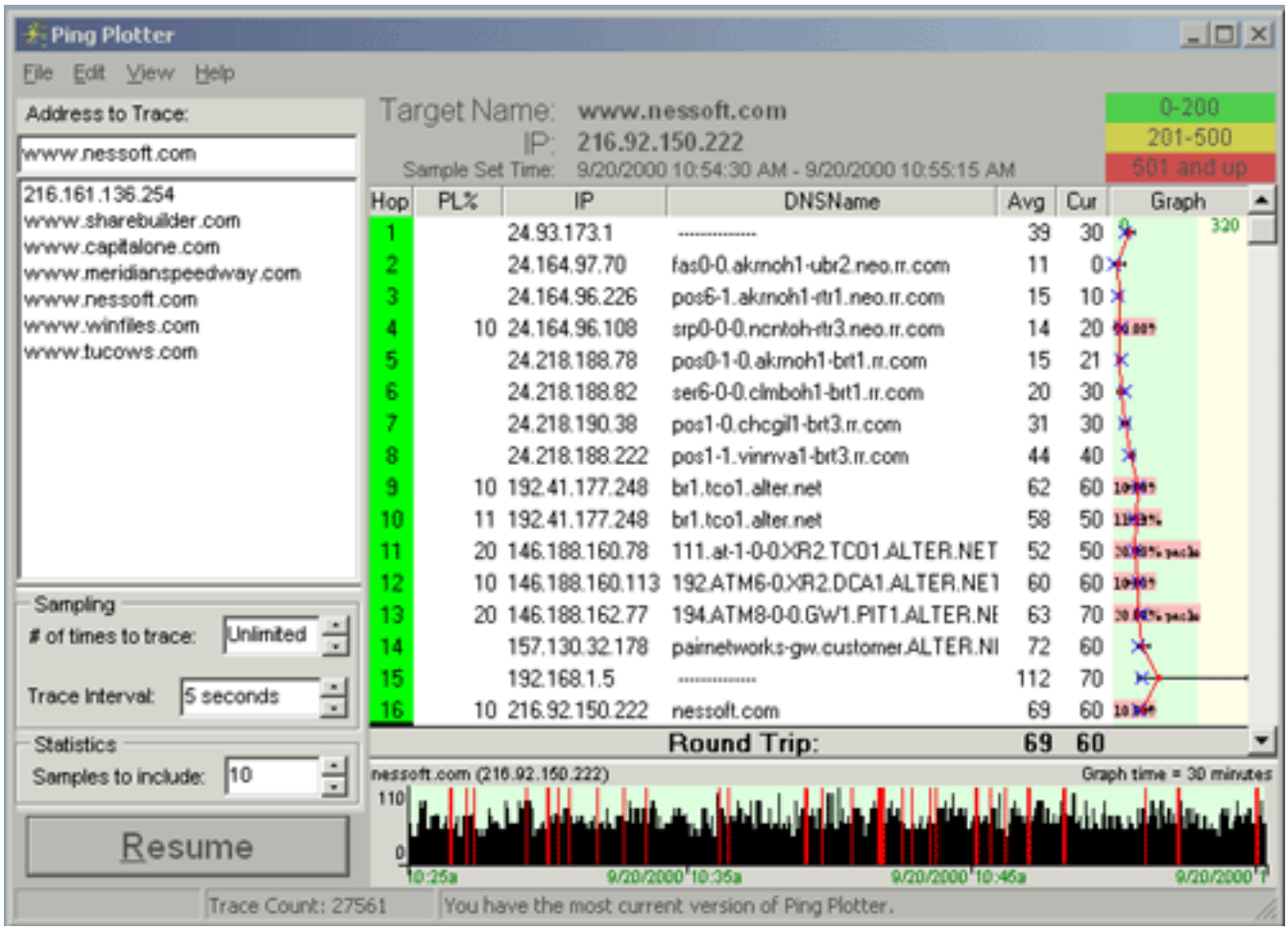
This method can help us determine the route a packet takes, but if we time each of these packets, we know how long it takes for a packet to make it from our source PC, to that router, and then back again. This is called Latency.

The last hop in a (successful) trace route is actually the round-trip time to the destination server. This is an important concept to understand. You don't add up all the times between you and the destination host - as that time has already been added. The time to the last hop in the chain is exactly the same as is if you'd used a ping utility to that host. So a trace route utility is actually two utilities - ping AND trace route.

Ping Plotter speeds up this process by sending out packets to the first 35 servers in the route all at the same time. This makes a HUGE difference in overall speed. It also means that the network conditions for each hop are very similar - so the numbers are better compared.

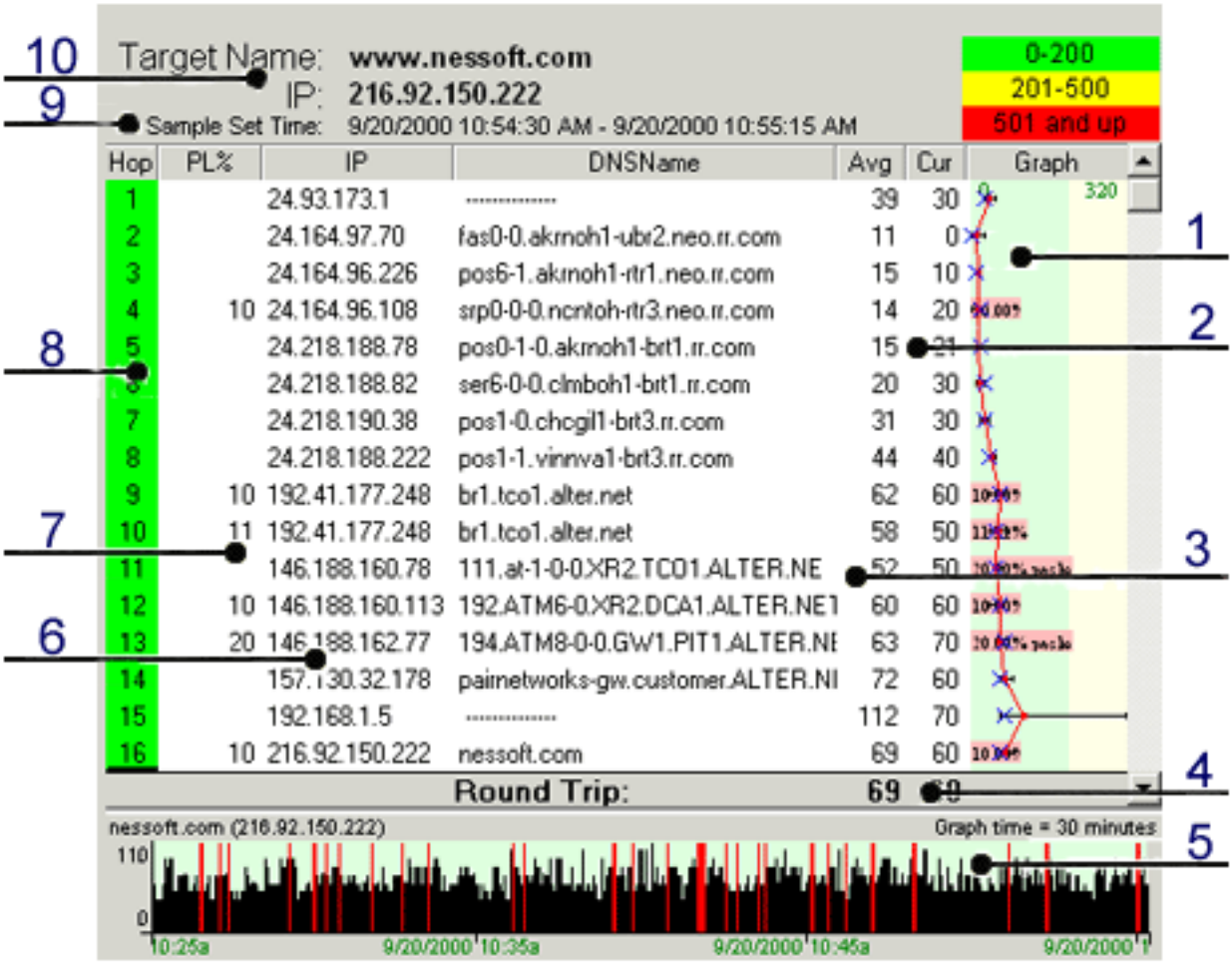
/the interface

One thing that we pride ourselves on is Ping Plotter's ease of use. Really, to get started with Ping Plotter all one has to do is enter an address and click the Trace/Resume button. However, most people prefer to adjust the time interval between traces, samples to include in the graph, etc. In the next two sections we'll explore Ping Plotter's interface. First we'll go over the basic settings. From there, we'll go into understanding what all that stuff on the graphs means.



/the interface - graphs

The graphs are where Ping Plotter shines. At a glance, you're able to visually see where a problem lies. There are actually two graphs available, the Trace Data Graph, and the Time-line Graph. We'll explore both in this section.

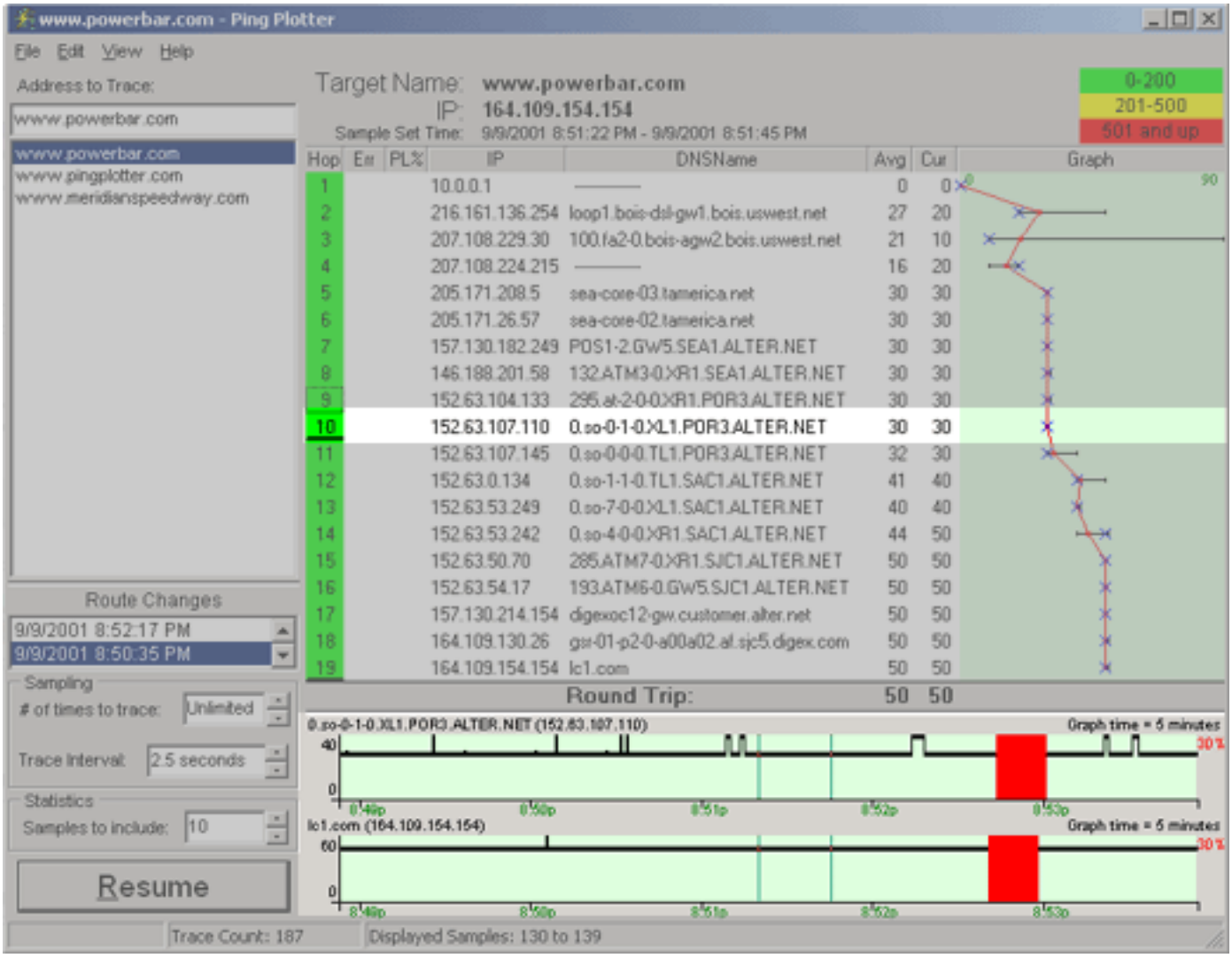


1. The red line on the graph represents the average response time for each host. The blue X represents the response time for the current packet (can be turned off if you're sending a graphic of your graph to somebody - some folks find it confusing when they're not actually there watching the live trace). The black horizontal lines represent the minimum and maximum response times. The red horizontal bar shows the packet loss for that hop (same as the PL% column, but there for readability). Ping plotter uses a dynamic scale for its graph. The bottom number is usually 0, and the top number represents the maximum response time in milliseconds. If you wish, you can change this to a fixed scale in Advanced Options under the Edit menu.

2. The Avg column shows the average response time of the last N samples (where N is the samples to include). Any time-outs/lost packets are not included in this value. The Cur column shows the individual sample time of the most recent sample included in the set. If a number is displayed as ERR, that means that the packet was lost, i.e. a packet was sent out, but never made it back. *These, as well as all other columns, are resizable.*

3. This column shows the DNS name of the device for that hop. A ---------- in this column indicates that Ping Plotter was unable to resolve a name for that device's IP address. This is not a flaw in Ping Plotter. It just means that your DNS server doesn't have a name for that IP address, or that address just doesn't have a DNS name period.

4. The Round Trip line is basically there for ease of reading. It's the same value as the last server in the route. This is the time it takes for a ping to get from your computer to the target device.



5. The time-line graph (TG) is one of the most powerful features in Ping Plotter, and particularly useful for long-term monitoring projects you may be doing.

- Double clicking anywhere on the TG will focus the trace data graph (top graph) to that particular point in time. This is particularly useful for investigating spikes or time-outs (see next item).
- A red line on this graph denotes a time-out for that period. Double clicking anywhere on the graph shows you the trace data detail for that period in the upper graph (denoted by the two vertical "focus" bars you see in the example above). This allows you to see what was happening along the route when that particular time-out occurred.

- Right clicking on the TG allows you to pick the time period you want to view - from 60 seconds up to 48 hours. This value affects all timeline graphs.
- You can slide the graph (by doing a "Click-Drag"), allowing you to look at the past data for this trace. You can right-click and select "Reset focus to current" to move all graphs back to current time. If you've been running the trace for a long time, it's helpful to adjust the time period you have set before you start moving back in the history, i.e. if you're going back a couple of days you might want to set the time period to 24 hours first.
- Shift-Right-Clicking on the graph, and then selecting "Old-style timeline graphs", allows you to change the view to the "histogram" look you see in the graph at the top of this page. The default graph style is shown in the second image.
- You can see a TG for any hop by right clicking on that hop in the trace graph and selecting "Show this timeline graph". You can also get rid of that TG by right clicking and deselecting it. In the example above, I have a the default TG showing for the last hop, and another one showing hop 10 (note the underline that appears under the hop #).
- To scroll with the keyboard, select the timeline graph and use one of the following keys:
ALT-HOME - scroll to the beginning of the collected data
ALT-END - scroll to the end of the collected data
ALT-LEFT - scroll back in time (about 5% of the graph width)
ALT-RIGHT - scroll forward in time
ALT-PGUP - scroll back in time (about ½ of the graph width)
ALT-PGDN - scroll forward in time

6. The IP address for that hop.

7. The PL% indicates the number of packet that have been lost in the current sample set. If you're only including the last 10 samples, then only the number of lost packets in the last 10 samples are shown here. If you want to find out how many time-outs have happened over the entire session, change the "Samples to Include" to 0. This is important. There is no ALL setting for this. 0 = ALL.

8. The number of hops that device in the route is from your computer. If a hop has brackets around it (like [8]), this means that hop is being monitored for an alert (alerts are covered in the advanced settings section of this tutorial). Multiple alerts can be configured for the same IP, and alerts don't work unless some IP in your current route is being monitored (i.e. has brackets around it). If a hop has an underline under it (like 8), that hop is being traced on a time-line graph.

9. Beginning and ending time for the trace. Very useful if you're saving off graphs. It's nice to know the time window the trace was done in.

10. The DNS name and IP Address for the host you're doing the trace route too. If you've got multiple instances of Ping Plotter going, this is in nice big letters so you quickly know which trace you're looking at.

Tools and other options available for the Trace Data Graph

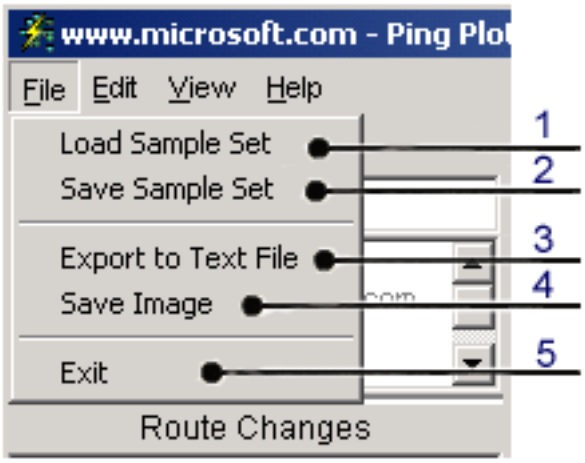
You can display the Minimum and Maximum columns by right clicking on the Trace Data Graph (TG) and selecting them.

You can copy the IP address or DNS name for a hop to the clipboard by right clicking, selecting the Clipboard option and then clicking on what you want to save.

You can do a WhoIs on a particular hop by right clicking on it and selecting WhoIs Information. Note that by default this only queries whois.networksolutions.com.

You can lookup who owns that particular IP range for a hop by right clicking and then selecting "IP Block Lookup (ARIN)".

/the interface - file menu



1. Load a previously saved sample set. The default extension for Ping Plotter saved sample files is .pp2, or Ping Plotter save file format.

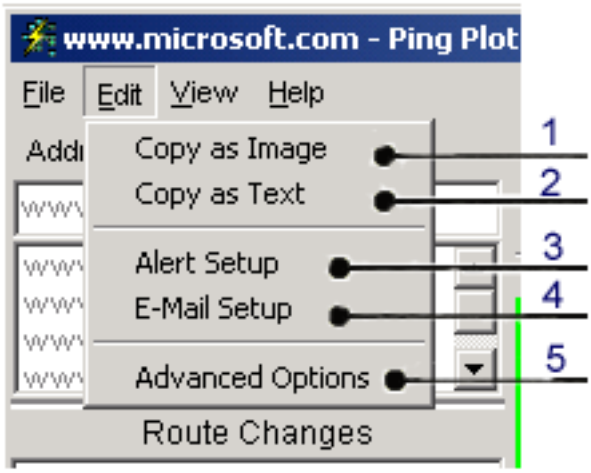
2. Saves a Ping Plotter save file. Allows you to save the current sample set to an external file. These files are saved in .pp2, or Ping Plotter's save file format.

3. Export your trace data to a comma delimited text file. Click here for an explanation of it's options.

4. Save the current graph in .png, .gif or .bmp format.

5. Exit Ping Plotter. By default, you'll be prompted to save your current sample set if you haven't done so already (click here to see how to change this option).

/the interface - edit menu



1.Copy the current graph to the clipboard as an image.

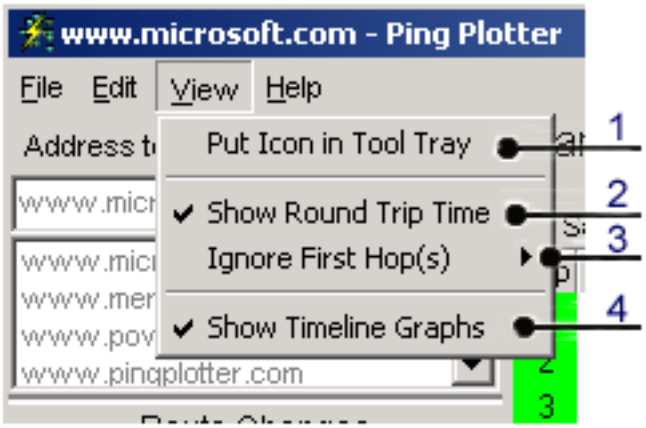
2. Copy the current graph to the clipboard as text.

3. Click here for Alert setup options.

4. Click here for E-mail setup options.

5. Click here to see the Advanced Options.

/the interface - view menu



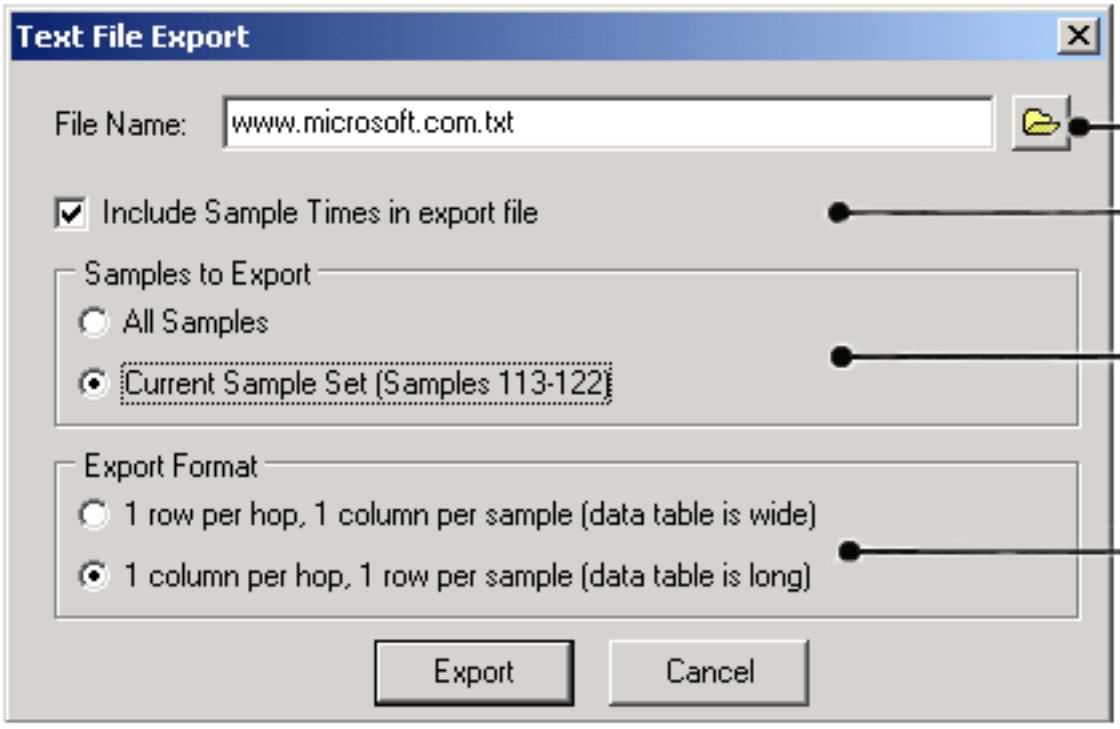
1. Ping Plotter minimizes down into the tool tray.

2. Don't show the Round Trip time below the trace data graph.

3. The default is "trace all hops". From this menu option you can skip hops 1, 2, 3 and 4. Say you're hooked up to a DSL modem and don't want the modem to show in your traces. You'd set this option to Start at Hop 2. If you wish, you can also from this option choose to only trace the final hop.

4. Don't show the Timeline Graphs (the bottom history graphs).

/the interface - exporting text



1. File Name and path to save your text export too.

2. If unchecked, the times for each trace don't get saved.

3. Select All Samples if you want to export your whole trace to text. Select Current Sample Set if all you want to save is the currently displayed sample set shown on the Time Line graph. The current sample set is the setting you'd use if you're wanting to email trace data to an ISP, etc. - though just saving a graph would be a better option.

4. Ping Plotter gives you two different Export Formats to save your data in. Both are shown below.

One row per hop, one column per sample

```
,Sample Times,,9/11/2001 11:13:29 PM,9/11/2001 11:13:30 PM,9/11/2001 11:13:31 PM,9/11/2001 11:13:32 PM,9/11/2001 11:13:33 PM,9/11/2001 11:13:34 PM,9/11/2001 11:13:35 PM
1,,,N/A,N/A,N/A,N/A,N/A,N/A,N/A
2,loop1.bois-dsl-gw1.bois.uswest.net,216.161.136.254,10,10,10,10,10,20,10
3,100.fa2-0.bois-agw1.bois.uswest.net,207.108.229.29,30,20,10,10,10,10,10
4, ---------- ,207.108.224.247,20,10,20,10,20,20,10
5,sea-core-03.tamerica.net,205.171.208.5,30,30,30,30,30,30,30
6,sea-core-02.tamerica.net,205.171.26.57,30,30,30,30,30,30,30
7,POS1-2.GW5.SEA1.ALTER.NET,157.130.182.249,30,30,30,30,31,30,30
8,132.ATM2-0.XR2.SEA1.ALTER.NET,146.188.201.70,30,30,30,30,30,30,30
9,194.at-2-0-0.XR2.POR3.ALTER.NET,152.63.104.145,30,30,30,30,30,30,30
10,0.so-0-0-0.XL2.POR3.ALTER.NET,152.63.107.114,40,30,30,30,30,30,31
```

11,0.so-0-1-0.TL2.POR3.ALTER.NET,152.63.107.157,30,30,30,40,30,30,31
12,0.so-2-0-0.TL2.SAC1.ALTER.NET,152.63.8.2,50,50,40,40,40,40,40
13,0.so-7-0-0.XL2.SAC1.ALTER.NET,152.63.54.9,50,40,40,40,40,40,40
14,0.so-4-0-0.XR2.SAC1.ALTER.NET,152.63.54.6,40,40,40,40,50,50,40
15,184.ATM6-0.XR2.SJC1.ALTER.NET,152.63.50.74,50,51,50,50,50,50,50
16,192.ATM7-0.GW5.SJC1.ALTER.NET,152.63.54.21,60,51,50,50,50,50,50
17,digexoc12-gw.customer.alter.net,157.130.214.154,50,50,50,50,50,50,50
18,gsr-01-p2-0-a00a02.af.sjc5.digex.com,164.109.130.26,50,50,50,51,50,50,50
19,lc1.com,164.109.154.154,50,50,50,51,50,50,50

One column per hop, one row per sample
Host Information
1,,
2,loop1.bois-dsl-gw1.bois.uswest.net,216.161.136.254
3,100.fa2-0.bois-agw1.bois.uswest.net,207.108.229.29
4, ---------- ,207.108.224.247
5,sea-core-03.tamerica.net,205.171.208.5
6,sea-core-02.tamerica.net,205.171.26.57
7,POS1-2.GW5.SEA1.ALTER.NET,157.130.182.249
8,132.ATM2-0.XR2.SEA1.ALTER.NET,146.188.201.70
9,194.at-2-0-0.XR2.POR3.ALTER.NET,152.63.104.145
10,0.so-0-0-0.XL2.POR3.ALTER.NET,152.63.107.114
11,0.so-0-1-0.TL2.POR3.ALTER.NET,152.63.107.157
12,0.so-2-0-0.TL2.SAC1.ALTER.NET,152.63.8.2
13,0.so-7-0-0.XL2.SAC1.ALTER.NET,152.63.54.9
14,0.so-4-0-0.XR2.SAC1.ALTER.NET,152.63.54.6
15,184.ATM6-0.XR2.SJC1.ALTER.NET,152.63.50.74
16,192.ATM7-0.GW5.SJC1.ALTER.NET,152.63.54.21
17,digexoc12-gw.customer.alter.net,157.130.214.154
18,gsr-01-p2-0-a00a02.af.sjc5.digex.com,164.109.130.26
19,lc1.com,164.109.154.154

Sample Information
"9/11/2001 11:13:29 PM",N/A,10,30,20,30,30,30,30,30,40,30,50,50,40,50,60,50,50,50
"9/11/2001 11:13:30 PM",N/A,10,20,10,30,30,30,30,30,30,30,50,40,40,51,51,50,50,50
"9/11/2001 11:13:31 PM",N/A,10,10,20,30,30,30,30,30,30,30,40,40,40,50,50,50,50,50
"9/11/2001 11:13:32 PM",N/A,10,10,10,30,30,30,30,30,30,40,40,40,40,50,50,50,51,51
"9/11/2001 11:13:33 PM",N/A,10,10,20,30,30,31,30,30,30,30,40,40,50,50,50,50,50,50
"9/11/2001 11:13:34 PM",N/A,20,10,20,30,30,30,30,30,30,30,40,40,50,50,50,50,50,50
"9/11/2001 11:13:35 PM",N/A,10,10,10,30,30,30,30,30,31,31,40,40,40,50,50,50,50,50

/advanced options

Ping Plotter by design is a very customizable program. In the Advanced Options menu (Edit/Advanced Options) you can change many of Ping Plotter's characteristics (Packet Settings, Display Settings, etc.) to meet your varying needs and requirements. Each network is different, and Ping Plotter tries to accomodate these differences. Ping Plotter also allows you to specify many Command Line Arguments that allow you to automatically load trace data, ony run one Ping Plotter instance at a time, and many more options. In this section we'll explore the various advanced options Ping Plotter gives you to customize.

/advanced options - alerts

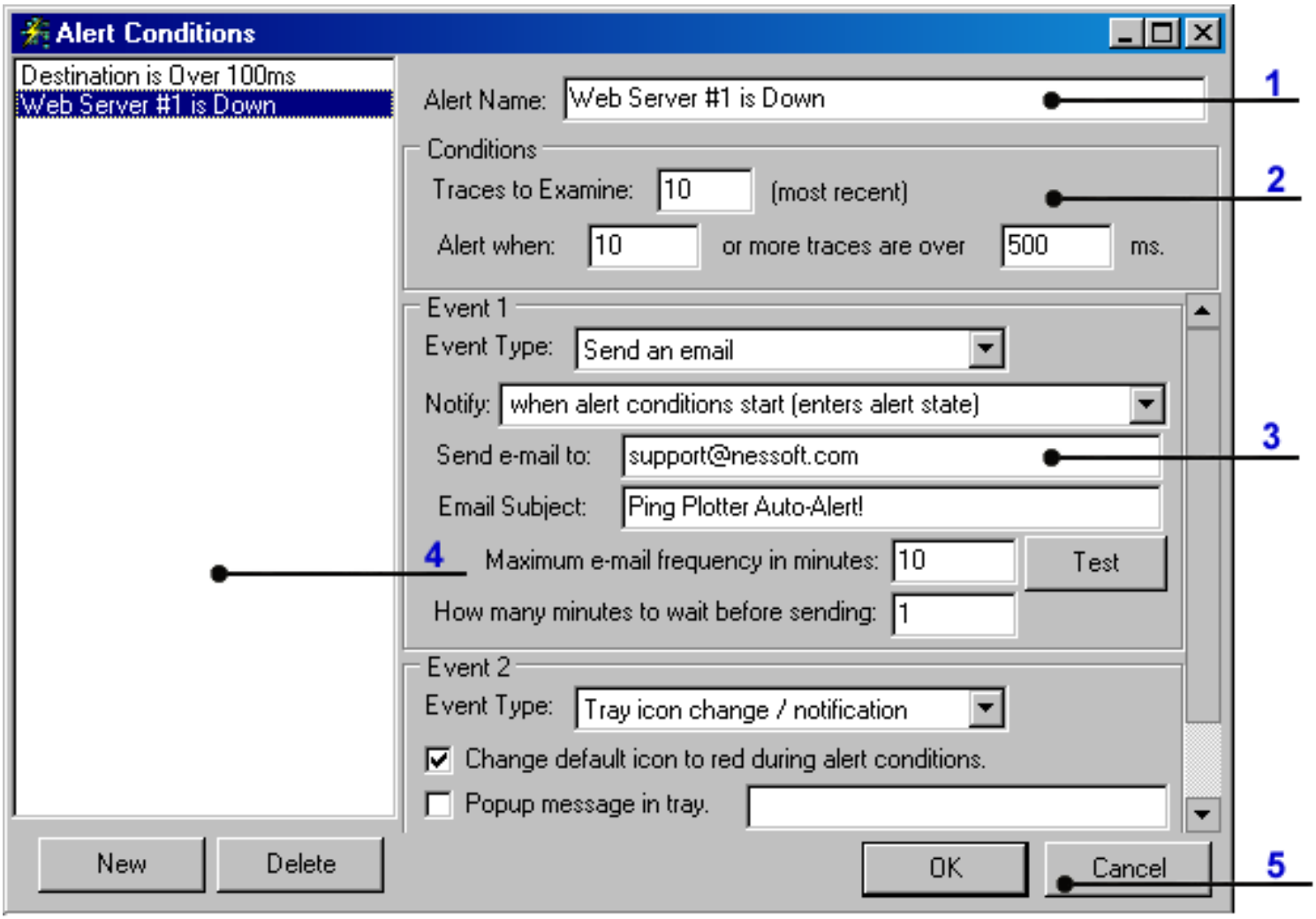
What is an alert? Alerts basically monitor the conditions of a specific IP address, and then do something when those conditions exceed a specific range. The things you can do with an alert are:

· Send an e-mail
· Play a sound (a .wav format file)
· Log to a text file
· Change the tray icon and/or show a message
· Launch an executable

For example, let's say you have a destination that you want to monitor so you know when it stops responding. You can attach an alert to that IP address that sends you an e-mail alert if the last 10 of 10 sample requests are lost.

Another possible alert condition to check for is if the average for the last 10 samples is > 500 (or any other number). You can send an e-mail alert, maybe play a .wav file (if you're usually within hearing distance) or both. Also, if you're trying to show your ISP there's a problem, you might log the data to a file so you have a record of every time the problem occured. One Ping Plotter user had hardware problems with his cable modem, and so he setup an alert that launched an executable that communicated with a device attached to his computer that reset his cable modem if certain conditions happened.

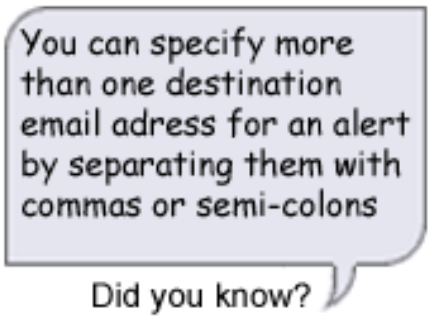
Alert setup can at first seem confusing. Basically it involves three steps:
1) Setting the Alert Name
2) Setting up the Condition that will trigger the alert
3) Specifying Event(s), or what you want Ping Plotter to do when your alerts are triggered.



To setup an alert you go to the "Edit/Alert Setup" menu. Once there, you'll see an image similar to the one to the left (Note: if you had never setup any alerts before then you wouldn't see any alerts listed in the list box on the far left of the screen). This screen is pretty busy, but also pretty self explanatory. From the screen capture to the left, you can see that we have:

1. The Alert Name. In this example we're using "Web Server #1 is Down".
2. The Conditions for the alert. In other words, what has to happen for this alert to fire.
3. The Event(s) for the alert, or put simply, what do you want Ping Plotter to do when the alert fires.
4. The list of alerts you currently have defined. You can see from the image that we've got two defined.
5. The New (alert) and Delete (alert) buttons, as well as the standard OK and Cancel buttons.

So, referring to the image, you can see we have an an alert with a Condition where when the last 10 samples are greater than 500ms we want Ping Plotter to e-mail us, and also change the tray icon to red (the Events). We've called this alert "Web Server #1 is Down". If you were



watching for a timeout, you'd enter 9999 instead of 500. Do note that 9999 is not a magic number. A lost packet is always greater than any number entered, so you can use 1000, or 20000 here and a dropped packet will exceed either of those numbers.

Setting up an Alert:

First of all, if you're going to setup a "Send an email" event, and you haven't done so already, you need to setup your e-mail options in the "Edit/e-mail Setup" screen. See the bottom of this page, or the e-mail Setup section of this tutorial on how to do this.

Ok, assuming we've got our e-mail setup done we:
1. Type in our alert name. In this case it's "Web Server #1 is Down".

2. Remember our Conditions (or when the alert will fire) we want for this alert are where when the last 10 samples are greater than 500ms. We enter 10 in the "Traces to Examine" box, because we want Ping Plotter to only use the last 10 samples it's done when deciding when to fire the alert. You could easily change this to, say, 2 so you're looking at two samples in a row or even increase this number. You've got a lot of flexibility here. We then enter 10 in the "Alert When:" box and 500 in the "or more traces are over" box.

3. Next we setup the Event(s), or what you want to happen when the alert fires. Remember that Ping Plotter allows you to specify five different types of events, each of which are explained in detail in their own sections of this tutorial. They are (note these are clickable links) launch an executable, log to a file, play a sound, send an e-mail and tray icon change. We're going to "Send an e-mail" (this is in the Event 1 area) as our first event. Notice that as soon as you change the "Event type" to "Send an e-mail", that "Event 2" will appear, with "(.. no additional notification ..)". You can have as many events as you like, and to delete an event just change it's type to "(.. no additional notification ..)". As soon as you pick an event type, a set of Notify options relating to that event type will come up. **Note:** We go into detail about the Notify properties in the alert events - conditions for triggering section of this tutorial. In addition to sending an e-mail, we want a second event in this alert that changes the tray icon to red (this is in the Event 2 area). Notice that if we wanted a balloon popup to appear in the tray we could also check that box and type in the text we wanted to appear.

Tying an alert to an IP

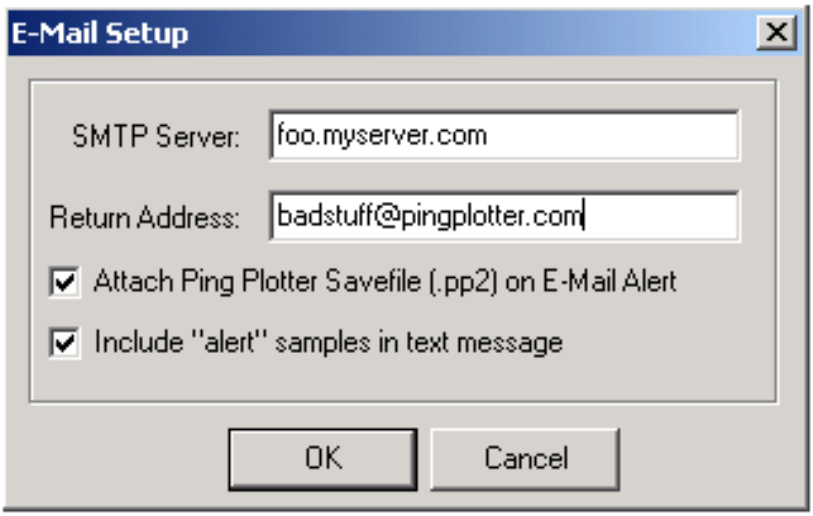
Once you've got your alert setup, you need to tell it which IPs to monitor for those conditions. To do this, trace to a destination just like you normally would. Once the path has listed, pick the router/destination from the trace graph that you want to monitor and right-click on the hop number. From the popup, select "Watch this host (Alerts)...". You'll get a dialog that shows the DNS name, if there is one, and the IP address you selected in the Title Bar of the window, and then a list of available and selected alerts. Move the alerts you want applied to this IP address into the "Selected Alert(s)" list by using the < and > buttons and then click the OK button. Monitoring will start immediately. If you want to monitor a destination that isn't responding for some reason, just right-click on the lower time-graph for that host to get the popup menu.

When a hop is being monitored for an alert, the hop number will have brackets around it (i.e.: [9]). You can stop monitoring by right-clicking on the hop number, selecting "Watch this host (Alerts)...", and then removing any alerts from the selected list.

E-mail Setup

If you want to set up an e-mail alert, you'll have to do your e-mail setup in this screen first, if you haven't already, by going into E-mail Setup from the Edit menu. This is a simple process where you just enter your SMTP server (i.e. outgoing e-mail server name) and e-mail address. This is important so Ping Plotter knows how to send messages. You can also specify whether you want Ping Plotter to attach a savefile when an e-mail alert is sent, and also whether you want to include the samples that triggered the alert in the e-mail message that is sent.

Below is what the setup screen would look like if you wanted to include the alert samples and attach a Ping Plotter save file, using SMTP server foo.myserver.com, with a return e-mail address of badstuff@pingplotter.com.



A note about "average" response times
Before version 2.30, Ping Plotter used to support alerting on average response times. The real problem with averages is when a server stops responding - what is the average of the last 10 samples if the last 10 were timeouts? Because of the problem with this, version 2.30 changed the alerts so you always have to do "when X or more samples is > Y". You can still get good alerts that work similar to how averages worked - by saying "when 5 or 10 samples exceeds 300 ms" (this would be like an average over 300ms, but would also fire when there were lost packets).

/alert events - launching an executable

New to Ping Plotter 2.40 is the capability to launch any executable (file, really) on alert. This gives you all kinds of capabilities to do cool things when network conditions go south.

While this event is called "Launch an executable", it can actually launch any file. It can launch documents, links, .mp3s, batch files, whatever – really anything with a file association that Windows will know what to do with. Of course, you have the option of when you want to launch the executable. See alert events - conditions for triggering section of the tutorial for these.

The following variables (below in blue) can be used. Note that these are always parsed, and there is no way to cause these to be passed as literals. If you need to have one of these strings as literals passed to an executable, then you'll need to set up an intermediate link, batch file, or something similar.

$host The monitored host – i.e.: the target that failed.
$dest The destination for Ping Plotter. This may, or may not be, the same as $host. It will match if you're monitoring the final destination, but won't match for intermediate hops.
$year Current 4 digit year (i.e.: 2003)
$month Current 2 digit month (i.e.: 03)
$day Current 2 digit day (i.e.: 08)
$date Date, 4-2-2 format (i.e.: 2003-03-08) for March 8th.
$hour 24 hour format, (i.e.: 06)
$minute 2 digit minute, (i.e.: 02)

Bear in mind that the launching program isn't closed, it's just launched. You'll need to configure your setup to close whatever you need here.

/alert events - logging to a file

The "Log to file" event writes data to a text file whenever alert conditions are met.

With the "log to a file" event you have an added option specific to this event called "Log times for entire route?".
This option specifies if you want to write data to the text file just for the monitored host, or the entire route. Leaving this off means that for each time alert conditions are met, one data item will be written to the file – for the monitored host. If this switch is turned on, then data for the entire route will be written.

The Filename box.
The filename is *required* to have the $host variable in it. If it is missing, then the file will be nonsensical if you attach this alert to more than one host. The following variables (below in blue) can be used as part of the filename. Note there is no way to "escape" the following sequences, so these are always parsed, and can't be specified as literals in the filename.

$host The monitored host – i.e.: the target that failed.
$dest The destination for Ping Plotter. This may or may not be the same as $host – it will match if you're monitoring the final destination, but won't match for intermediate hops.
$year Current 4 digit year (i.e.: 2003)
$month Current 2 digit month (i.e.: 03)
$day Current 2 digit day (i.e.: 08)
$date Date, 4-2-2 format (i.e.: 2003-03-08) for March 8th.
$hour 24 hour format, (i.e.: 06)
$minute 2 digit minute, (i.e.: 02)

Note that one directory level of depth will be created automatically, if it doesn't already exist, so you can specify c:\ppdata\$host\filename.txt, and the $host directory will be created as needed. Only one directory of depth will be created, however, so if the c:\ppdata directory didn't already exist, an error will occur.

/alert events - playing a sound

One of the most simple event types is to play a sound (i.e.: .wav file) of some kind.

This event can happen based on the standard notification rules, and can play anything that Windows multimedia sound function wants to play. If you want to launch a sound file that this event type doesn't support, use the "Launch an executable" option instead, as it will launch any file, including sound files.

Click the folder on the right side of the file name to browse for a file. When browsing for files, you can right-click on any sound file to play it (this is an operating system feature, and may not be supported on all operating systems).

Enter "BEEP" (no quotes) here if you just want to beep the computer speaker instead of playing through the sound card.

/alert events - sending an email

A very popular event type is the "Send Email" event.

Before you can create an event to send an email, you must configure your SMTP server and return email address in the Edit/E-mail Setup menu option. Note that your SMTP server must be accessible on the network to be able to send emails, so it's possible in the case of a network failure that Ping Plotter may not be able to email you. Ping Plotter will continue to try to send emails once a minute until it is able to get an email out.

Emails are a bit more complicated to set up than most Event types, as it is dependant on your SMTP server, and you don't want to be overwhelmed with emails when conditions are bad, but you *do* want to know what's going on.

You can fire e-mail alerts based on the standard Ping Plotter notification types.

For the Send an email event you have the following options:

Send e-mail to:
This can be an individual email address, or a list of addresses separated by either a , or a ; (both work equally well). Please do not set this up to be someone at your ISP unless they have agreed that they want to see this information. A huge portion of getting problems solved is playing the game right, and overwhelming people with automated emails is almost certainly going to work against you.

Email Subject:
This defaults to "Ping Plotter Auto-Alert!", but can be customized with a variety of variables / text. The following list of variables applies (below in blue):

$host The monitored host – i.e.: the target that failed.
$year Current 4 digit year (i.e.: 2003)
$month Current 2 digit month (i.e.: 03)
$day Current 2 digit day (i.e.: 08)
$date Date, 4-2-2 format (i.e.: 2003-03-08) for March 8th.
$hour 24 hour format, (i.e.: 06)
$minute 2 digit minute (i.e.: 02)

For emails, the $host makes a huge amount of sense (i.e.: $host is down!), while the time/date options aren't as useful because the email contains data about this in most cases.

Maximum email frequency and minutes to wait:

The next two settings control the frequency at which you'll get e-mails during alert conditions.
1. "Maximum e-mail frequency" is pretty self-explanatory, you'll only get e-mails that often.
2. "How long to wait for worse conditions" specifies how long Ping Plotter will wait after its first alert condition to send an e-mail. This option allows you to wait a few minutes to find out if it was a temporary or more permanent alert condition. You may not want one immediately because you'll want to wait a bit for more information to be included. For instance, you may want to wait 5 minutes or so before that first e-mail gets sent off.

Testing and error messages

Once you have your e-mail set up, use the "test" button to see what the message will look like (and also to make sure all the settings are working). Any errors should be displayed here.

Many of the errors that occur during testing can be attributed to incorrect email setup, so go there first and validate your settings. An 11004 Winsock error usually happens because of an invalid SMTP server, for example.

/alert events - tray icon change

This is a great event to add to most of your alerts. It's helpful to be able to see if there's an alert condition under way, and a quick glance at the tray can let you know by using this event.

The Tray Icon Change event can do one (or both) of the following:

Change default icon to red during alert conditions:
If you already have Ping Plotter showing in the tray, this will change the existing green icon and add red to indicate that an alert has fired. If you don't have Ping Plotter in the tray already, then a red icon will be added to the tray. When the alert condition(s) are over, the icon will change back to green.

Popup message in tray:

This shows a "balloon" message coming out of the tray (see image). Not all versions of Windows support this message (ie: some versions of Windows 95), in which case no balloon will show. Only one balloon can be shown at a time, so the newest balloon always wins (a new balloon message will replace an older one).

The following commands can be used in your message text (below in blue):

$host The monitored host – i.e.: the target that failed.
$year Current 4 digit year (i.e.: 2003)
$month Current 2 digit month (i.e.: 03)
$day Current 2 digit day (i.e.: 08)
$date Date, 4-2-2 format (i.e.: 2003-03-08) for March 8th.
$hour 24 hour format, (i.e.: 06)
$minute 2 digit minute, (i.e.: 02)

Alert on "$host, $date $hour:$minute"
This is a great message because it stays up until you acknowledge it, so when you come back to a PC, you can see what alert fired, what host it happened on, and what time it *last* happened. This may be over a weekend, but the message will still be there telling you that an alert happened

/alert events - event notifications/conditions for triggering

Many of the events share a notification mechanism. Here is a list of the types. Note that any alert can have multiple events of the same type, so you can set up a single alert to do something at any one, or all, of these times.

Each time alert conditions are met (repeating)

The event will happen every time conditions are met. This means the event will happen over and over again on each sample that causes the alert to fire. In previous versions, this was the only supported notification type.

When alert conditions start (enters alert state)

The first time alert conditions occur, the event will happen. As long as the conditions continue, though, the event won't be repeated. This is a popular notification because you find out about new conditions when they happen, but don't have to be bothered again.

When alert conditions end (leaves alert state)

This happens when network conditions improve so that the alert is no longer firing. As soon as the conditions move from bad to good (based on your settings), then this event will happen. A use of this is to have Ping Plotter e-mail you each time conditions go bad (see above), and then when they improve again, but not to tell you anything in between.

Each time alert conditions are *not* met

This is the exact opposite of the first notification type above. As long as things are good on the network, this event will fire each time a sample is collected.

/alerts - troubleshooting alerts

If alerts aren't working, there are a number of things you can do to troubleshoot. Here are some specific suggestions and we also recommend you checkout the Alerts - Setup section of this tutorial.

Make sure you're "Watching" a host with the alert.

By far, the most common reason that an alert isn't working is because it isn't tied to an IP address. An alert won't just start working automatically, you need to tell it which host (s) you want that alert to watch.

To attach an alert to an IP, trace to the host you're interested in, then, right-click on the hop you want to monitor and select "Watch this host (Alerts)..." from the menu. In previous versions of Ping Plotter, this was called "Monitoring".

Note that if you're tracing to a destination that doesn't respond, and you want to watch that destination (even though it's not on the upper graph), just right-click on the time-graph on the bottom and this same menu item should be on that menu.

From here, you can move an alert from the "Available" to the "Selected" list. Any alerts on the "Selected" list will watch this host whenever this host is involved in any route (be it an intermediate host, or the final destination).
When a host is being watched by the alert system, there will be brackets around the hop number in the upper graph. If those brackets aren't showing, then that host isn't being watched. This should put a [...] around the hop that's being monitored.

Set up an alert that will fire instantly, with an event that is very evident.

If you have an alert set up, and tied to a host (see above), but it seems like the alert isn't working, then changing your alert parameters (or create a new "test" alert) can be helpful.

Set up "Traces to Examine:" to 10. Alert when "1" or more traces are over 1ms.
Unless your network is responding in 1ms or less, this alert will fire on the first collected sample with the alert enabled.
For an event type, use "Play a sound", or "Tray icon change/notification" as both of these events happen immediately with no wait. In addition, for the "Play a sound", use "each time alert conditions are met (repeating)", as this will continuously make sound, rather than just when conditions start / stop.

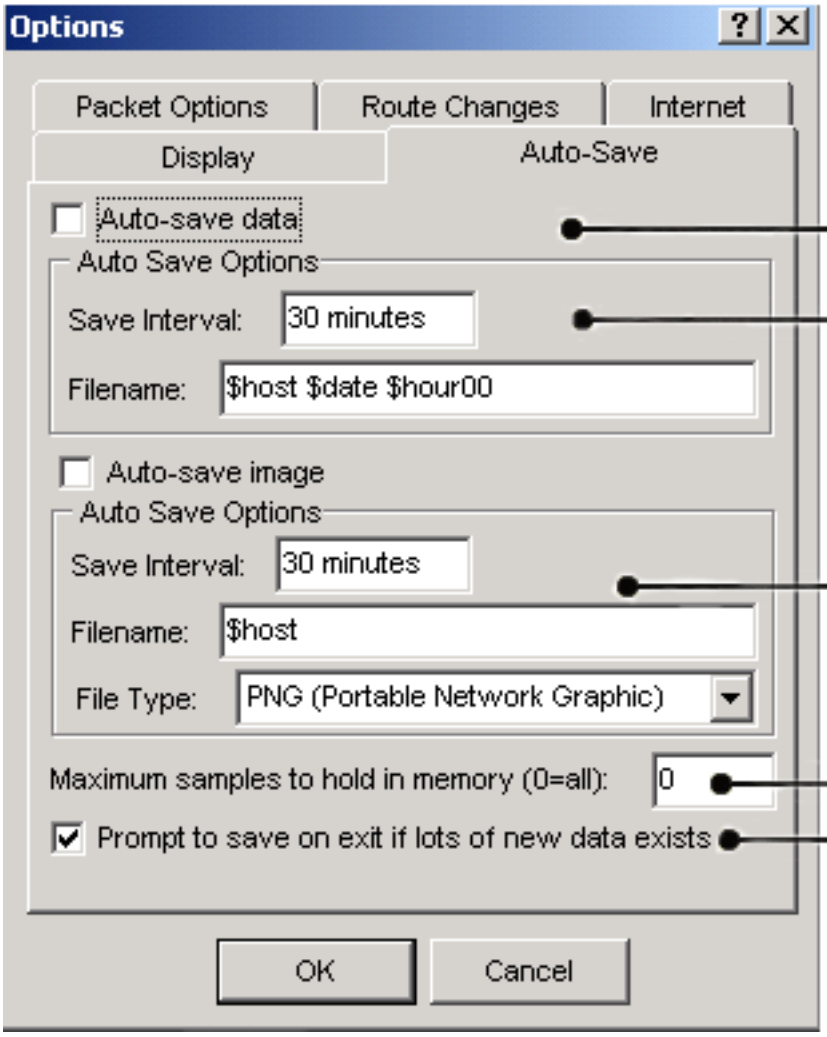
Using this sequence, you should be able to tie an alert to just about any host and have

the alert conditions fire immediately. Now, add on another event type (ie: email).

You can leave multiple events tied to a single alert. That way you can continue to hear the sound while you're troubleshooting another event type.

/advanced options - auto save

Ping Plotter can be set to automatically create a .PP2 save file at a specified interval. This can be coupled with "Maximum samples to hold in memory" to minimize the amount of memory used on long monitoring projects. Ping Plotter can also be setup to create an image of the current data, as seen on the graphs. Using this, you could auto-save for a time period, then create some kind of "album" to post for proof of a problem. The save interval must have elapsed before the first save happens. This is so short-term tests don't automatically create images.



1. Toggle on/off the auto-saving of data.

2. In the auto-save data section you can set the save interval, to tell Ping Plotter how often to save the data, and what filename to save the data to. If the file already exists, it will be overwritten. This means you can combine a pretty fast save interval, coupled with a generic file name (ie: $host), and save your data often without creating a lot of extra files. The file name defaults to the current path. The following variables can be used in the name:
$host - Host name (or IP address)
$year - Current Year
$month - Current Month
$day - Current day of month
$hour - Current hour
$minute - Current minute
$date - Same as $year-$month-$day

3. In the auto-save image section you can set the save interval, to tell Ping Plotter how often to save the images, what filename to save the data to and what type of image format to save the graph in (BMP, GIF or PNG - PNG being what we recommend though it's not as universally supported). Just like the auto-saving of data, the file name defaults to the current path and if the file already exists it will be overwritten. The same variables used for the data saves are also used for the file name here:
$host - Host name (or IP address)

$year - Current Year
$month - Current Month
$day - Current day of month
$hour - Current hour
$minute - Current minute
$date - Same as $year-$month-$day

A note about valid characters in filenames: Using colons (:), quotes, slashes or backslashes are not valid in the file names for save files or images. Because these characters are invalid for use in file names at the operating system level, we can't create files with those! Keep especially close attention to this when creating files with times in them - as we all naturally want to use a colon to separate the hours and minutes, but the Windows files system doesn't allow this.

4. This is the maximum number of samples that will be held in memory at any one time. Older samples are purged from memory. This can be coupled with auto-saving of data to keep your memory images small, but still have access to all the data collected.
Ping Plotter averages about 44 bytes per sample (this can be more or less, but this is the memory for a 20 hop route), so 20,000 samples is still less than 1 megabyte of memory.

5. Toggle on or off to have Ping Plotter prompt you to save your data when exiting the program. Ping Plotter will only prompt you if there is at least 75 new samples in memory since the last save.

/advanced options - command line arguments

You can have Ping Plotter do a few things automatically on startup by specifying command line arguments. You can put these arguments in a shortcut - or enter them from a DOS command line window.

The format to use is:
PingPlotter [File to Load] [/TRACE:[Address To Trace]] [/SAVE]

Loading a file at startup
If you enter a argument without a / on it, PingPlotter will try and find a file by this name and will load it if found.

Example:
pingplotter www.pingplotter.com.pp2

/TRACE
This argument will start tracing automatically when PingPlotter loads. If you use this with the argument to load a save file on startup, then tracing will begin to this address. Otherwise, add a colon (:) and the IP Address or server name you want to trace to.

Example:
pingplotter www.pingplotter.com.pp2 /TRACE
or
pingplotter /TRACE:www.pingplotter.com

/SAVE
This option can only be used when you specify a file name on the command line. If you use /SAVE, then any new traces (to the original address specified in the save file only) will be saved to that file on shutdown automatically without asking you if you want to save.

Example:
pingplotter www.pingplotter.com.pp2 /TRACE /SAVE

/SINGLEINSTANCE
If Ping Plotter is ran with this argument it checks to see if another copy of the program is running. If it is running, then it exits.

Also, if you passed in an address to trace (via the /TRACE:address option above), then this address will be passed to the currently running version. The currently running one

will start tracing to that address.

Example:
pingplotter /SINGLEINSTANCE /TRACE:www.pingplotter.com

/INIFILE
You may want to start Ping Plotter with a different set of parameters and setups. This is particularly useful if you're auto-starting Ping Plotter and having it trace automatically. In this situation, you may want to have different trace intervals, or graph times, etc. Starting Ping Plotter with an alternate INI file allows you to save multiple setups and use these different setups as needed.

Example:
pingplotter /INIFILE:alternatesetup.ini

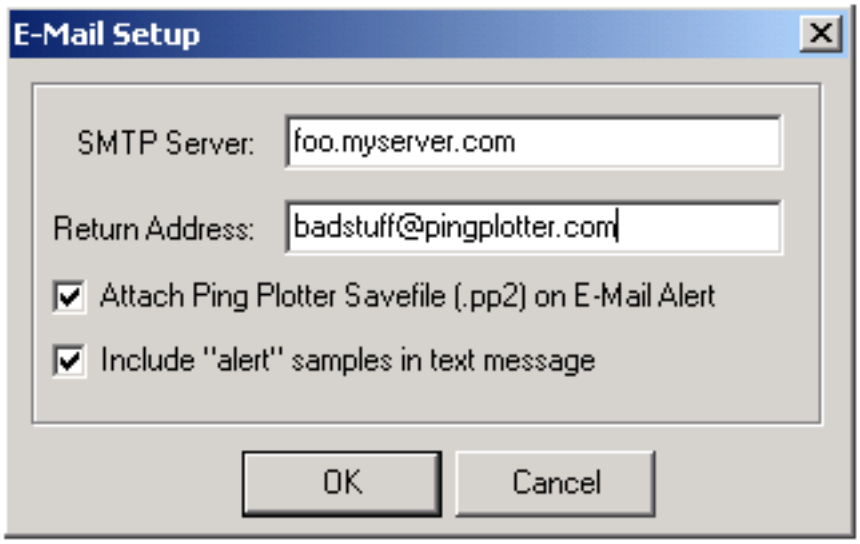
/?
Show the command line argument section of the online help.

Example:
PingPlotter ?

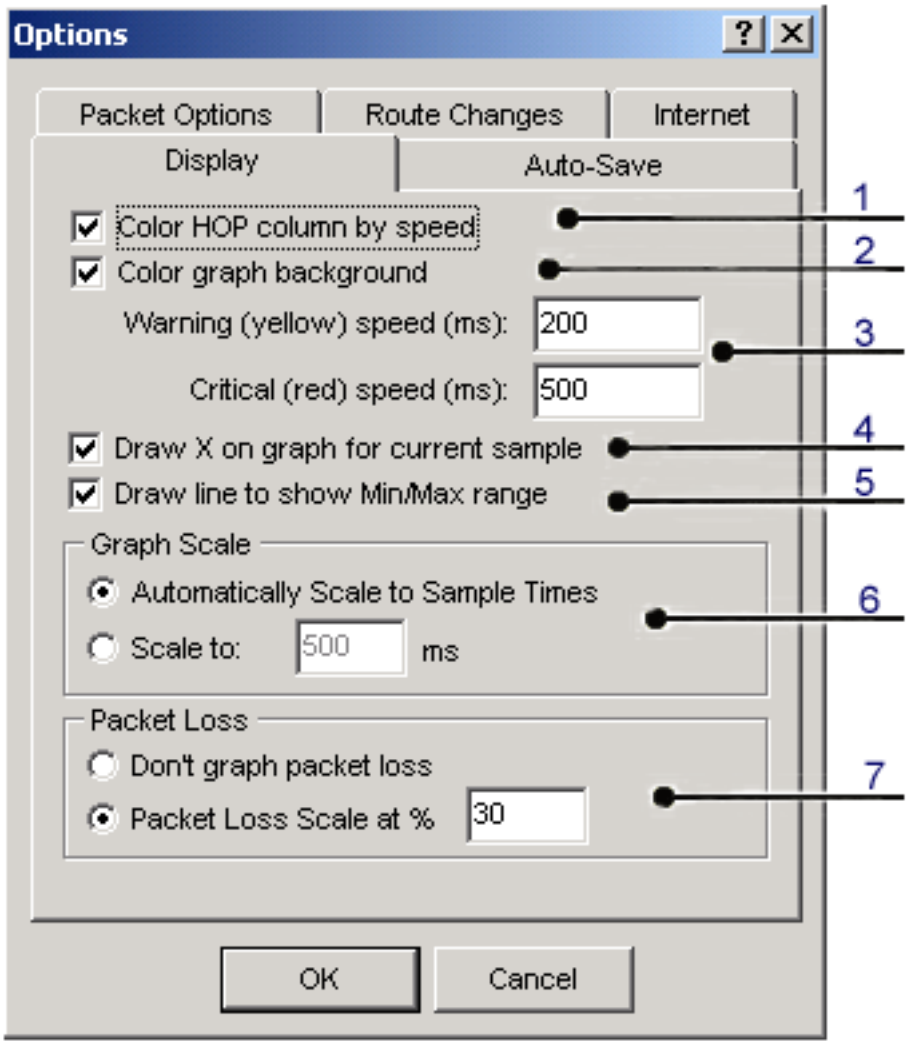
/advanced options - email setup

If you want to set up an e-mail alert, you'll have to do your e-mail setup in this screen first, if you haven't already, by going into Email Setup from the Edit menu. This is a simple process where you just enter your SMTP server (i.e. outgoing email server name) and e-mail address. This is important so Ping Plotter knows how to send messages. You can also specify whether you want Ping Plotter to attach a savefile when an e-mail alert is sent, and also whether you want to include the samples that triggered the alert in the email message that is sent.

Below is what the setup screen would look like if you wanted to include the alert samples and attach a Ping Plotter save file, using SMTP server foo.myserver.com with a return email address of badstuff@pingplotter.com.



/advanced options - display settings



1. This option can probably be left on all the time - it marks whether or not the colors green, yellow and red are painted onto the background of the HOP column on the trace graph. The colors used should work fine on even a 16 color screen. If you want a "Copy as Image" to show up without color, turn this off.

2. The background of the graph uses colors that don't display well unless your video drivers are set for more than 256 colors. Turn off this option if you're having problems seeing the graph, i.e. it has little speckled dots instead of a solid color.

3. These boxes control the point at which the colors change. By default, all response times 200 ms and below will paint green, from 201 to 500 will paint yellow and over 500 will paint red. These numbers apply to both the HOP column and the graph background. In addition, the legend on the graph screen will be updated with this number.

You'll probably want to change the numbers based on your internet connection speed. If you've got a T1, a cable modem or DSL, the listed numbers are probably pretty good, though you might move them down a little if you're tracing to a fast site. If you're using a dial-up via modem, you probably want to crank these numbers up a bit.
A reasonable number for a modem would be 350 for Warning and 600 for Critical. You might want to play around a little with these, though.

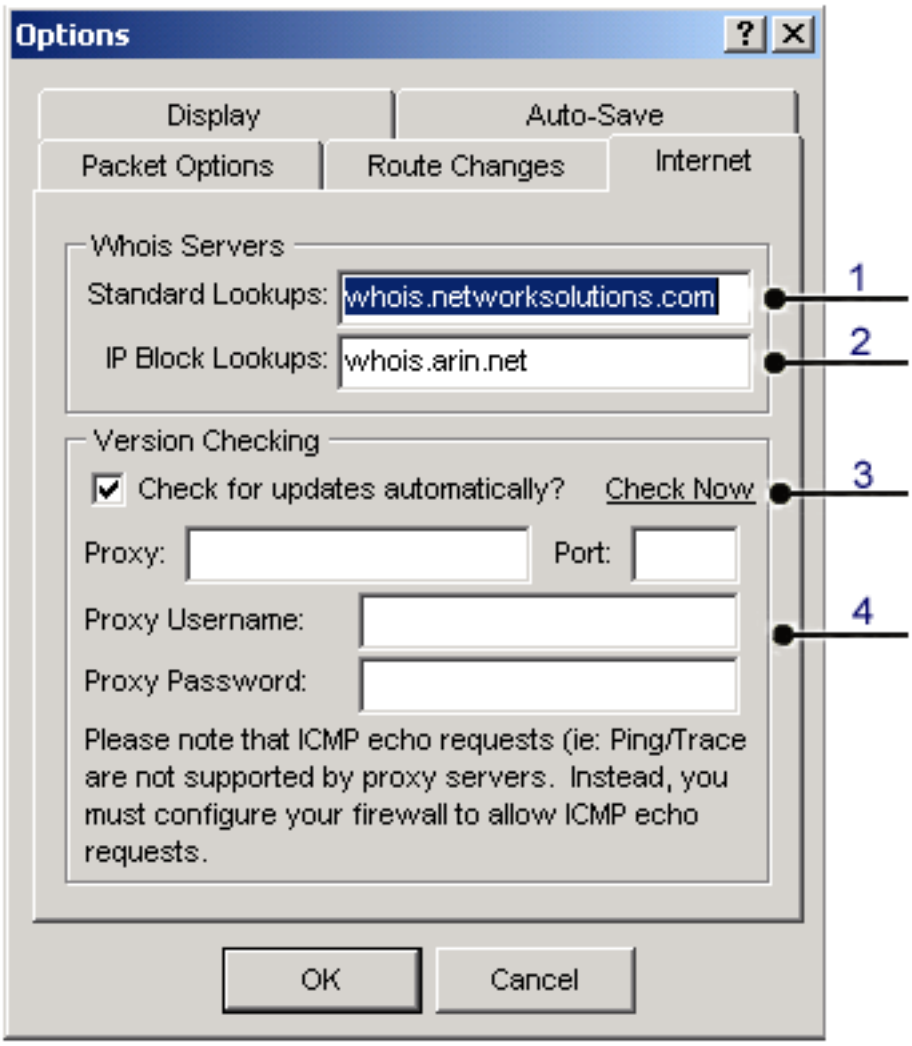
4. To watch "trending", it's sometimes nice to see what the most recent sample is. This option will enable that. A little blue X will be drawn on the graph that represents the most recent sample. You might want to turn this off when submitting an image to an ISP, so as not to confuse them or add anything they can question.

5. Show the Min/Max Line. Hide this line to keep the scale of the upper graph in better range. Also, like option four above, you may want to turn this off if submitting an image to an ISP, etc.

6. By default, Ping Plotter will automatically adjust the graph scale to fit the data you're collecting. Sometimes, if one of the hops in your trace has really bad performance, this can cause the graph to become almost unreadable. If this happens, you can fix the scale of the graph so it doesn't change. Both the trace graph, and the time-line graph, are fixed by this number when set.

7. Show/Hide the packet loss percentage in the upper and lower graphs.

/advanced options - internet settings



1. The Standard Lookups address is the WHOIS server to query for named lookups. The default value in 2.30 is whois.networksolutions.com.

2. The IP Block Lookups address is the WHOIS server to query for IP block lookups. This will look up who owns a particular IP address. The default for this is whois.arin.net.

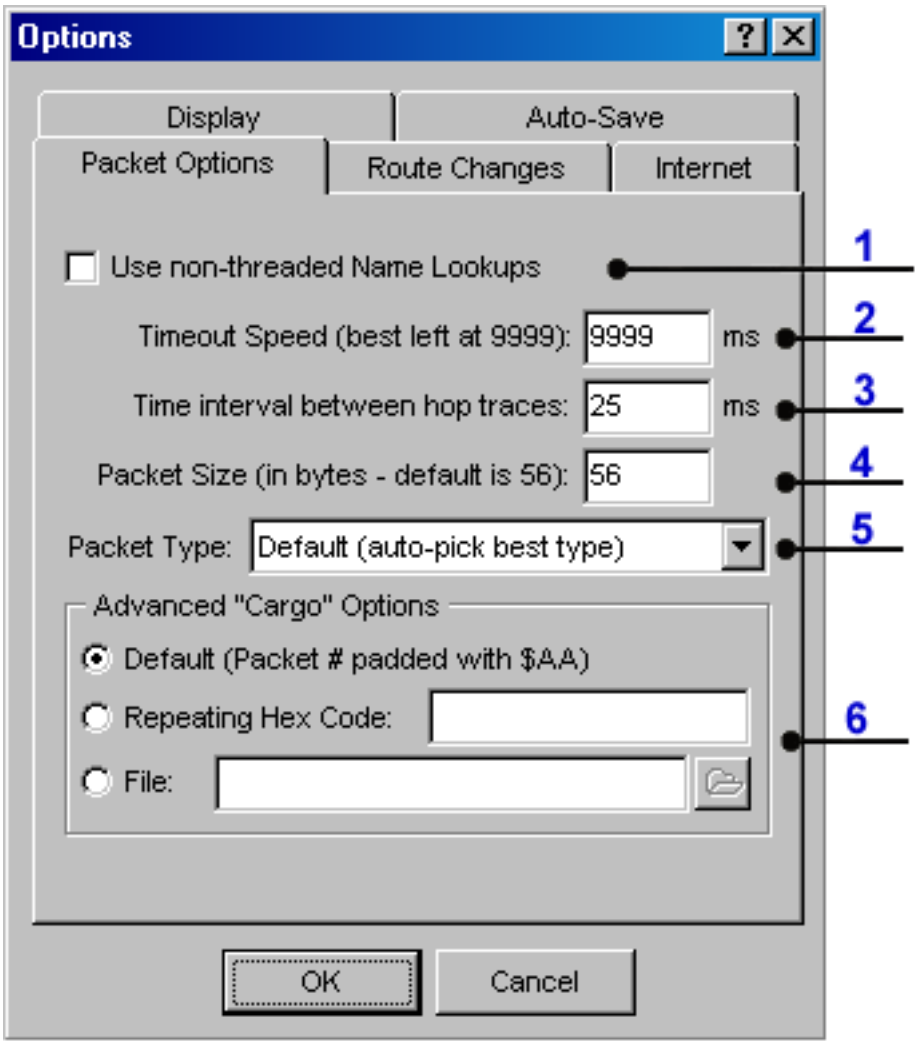
To see how to add additional whois servers click here.

3. Check this option to have Ping Plotter occasionally look on the pingplotter.com servers to see if there's a new version available. If there is an update available, **the main window's status bar** will show the update message. Double-clicking on the status bar will launch your web browser to the site where the new version is available. If you want to check for a new version immediately, click on Check Now. Again, if there's an update

available Ping Plotter will show "Update Available" in the main window's status bar.

4. If you access the internet through a proxy server, you can set up this server here. In the current version of Ping Plotter, this is not required. Ping Plotter doesn't have any features that require the ability to access the internet via HTTP. Automatic version checking (if turned on in option 3 above) doesn't work if Ping Plotter can't access the internet via HTTP, however. Do not confuse this setting with having to open up a firewall, if the computer you're tracing from is sitting behind one, to allow ICMP echo requests. ICMP echo requests are not supported by proxy servers.

/advanced options - packet settings



1. NT 3.51 in particular doesn't like to have multiple IP addresses resolved into names at the same time. NT 4.0 and Windows 95/98/2000 work fine with this check mark turned off and performance is best with this turned off.
When this switch is on, Ping Plotter still uses multiple threads to do tracing, but the looking up of names is done one at a time. When installing onto a machine running NT 3.51, this option is turned on by default.
A symptom of having this switch off under NT 3.51 is that Ping Plotter stays in memory even after you close Ping Plotter and when you close Windows NT it notifies you that Ping Plotter is still running. If you run into this problem, turn this switch on.

2. This option allows you to fine-tune your performance a little. By default, Ping Plotter will wait for 10 seconds for any packet to return. If the packet doesn't return in 10 seconds, then it is counted as a lost packet. If patience isn't one of your virtues, you can turn this down somewhat. No matter what your value is here, timed out packets will

show an "ERR".

Because of the performance enhancements offered by Ping Plotter, it's unlikely that this option needs to be changed. If it's set too low, it can cause misleading data to be generated. For best results, leave this at 9999.

3. This can be an interesting number to manipulate. It's really meant for advanced users, so you don't *need* to change it.

For the most part, Ping Plotter sends out multiple packets at the same time and times everything at once. More precisely, however, it leaves a tiny interval between each packet so you don't completely saturate your bandwidth when it sends out 30 packets. This time interval is adjusted by this parameter. Most of the time, 25ms is good. This falls within the realm of what a 28.8 modem can perform. If you've adjusted your packet size, or your connection to the internet is really slow, you might want to crank this number up a little. If you have just oodles of bandwidth, you can crank it down a little. Be aware that too small of a number here can adversely affect your data.

4. This adjusts the size of the packet that Ping Plotter sends out to the host. Sometimes routers in the path can be adversely affected by packet size. You can play with the packet size if you suspect that one of the routers is incorrectly configured, or is likely to have problems with larger (or smaller) packets.

Having this number too high will HUGELY affect your performance. It's best to leave this pretty small. Valid ranges are from 10-512 bytes. Actually, anything up to 32K will be accepted, but using a packet size over 512 bytes is just asking for trouble.

Note that setting this too high can cause the final hop in the trace to appear to be responding poorly. This is because all hops before the final one are timing out and returning a small "Timeout" packet, but the final destination will be returning the full data that was sent. Keep this number small for the most consistent response times.

Conversely, if you want to load your connection down a bit, crank this number up. You may get some "interesting" results.

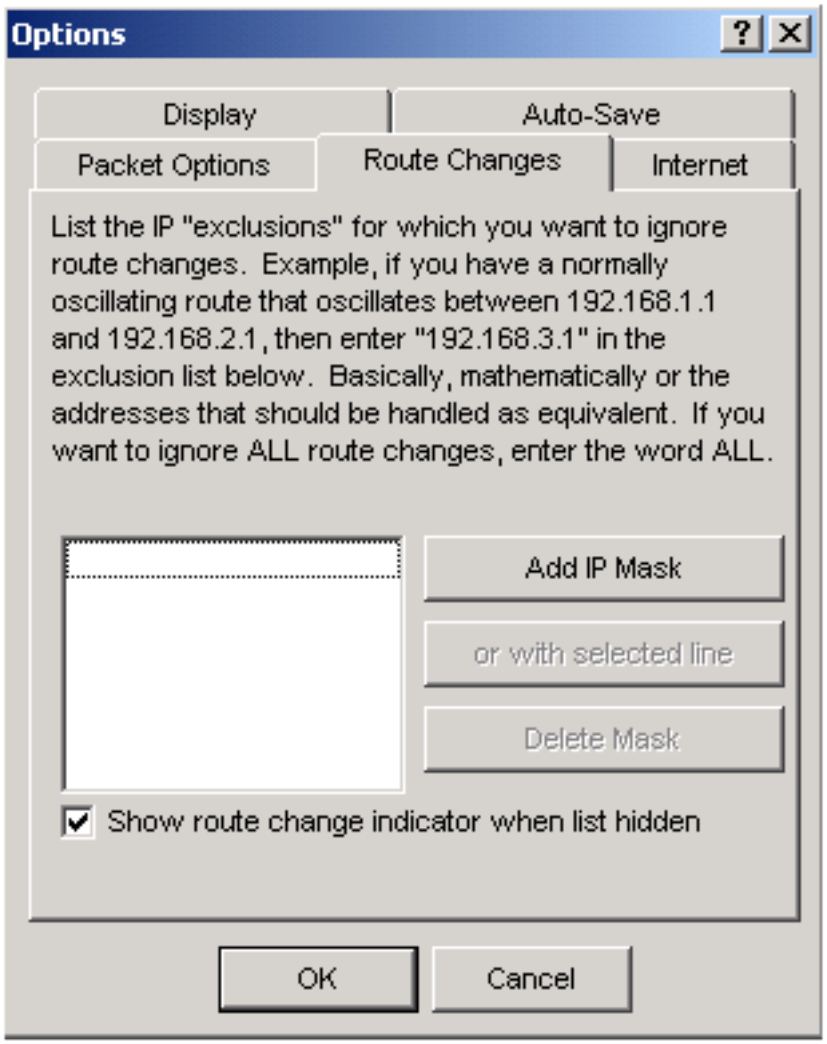
5. There are three separate (but somewhat similar) packet types that Ping Plotter can use.
• Windows ICMP.DLL. The best method is the standard Windows ICMP.DLL. This is the most reliable with the least CPU usage (on most operating systems), but is only accurate to 10 ms on Windows NT and 2000 (95, 98, ME and XP are all accurate to 1ms with this method).
• ICMP.DLL (Windows 2000/NT only). On Windows NT/2000, Ping Plotter can use its own timing mechanisms to increase accuracy beyond 10 ms. This can take a bit more CPU and causes *major* problems on the 9x line of operating systems (95/98/ME).
• Raw Sockets (advanced use only). In some rare cases, the standard Windows method

doesn't work. Ping Plotter can compose its own ICMP packets, although in most cases this is no more reliable or better than ICMP.DLL.

Default (auto-pick best type) will automatically pick between the first two methods above, based on the operating system being run. This makes the right choice up to and including Windows XP, but doesn't know about any operating systems newer than this.

6. This is an advanced option that should probably not be changed. This is used to diagnose network problems when specific *data* is sent, which is a highly unlikely problem for most networks.
By default, Ping Plotter pads the outgoing packet with repeating $AA. If you suspect that your network may be having problems when you send specific byte codes, you can enter the hex code that you want repeated, or a link to a file to read the byte string from. The cargo space for the packet will be padded with this data. Use this in conjunction with the packet size to create the network scenario you're looking to duplicate.

/advanced options - route changes settings



By default, any route change is recorded and noted by Ping Plotter. In some cases, this may not be desired behavior. An example of this is if something in your regular trace route oscillates between 2 (or more) routers based on load.
If you're seeing route oscillation (where a specific hop regularly changes between 2 or 3 different IP addresses, but the rest of the route doesn't change), then you can add a mask to this list to suppress route change notifications when this happens.
To do this, click on Add IP Mask, and then enter the first IP address. Once it's in the list, select it, and then click on or with selected line (Or with XXX.XXX.XXX.XXX). In the popup, enter the next IP address of the oscillating set. Repeat this if there's a third one (or more).

Normally, the route change window is hidden on the main screen. If this is the case, then a red notification will pop up whenever there is a route change which you can then click

on to show the route change window.
If you're getting a lot of route thrashing that you don't want to know about, you can turn off this indicator by unchecking the show route change indicator when list hidden option. This is option is on by default.

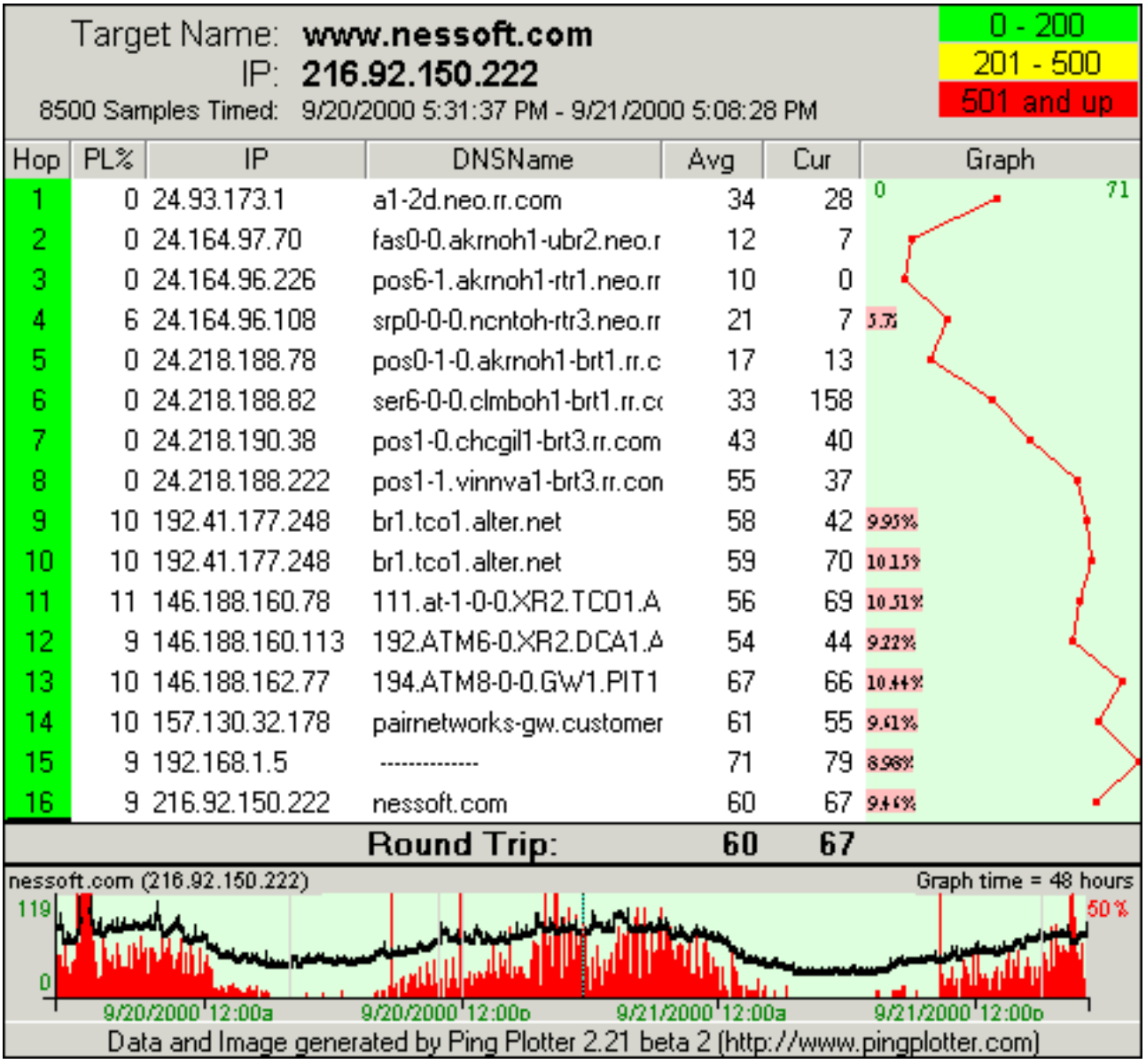
/interpreting results - introduction

In this section we get into some specific examples of how to interpret the data you get from Ping Plotter. Please bear in mind that these are our interprations and best guesses as to what's happening in these examples. You may have different interpretations, or just flat out disagree. If so, we welcome your comments.

/interpreting results - a quick example

So let's get into some specific examples of how to interpret the results from Ping Plotter.

For the first example, you're getting intermittent packet loss to nessoft.com. What can we determine from the graph below?



First off, the final destination shows 9% packet loss - there's a problem someplace in the route, but we need to determine where....

Hop 4 shows 6% packet loss. Hop 5 doesn't show packet loss, though, so you know that the problem in hop 16 isn't because of hop 4 - it's likely just a router using a different CPU path for TTL=0 packets than it does for routing data through.

Hop 9, however, shows 10% packet loss - and this packet loss is carried on through to

the final destination, so this is a huge, huge indication of where the problem lies.

Now, all we know from this is that the problem happens after hop 8 - we don't know if it actually happens becuase of CPU overloading in hop 9, a router problem in hop 9 (or even on the exit side of hop 8), or if it's the connection between hop 8 and 9. A little bit more troubleshooting is needed for this.

Digging deeper, we can see (from the domain names) that hop 8 is in the rr.com domain, while hop 9 is in the alter.net domain. Also, the IP addresses show decidedly different ranges. This is a strong clue that it's actually the connection between hop 8 and 9 that's causing the problem - likely that there's not enough bandwidth between those two locations.

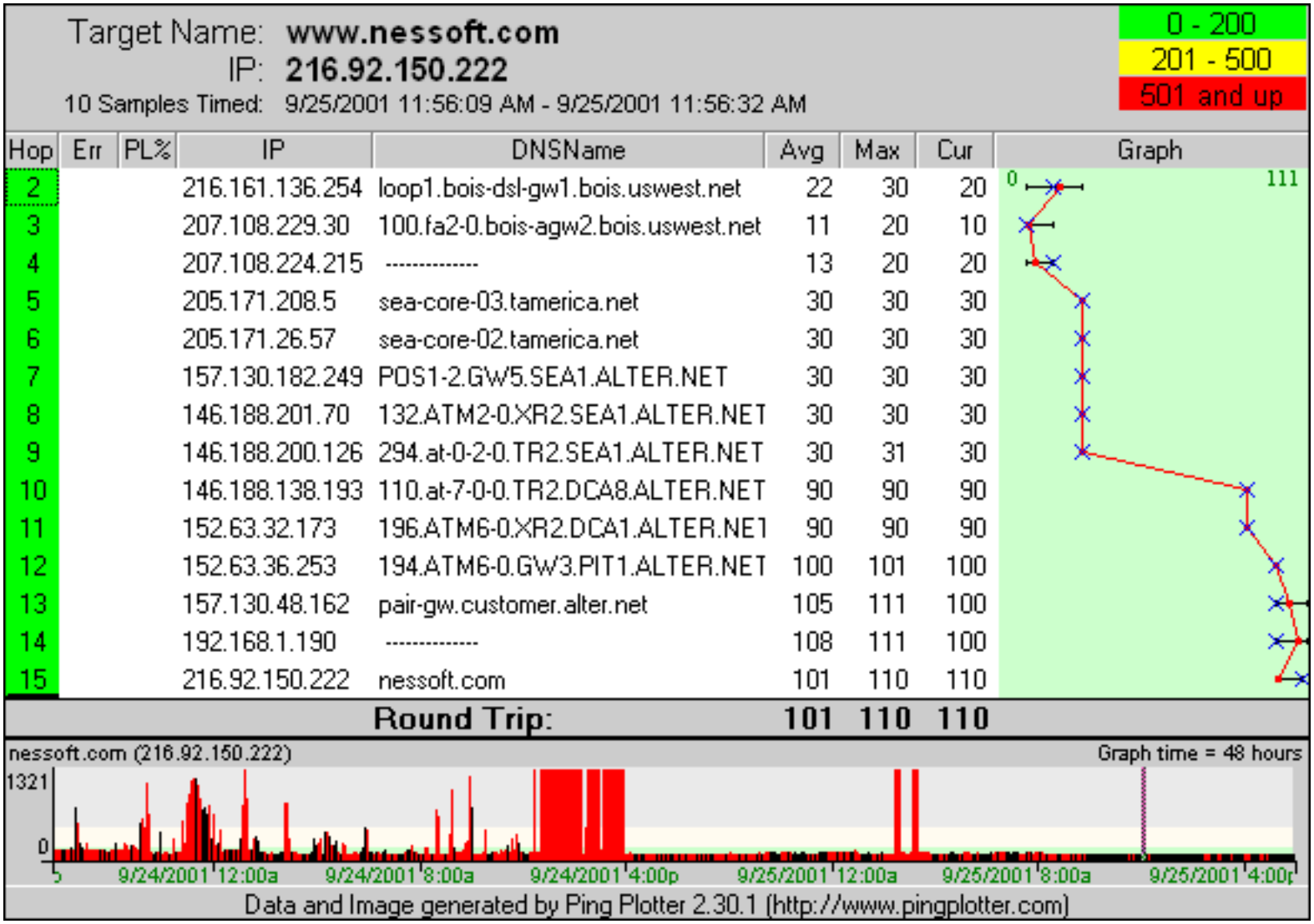
/interpreting results - beating up on your ISP

For this example, we're assuming the role of a user that's having problems with a broadband connection. What we'll be taking a look at is snapshots of six continuous days worth of trace data. One thing to keep in mind is that if you're doing long term monitoring and want to look at more than the largest default time span on the time-interval graph (48 hours), you can add custom time intervals in the pingplotter.ini file located in Ping Plotter's installation directory.

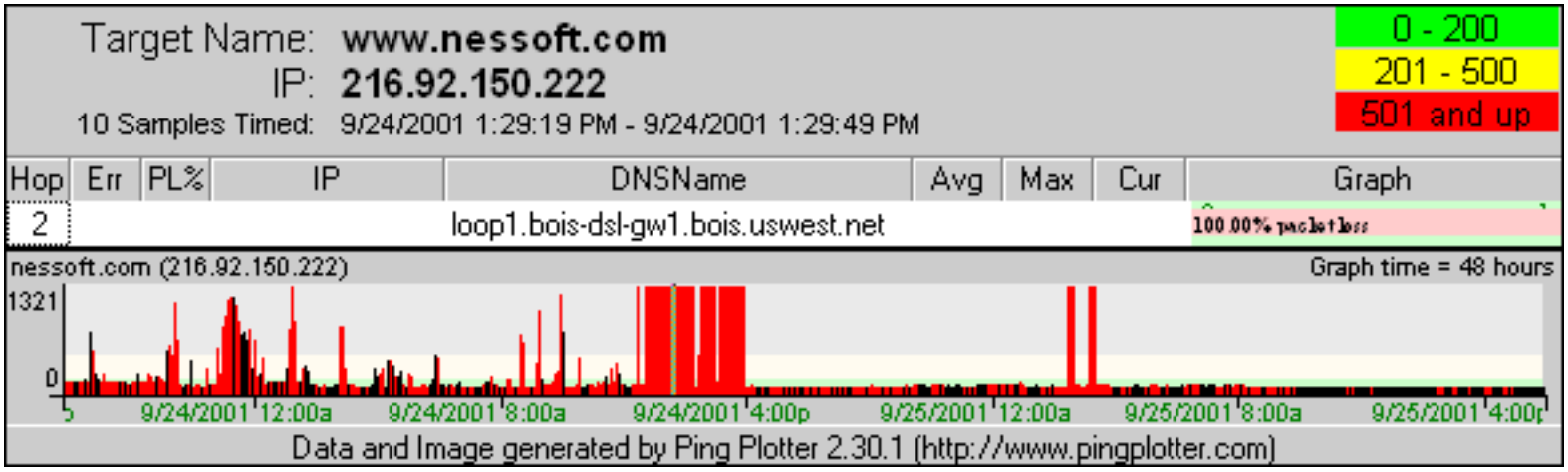
Before continuing, if you're not familiar with how the graphs work in Ping Plotter please make sure you've read the introduction to graphs earlier in this tutorial.

One common mistake we see folks make is that they'll trace to their ISP's border router. This is a bad thing. If you're tracing to the border router and your route changes (i.e. they take that router down for maintenance or you get load balanced onto another router) you really have no idea what happened. If you want to keep your traces local to your ISP, trace to an address that isn't going to change on you like you're ISP's mail server. This is actually a good thing to do if you're having mail problems and it's your ISP's mail server going down. Otherwise just pick a destination that you know has a reasonably good chance of always being up. This is a better choice since routes within your ISP can change, and Ping Plotter keeps track of those route changes. The cool thing is that you're doing a traceroute here, not a ping, so even if that destination host goes down you can drill down on the timeline graph and see if it's your connection, or if it's just the destination being down (as in all hops but the destination don't show timeouts).

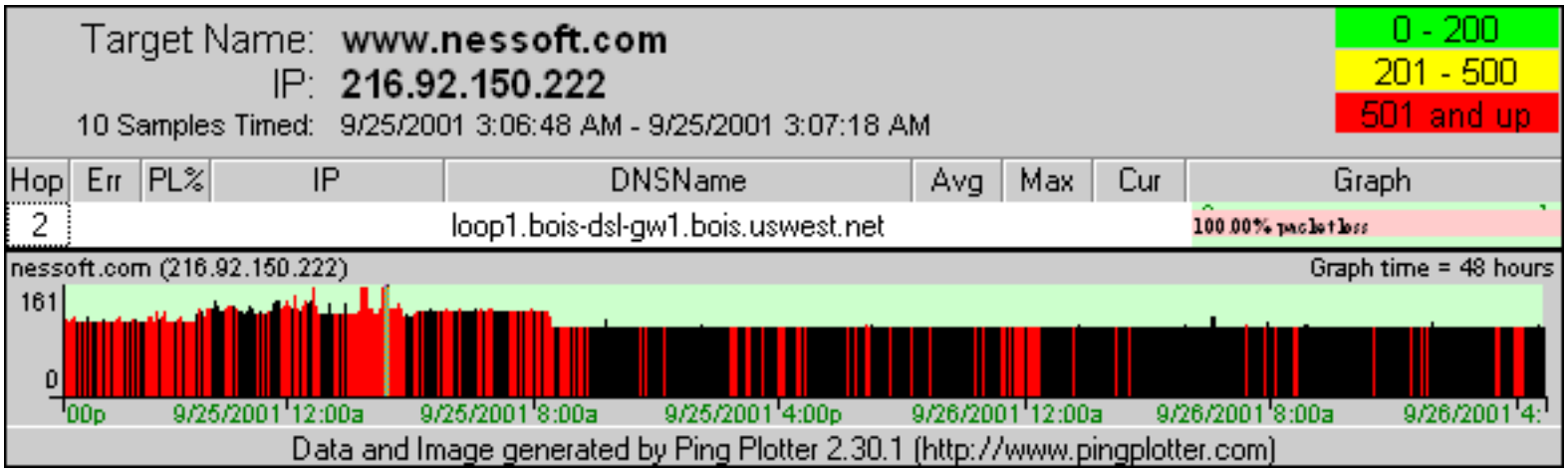
Note: For clarity, all the graphs below show us ignoring Hop 1 which you to can do from the View Menu. All the graphs were saved with the File/Save Image command within Ping Plotter then converted to .gif for this tutorial.



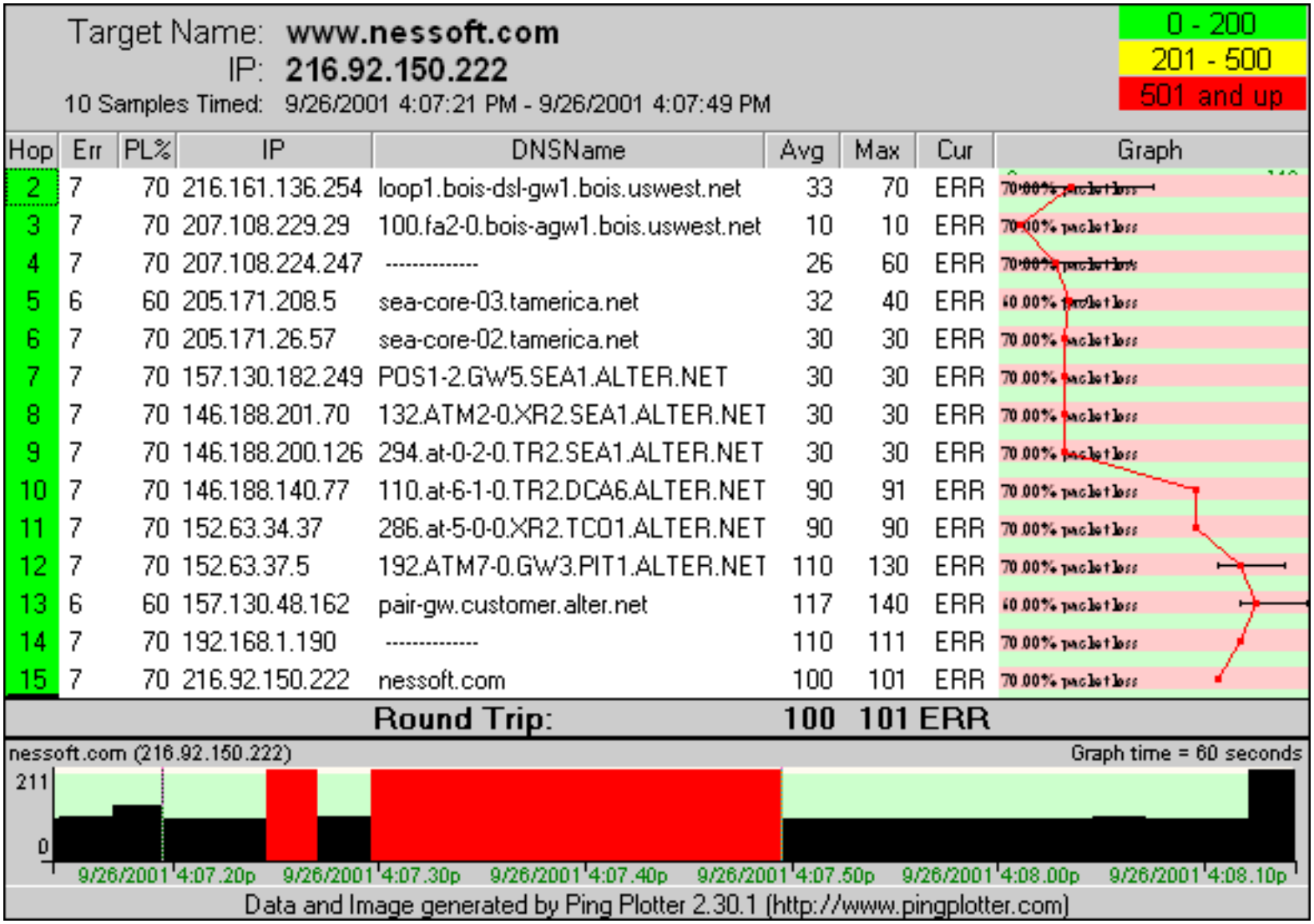
This first graph shows what the traceroute should look like with no load on the connection, i.e. no downloads, streaming audio, on-line game playing, etc. "What about all that red on the history graph? I thought red was bad?", you ask. Actually red is bad, however before I saved out this graph I double-clicked on the timeline graph to drill down, or zoom-in, and am looking at the data for 9/25/01 at 11:56 a.m. If you look at the top of the graph you see "10 Samples Timed: 9/25/01 11:56:09 AM - 9/25/2001 11:56:32 AM". So basically the above graph's trace for that *particular time* looks good. However when you look at the timeline graph, you can start to see the tale of woe. What we have here is a really flaky broadband connection. So how do we prove it? Read on.



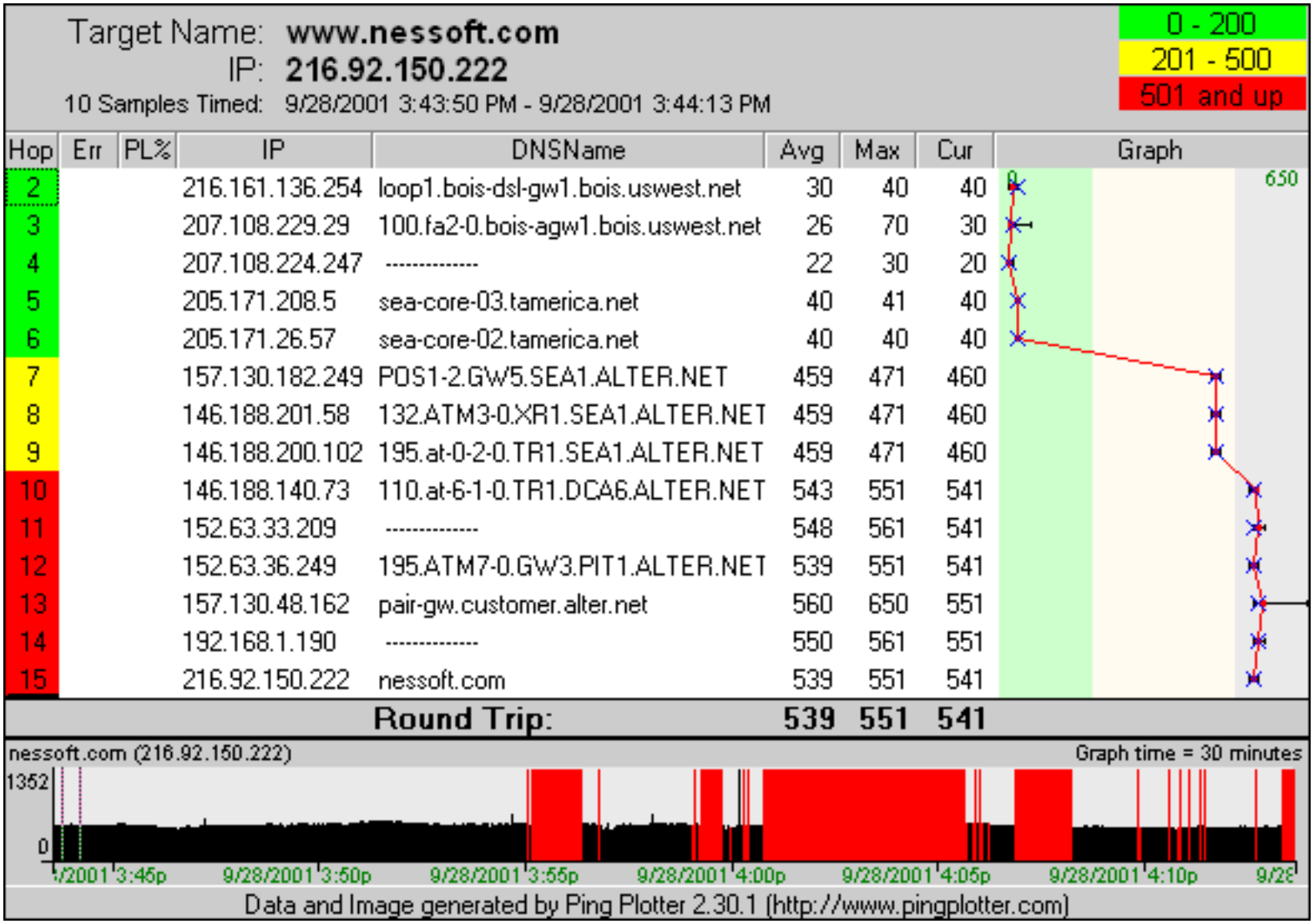
Just sending your ISP a graph with red lines isn't very convincing. However, when you start zooming in on those sections with timeouts, and send graphs of them as well like this second saved graph, it's pretty obvious the connection's hosed when you can't see out to Hop 2. This is the same time interval as the first graph, just showing a different period in time for trace data.



For our third graph we've got data for early on the second day of our trace. Lots of red, and when we focus on the 3:06 a.m. time period the connection's still poor. You're unable to see out. It's hard to argue with the graph. Also keep in mind that what we're showing here is that the whole timeline graph isn't solid red. This isn't an issue where you accidentally kicked the plug on your router.



For our fourth graph, you can see from the timeline graph's times that we've adjusted the time-interval so we're only looking at 60 seconds worth of data. The trace graph is showing the section of the time-interval graph that we double-clicked on which is 4:07:21 p.m. through 4:07:49 p.m. So what's up with the 60-70% packet loss showing up on the trace graph? Notice that we didn't have timeouts for that whole 28 second period (the right vertical bar is kind of hard to see in this example, but it's at the end of the last time-out there at 4:07:49). Out of the ten samples we're looking at (depending on what hop we're looking at - remember Ping Plotter is tracing each hop at the same time so it's logical that Hops 5 and 13 could at this point only be showing 60% loss), roughly 70% of them were timeouts. This is important. When we're looking at the trace data we're looking at those 10 samples we selected and the numbers for those samples, not the whole range of data shown on the time-interval graph! This is not a graph you want to send to technical support. All it's going to do is confuse them.



Ok, so what's up with the graph above? Well, like parents we try to be fair, and what you see above is a flaky connection (as you can see from the timeline graph though you'd want to zoom in to be sure where), and trace data (notice the vertical focus bars at the left of the timeline graph that denote the section of data we're looking at) that shows a problem out of your ISP's control. The ten samples we're looking at actually show a problem with the connection between Touch America (tamerica.net) and UUNET (alter. net), or Hops 6 and 7. It's hard to say exactly what's going on there, but more than likely the link between those two routers is saturated. We could try and blame a flaky router at Hop 7, but there isn't any packet loss. It's a good guess that it's the link, not the router, or we'd see the router at Hop 7 dropping packets.

So in summary, as you can see Ping Plotter allows you to show your ISP where the problem's are. In the above examples, we were essentially showing the whole link going down. However, we could've just as easily seen if the ISP's connection to the Internet was down at Hop 4, because we were tracing to a destination not on our ISP's local network. If there was indeed a problem at Hop 4, we would've had good trace data at Hops 2 and 3, timeouts at Hop 4 and possibly no trace data past Hop 4. If the router at Hop 3 was being flaky, and for instance you saw a lot of packet loss, it's easy to save an image showing just that so you can email it. When sending graphs to your ISP, we've

found it's best to send one graph showing data for an extended time period, and then drilling down on the timeouts and sending graphs that truly show them what's going on. Ping Plotter allows you to save in .png or .bmp format. We recommend .png because they're smaller.

/interpreting results - long-term monitoring/working with historical data

PingPlotter allows you to use the timeline graphs to zoom in on any particular time, so even if you weren't there (or didn't save an image) when something was happening, you can still recover that exact image later. You shouldn't ever have to be sitting in front of your computer when an outage happens, or you experience other problems on your network, to get the data you need from PingPlotter.

The Scenario:

You're having outages (or situations you want to communicate to your ISP) randomly throughout the day. Let's say twice a day. The problem is that you can't be there everytime an outage happens so you can save a graph image.

For this example, you're keeping 24 hours of data in memory or even more. We suggest that you normally use 2.5 second trace intervals and keep 200,000 samples in memory. This is almost a week's worth of data. You can change the number of samples to keep in memory in the Advanced Options/Auto-Save section under the Edit menu selection.

Using Ping Plotter's timeline graph, you can see over the past X time period (see below) to identify a time period where there was problems. Problems will demonstrate themselves as packet loss (red), or high latency.

Now you want to show the route, and the packet loss/latency in the upper graph for that time period. Since that time has already passed, you need to change the focus of the upper graph to that time in the past.

First off, you need to make sure your "samples to include" focuses in on just the period in question, so let's change that to 100 (it's important to not have it set to 0/all, but to have it be a number smaller than the number of samples in memory to be able to focus the upper graph). Right click on the timeline graph and pick a reasonable period of time to set the viewable time period. For instance, you may want to set it to six hours so you're not scrolling forever. You can then "click and drag" the graph to the left to go back to the time period you want to focus on and drag it to the right to go forward in time. Note: You can have custom timeline intervals show up in your right-click menu by adding a setting in the pingplotter.ini file. Go here to see how to do this.

Double-click on the "problem period" in the lower graph. You'll see a focus rectangle appear on the lower time graph, and the upper graph will change to represent the data

you have "focused" in the lower graph. Once you've done this, you might want to change the scale of the lower graph to show more detail. Right-click on the lower time graph again and change the scale to an hour (or maybe even 30 or 10 minutes depending on how long the outage was). The focus rectangle should still be visible (PingPlotter versions 2.3 and higher try to keep the focus in view when you change graph scales). You can fine tune the data being displayed in the upper graph by double-clicking on the lower graph again.

Using these techniques, you should be able to zoom in on exactly the right data to best illustrate the problems you're seeing. You can look at the data after the problem occurs and get the perfect picture and not have to sit there watching PingPlotter all day and night.

You can auto-save that data by for instance having the auto-save function in PingPlotter create new files every day, and then load up a prior day to do the same thing you did above for a particular time. This gives you the capability to have pretty close to 100% coverage of your network performance and be able to zoom in on any particular outage, period of slow response, etc.

The options in the alert setup do allow you to have the .PP2 file (trace data) emailed, and then you can use these same capabilities to zoom in on that data.

/undocumented features - advanced whois setup

If you'd like to add additional whois servers to have available from the trace graph's right-click menu, you can edit the pingplotter.ini file. Currently Ping Plotter only supports xxx.yyy style addresses. Not, for example, xxx.yyy.uk. You can also change the default servers directly in the .ini file instead of changing them from the Advanced Options/ Internet menu.

To change the default settings, add the following to your pingplotter.ini file:

```
[Internet]
StandardWhoisHost=whois.networksolutions.com
BlockIPWhoisHost=whois.arin.net
```

Also, you can add addtional servers with a list of commands like the following:

```
[Internet]
AddlWhoIsServers=Internic Whois Lookup, whois.networksolutions.com, name, Arin (IP) Whois Lookup, whois.arin.net, ip
```

Basically, each whois server is defined by 3 settings - Description (as it appears on the menu), Server address (IP or name), and lookup type (Name or IP). The last setting specifies if it queries the whois server for the IP address, or the name of the specific hop.

If you're adding a server that's not specified in Ping Plotter by default, add that server as the first server on the AddlWhoIsServers line (ie: don't include the default servers shown in the example above, since they're always included no matter what you put in the INI file). If you have more than 1, just add 3 more comma delimited sections. There is no limit to the number of sections you can include, though more than a few will make the menu a bit unwieldy.

/undocumented features - automatic license key entry

The Ping Plotter install has the capability of automatically entering a license key to make multi-user deployment in an organization easier. There are several ways to do this, via a pre configured License File, from the Command Line and Custom Options.

License File

The easiest way to have this work is to put a file called "Ping Plotter Registration Info. dat" into the same directory as the Ping Plotter installation (i.e.: where the pngplt_2.exe is). When the install is launched, this file (the .dat file) is read for a license key and user name, and then the install will enter this key so the user is never prompted for a license key.

The file should resemble the following, so if you wish, simply cut and paste the text in blue below into a text file called "Ping Plotter Registration Info.dat" and modify it with your information accordingly.

```
; Ping Plotter multi-user license
; (Your company name)
; Issued (Purchase date)
;
; A username can be specified as below, but if not specified, the user name is
; pulled from the machine being installed (the preferred method).
; USERNAME=(Your company name).
;
REGCODE=(your license key)
```

An actual file (with fictitious values for illustration purposes) would be:

```
; Ping Plotter multi-user license
; Highly Successful Corporation, Inc.
; Issued July 23, 2003
;
; A username can be specified as below, but if not specified, the user name is
; pulled from the machine being installed (the preferred method).
USERNAME= Workstation User
REGCODE=ABCD-EFGH-1234-5678
```

While this file can actually have just the one line (i.e.: REGCODE=license key), the rest is helpful if you ever need to edit the file.

This method works especially well on a CD, or a network drive where the install and the .dat file can be in the same directory. Ping Plotter will only look in the same directory that the install is ran from (the location of the pngplt2.exe file).

Command Line

Another option is to pass the installation command line parameters with the license key:

```
pngplt_2.exe REGCODE=(your license key)
```

This method works well if Ping Plotter is being installed by some other program that can easily specify a command line parameter like this. If this is the case, you might want to have the Ping Plotter installation user interface suppressed - which is done by adding the /s command line to the install:

```
pngplt_2.exe /s REGCODE=(your license key)
```

In silent (/s) mode, no dialogs will appear on a successful install, and the default directory of c:\program files\ping plotter will be used (note that the Program Files drive is pulled from the system setting, so this might be something besides c:\program files).

You might be tempted to wrap your own installer rather than using the Ping Plotter installation. This is acceptable with a few caveats:

- You will have to rework your install package each time Ping Plotter is updated.
- We don't support the customization of your own installer unless you leave our installer intact.
- You cannot distribute your repackaged version of Ping Plotter outside your own company.
- You know the environment in your company and can account for variances. Once you get outside your own company there may be additional problems, and we can't support these customizations.

Using the /s option will allow you to embed the standard Ping Plotter installer inside of your own installer. This will install the Ping Plotter uninstaller as well - if you're installing additional Ping Plotter related files that you want the uninstall to clean up, you'll need to account for that. Contact our support team and we'll be happy to help you with this.

Custom Options

There are several other options available through the command line interface of the installer. You can specify a different install directory, or you can have Ping Plotter automatically launched with the install is complete. Please contact our support team with your needs, and we'll help you build the right install package.

/undocumented features - modifying thread count

When tracing to a host where there are unresponsive "hops" just before the target hop, Ping Plotter can seem to pause for about 5-7 seconds or so after a few passes, then perform a few more passes and pause again, etc. Here's an explanation on how Ping Plotter allocates threads, and tips on how to reduce the overloading of the thread queues.

By default, Ping Plotter allocates a maximum of 45 threads it can use. Each ping request takes one thread. As a ping returns, the thread can be re-used for another ping. After 5 minutes of inactivity (i.e. there are more threads allocated than being used), a thread is freed. If you're running under NT, you can see your thread count under the task manager.

If there are a lot of unresponsive hops, then there's an opportunity for a LOT of threads to be tied up waiting for responses. If all 45 threads are being used, every trace attempt will be discarded until there are free threads. This is so it doesn't queue up a bunch of requests that finally get serviced a LONG time after they're asked for. You can imagine if your service rate was less than your request rate, that this would continue to grow forever. If only 44 threads are in use, then the entire batch needed for the next request (for example, in the case of zd.net that's about 25 of them) are pushed into a queue that is serviced as threads free up.

Anytime the thread queue is full, there's an asterisk displayed beside the word "Querying" in the status bar.

By the way, DNS lookups also use a thread, and this comes from the pool of 45.

Now there's a couple ways to reduce the overloading of the thread queues.

The most resource friendly way is to go to advanced options and change your "Timeout Speed" to something other than 10 seconds. If you get responses back in 350 ms, it's pretty safe to reduce this to something like 2000. This means that any thread will only wait 2 seconds instead of 10 for a packet to timeout. Depending on your network, a lower number may work also.

A less resource friendly way to handle this is to up the number of threads that Ping Plotter will allocate. Under Windows NT/2K, this doesn't seem to cause much of a problem, but under Windows 98 too many threads allocated seems to actually lock up the system at some point. Keep in mind also that fast attack rates can really use a LOT of threads if you have a lot of timeouts and a high "Timeout speed".

To change the number of threads that Ping Plotter can use, you have to manually edit the

PingPlotter.INI file. Add the following to the advanced section:

```
[Advanced]
MaxThreadCount = 45
```

Obviously in place of 45 above you'd set it to whatever value you want.

Keep in mind that the initial burst that happens on hop 1 will always use 35 threads. Changing this to a number less than 35 can severely affect your starting performance if there are any timeouts, although some fast responding hops in the route can make it so it's not noticeable.

/undocumented features - changing timeline intervals

You can change, and also add, additional timeline intervals for the timeline graph if the defaults available from the right-click menu don't fit your needs. For example, you may want to look at results farther out than the default maximum value, which is 48 hours.

The default set isn't written in the .INI file, however you can add an entry and it will override the default values.

For example, if we wanted to add "2 hour" and "120 hour" intervals to the right-click menu, your .INI file entry would be what you see in the example below. It's important to note that the values are in minutes. It's also important to note the "Count" value. If the value was set to "Count=11" in the example below, the value for "Interval12" wouldn't show up in the menu.

```
[TimeGraphIntervals]
Count=12
Interval1=1
Interval2=5
Interval3=10
Interval4=30
Interval5=60
Interval6=120
Interval7=180
Interval8=360
Interval9=720
Interval10=1440
Interval11=2880
Interval12=7200
```

/ping plotter - frequently asked questions

I've got Ping Plotter installed. Now what do I do? I don't have a clue how to get started.

Ideally you'd go from start to finish through our online tutorial. If you're in a hurry, the Interpreting Results section is probably a good place to start. Again, the preferred way to get started is to peruse the tutorial. It is arranged logically and there are lots of little tidbits and not-so-obvious features in there.

Back to Top

Why do I sometimes see blank lines in the graph display? There's a hop number but no IP address, etc. listed.

The absence of an IP address for a specific hop means that no router has responded for that hop. This happens on occasion when a router is configured to not respond to TTL=0 ICMP echo requests. This is not common, but does happen occasionally. Another possibility is that the router is configured to "down-prioritize" TTL=0 ICMP echo requests - in which case any load might be prioritized higher - and these packets are discarded. When this happens, you'll sometimes see a hop respond, but sometimes it doesn't, leading to a high packet loss rate.

The really important point to know about these routers is that if they are not affecting the downstream hops, then their behavior should be considered "normal". For example, if you're seeing 75% packet loss at hop 6, but 0% packet loss at hop 7, but 10% packet loss at hop 8 (the final destination), then the problem isn't at hop 6 at all, but somewhere else (for example, between hop 7 and hop 8).

Something to note here is that the moment a router *does* respond on that hop, Ping Plotter will record that information, so whenever you have a blank line, that means that no router has responded at all.

Another possibility is that there is a configuration on the router at that hop where under heavy loads it drops timed out echo replies. The important thing to remember is that what **really** matters is the final destination. If the final hop is showing 0% packet loss and acceptable latency, then all the hops before that can barf or just not even respond. Point being that you can't blame the machine at the final hop and there probably isn't anything seriously wrong with the route.

Back to Top

Do you know of any sites that will do a traceroute back to me, as opposed to me initiating the traceroute from my location?

ISPWorld has a list of servers worldwide that will do this for you.

Back to Top

When I export to a text file, some lines end with * - which seems to mean no response. I also get a few that end with N/A. What does that mean?

Because of the limitations of text files (and the tools you're probably trying to import this data into - like Excel), only a single route is listed, and then the data is all printed with respect to that route. Sometimes, this means that there are routers in the collected data that aren't in the route you had selected when you export. Usually, the best way to do an export is to set up your graphs so it's focused in on the period you're interested in exporting - and then making sure that you have the right route selected for that (version 2.30.1 helps you do this by automatically selecting the most current route for the time period you have selected). Even then, though, only a single route can be used in an export, so if you have a bunch of routes in your data, the export will exclude some of this data.

Now, if you really don't care about route changes, but really care only about your final destination (you're planning to do an export) there are ways to get rid of the N/As and to combine data collected by multiple routers (at a particular hop) into a set of data that can be exported. This is done by setting up Ping Plotter to ignore some of the internal route changes. You can either do this for specific router groups, or just say you don't care about anything except for the most major (i.e. changing lengths) route changes by putting an "ALL" in for the exclusion list.

Another opportunity for N/As to show up is when you're snap a "Copy as Text" when you're still in the midst of a trace. There might be some outstanding requests out there that just haven't had an opportunity to respond yet. Because we don't know yet. They're not time-outs, so we show that as N/A.

Back to Top

Why does one particular hop in the route often show a really bad time - but the hop right after it performs well?

It appears that some routers just don't prioritize timed out ICMP requests very high (ICMP requests where the TTL equals 0 after reaching them). If the hop right after consistently performs well, just don't factor this hop into your troubleshooting equation (i.e. ignore it).

Back to Top

Why does hop 1 (or any number of initial hops) lose packets 100% of the time?

Often your local router just doesn't respond (or respond fast enough) to ICMP requests. If you have this happening, you can ignore the initial hops that are timing out (View/Ignore first hop(s)).

Back to Top

When I set up an alert, it never seems to fire - although the "Test" button sends me an e-mail just fine.

Once you've set up an alert, you have to attach the alert to the IP address you want to monitor. This gives you the capability to use different alerts for different IP addresses.

To attach an alert to an IP, trace to the host you're interested in. Then, right-click on the hop you want to monitor. Select "Add Monitor". Then select an alert (or multiple alerts) from the list. This should put a [...] around the hop that's being monitored.
For a detailed explanation of alerts go here.

Back to Top

Whenever I try to run Ping Plotter I get an error message "Can't get a handle on icmp.dll".

Ping Plotter uses a .DLL that's provided by Microsoft and is used by their "PING" and "TRACERT" packages. If you haven't installed these, then that .DLL might not be installed. If you're running Windows NT, these are installed by adding "Simple TCP/IP Services" to the "Services" tab of your network setup. If you're running 95/98, they should have been already installed - you may need to reinstall your TCP/IP protocol.

Back to Top

Why do traces to some sites always return "Destination Host Unreachable" (an example of a site that does this is www.microsoft.com). I can connect to that site fine with Internet Explorer or Netscape!

One of the routers used between you and the destination site are not passing through ICMP echo requests. Some sites, for security reasons, have their firewalls setup to not echo back ICMP packets so they can appear "invisible" to automated hacker scanning tools.

Back to Top

The ping times don't always seem to add up logically to me. For example, I commonly see the avg. time for a single hop being longer than the total return trip number. This doesn't make sense to me. Can you explain this to me?

One of the routers used between you and the destination site are not passing through ICMP echo requests. Some sites, for security reasons, have their firewalls setup to not echo back ICMP packets so they can appear "invisible" to automated hacker scanning tools. It appears that some routers just don't prioritize timed out ICMP requests very high (ICMP requests where the TTL equals 0 after reaching them). This often means that a specific site will take a lot longer to respond back to you than it does to send the packet on to the next host. If the hop right after consistently performs well, you can often just not use this hop in your troubleshooting equation. On the other hand, if you start dropping a lot of packets at this hop (that show up in later hops as well), this may indicate that the router is overloaded (i.e. - doesn't have enough processor time to do all it's tasks).

Back to Top

I'm using a proxy server. Why can't I see anything beyond the proxy server with Ping Plotter?

We don't know of any proxy servers that pass on PING/TRACERT requests. This means that Ping Plotter doesn't work with a proxy server at all. The only way you can really measure network performance on the other side of the proxy server is to run Ping Plotter on the proxy server (or a machine that's not behind the proxy). You can always ask your network administrator to pipe you directly out through your firewall (if you have one), effectively bypassing any proxy.

We've had some really good success with NAT type IP sharing, though - NAT seems like it works much better than proxy solutions do for hooking a network up to the Internet and only using a single IP address. WinRoute is an example of a product that seems to do this very well.

Somewhat unrelated, but if you want auto-version checking to work, and you're behind a proxy, you have to set it up in the Internet settings under Advanced Options.

Back to Top

I have a router in my path someplace that doesn't handle multiple outstanding ICMP requests. Can I change Ping Plotter to use a single thread for tracing?

Absolutely! Using a single outstanding trace thread seriously impacts the performance of Ping Plotter, but sometime's it's necessary to do this. Note: You need to close all instances of Ping Plotter before doing these steps.

- Open up your PingPlotter.INI file in your editor of choice (this file is in the Ping Plotter directory).
- Insert a new line in the "Advanced" section of the .INI file. This line should read "MaxThreadCount=1" (without the quotes).
- Open Ping Plotter. In the "Edit" menu, go to "Advanced Options" and the "Packet Options" tab, change the "Time interval between hop traces" to 0. (This ups the performance somewhat, isn't necessary, but very helpful).
- Review the "Timeout speed" setting (this setting is in milliseconds - or 1/1000 of a second). If you never expect a hop to take more then 1 second to respond, enter 1000 here. Try to set it to the lowest reasonable number.
- Turn *ON* "Use non-threaded Name Lookups".

To reverse this, remove the "MaxThreadCount=1" line from your PingPlotter.ini file. Change the "Time interval between hop traces" back to the default of 25, then change the "Use non-threaded Name Lookups" off again in advanced options. You can change the "Time-out speed" back to 9999 at this point as well, but you don't have to.

Go here to see information on thread counts.
Go here for more packet options.

Back to Top

A "pure ping" using -t switch shows no problems, but Ping Plotter shows many packet losses. What would cause that?

- The packet size could be different, and that different packet size in Ping Plotter may be causing some packet loss. Note that this is a problem with the router, not Ping Plotter, but you can change the packet size to something smaller than default to see if this affects it. Go here to see how to change the packet size.
- Having multiple simultaneous outstanding ICMP echo requests may be causing a problem in one of the routers. This isn't too uncommon, but is almost always traced back to a hub on the local side (BIOS updates often help this). See the FAQ entry above if you want Ping Plotter to do one outstanding request at a time.
- In some **very** isolated cases, we've seen a difference in packet loss based on the contents of the packets. Ping -t uses a repeating sequence of "abcdefghijklmnopqurstuvw" while Ping Plotter uses repeating $AA. You can change Ping Plotter to be the same as Ping by creating a text file with the same thing that PING sends (i.e.: create the file with abcdefghijklmnopqrstuvw in it), and then go to Advanced options and change the packet cargo to use this file. This is kind of a long shot, though, as in all cases where we've seen this make a difference, Ping Plotter was used to simulate and extraordinary bytes sequence that stimulated the packet loss, and the $AA wasn't that sequence. This is worth trying though since it's quite easy to do.

Back to Top

I set an alert condition for an IP. The condition is to send an alert when there are 3 incidents over 2000ms in the last 6 pings. The max e-mail frequency is 30 minutes, and the duration to wait for worse condition is zero. However, I sometimes received alerts in which the most recent 6 pings, as it showed in the alert e-mail, are below the threshold. What settings did I do wrong to create these false alerts?

Check to make sure that your "Maximum samples to hold in memory" isn't set too low. The setup in this case had e-mails going out at maximum every 30 minutes. The "Max samples in memory" was actually set to only hold about 25 minutes worth of data at a time, so sometimes the alert would go out based on conditions that had already dropped out of memory.

To fix this problem, just change the "Max samples to hold in memory" to hold at least the amount of time your maximum e-mail frequency is, preferably a bit more (as the history files that can be included in the e-mails can actually show more data than this).

To see how to change this setting go here.

Back to Top

Why am I seeing continual route changes when I run PP? There also are 10-50% packet loses on various hops. This doesn't seem to manifest itself when I download files. I am connected to Qwest dsl via a Cisco 678 router.

Route changes are a pretty normal fact of life with the Internet. It sometimes happens for load balancing reasons, sometimes to route your data around problem areas, or a number of other possible reasons.

Ping Plotter, by default, keeps track of ALL route changes. Normally, this works really well - and pretty much without notice by anyone (unless you're looking for it). The time when it can start to cause problems in the data that Ping Plotter displays is when the length of the route changes (when your destination shows up at different hops, depending on the route being used) - as the changing routes cause problems in the final hop.

If you want to suppress recording information about route changes, you can do this in Ping Plotter unless the length of the route is changing, in which case recording these changes can't be suppressed

Now, there are a few different variations of things that could cause problems, and causing your packet loss. A big variable in this is whether or not your route length is changing.

One thing to know about Ping Plotter (and all ping tools) compared to HTTP web access is that HTTP uses error correction in its communication. If you get a lost packet when transferring HTTP, you often don't notice this because the protocol corrects for errors. The ICMP protocol (which is used by Ping Plotter and other ping tools) is lossy - so if something along the way drops data, it's never corrected - just reported by whatever tool sent it out. This is one possible reason why you're not seeing lost data when browsing the web or downloading something, but are seeing it with Ping Plotter.

The symptoms seen when data is lost in an error correcting protocol is that performance suffers. When data is lost, the protocol negotiates for it to be resent and this takes time. If you're seeing slow performance when downloading files, or browsing the web, it's possible that the drop in performance is being caused by packet loss.

Back to Top

The route to the destination changes, i.e. gets longer and shorter, and Ping Plotter reports what seems like erroneous packet loss to the destination.

Whenever a route gets longer, Ping Plotter will show one lost packet at your final destination. This is what could possibly be happening.

Here's a brief description of why this happens:
When Ping Plotter determines that the final destination has been reached, it only sends out enough packets to reach the final destination. So if your route is 13 hops long, it only sends out enough packets to reach hop 13. Whenever the route gets longer, another router reports in at hop 13 and Ping Plotter figures out that it needs to send out more packets to reach the final destination - but it doesn't do this until the next sample set is sent out. This means there is always a single lost packet associated with this route lengthening. This doesn't occur when the route shortens - only when it gets longer.

Some other tools address this by only grabbing the route on the first set, and then just "pinging" each destination directly on future samples. Ping Plotter versions before 2.30 handled this a bit differently - by ignoring the information about the hop's IP address when it came back, and always just using the hop number (rather than the IP address) to decide where to put things. In both of these cases, you wouldn't see packet loss at the final hop - but the data being reported would be flat wrong (because data was being associated with a router that was no longer even in the route!).

This is a very rare, but documented issue that will be handled in a future release.

Back to Top

My DSL/Cable/whatever modem shows up in the trace. Is there a setting to ignore the first x hops so it doesn't?

Yes, you can change this in the View/Ignore First Hop(s) menu. The default is "trace all hops". From this menu option you can skip hops 1, 2, 3 and 4. To eliminate your modem from the graph display you'd set this option to Start at Hop 2. If you wish, you can also from this option choose to only trace the final hop.

Back to Top

Can I specify more than one e-mail address for an alert?

Yes, to specify more than one destination e-mail address for an alert, just separate the e-mail addresses by commas or semicolons.

Back to Top

After running Ping Plotter for an extended amount of time my machine gets low on memory. Can Ping Plotter save out my data at predefined intervals so the data doesn't eat up a lot of memory?

Definitely. Ping Plotter's overall footprint on your machine should be very small. By tweaking the maximum number of samples to be held in memory, along with the auto-saving of data, you can limit the amount of memory used but still have access to all the data collected. Go here to read more than you'll ever want to know about auto-saving of data. We've seen sample sets of over one million contiguous samples with no noticeable effect on the computer running Ping Plotter other than the amount of disk space used for the save files.

Back to Top

Can I auto-save out graph images for use on a web page, for ftp transfer, etc.?

Yes, in either BMP or PNG format. In the auto-save image section you can set the save interval to tell Ping Plotter how often to save the images, what filename to save the data to and what type of image format to save the graph in. Go here to find out more.

Back to Top

How do I setup the trace graph so I can see the average, maximum, minimum, packet loss percentage, etc? I had them visible once and now I seem to have lost them.

Do a mouse "right-click" anywhere on the upper graph area. You will then see the menu that gives you the options to turn those columns on and off. One thing to keep in mind is that if you plan on sending a graph to your ISP, etc. you may want to turn off the average, maximum and minimum and only show the packet loss percentage. See the Beating Up on Your ISP section of the tutorial for more details.

Back to Top

Wow! I can't get enough of this traceroute and ping business. My mind hungers for more knowledge! Got any web links where I can read up?

Sure thing. We've got a few links at the bottom of our table of contents for the tutorial including The Ping Page and The History of Ping. If your dreams are still haunted by visions of ping you can see a ping packet decode here, learn about the inventor of ping (who sadly died in a car accident in November of 2000) and of course visit our How Ping Plotter Works page in the Ping Plotter tutorial.

Back to Top

Do you have a support message board? Is it only available to registered users?

We sure do. While we'd like to think everybody that finds Ping Plotter useful will register the software, sometimes it just doesn't happen. With that, the support boards are freely available to all by clicking here.

Back to Top

What's the Export Controls Classification Number (ECCN) for the shareware version of Ping Plotter?

Ping Plotter shareware would fall under the ECCN of EAR99

Back to Top

The first ping that I send somewhere is always slow the first time, then every subsequent time it is significantly better (the first hop is really fast; its the first ping that is slow). My first pings run 300-500 ms, then subsequent ones are usually under 100ms, depending on the route.

We usually see this more on dial-up connections as compared to broadband connections. The first sample with Ping Plotter has significantly more bandwidth usage than subsequent ones. First off, the first sample *always* sends out 35 packets. Ping Plotter has no idea how long the actual route is (and it wants to return data as fast as possible), so it sends out 35 packets each separated by a small time period (as specified in Advanced Options / Packet Option tab / Time interval between hop traces. This defaults to 25ms which means with a 56 byte packet, you're looking at a bit over 2 K/s of bandwidth used. If you have more than a 56 byte packet specified, this is higher. Once Ping Plotter knows the route length ie: sample 2 and beyond, it only sends out as many packets as is necessary to make the final destination. There is a *small* chance that this will impact your bandwidth the first time the trace is initiated.

Second, as individual results come back on the first sample, the routers that have responded also need to have their names looked up. This happens immediately as each hop responds back. This means that there is additional bandwidth being used at this point as Ping Plotter talks to the DNS server(s). This handshaking doesn't take a lot of time, but it can overlap and has a chance to impact the first sample set's times.

If you want to see if this is impacting you at all, there are several ways to set Ping Plotter. First off, to disable the impact of the reverse DNS lookups, there's an option to disable threaded (concurrent) DNS lookups. Reset your trace and see if the behavior is any different.

Another way to minimize the impact of Ping Plotter's network usage is to change the time interval between hop traces. If you've got it set to 25, try changing it to 75 or 100. This will slow the rate at which Ping Plotter uses network resources.

Back to Top

A colleague and I are pinging the same website from different locations (geographically, we are about 30 miles apart, both pinging a server about 1500 miles away) at 15 second intervals. Oddly, I will show a whole spurt of packets dropped by the target server during a particular period, indicating server difficulties, but my colleague may not show that at all. Why would this be? We want to reliably know when the server is having problems, but these differences make it difficult to be sure.

This definitely sounds like the RETURN route. Due to the way traceroute is implemented, Ping Plotter can only find the route a packet follows to get TO the destination, not how it gets back. What's more important is that the route your packets take TO the server from your computer is more often than not completely different than the route taken FROM the server back to your computer. This is what's known as asynchronous routing.

So in cases where you see only the final destination with packet loss, the return route *may* be significantly different when coming back from the final destination than it is when coming back from the hop right before it.

The best way to troubleshoot this is to have access to traceroute from that server. This isn't feasible for most situations, but if you have a business relationship with them, you may be able to get them to run a traceroute back to you so you can see where the packet loss is occuring. Some sites even have tools installed for you to check this yourself. For instance, TheNetGamer.com provides this type of tool for their customers.

To that end, here is a nice page of servers that will trace back to you located at ISPWorld. In your troubleshooting you would want to select a traceroute server listed there and use the IP address you believe to be the problem, i.e. the one you're tracing to in Ping Plotter. If that trace returns an abnormally high ping also, you have found the problem router, and it is on the TO route. If not, it is time to turn your attention to the FROM route. If you suspect a problem on your return route, you can use one of the server-side traceroute facilities (if one exists at that end point) to find out what the route BACK is. This should point to the problem router. If not, then unfortunately you've found one of the weaknesses of trace route troubleshooting in that it only shows the route in one direction.

There are also very rare instances where you may have ran into a multi-homed router. This is where multiple backbone providers are using the same router. These are pretty rare, but have been becoming more and more common (F5 networks makes one of these monsters that can handle insane amounts of traffic) as providers consolidate/merge/etc. If you are at a total loss trying to find the problem, you may have run into one of these puppies. If you suspect this is the case, email us your trace data at support@pingplotter.com and we'll try and take a look for you.

Back to Top