Fasthosts Customer Support

Troubleshooting with the command line

The command line contains a powerful suite of tools that can be utilised in a variety of ways. This guide will show you how to use some common tools to diagnose issues with websites, domain names and DNS.

Table of Contents

Introduction **2**
Overview of the command line tools **2**
Accessing and setting up the command line interface 3
Useful Commands **5**
Ping 5
Whois 8
NSlookup 12
Tracert 18
Pathping 20
Netstat 24
Telnet 26
IPConfig 34
Troubleshooting websites **37**
404 errors (Page cannot be displayed) 37
I can't see the changes I made to my website 38
Troubleshooting email **39**
I can't send email 39
I can't receive email 40
Troubleshooting Broadband **41**
Slow connection 41
Unable to connect 42
Appendix **43**
Additional Ping options 43
List of useful Whois Servers 43
NSlookup options 46
NSlookup Error Messages 47
Telnet Email commands 48
IPConfig Additional Switches 50

Introduction

Most calls to Fasthosts customer services team can be resolved without the need for "in-house" tools or "special access", and can be diagnosed quickly and easily using command line tools built into most operating systems. This guide will show you how common command line tools can be used to diagnose most enquiries.

Quick tip: At the end of this guide are troubleshooting flowcharts, allowing you to work through most customer issues you are likely to encounter as you grow your business.

This guide will focus on the command line tools that are most relevant to you and web hosting, although these tools are also useful in diagnosing a number of other faults or issues your computer may experience over time. It concentrates on command line tools as these remain the same for each operating system, and are unlikely to change over time.

Each chapter contains a tool, how it works, and how it is useful to you and your business. First let's look at the reasons why we need these tools.

Overview of the command line tools

We will be looking at 8 different tools in this guide, a brief description can be found below:

- **Ping**: Allows you to check the IP address of a website.
- **Whois**: Provides you with information regarding a domain name, allowing you to check that the domain itself is operating correctly.
- **NSLookup**: Allows you to check the IP address of other services, such as mail, matrixstats etc.
- **Tracert:** Checks the actual route across the internet to a website.
- **Pathping:** Provides further information regarding the route to a website, with each step of the route tested.
- **NetStat:** Allows you to see the status of any connections on your computer.

- **Telnet:** Allows you to connect to a mailbox, check for corrupt emails and ensure that firewalls or antivirus software is not blocking the ports needed for connection.
- **IPConfig:** Used to see your customers internet connection. Can also be used to remove any “cached” data that may be causing website errors.

Accessing and setting up the command line interface

It’s easy to access the command line prompt; the process is slightly different depending upon which operating system you are using.

Vista and Windows 7

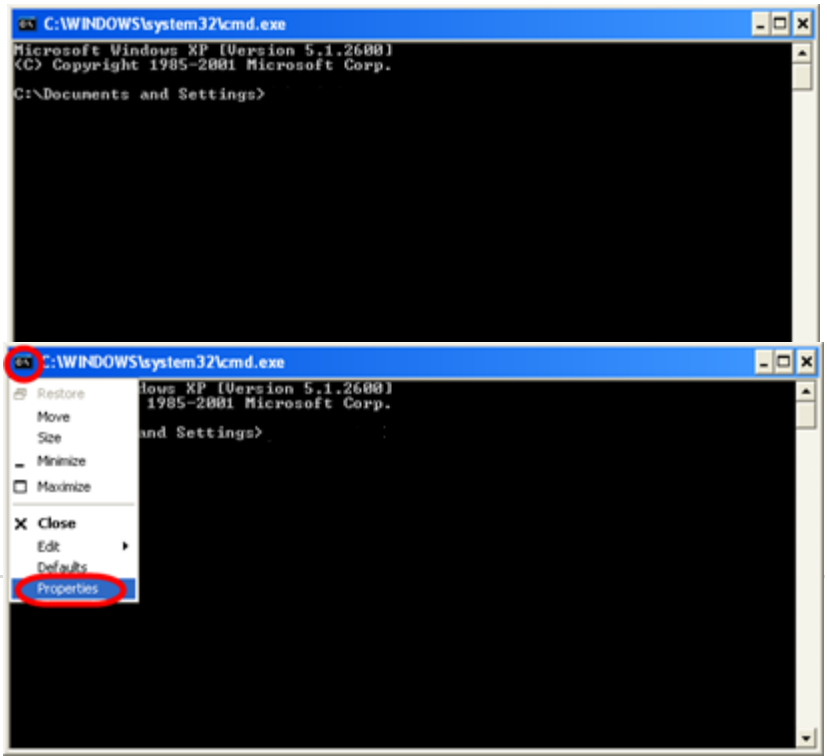
Click the windows button in the bottom left corner of the screen, then enter *cmd* into the search box. Press the <enter> key on your keyboard once complete.

Windows XP

Click Start, then Run. A new text box will appear. Enter *cmd* into this box and click **OK**.

Customising the command prompt

The command prompt will now open with a brief description of your operating system, and information about your current working directory (typically C:\documents and Settings\<your name>).



While I am happy to leave this console on the default settings, you may find that some

small tweaks to this view will make your life easier. You can changes the console settings by clicking on the console button in the top left of the screen, then clicking **Properties** in the drop down menu.

The properties box allows you to change Font and background, as well as allowing you to adjust the size of the console itself. Once useful feature can be found within the *Options* tab. This is the command history buffer. As you enter more commands older information is dropped. If you are running a large report, or want to save more of your command history, increase this buffer size.

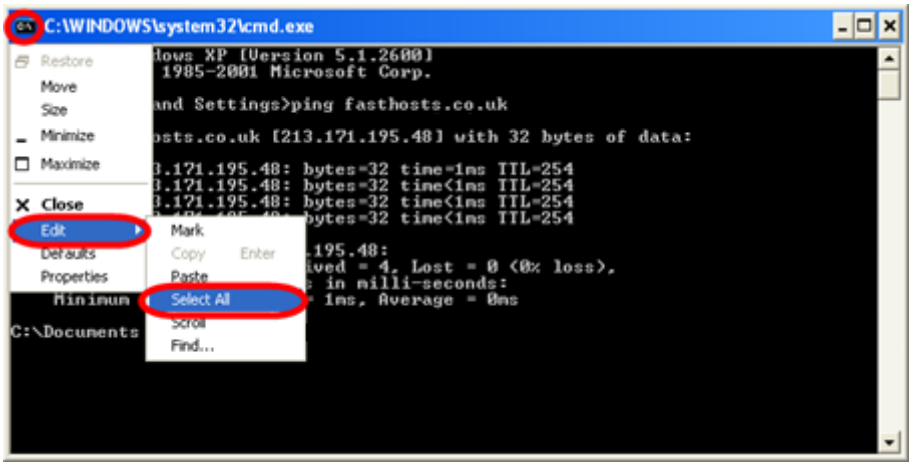
Retrieving information from the command prompt

There will be times when you will want to forward information given by the command prompt to Fasthosts, or you would like to retain a copy of the information yourself.

Using the command console it is not a simple case of using your mouse to copy and paste information, however it can be easily retrieved by clicking on the console button in the top left of the screen.

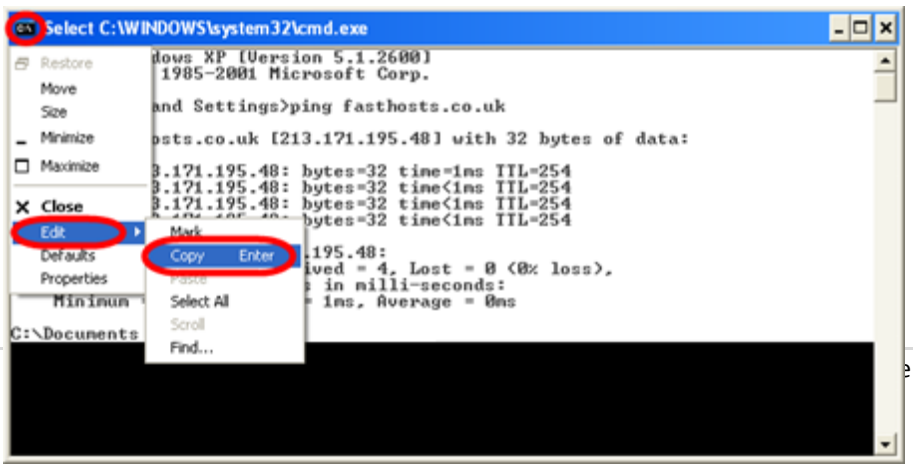
Step 1

Select the information in the command console by clicking the console button, then selecting *edit>Select all* from the drop down menu.



Step 2

Your text should now be highlighted. Click the console button, then select *edit>copy* to move the text onto your clipboard.



You can then paste this information into a text editor, an email, or any other program that you find suitable.

Useful Commands

Ping

Introduction:

The Ping (Packet Internet Grouper) command was first developed in 1983 and is one of the simplest and most effective tools you can use to resolve issues. It works in the same way as active sonar on a submarine, where a submarine will send out a loud sonar "ping" and then listening to the resulting sound bounce back off the target. This provides information on the direction of the target, while measuring the time taken for the sound to bounce back will provide some indication of the distance of the target.

The Ping command works in the same manner, providing direction information, and the time taken to respond to the Ping request.

Note: Fasthosts filter Ping traffic across their network, so although you will still be able to gain the IP address of a website, you will not receive replies for any websites hosted on the Fasthosts network.

How it works

First, Ping uses DNS to match a domain name to an IP address. Once it has the IP of the domain name it sends a request (called echo request) to that IP address using ICMP protocol and then starts an internal timer. The protocol used by Ping is slightly different than TCP which is used when looking at a website through a web browser, but is useful for sending small amounts of information across the internet.

When the receiving IP address receives these echo requests it will send an echo reply to the originating computer. When the originating computer receives this reply it will see how long it took to receive the reply and display this in a report.

Quick tip: By default Windows operating systems will send 4 separate requests to the destination. Unix based operating systems will continue to send ping requests until you click CTRL-C to cancel the command.

Uses

The ping command is most commonly used by network administrators to check that remote computers are able to respond to communications. It can also be used to check that the DNS for a domain name is set up correctly and the domain name resolves to the correct server.

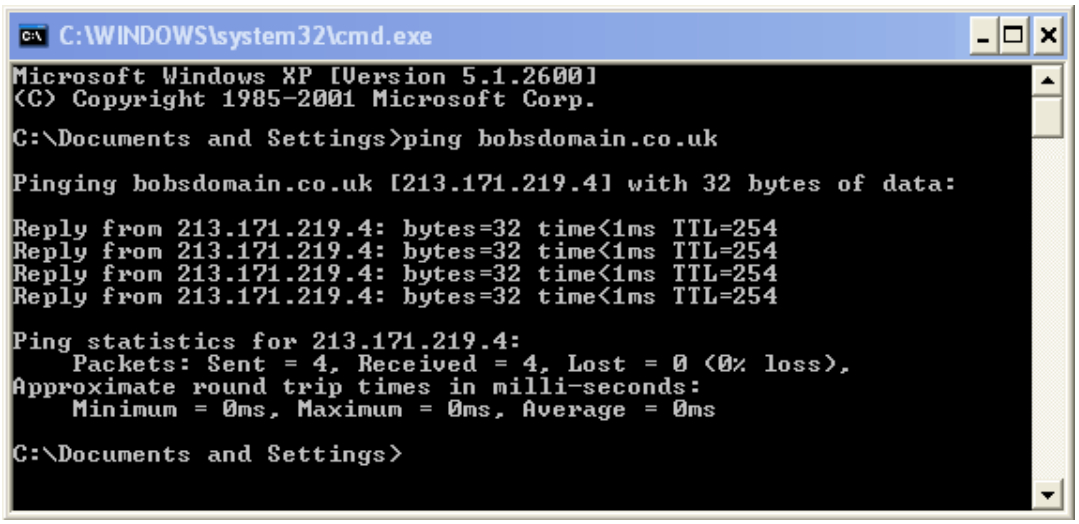
Syntax

```
Ping domainname_or_IP_address
```

Example

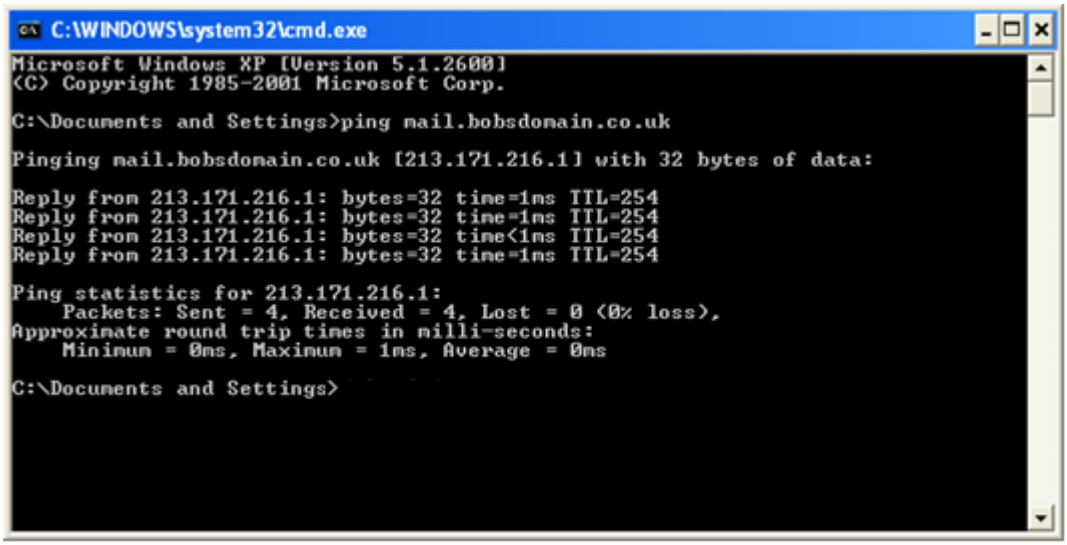
In this example, I will ping bobsdomain.co.uk, to find where the website is located and if the server is responding.

```
Ping bobsdomain.co.uk
```



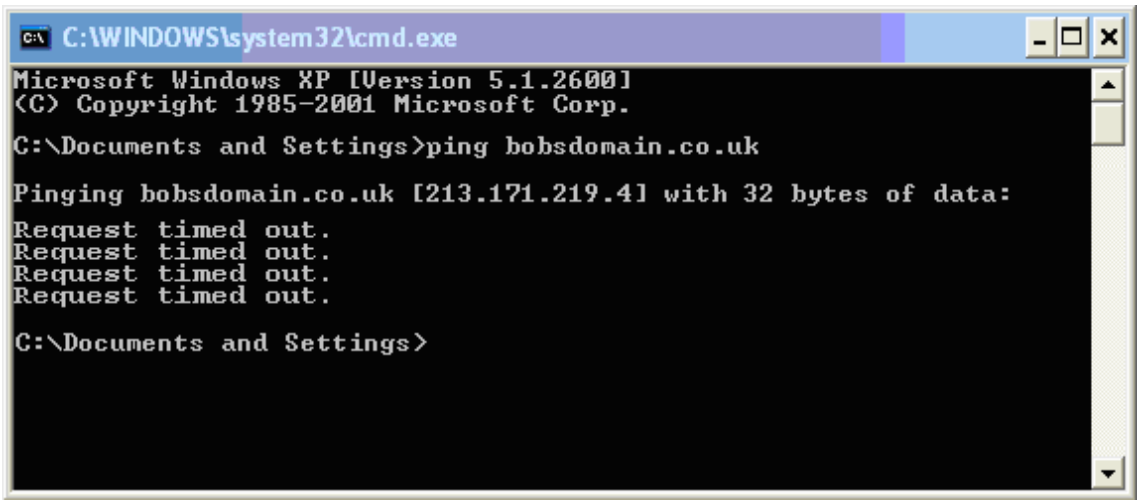
The Ping command can also be used to look up subdomains. For example, I could search for mail.bobsdomain.co.uk, and get the following result:

Quick tip: You can find out how I know there is a record called mail.bobsdomain.co.uk set up in the section on NSlookup.

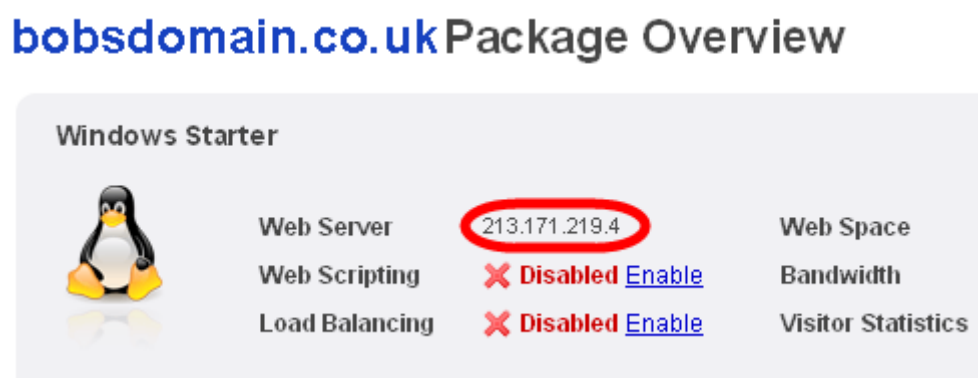


How to use the information

If you are "pinging" a domain name that is hosted on the Fasthosts hosting platform you will not receive the replies from the webserver, and will get a result similar to the following:



This is because we filter incoming ICMP traffic across our network. However, the location information is still shown (In the case above the IP address is shown in the square brackets just after the domain name). This is where the rest of the internet is looking for the website of the domain name. You can then look at the IP address shown in your control panel. If the IP addresses do not match you know there is an issue with DNS and can investigate further.



In this example the IP address returned by the Ping matched the IP address of the web server so we know the domain should be working.

Whois

Introduction

It should be pointed out that it is far easier to use an online Whois tool than to download and install a command line whois for your computer. Simply searching for “whois” will return a number of online whois searches that are free and easy to use, however if you would like a command line whois facility on your PC, there is one available to download from Microsoft

Technet. It can be located at: http://technet.microsoft.com/en-us/sysinternals/bb897435.aspx.

Copy the extracted file to C:\WINDOWS\system32 to use the tool directly from the command line.

How it works

When you registered your domain name you submitted certain information to the registry of the domain (for example, Nominet is the registry for .uk domain names). This information, in turn can advise the rest of the internet where to look for additional information on your domain name. Each registry has a special "whois" server that supplies this information upon request. This command sends a request to the whois server of your choice requesting information on your chosen domain name.

Note: Whois servers will only hold information on domain names that they are responsible for. You should choose the correct whois server for the type of domain name you are searching for.

Uses

A whois search will show you if a domain name is valid, or has expired. It also lets you know which nameservers hold DNS information for the domain name. If the domain name is using Fasthosts nameservers then quite often this is all the DNS information that you will need to know.

In addition to this a whois search will often give you an indication of any changes that have happened in the last 72 hours. If there have been changes to the whois during this period it is likely that propagation is still taking place. This can be the cause of a number of abnormalities.

Syntax

```
Whois domainname [whois.server]
```

Useful Whois Servers

Domain Extension	Whois Server	Domain Extension	Whois Server
.biz	whois.neulevel.biz	.name	whois.nic.name
.com	whois.internic.net	.net	whois.internic.net
.eu	whois.eu	.org	whois.publicinterestregistry.net
.info	whois.afilias.info	.tv	whois.nic.tv
.mobi	whois.dotmobiregistry.net	.uk	whois.nic.uk

Quick tip: A complete list of domain extensions and whois servers can be found within the appendix of this guide.

Example

For example, if I wanted to look up *bbc.co.uk* need to know the whois server for .uk domain names. I can see from the table above that this should be *whois.nic.uk*. So from the command line I will enter the following:

```
whois bbc.co.uk whois.nic.uk
```

How to use the information

A whois search provides a wealth of information regarding a domain name. For diagnostic purposes there are a few fields that are of particular importance.

Quick tip: Some whois searches will look slightly different from the image above. However the information shown within the search will remain the same regardless of the layout.

Relevant Dates

- **Registered on:** This is the date that the domain name was first registered. If this date is within the last 72 hours then it's possible that propagation is still taking place.

- **Renewal Date**: This will generally advise you if the domain name has expired, or is about to expire. However sometimes registries will add a year onto this date after a domain has expired in order to keep the information available in their whois search. If the renewal date occurs at the same time that the domain name experiences issues it may be an idea to investigate a little further.

- **Last Updated**: This is the date that the last changes were made to the whois search. While it will not tell you what has been changed, if this date occurs within the last 72 hours it is possible that a nameserver change has occurred and propagation is taking place.

Nameservers

This tells you which nameservers control the DNS records for the domain name. If Fasthosts nameservers are listed here then, by default, the domain name should point to any services within your control panel (however the advanced DNS settings within your control panel can override this). If the nameservers are elsewhere then further investigation may be required.

Registrar

This lets you know who is looking after the domain name registration. For example, if you wanted to change the nameservers on the domain name you would need to contact the registrar to request this.

NSlookup

Introduction

NSlookup is a useful suite of tools for looking at specific DNS records. While the ping command can only look at A records, the NSlookup command allows you to question your domains nameservers, and find out much more information regarding your domains DNS.

As NSlookup is a suite of tools, rather than the tools listed above, you actually enter the nslookup suite, complete any checks you want to make, and then exit the suite back into the command prompt when you are done.

How it works

To find services associated with your domain name, your Internet Service Provider will find the nameservers assigned to your domain name, then question these nameservers to find the information that they need. NSlookup sends these requests to a server of your

choice, allowing you to question your domains DNS servers in a similar manner to the rest of the internet.

Uses

NSlookup is useful for checking that certain subdomains that you want to use exist (sitebuilder.yourdomain.com) for example. It's also really useful for analysing multiple MX (email) records. Often people create multiple email records on their domain name, and then don't know where the email is sent to. It's also a useful tool if a domain name is not on our nameservers, as you can gain DNS information without having to contact the owners of the namesevers.

Syntax

```
Nslookup [-option][hostname][server]
```

Useful Commands

Command	Option	Description
nslookup		Opens the nslookup suite and allows you to start using the tool.
Server *name*		Set the default server to *name* using the current default server.
Set type=*option*		Will set the type of record that you are requesting.
	All	Will show you all the records for the domain name on that nameserver
	Any	Will show you any records on the server that it can find.
	Ns	Will show you the nameservers in use for the domain name.
	Mx	Will show any MMX (email) records that have been set up for the domain name.

	Txt	Will show and dns txt records that have been created. These could contain notes, or may hold SPF records to control email.
	A	Will show any A records that have been created.
	Cname	Will show Cname (Canonical names) for the domain name.
exit		Exits the program and returns you to the command prompt.

Note: When using the Server name command to change servers nslookup will attempt to find the server by asking the current default server for the location. This can cause errors. A way of getting around this is to enter the IP address of the server you want to query. You can find the IP address of the server using the Ping command described earlier.

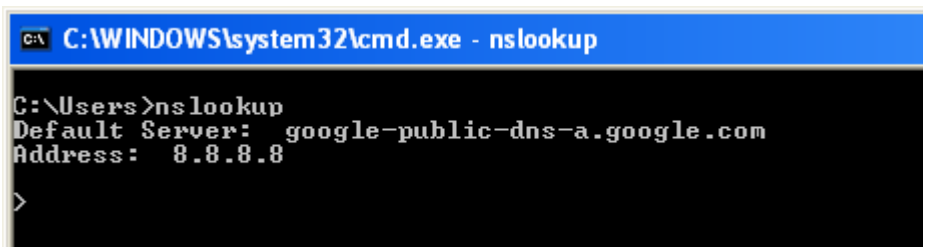
A full list of commands and error codes is available within the appendix of this guide.

Example

In this example we will have a look at the email records for *bbc.co.uk* and check to make see if any txt records exist for the domain name. From a whois search we already know that the domain uses ns1.bbc.co.uk as its nameservers, and by pinging the nameserver we know that the IP address is 132.185.132.21.

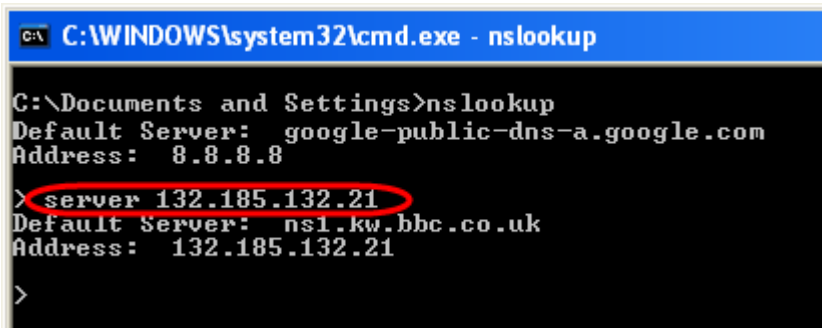
Step 1

Open the nslookup tool by entering *nslookup*



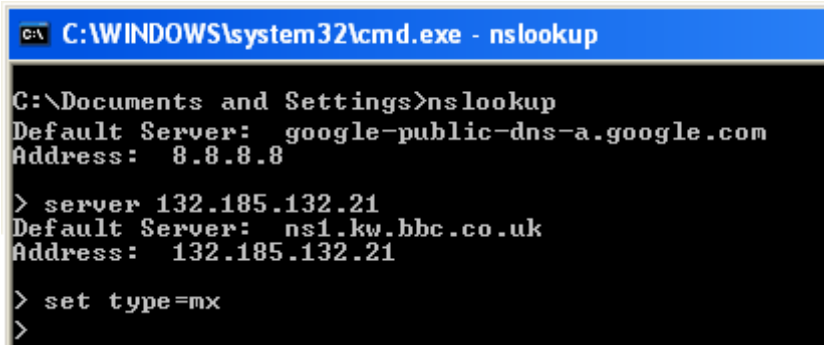
Step 2

Next, we need to change the server so that we are asking ns1.bbc.co.uk (132.185.132.21) for the information we require.



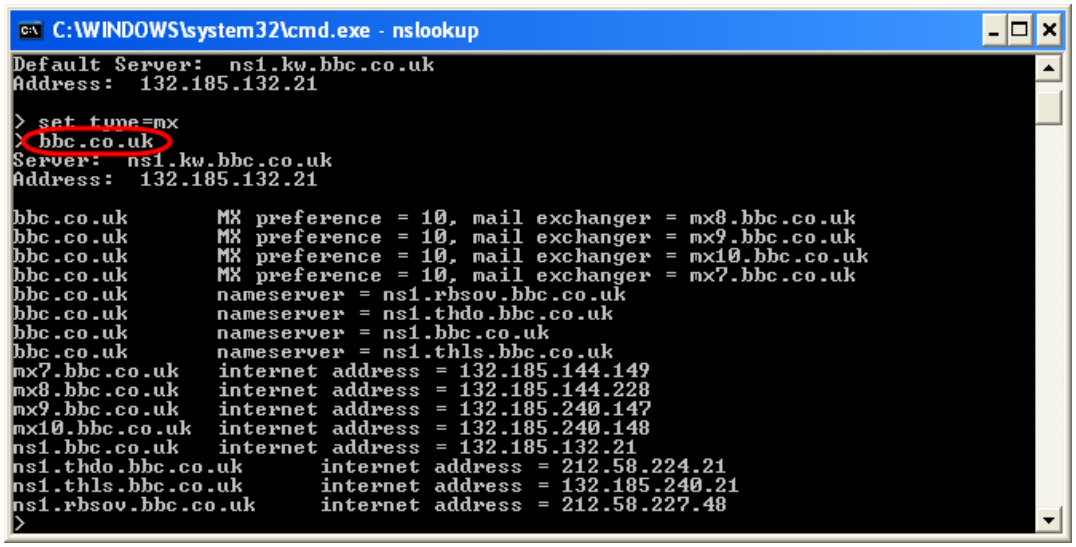
Step 3

Now we want to look for any MX (email) records that exist for this domain name, so we use the *set type=mx* command.



Step 4

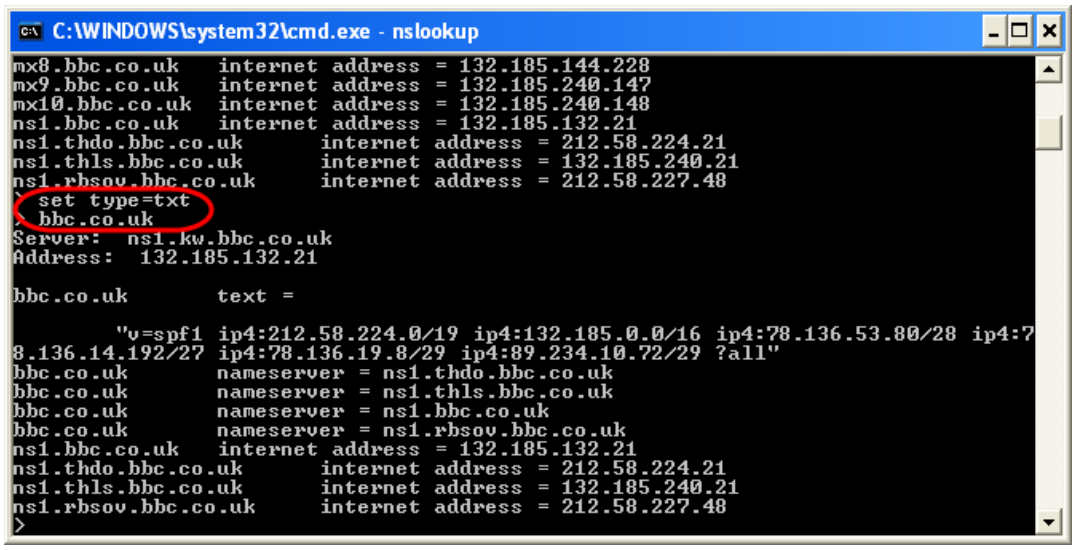
Finally we enter the domain name that we want to query.



We can see that bbc.co.uk actually has 4 mx records set up, so if they were experiencing a loss of some emails we could then check each of these mail servers to track down the issue. Most customers will only have one (or sometimes two) MX records.

Step 5

Next, let's see if there are any notes by checking for txt records associated with the domain name. So enter *set type=txt* and enter the domain name again.



We can see that they do have a TXT record set up, however, rather than a text message for other humans it reads:

```
"v=spf1 ip4:212.58.224.0/19 ip4:132.185.0.0/16 ip4:78.136.53.80/28
ip4:78.136.14.192/27 ip4:78.136.19.8/29 ip4:89.234.10.72/29 ?all"
```

The *v=spf* section of this note says that this txt record is actually used as an SPF record. SPF records regulate who can send email from the domain bbc.co.uk, so if they were experiencing issues sending email, this may be worth a check.

How to use the information

In the example above we can see that bbc.co.uk has 4 mailservers as follows:

- Mx8.bbc.co.uk
- Mx9.bbc.co.uk
- Mx10.bbc.co.uk
- Mx7.bbc.co.uk

As well as listing the mailservers there is also a "MX preference" setting shown. This tells computers which mailserver to send mail to first. If they don't get a reply they will try the next mail server, and so on until they reach the bottom of the list. The mail preference can be any number between 1 and 20. The lower the number the higher the priority.

For example if you had 2 mx records, one with a preference of 5 and one with a preference of 10. The email server with a preference of 5 would receive all email, with the other mailserver only taking over if the first one was unobtainable. In the case above, each mailserver has the same priority, so email is sent to each of the mailservers in a "round robin" fashion.

If the BBC were experiencing intermittent issues in receiving email we would be able to look at the records and see the multiple records. If one of the mailservers failed this would stop around ¼ of emails from being received, and would certainly appear to be intermittent to the end user so we would have a good place to continue our investigations. (I would then "ping" each mailserver to see if they respond).

Tracert

Introduction

This is another tool that has been around since the early days of Unix machines. It is useful for tracing a path to a website or server across the internet, to look for any issues along the way.

How it works

It works the same as a ping request, but sends out packets with differing TTL (Time To Live) levels. Each time the TTL level is reached the router responsible for that "hop" will reply. Tracert then displays these bouncebacks as a way of showing a route through the internet.

Quick tip: In theory, packets could be sent across many different routes to their destination. Tracert is not necessarily showing you a packets route through the internet, but where multiple packets end up along the way (which may be different).

Uses

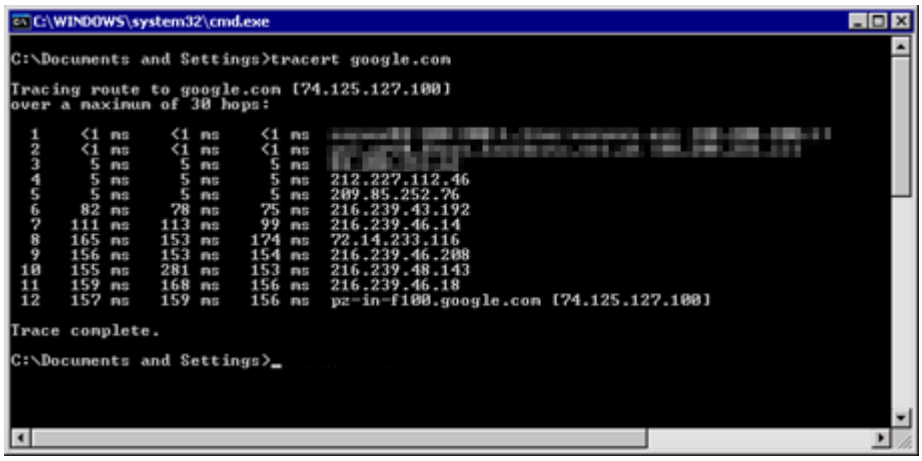
Tracert is a useful tool for checking for speed of connectivity, you can find out if your connection to a website is short, or is across many hops. As you can see the time at each hop, it will also give you an indication if there is a particular area of your route that is slower than the others.

Syntax

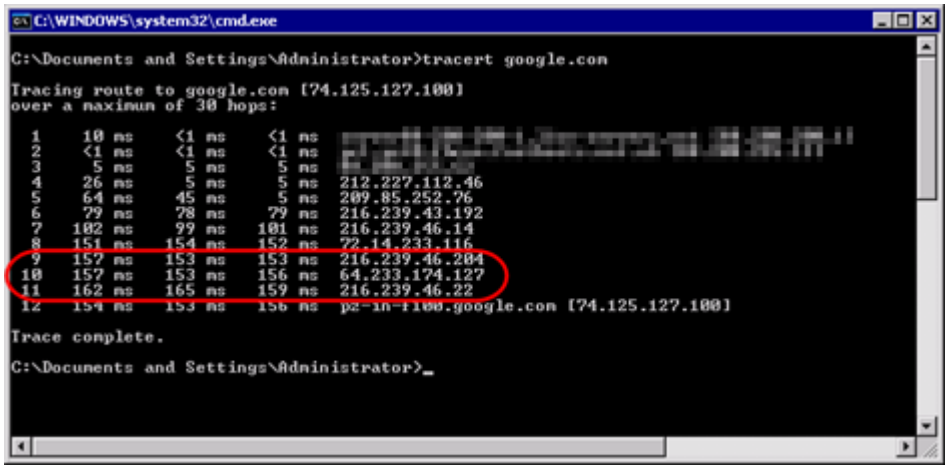
```
Tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
target_name
```

Example

In this example we can find the path from my server to google.com, so will use the command *tracert google.com*



However, something to mention is that this route is not always the same. If we run the same trace route again we may get a different response.



In the above example you can see that the start points and end points of the trace route are the same, but the actual routes that the computer takes to get there are different. For this reason it's always useful to create a couple or trace routes to get a better understanding.

How to use the information

This information is useful for diagnosing speed issues across the internet, it allows you an insight into where any delays may be occurring.

Pathping

Introduction

Pathping is a useful combination of tracert and the ping command. It's a good tool for finding out additional information regarding a connection across the internet and can be used to identify issues that tracert and ping used individually may not spot.

Quick tip: Pathping can take a while to complete so this is not a great tool to use if you are on the phone to a customer. However the additional information that it provides makes it a useful tool for end users to complete and copy the results to you.

How it works

Pathping will perform a tracert to a website or IP address of your choice, then ping each of the hops across that route. It will then display the degree of packet loss at any given router or link.

Uses

Pathping provides useful information regarding packet travel across the internet, it not only shows the path across the internet that your packets are taking to the destination, but also analyses each hop along the route to identify the time a router may take to respond and any packet loss that may be occurring along each of these hops.

It can also be used by ISP's to check routes and configuration settings of routers across their network.

Syntax

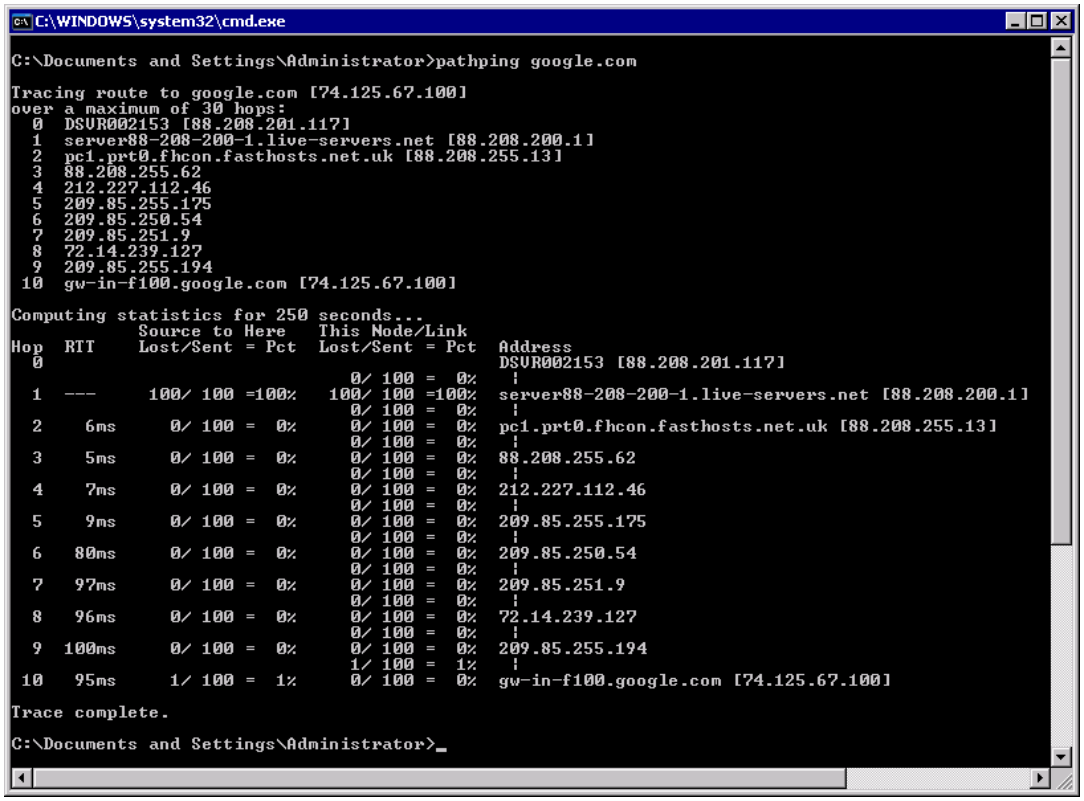
`Pathping hostname`

```
Pathping hostname
```

Example

In this example we will use the pathping command to check the route between a server and google.com using the command:

```
Pathping google.com
```



There is quite a lot of information listed here, but let's break this report up a little and see what information it contains.

```
C:\Documents and Settings\Administrator>pathping google.com

Tracing route to google.com [74.125.67.100]
over a maximum of 30 hops:
  0  DSVR002153 [88.208.201.117]
  1  server88-208-200-1.live-servers.net [88.208.200.1]
  2  pc1.prt0.fhcon.fasthosts.net.uk [88.208.255.13]
  3  88.208.255.62
  4  212.227.112.46
  5  209.85.255.175
  6  209.85.250.54
  7  209.85.251.9
  8  72.14.239.127
  9  209.85.255.194
 10  gw-in-f100.google.com [74.125.67.100]
```

First the report completes a trace route to find the path that it should analyse. This shows the number and location of each hop on the internet, but does not provide you with response times as tracert will do.

Next it will analyse each of these hops. This can take some time, depending upon the number of hops it needs to analyse. In this 10 hop example, it takes around 250 seconds to collate and analyse the data it needs.

```
Computing statistics for 250 seconds...
```

Finally, it will provide a report for each of the hops along the route. This is displayed as a table, with statistics shown in each column and the hops along each row of the table. You will notice that each hop has two figures. One (identified by the IP address) shows response times and packet loss on the router itself, while the other figures (denoted by the | symbol) shows the packet loss across the link between hops.

Looking at each column we can see the following:

- **Hop**: Shows which hop along the route is being analysed.
- **RTT**: (Round Trip Time) shows the number of milliseconds it takes for the router on each hop to respond.
- **Source to here**: Shows cumulative information across the route
    - **Lost**: The number of packets that have been lost.
    - **Sent**: The number of packets that have been sent.
    - **Pct**: Percentage of packet loss.
- **This Node/Link**: Shows information relating to the particular hop
    - **Lost**: The number of packets that have been lost.
    - **Sent**: The number of packets that have been sent.
    - **Pct**: Percentage of packet loss.

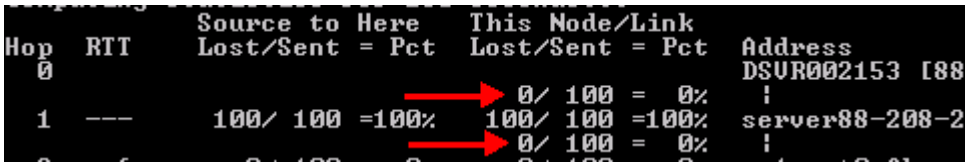
Address: The IP address (and any reverse DNS information) of each router in along the route. The | symbol denotes the actual connection between the hops/routers along the route.

Interpreting the information

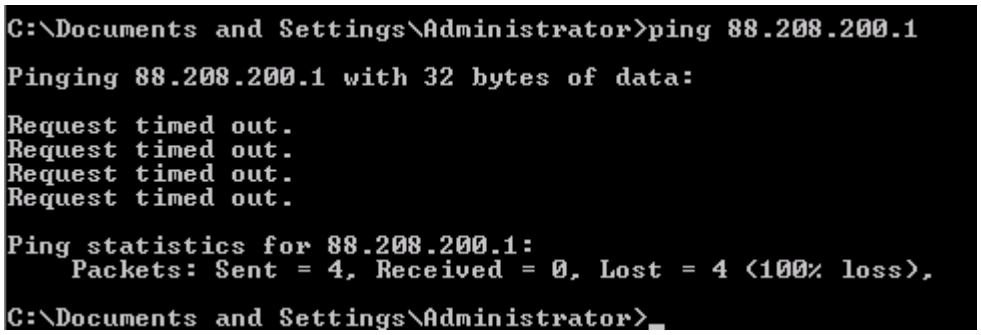
There are a couple of hops in the example shown above that show how we can use the information in a pathping report. First let's have a look at hop 1.

```
                Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                          DSVR002153 [88
                                   0/ 100 =  0%   |
  1  ---     100/ 100 =100%  100/ 100 =100%  server88-208-2
                                   0/ 100 =  0%   |
```

This particular hop appears to have lost all 100 packets that were sent to it. The row highlighted above show packets sent directly to that router. Looking at the row above and below the router, we can see that all packets are reaching the router, and are being forwarded by it.

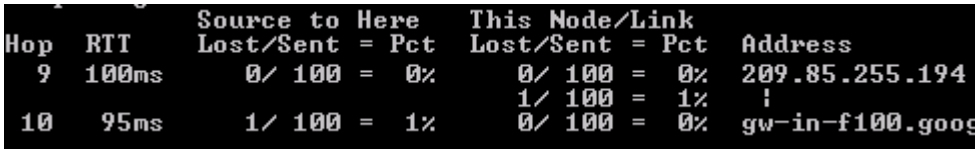


So this is only traffic addressed directly to that router that is being affected. Next we need to remember how pathping is sending traffic to the router. The command sends packets directly to the router using the same type of packet that ping uses. So it's likely that this router is operating correctly, but does not respond to ping requests. Let's ping the router and find out.

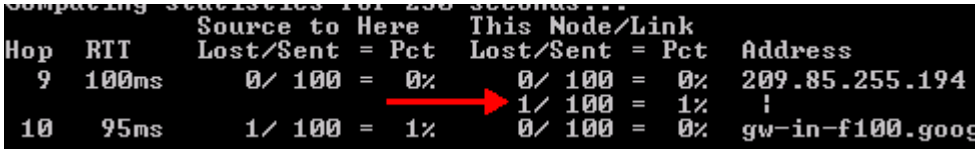


Ok, so this originally looked like it may have been a router failure, but it is just how the router is configured. However this is always worth bearing in mind if you see 100% packet loss on any hop, as in most cases it just shows that the router is configures not to respond to these requests.

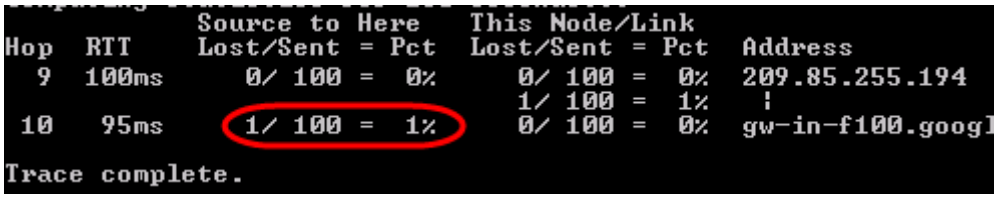
Next let's look at hops 9 and 10.



The routers at hops 9 and 10 both appear to be working well, both are responding to ping requests and don't take too long to reply. However a look at the connection between them shows a 1% packet loss. This in itself is not too bad, but it does indicate that the connection between these routers is busy at the moment and a small amount of traffic is being dropped.



Hop 10, now shows that getting this far you may receive a 1% packet loss. Any further packet losses between other hops would also be recorded in this column to show you the overall loss across this route.



How to use this information

As the internet is more popular and files become larger, more and more data it passed between routers each hour. Sometimes routers can become bogged down in traffic and drop packets along a connection (some ISP's may also do "packet shaping" this is when they selectively drop certain packets in order to maintain quality of service for the rest of their customers).

If any of the above is happening on a connection, pinging the routers or a tracert will not show this clearly.

If you complete a pingpath and spot packet loss between two hops you have identified a reason why your connection may be running slowly. Unfortunately, there is nothing you as a user can do to remedy the error (without contacting the administrators of the router). However, issues of this nature are generally short lived and intermittent in nature.

Netstat

Introduction

Netstat is an early tool, dating back to the days of Unix machines. As such, it can still be found on all operating systems (although some of the options may differ between operating system manufacturers).

How it works

Netstat displays instant statistics regarding your network connections. It will tell you what connections you have open, what applications are using these connections, and the status of each connection.

Uses

This is useful for finding out which applications are active on the internet and to ensure that unauthorized software is not connecting to the internet without your knowledge.

Syntax

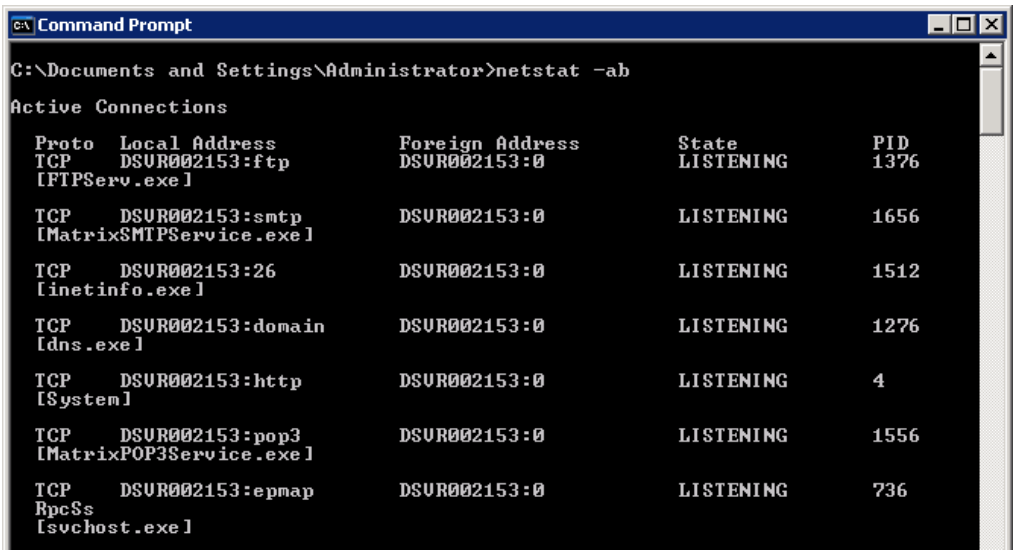
```
Netstat [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]
```

Switches

Switch	Description
-a	Displays all the connections and ports that are listening (open)
-b	(Windows XP SP2 or later) Displays the executable file responsible in creating each connection or listening port.
[interval]	Will display a new set of results each [interval] seconds. This will continue to display updates every [interval] seconds until the <ctrl>+C key combination is used.

Example

In this example I have used netstat –ab to see all connections, and the executable that is responsible for the connection.



Because this screenshot was created on a dedicated webserver, there are too many open connections to show in one image, but it is a good demonstration of what services may be open.

How to use this information

Once you have completed a netstat you should look at open connections. Each open program or connection will be sharing your broadband line. If you have a large number of connections open, the share of the line for each program will be less, making your broadband connection appear slow.

Netstat can also be used to check that only programs you know are using your internet connection. Sometimes viruses or other malicious software can become installed on your machine, these will often connect to the internet to report in to their operator, to send unsolicited emails, or another similar purpose. As netstat displays all your connections, it can often show these unauthorized connections. If, after using the netstat command you notice a program running that you don't recognise, it may be worth investigating further, or running a virus scan, to ensure that your computer is kept clean of malicious software.

Quick tip: A proportion of malicious software communicates back to its controller using Internet Relay Chat (IRC). If you have a connection open on port 6667 and do not use IRC yourself then there is a good chance your computer has been infected.

Telnet

Introduction

Telnet is a set of tools that allow users to remotely access another computer. It is a useful and easy tool to use. Although it's only available by default on Windows 2000 and XP operating systems, it's easy to add to Vista and Windows 7 operating systems.

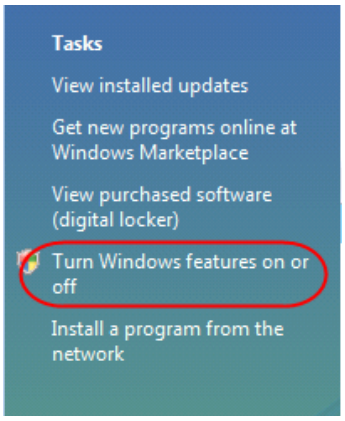
Adding Telnet to Vista and Windows 7

Step 1

Open the Vista control panel.

Step 2

Click **programs>Uninstall a program** (In classic view click **Programs and features**).

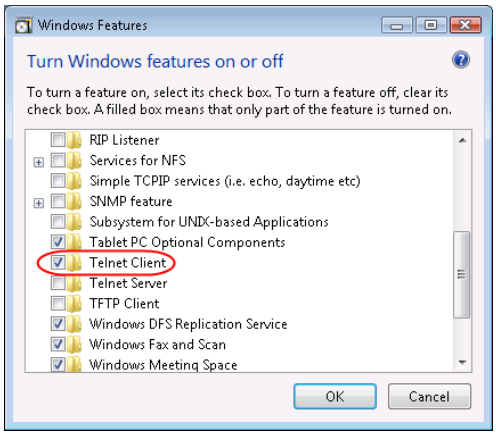


Step 3

Click **Turn Windows features on or off**.

Step 4

Scroll down the list of windows features and tick the box marked **Telnet Client**.



Step 5

Click **OK** to add the telnet client to your computer. This may take a few minutes to take effect.

How it works:

Telnet is a client/server based program. Your operating system takes the role of a client, while the telnet server is installed on most internet servers. This allows you to log onto the server and perform basic tasks.

Uses

Telnet is useful for testing mailservers. It also allows you to solve issues relating to corrupt emails. If an email becomes corrupt your mail client may not be able to download it onto your local machine. This can often case a “blockage” with additional emails that arrives after the corrupt email not being downloaded by the email client either. By logging directly into the email server you can delete the corrupt email and download the rest of your mailbox again. It’s also a very useful tool for identifying if a firewall or virus scanner is blocking the connection to the mailserver. Often this software will not show what ports it’s blocking. By connecting via telnet you force the software to notify you of its presence in a popup window. Making it very easy to diagnose this type of fault over the phone.

Syntax

```
telnet [hostname][port]
```

While you can use telnet to communicate to a number of services, this guide will show you how to connect to email, so if we were to connect to our mailbox at bobsdomain.co.uk we would enter the following command.

```
telnet bobsdomain.co.uk 110
```

Useful Ports

Port	Description
110	POP3 mail server (for receiving email)
143	IMAP Server (for receiving email)
25 or 587	SMTP server (for sending email)

Quick tip: By default your computer will try and send mail using port 25. However many ISP's will block this port, so you may actually be connecting on port 587 to our SMTP server. This information can be found within the settings for your email client.

Useful Commands

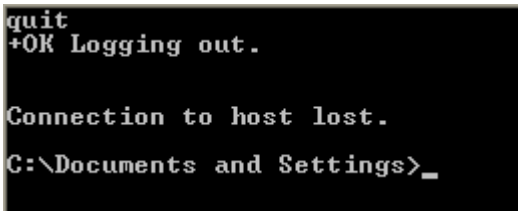
Command	Description
User *username*	Allows you to enter your username when connecting to the email server.
Pass *password*	Allows you to enter your password when connecting to the email server.

Stat	Will show the number of messages in your mailbox and the size (in bytes) of mailbox space used.
	
	`+OK Logged in.`
	`stat`
	`+OK 4 269101`

List	Will list a line for each message in your mailbox, with its number and size (in bytes).
	
	`list`
	`+OK 4 messages:`
	`1 8090`
	`2 249862`
	`3 8462`
	`4 2687`
	`.`

Top *msg# #lines*	This is an optional POP3 command that will not work on all mailservers (Although it is enabled on Fasthosts servers). It lists the email header for each message along with the first #*lines* of the message text itself.
	
	`top 1 10+OK`
	`Return-Path: <[redacted]>`
	`Delivered-To: bob@bobsdomain.co.uk`
	`Received: from virus_17.livemail.co.uk (virus-cluster.livemail.co.uk [213.171.21`
	`6.10])`
	`by smtp-in-129.livemail.co.uk (Postfix) with SMTP id 9C64261B715`
	`for <bob@bobsdomain.co.uk>; Fri, 29 May 2009 10:54:49 +0100 (BST)`
	`X-Span-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on`
	`span-87.livemail.co.uk`
	`X-Span-Level:`
	`X-Span-Status: No, score=-98.2 required=5.0 tests=HTML_MESSAGE,`
	`MIME_QP_LONG_LINE,USER_IN_WHITELIST autolearn=disabled version=3.2.5`
	`Received: from smtp-out-57.livemail.co.uk (smtp-out-60.livemail.co.uk [213.171.2`
	`16.60])`
	`by smtpin-133.livemail.co.uk (Postfix) with ESMTP id 505B424E4FE`
	`for <bob@bobsdomain.co.uk>; Fri, 29 May 2009 10:54:46 +0100 (BST)`
	`Received: from EDG01.fasthosts.com (unknown [213.171.217.138])`
	`by smtp-out-57.livemail.co.uk (Postfix) with ESMTP id 2723A5FB895`
	`for <bob@bobsdomain.co.uk>; Fri, 29 May 2009 10:54:46 +0100 (BST)`
	`Received: from FH-EXCH07-01.fasthosts.local (10.44.244.94) by`
	`EDG01.fasthosts.com (10.44.224.192) with Microsoft SMTP Server (TLS) id`
	`8.1.358.0; Fri, 29 May 2009 10:47:49 +0100`
	`Received: from FH-EXCH07-01.fasthosts.local ([10.44.244.94]) by fh-exch07-01`
	`([10.44.244.94]) with mapi; Fri, 29 May 2009 10:53:58 +0100`
	`From: [redacted]`
	`To: "bob@bobsdomain.co.uk" <bob@bobsdomain.co.uk>`
	`Date: Fri, 29 May 2009 10:53:57 +0100`
	`Subject: holiday`
	`Thread-Topic: holiday`
	`Thread-Index: AcngQ2KpL83VcOIMT+O61rORIoNjuw==`
	`Message-ID: <A06CDC05133A0241BEC530BD1ED160D4862643A7@fh-exch07-01>`
	`Accept-Language: en-US, en-GB`
	`Content-Language: en-US`
	`X-MS-Has-Attach:`
	`X-MS-TNEF-Correlator:`
	`acceptlanguage: en-US, en-GB`
	`Content-Type: multipart/alternative;`
	`boundary="_000_A06CDC05133A0241BEC530BD1ED160D4862643A7fhexch0701_"`
	`MIME-Version: 1.0`
	`X-Original-To: bob@bobsdomain.co.uk`
	`X-AntiVirus: checked by Vexira MailArmor`
	
	`--_000_A06CDC05133A0241BEC530BD1ED160D4862643A7fhexch0701_`
	`Content-Type: text/plain; charset="us-ascii"`
	`Content-Transfer-Encoding: quoted-printable`
	
	`Hi Bob,`
	
	`.`

Dele *msg#*	Will mark the message number *msg#* for deletion. This is the best way to delete a corrupt email. This will not delete the message straight away, but

	will mark if for deletion until you sign off the telnet server.
Rset	This will reset any emails that are marked for deletion (so that they will no longer be deleted when you quit.
quit	Deletes any messages marked for deletion and logs you off the mail server. 

Example

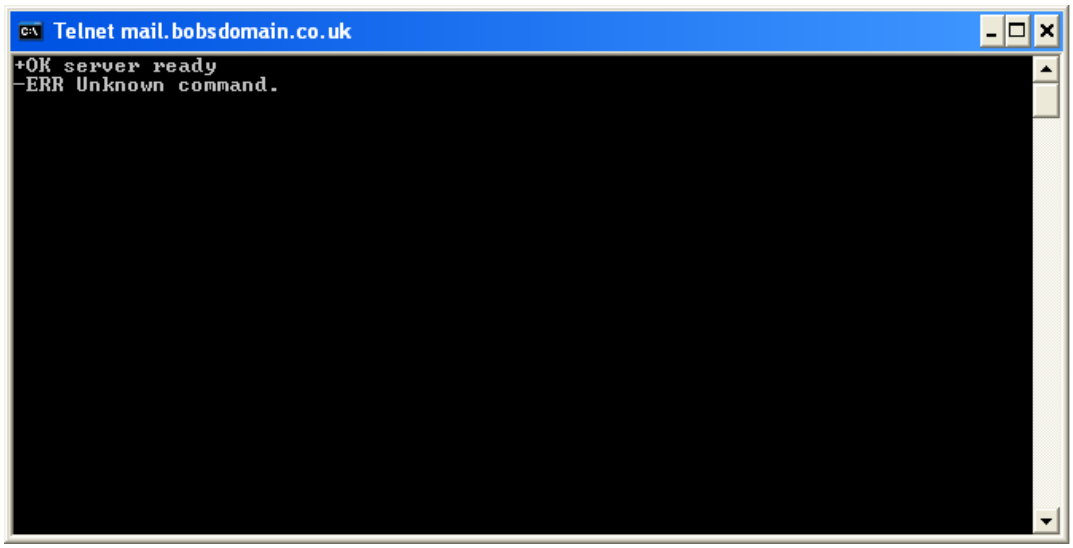
In this example we will try and connect to the mailbox bob@bobsdomain.co.uk, list all the emails. Then delete a sacrificial "corrupt email".

Step 1

Attempt connection to the email server using

```
telnet mail.bobsdomain.co.uk 110
```

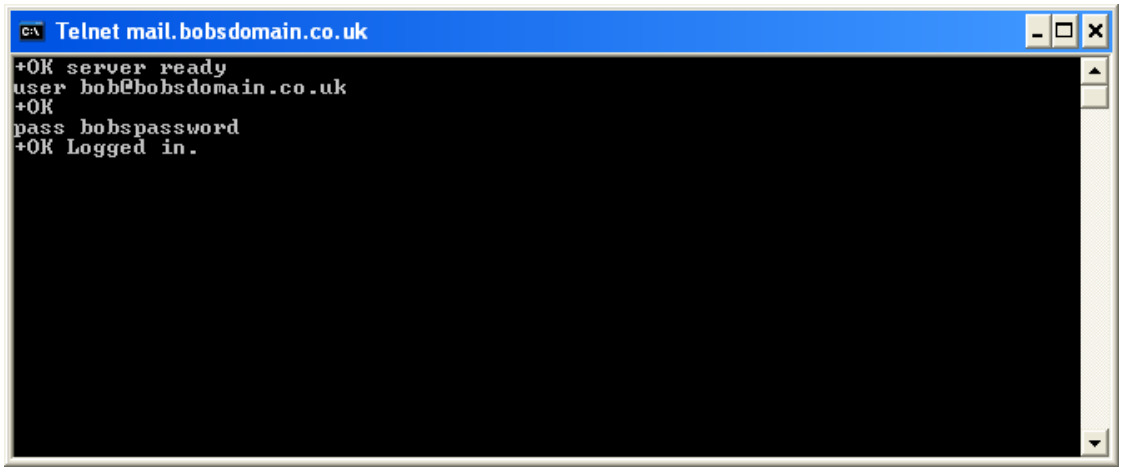
You will see a message to show that you have been connected.



Step 2

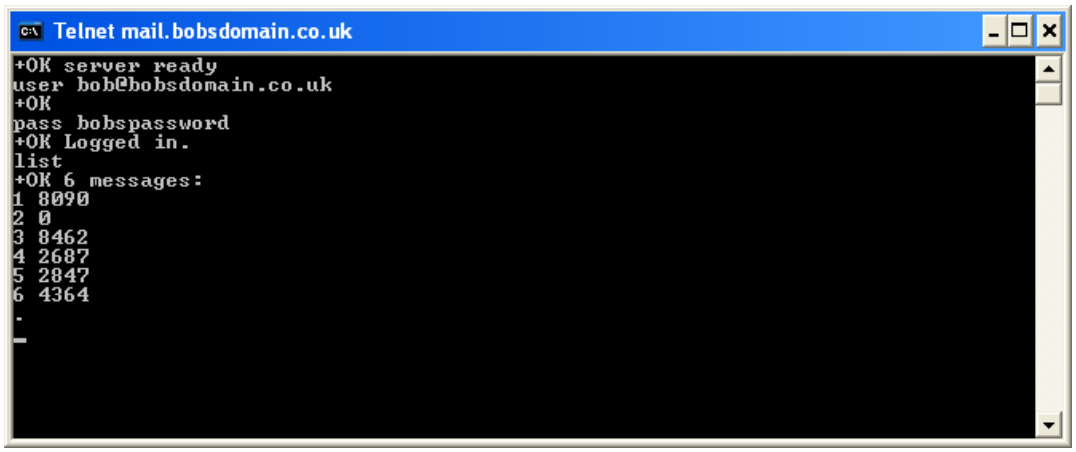
Log onto the mailbox using the mailbox username and password.

Quick tip: Telnet sends each letter to the server as you type your details, so if you make a mistake you will not be able to use the [del] key to remove typing mistakes. It's easier to press enter, then enter your command again.



Step 3

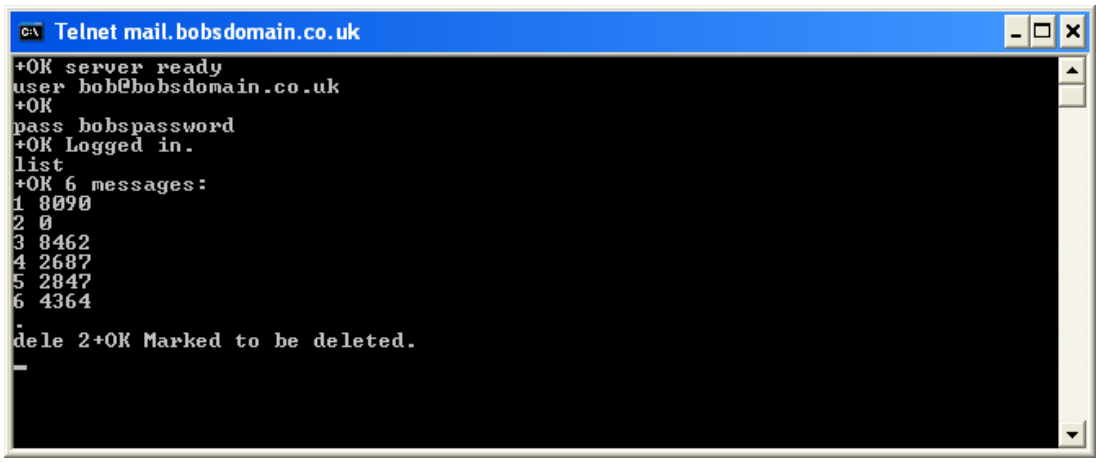
List the emails within the mailbox.



Message 2 is showing up as 0 bytes in size. This is a corrupt email and will cause problems in downloading any future emails.

Step 4

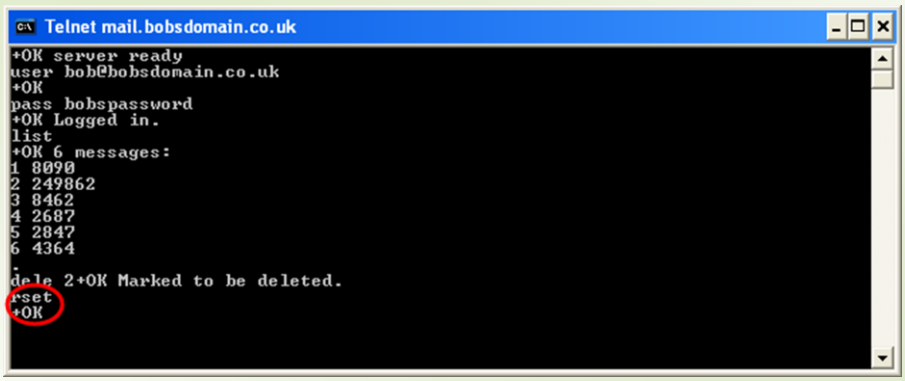
Mark message 2 for deletion using the *dele* command.

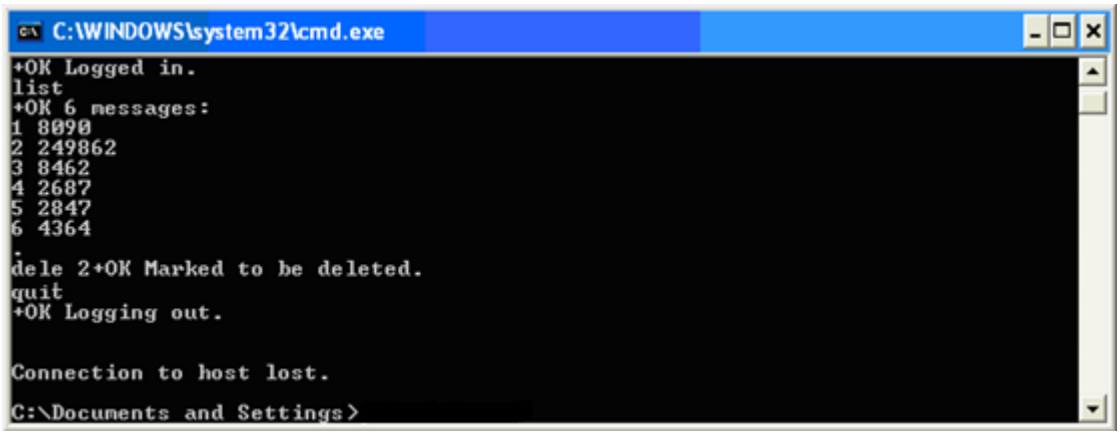


Step 5

Use the *quit* command to close your connection and delete any emails.

Quick tip: If you accidently set the wrong message for deletion you can "unset" the deletion status using the *rset* command.





You can also use Telnet to connect to the SMTP server. You would connect to the SMTP server with a command similar to the following:

```
telnet smtp.bobsdomain.co.uk 25
```

However, once you have established connection to the server there is little troubleshooting that can be done, so we will not go into further detail at the moment. There are many additional guides on the internet if you want to send email via the telnet command.

IPConfig

Introduction

The Windows IP Configuration tool (ipconfig) allows you to find information regarding your network card and connection to the local area network. It is used more with broadband troubleshooting, but can have limited benefits for some website issues.

How it works

The ipconfig command gathers data relating to your network card and connections from your operating system and displays the results. You can also use this command to make changes to your network settings if you need. Further information on this is available in our guide to broadband.

Uses

While this is a useful command to know if you are supporting broadband for your customers, from a hosting point of view it has limited benefits. The main use is to clear the operating systems dns cache. This is useful if a customer has made changes to their website, but when visiting the website a short time afterwards, is unable to see the changes.

Syntax

```
Ipconfig [/?] [[/all] [/renew adaptor] [/release adaptor] [/flushdns]
[[/displaydns][/registerdns] [/showclassid adapter] [/setclassid adapter
classid]
```

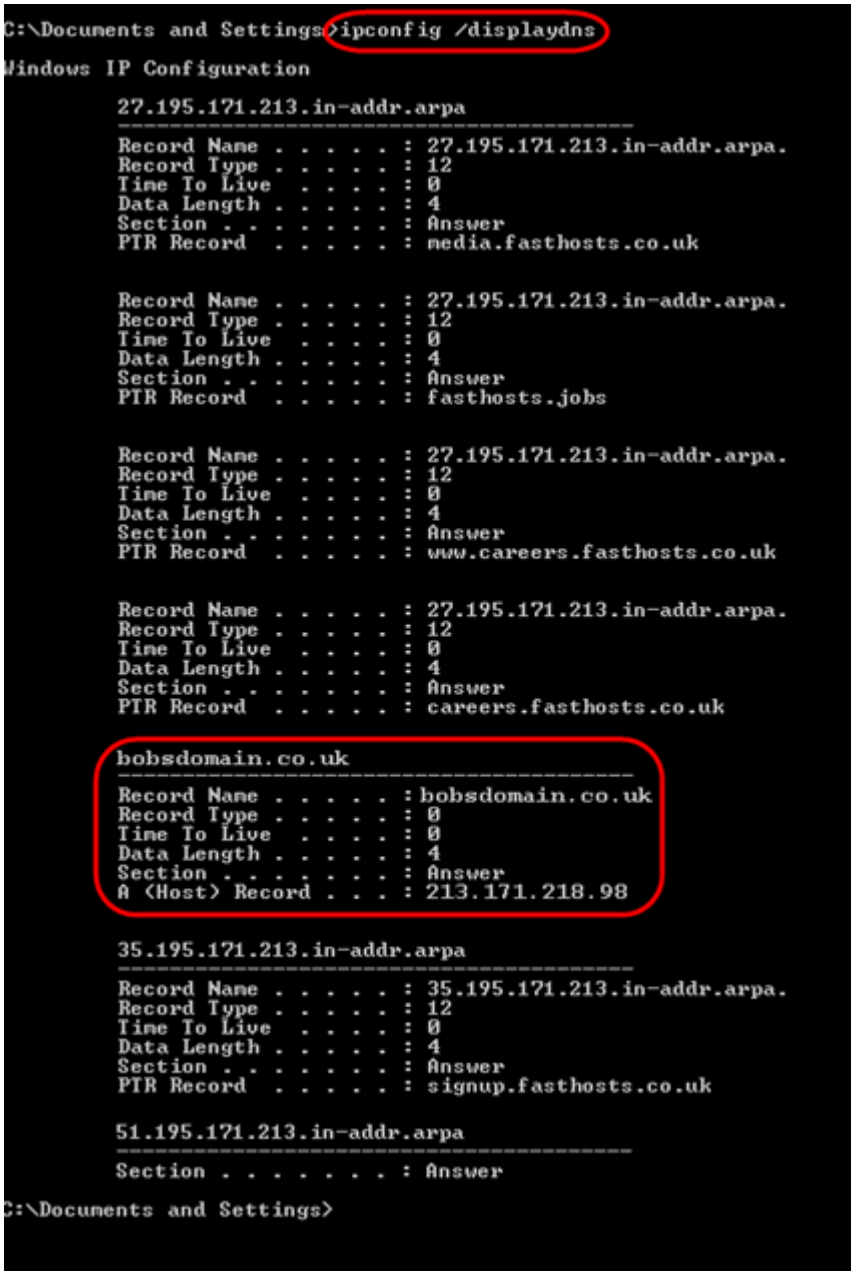
Options

Option	Description
/?	Displays help information
/all	Displays full configuration information
/displaydns	Displays the contents of the DNS resolver cache
/flushdns	Purges the DNS resolver cache

Example

In this example the owner of bobsdomain.co.uk is unable to see the changes that they have just made to their website. I have checked the website myself and can see the changes clearly. This indicates that the previous version of the website is cached somewhere. While this may be cached with the ISPs server, it may also be cached on the end users PC. In this example we will look for the website in the cache, then if found, clear the cache.

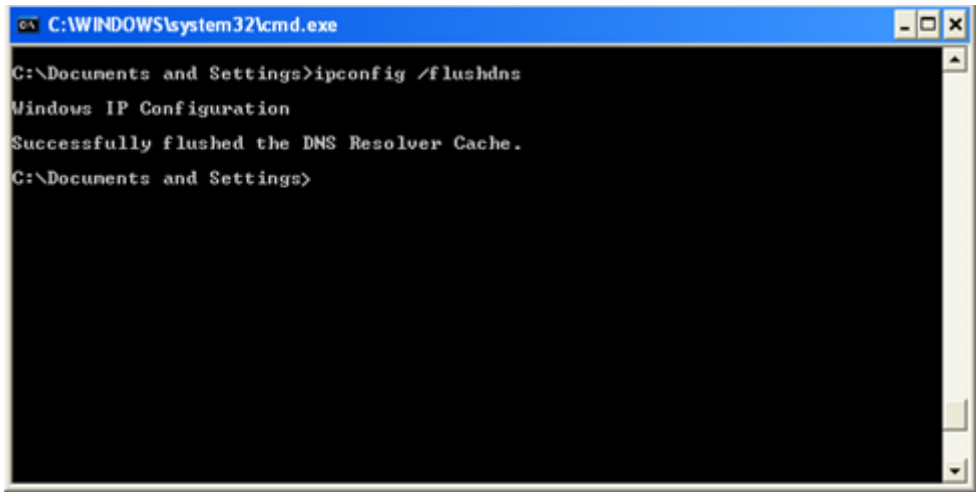
First let's use the ipconfig /displaydns command to see what records are in the resolver cache.



In practice it may be tricky find a domain name in the report (as it can become quite long). So often it's worth just clearing the cache and then trying to find the website again.

Clearing the cache is easy, just use the command:

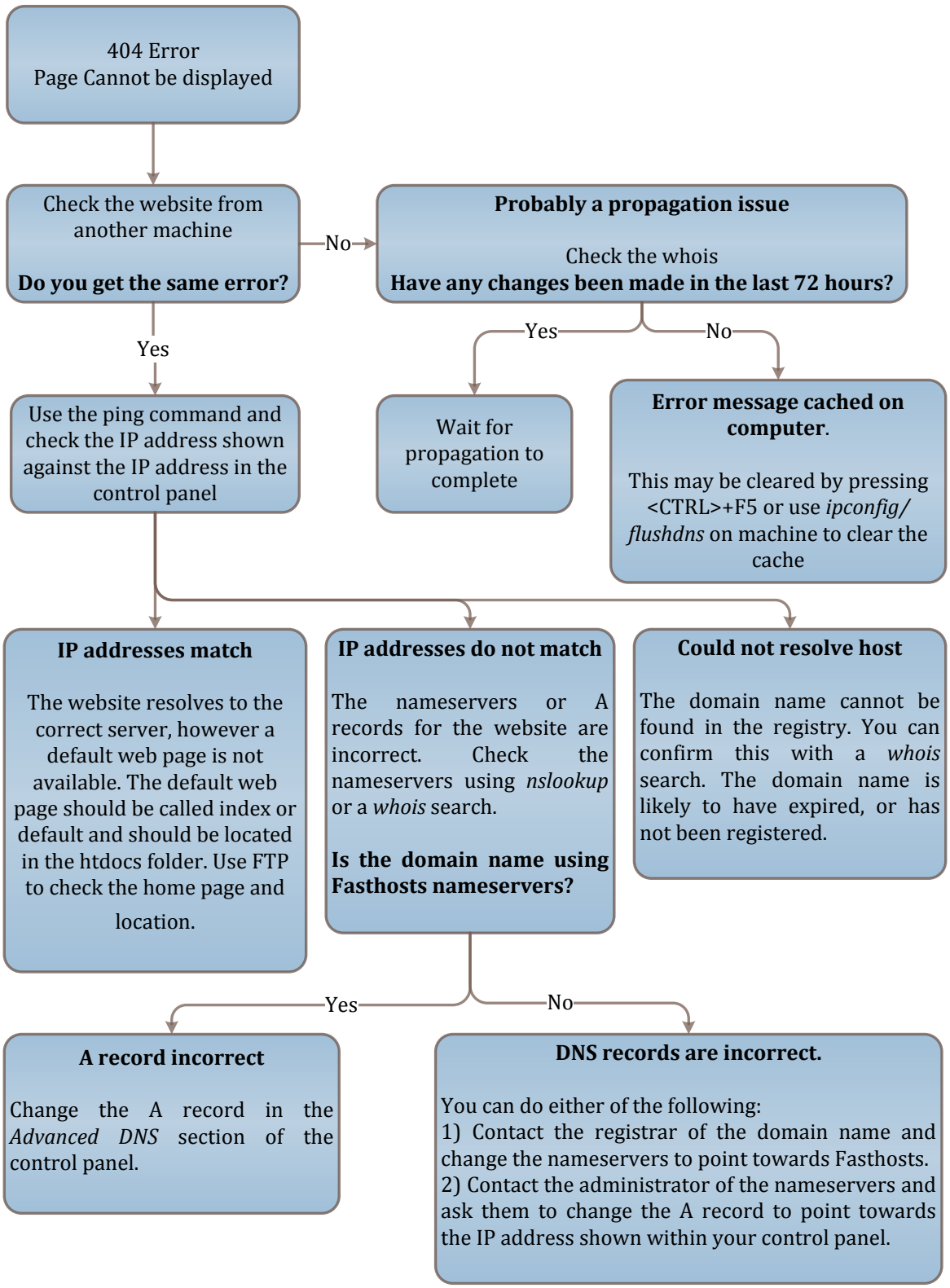
```
Ipconfig /flushdns
```



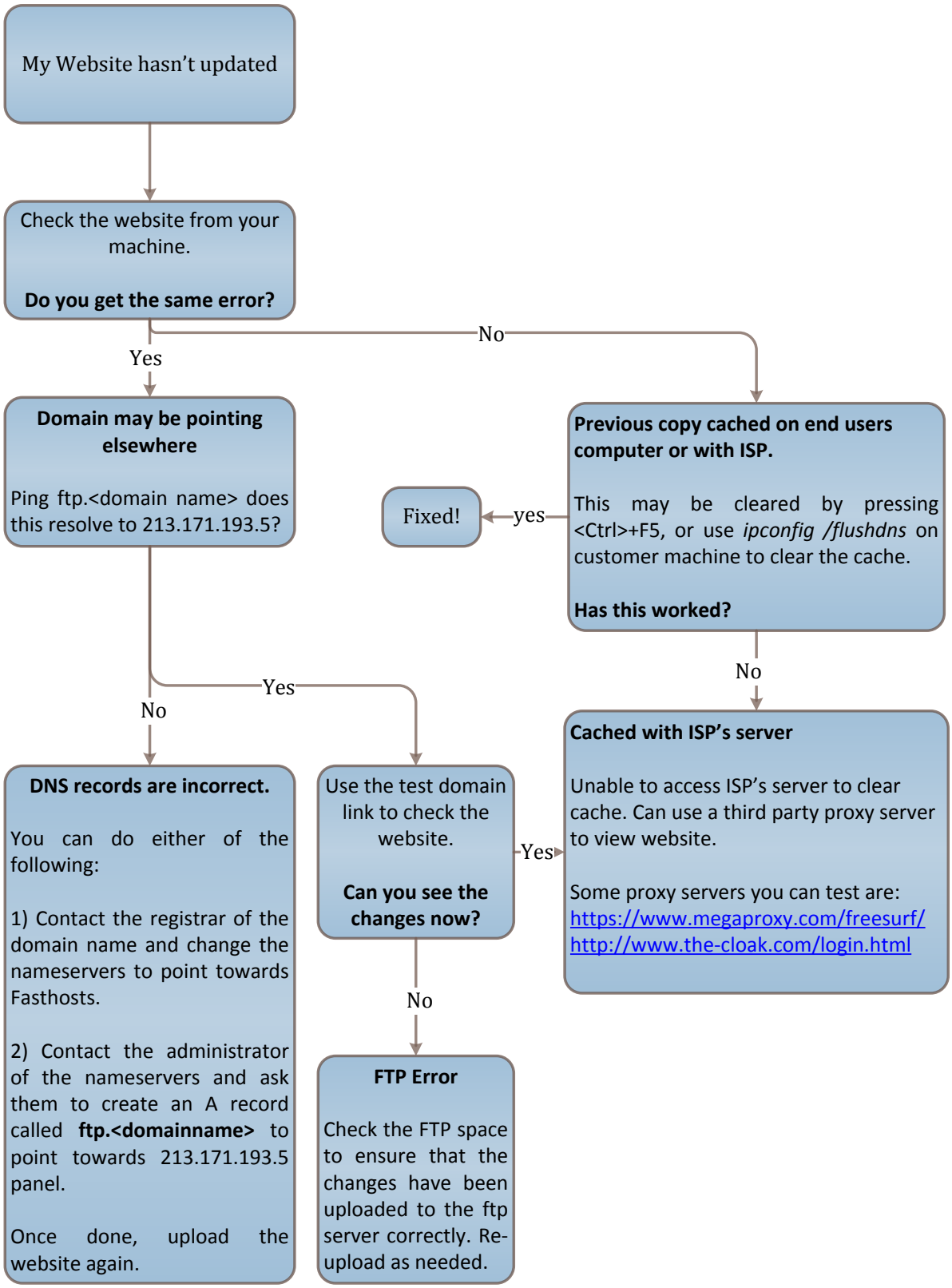
You will receive confirmation that the cache has been cleared. Once cleared the customer should look at their website again. If they are still unable to see the changes that they have made to their website the issue is likely to be with their ISP's servers. This can be tested using a third party proxy server.

Troubleshooting websites

404 errors (Page cannot be displayed)

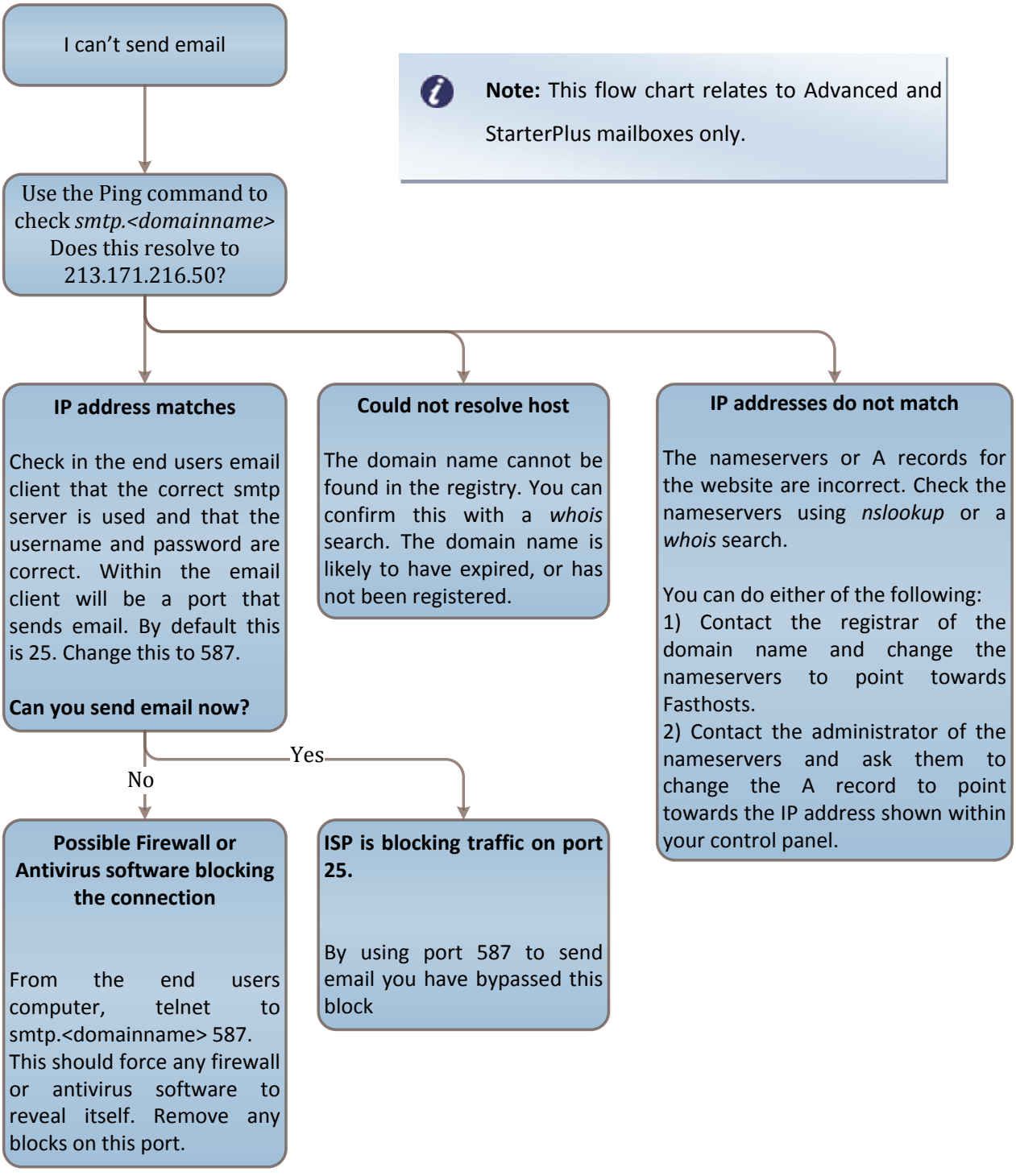


I can't see the changes I made to my website

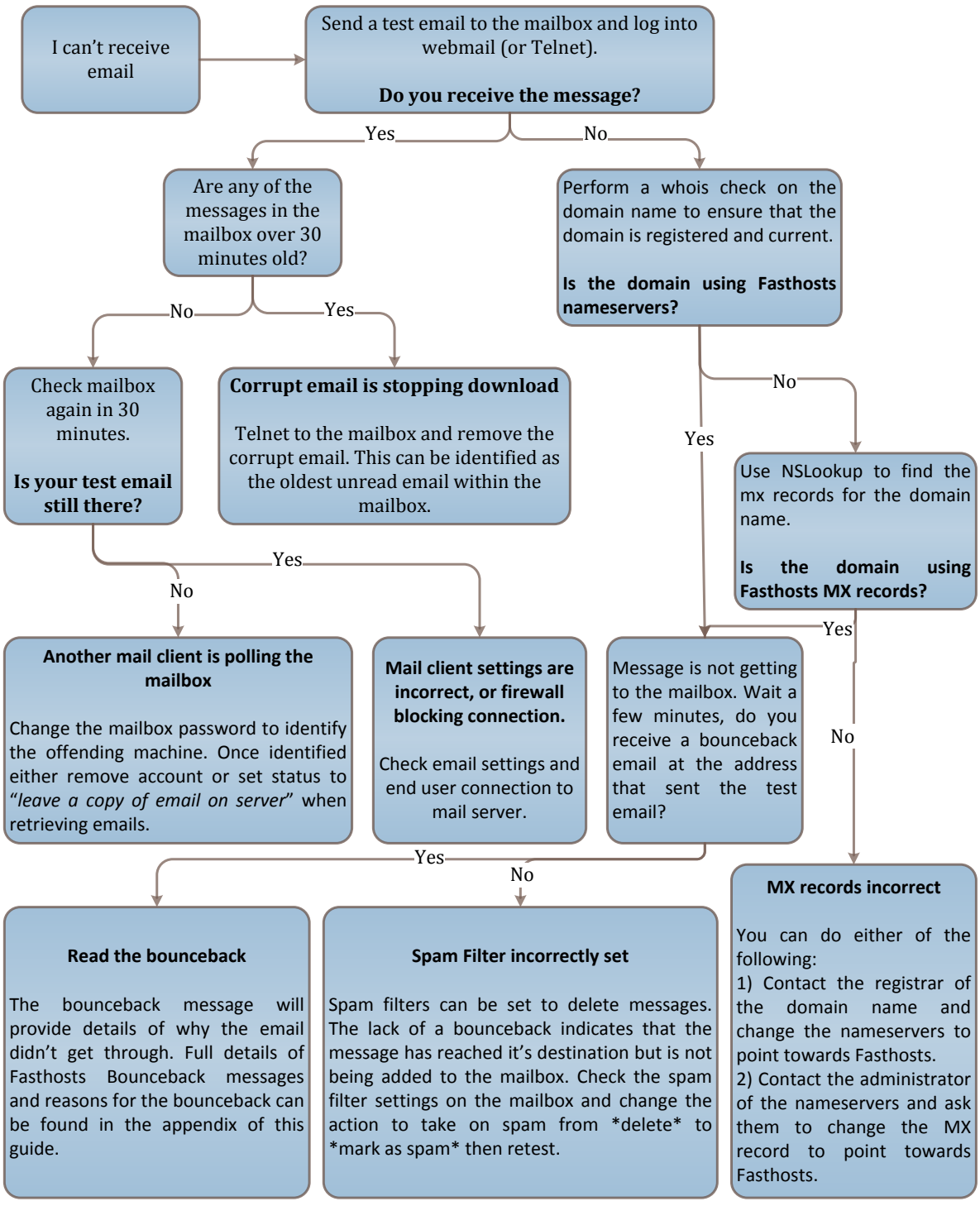


Troubleshooting email

I can't send email

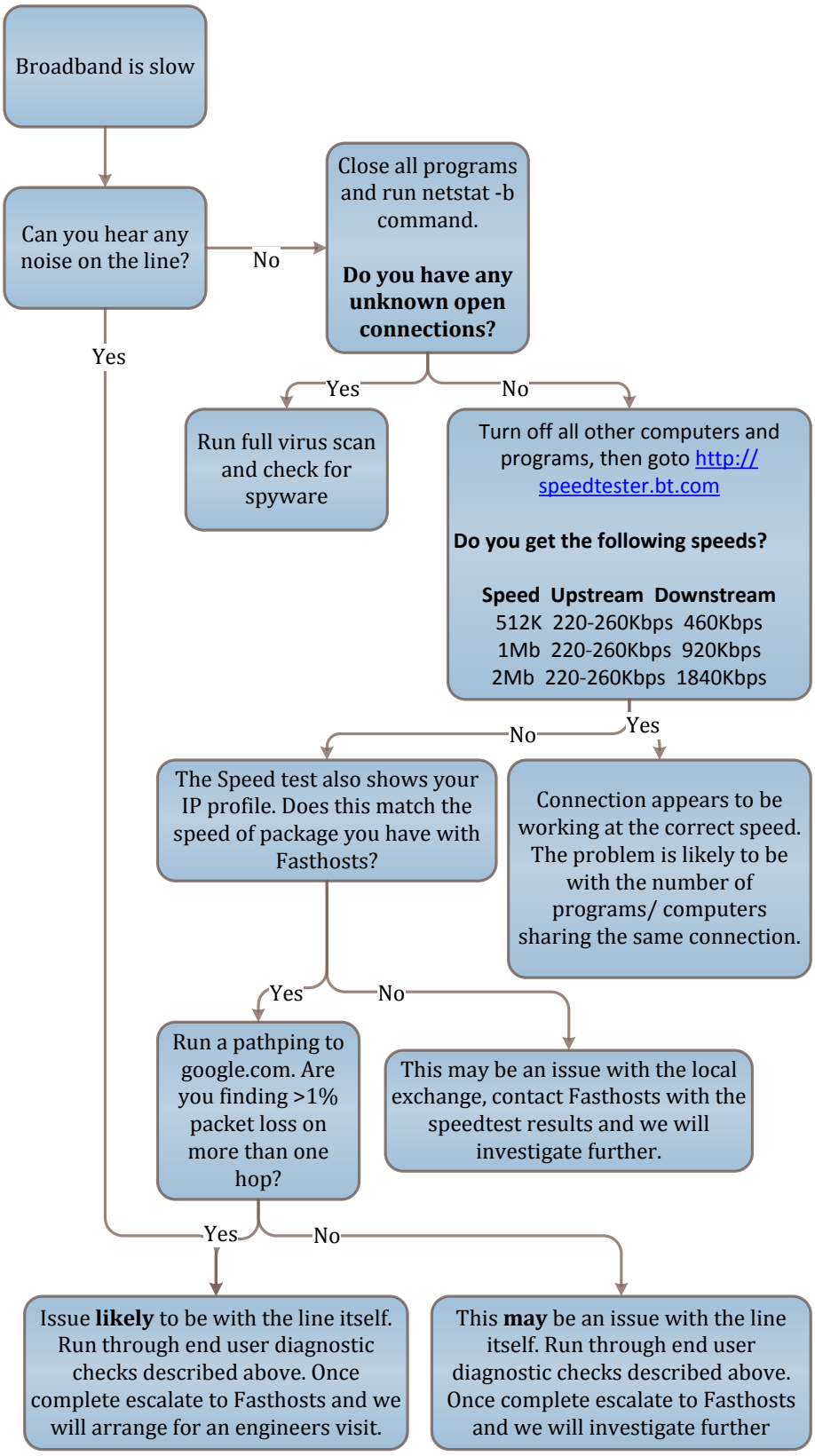


I can't receive email

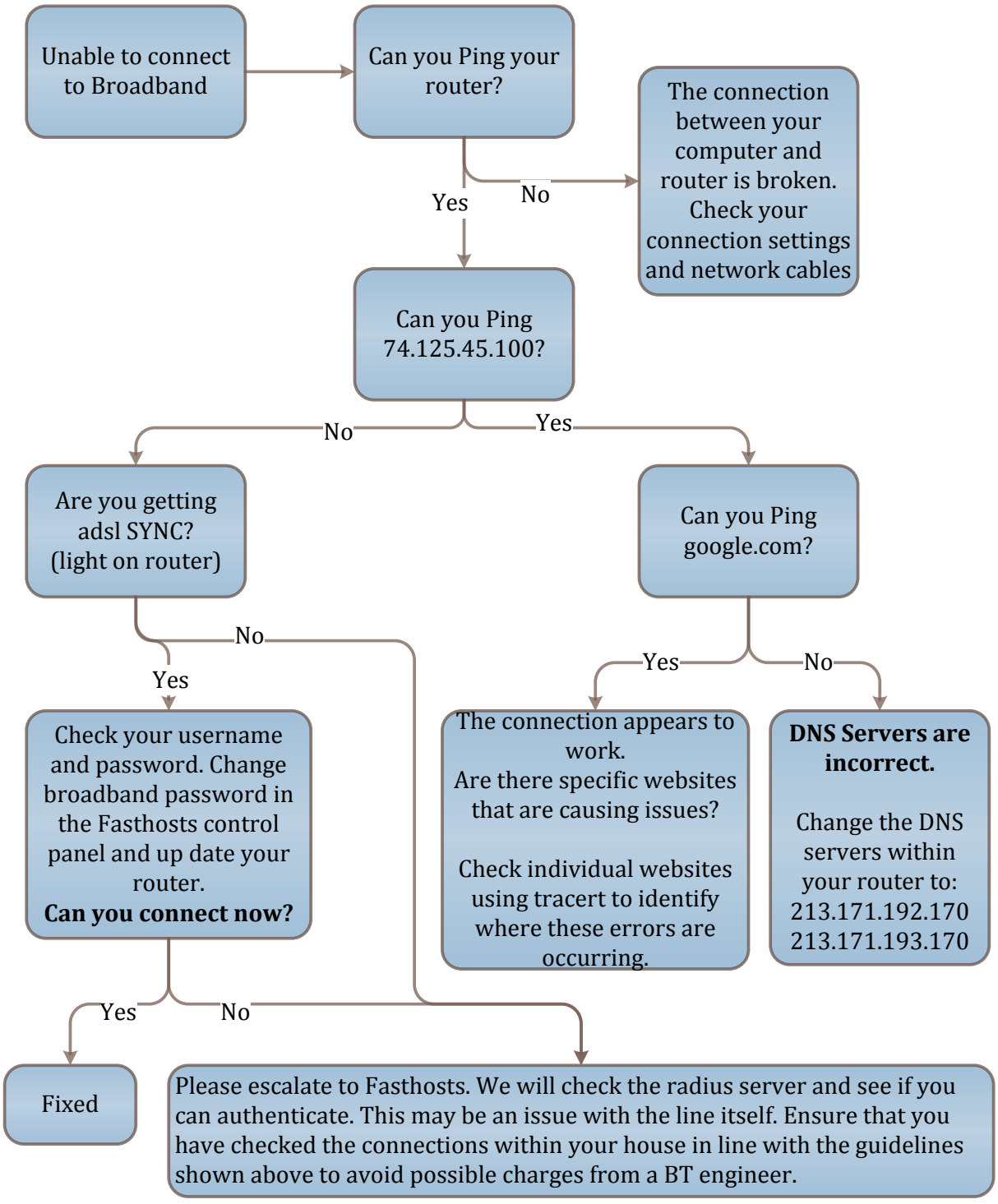


Troubleshooting Broadband

Slow connection



Unable to connect



Appendix

Additional Ping options

Option	Description
-t	Pings the specified host until stopped using the <Ctrl>+C key combination. To
-a	Resolves addresses to hostnames
-n *count*	Specifies how many echo requests to send. E.g `ping google.com –n 5` will send 5, 32 bit packets to google.com
-l *Size*	Send buffer size
-f	Set's the "Don't fragment" flag within the packets being sent.
-i *TTL*	Sets the Time To Live for the packet (specifying the maximum number of router hops the packet should take before being dropped.
-v *TOS*	Type Of Service (In the ICMP packet header)
-r *count*	Record route for count hops
-s *count*	Timestamp for count hops
-j *host-list*	Loose source route along host-list
-k *host-list*	Strict source route along host-list
-w *timeout*	Timeout in milliseconds to wait for each reply

List of useful Whois Servers

Country Code Top Level Domains (CCTLDs)

Domain Extension	Whois Server		Domain Extension	Whois Server
.ac	whois.nic.ac		.ag	whois.nic.ag
.am	whois.amnic.net		.as	whois.nic.as

.at	whois.nic.at	.au	whois.aunic.net
.be	whois.dns.be	.br	whois.registro.br
.bz	whois.belizenic.bz	.ca	whois.cira.ca
.cc	whois.nic.cc	.ch	whois.nic.ch
.ck	whois.ck-nic.org.ck	.cl	whois.nic.cl
.cn	whois.cnnic.net.cn	.cx	whois.nic.cx
.cz	whois.nic.cz	.de	whois.denic.de
.dk	whois.dk-hostmaster.dk	.ee	whois.eenet.ee
.eu	whois.eu	.fr	whois.nic.fr
.gg	whois.isles.net	.gs	whois.adamsnames.tc
.hk	whois.hkirc.net.hk	.hm	whois.registry.hm
.hu	whois.nic.hu	.id	whois.netzone.web.id
.ie	whois.domainregistry.ie	.il	whois.isoc.org.il
.in	whois.ncst.ernet.in	.io	whois.nic.io
.ir	whois.nic.ir	.is	whois.isnet.is
.it	whois.nic.it	.je	whois.isles.net
.jp	whois.jprs.jp	.ke	whois.kenic.or.ke
.kr	whois.nic.or.kr	.la	whois.afilias-grs.net
.li	whois.nic.li	.lt	whois.domreg.lt
.lu	whois.dns.lu	.lv	whois.nic.lv
.mn	whois.nic.mn	.ms	whois.adamsnames.tc
.mx	whois.nic.mx	.nl	whois.domain-registry.nl
.no	whois.norid.no	.nu	whois.nic.nu
.nz	whois.srs.net.nz	.pl	whois.dns.pl
.re	whois.nic.re	.ro	whois.rotld.ro
.ru	whois.ripn.net	.se	whois.nic-se.se
.sg	whois.nic.net.sg	.sh	whois.nic.sh
.si	whois.arnes.si	.st	whois.nic.st
.tc	whois.adamsnames.tc	.tf	whois.nic.tf
.th	whois.thnic.net	.tk	whois.dot.tk
.tm	whois.nic.tm	.to	whois.tonic.to
.tr	whois.nic.tr	.tv	whois.nic.tv

.tw	whois.twnic.net		.ua	whois.net.ua
.ug	whois.co.ug		.uk	whois.nic.uk
.us	whois.nic.us		.vg	whois.adamsnames.tc
.ws	whois.worldsite.ws			

Generic Top Level Domains (GTLDs)

Domain Extension	Whois Server		Domain Extension	Whois Server
.aero	whois.information.aero		.biz	whois.neulevel.biz
.com	whois.internic.net		.coop	whois.nic.coop
.edu	whois.internic.net		.gov	whois.nic.gov
.info	whois.afilias.info		.int	whois.iana.org
.me	whois.nic.me		.mil	whois.nic.mil
.mobi	whois.dotmobiregistry.net		.museum	whois.museum
.name	whois.nic.name		.net	whois.internic.net
.org	whois.publicinterestregistry.net			

Second Level Domain Names

Domain Extension	Whois Server		Domain Extension	Whois Server
.au.com	whois.au.com		.ac.uk	whois.ja.net
.eu.org	whois.eu.org		.gov.uk	whois.ja.net
.ae.org	whois.centralnic.com		. br.com	whois.centralnic.com
.cn.com	whois.centralnic.com		.de.com	whois.centralnic.com
.eu.com	whois.centralnic.com		.gb.com	whois.centralnic.com
.hu.com	whois.centralnic.com		.jpn.com	whois.centralnic.com
.kr.com	whois.centralnic.com		.no.com	whois.centralnic.com
.qc.com	whois.centralnic.com		.ru.com	whois.centralnic.com
.sa.com	whois.centralnic.com		.se.com	whois.centralnic.com
.se.net	whois.centralnic.com		.uk.com	whois.centralnic.com

.uk.net	whois.centralnic.com		.us.com	whois.centralnic.com
.uy.com	whois.centralnic.com		.web.com	whois.centralnic.com
.za.com	whois.centralnic.com			

NSlookup options

Command	Option	Description
name		Displays information about the host/domain *name* using the default server
name1 name2		As above, but uses *name2* as the server
Help or ?		Displays information on common commands
Set *option*		Sets an option.
	all	Displays options, current server and host
	[no]debug	Displays debugging information
	[no]d2	Displays verbose debugging information
	[no]defname	Appends domain name to each query
	[no]recurse	Asks for a recursive answer to query
	[no]search	Use domain search list
	[no]vc	Always use a virtual circuit
	Domain=*name*	Set default domainname to *name*
	Srchlist=N1[/N2……/N6]	Set domain to N1 and search list N1, N2 etc
	Root=*name*	Set the root server to *name*
	Retry=*x*	Sets the number of retries to *x*
	Timeout=*x*	Set initial time-out interval to *x* seconds
	Type=*x*	Set query type (A, ANY, CNAME, MX, NS, PTR, SOA, SRV etc)
	Q[uerytype]=*x*	Same as type
	Class=*x*	Set query class (IN, ANY)
	[no]msxfr	Use fast zone transfer

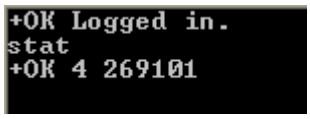
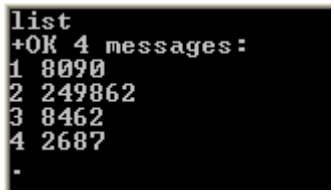
	Ixfrver=*X*	Current version to use in IXVR transfer request
Server *name*		Set the default server to *name* using the current default server
lserver *name*		Set the default server to *name* using the initial server
Finger [*user*]		Finger the optional *name* at the current default host
root		Set the current default server to the root
ls [opt] DOMAIN [> FILE]		List addresses in DOMAIN (optional: output to file)
-a		List canonical names and addresses
-d		List all records
-t *type*		List records of the given *type* (A, CNAME, MX, NS, PTR, SOA, SRV etc)
View *file*		Sort an "ls" output file and view it with pg
exit		Exit the program

NSlookup Error Messages

Error Message	Description
Timed Out	The server did not respond to a request after a certain amount of time and a certain number of retries. You can set the time-out period with the **set timeout** subcommand. You can set the number of retries with the **set retry** subcommand.
No response from server	No DNS name server is running on the server computer.
No records	The DNS name server does not have resource records of the current query type for the computer, although the computer name is valid. The query type is specified with the **set querytype** command.
Nonexistant domain	The computer or DNS domain name does not exist.

Connection refused -or- Network is unreachable	The connection to the DNS nameserver or finger server could not be made. This error commonly occurs with Is and finger requests.
Server failure	The DNS name server found an internal inconsistency in its database and could not return a valid answer.
Refused	The DNS name server refused to service the request.
Format error	The DNS name server found that the request packet was not in the proper format. It may indicate an error in **nslookup**.

Telnet Email commands

Command	Description
Stat	Will show the number of messages in your mailbox and the size (in bytes) of mailbox space used. 
List	Will list a line for each message in your mailbox, with its number and size (in bytes) 
Retr *msg#*	
Top *msg# #lines*	This is an optional POP3 command that will not work on all mailservers (Although it is enabled on Fasthosts servers). It lists the email header for each message along with the first #*lines* of the message text itself.

<table>
<tr><td></td><td>
<pre>top 1 10+OK
Return-Path: <[redacted]>
Delivered-To: bob@bobsdomain.co.uk
Received: from virus_17.livemail.co.uk (virus-cluster.livemail.co.uk [213.171.21
6.10])
        by smtp-in-129.livemail.co.uk (Postfix) with SMTP id 9C64261B715
        for <bob@bobsdomain.co.uk>; Fri, 29 May 2009 10:54:49 +0100 (BST)
X-Span-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on
        span-87.livemail.co.uk
X-Span-Level:
X-Span-Status: No, score=-98.2 required=5.0 tests=HTML_MESSAGE,
        MIME_QP_LONG_LINE,USER_IN_WHITELIST autolearn=disabled version=3.2.5
Received: from smtp-out-57.livemail.co.uk (smtp-out-60.livemail.co.uk [213.171.2
16.60])
        by smtpin-133.livemail.co.uk (Postfix) with ESMTP id 505B424E4FE
        for <bob@bobsdomain.co.uk>; Fri, 29 May 2009 10:54:46 +0100 (BST)
Received: from EDG01.fasthosts.com (unknown [213.171.217.138])
        by smtp-out-57.livemail.co.uk (Postfix) with ESMTP id 2723A5FB895
        for <bob@bobsdomain.co.uk>; Fri, 29 May 2009 10:54:46 +0100 (BST)
Received: from FH-EXCH07-01.fasthosts.local (10.44.244.94) by
 EDG01.fasthosts.com (10.44.224.192) with Microsoft SMTP Server (TLS) id
 8.1.358.0; Fri, 29 May 2009 10:47:49 +0100
Received: from FH-EXCH07-01.fasthosts.local ([10.44.244.94]) by fh-exch07-01
 ([10.44.244.94]) with mapi; Fri, 29 May 2009 10:53:58 +0100
From: [redacted] <[redacted]>
To: "bob@bobsdomain.co.uk" <bob@bobsdomain.co.uk>
Date: Fri, 29 May 2009 10:53:57 +0100
Subject: holiday
Thread-Topic: holiday
Thread-Index: AcngQ2KpL83UcOIMT+O61rORIoNjvw==
Message-ID: <A06CDC05133A0241BEC530BD1ED160D4862643A7@fh-exch07-01>
Accept-Language: en-US, en-GB
Content-Language: en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
acceptlanguage: en-US, en-GB
Content-Type: multipart/alternative;
        boundary="_000_A06CDC05133A0241BEC530BD1ED160D4862643A7fhexch0701_"
MIME-Version: 1.0
X-Original-To: bob@bobsdomain.co.uk
X-AntiVirus: checked by Vexira MailArmor

--_000_A06CDC05133A0241BEC530BD1ED160D4862643A7fhexch0701_
Content-Type: text/plain; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable

Hi Bob,

.</pre>
</td></tr>
<tr><td>Dele msg#</td><td>Will mark the message number msg# for deletion. This is the best way to delete a corrupt email. This will not delete the message straight away, but will mark if for deletion until you sign off the telnet server.
<pre>.
dele 4+OK Marked to be deleted.</pre>
</td></tr>
<tr><td>Rset</td><td>This will reset any emails that are marked for deletion (so that they will no longer be deleted when you quit.
<pre>rset
+OK</pre>
</td></tr>
<tr><td>quit</td><td>Deletes any messages marked for deletion and logs you off the mail server.
<pre>quit
+OK Logging out.

Connection to host lost.

C:\Documents and Settings>_</pre>
</td></tr>
</table>

IPConfig Additional Switches

Switch	Description
/all	Displays a detailed report for all interfaces
/flushdns	Removes all entries from the DNS name cache
/registerdns	Refreshes all DHCP leases and reregisters DNS names
/displaydns	Displays the contents of the DNS resolver cache
/release <*adaptor*>	Releases the IP address for a specified interface
/renew <*adaptor*>	Renews the IP address for a specified interface
/showclassid <*adaptor*>	Displays all the DHCP class ID's allowed for the adaptor specified
/setclassid <*adaptor*> <*class ID to set*>	Changes the DHCP class ID for the adaptor specified
/?	Displays the list of switches

Fasthosts MasterClass Range

Introducing HTML and CSS

This guide will show you how to download and use all the tools needed to upload a business card website from scratch costing you a couple of evenings of your time. At the end of the guide you should know all about hosting websites and be confident in most aspects of web hosting.

Download guide

Introducing domain names and DNS

This guide is designed to give you a broad introduction into how Domain names operate and how the Domain Name system works.

Download Guide

Introducing FTP

This guide is designed to show you the different ways of uploading your site using ftp, including the basic principles of understanding and troubleshooting ftp issues.

Download Guide

An Introduction to PHP scripting

This guide will introduce some simple yet powerful features of PHP, a popular scripting language, and help you take your first steps towards building a strong web presence.

Download Guide

An Introduction to MySQL Databases

This guide will introduce MySQL, a powerful and popular free relational database system.

Download Guide