

PING and How It Works

By Mark E. Donaldson

"Ping" (Packet INternet Groper) is without a doubt the best-known network administration tool. It is one of the simplest tools, because all it does is send packets to check if a remote machine is responding and, by extension, if it is accessible over the network. The ping tool, then, is used to diagnose network connectivity using commands of the type:

```
ping name.of.the.machine
```

name.of.the.machine represents the machine's IP address, or its name. It is generally preferable to test it first using the machine's IP address.

PING is an application that makes use of the Internet Control Message Protocol (ICMP) protocol, and allows the user to test the reachability of another host:

Reachable (definition): Given a host A and a host B. The host B is reachable from host A, if (IP) packets send by host A arrive at host B and can/are being processed by host B.

Hence, a host a reachable is there is a communication path from A to B and B is up and running.

When a host is reachable, we are pretty much sure that we can use an application in order to come into dialog with that other host (e.g. FTP, Telnet or HTTP).

If a host is unreachable, there can be either a problem with the communication path (i.e. there is no communication path) or the other host may be down. Further diagnostics is needed, one can use for instance TRACEROUTE for this purpose.

Ping relies on the ICMP protocol, which is used to diagnose transmission conditions. For this reason, it uses two types of protocol messages (out of the 18 offered by ICMP):

- Type 0, which corresponds to an "echo request" command, sent by the source machine;
- Type 8, which corresponds to an "echo reply" command, sent by the target machine.

At regular intervals (by default, every second), the source machine (the one running the ping command) sends an "echo request" to the target machine. When the "echo reply" packet is received, the source machine displays a line containing certain information. If the reply is not received, a line saying "request timed out" will be shown.

Among the various measurement packages is the original PING (Packet InterNet Groper) program used over the last six years for numerous tests and measurements of the Internet system and its client nets. This program contains facilities to send various kinds of probe packets, including ICMP Echo messages, process the reply and record elapsed times and other information in a data file, as well as produce real-time snapshot histograms and traces.

Mills, D. L; "Internet Delay Experiments"; RFC 889; Dec 1983.

This program is intended for use in network testing, measurement and management. It should be used primarily for manual fault isolation. Because of the load it could impose on the network, it is unwise to use ping during normal operations or from automated scripts...

Muuss, Mike; Ping source code comments; 7 August 1992.

PING and How It Works

By Mark E. Donaldson

The Internet Ping command bounces a small packet off a domain or IP address to test network communications, and then tells how long the packet took to make the round trip. The Ping command is one of the most commonly used utilities on the Internet by both people and automated programs for conducting the most basic network test: can your computer reach another computer on the network, and if so how long does it take?

Every second of the day there are untold millions of pings flashing back and forth between computers on the Internet like a continuous shower of electronic neural sparks. The following subsections provide information on how Ping was invented, how Ping works, how to use Ping, Ping web sites, and info on the original Unix Ping version.

How Ping was invented

The original PING command stood for "Packet Internet Groper", and was a package of diagnostic utilities used by DARPA personnel to test the performance of the ARPANET. However, the modern Internet Ping command refers to a program was written by Mike Muuss in December, 1983, which has since become one of the most versatile and widely used diagnostic tools on the Internet. Muuss named his program after the sonar sounds used for echo-location by submarines and bats; just like in old movies about submarines, sonar probes do sound something like a metallic "ping".

How Ping Works

The Internet Ping program works much like a sonar echo-location, sending a small packet of information containing an ICMP ECHO_REQUEST to a specified computer, which then sends an ECHO_REPLY packet in return. The IP address 127.0.0.1 is set by convention to always indicate your own computer. Therefore, a ping to that address will always ping yourself and the delay should be very short. This provides the most basic test of your local communications.

The PING application uses ICMP messages to test the reachability, such ICMP messages are encapsulated in IP packets. The PING application uses two ICMP messages: the ICMP echo request message, and the ICMP echo reply message.

The message-format are shown in the figure below.

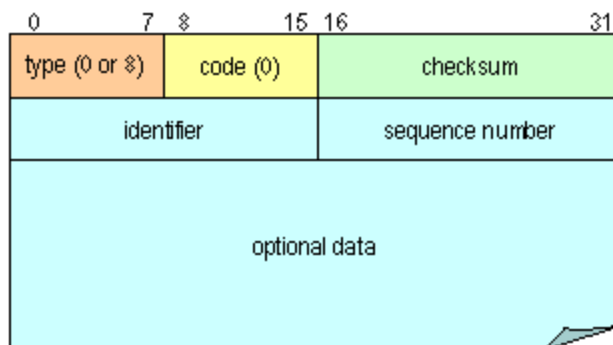


Figure 1: "PING messages"
type=0 : ICMP echo request messages,
type=8 : ICMP echo reply message.

PING and How It Works

By Mark E. Donaldson

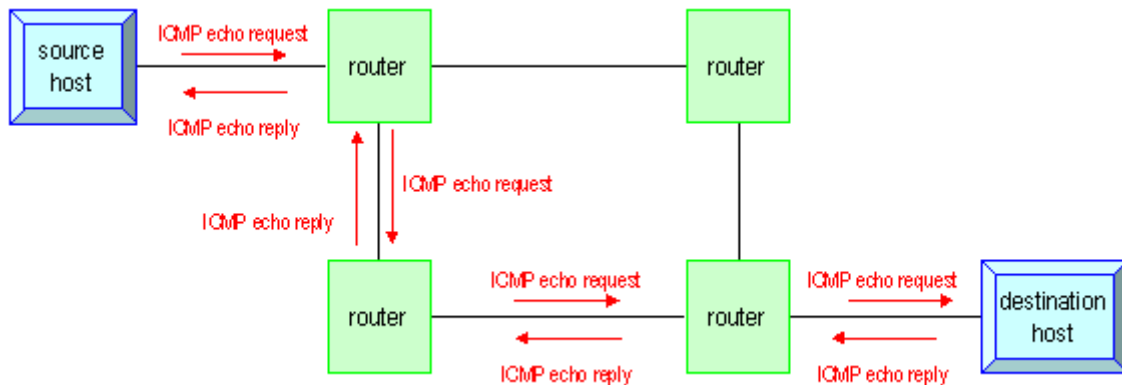


Figure 2: Example of how PING messages traverse the IP network.

When a PING message is received by the receiving host, it sends back an echo reply message in which the identifier, sequence number and optional data field are left unchanged.

The identifier field in the ICMP echo reply message is used to allow identification of the PING process running at the sending host.

By the sequence number field the sending host can keep track of for which ICMP echo request messages a reply message has been received.

The optional data field is used to store the time at which the ICMP echo request message has been sent. On receipt of the associated reply message the sending host can determine the time that was needed for the packet to travel through the Internet to the target host and back again: i.e. the round trip time (RTT).

How to Use Ping

You can use the Ping command to perform several useful Internet network diagnostic tests, such as the following:

- **Access.** You can use Ping to see if you can reach another computer. If you can't ping a site at all, but you can ping other sites, then it's a pretty good sign that your Internet network is fine and that site is down. On the other hand, if you can't ping any site, then likely your entire network connection is down -- try rebooting.
- **Time & distance.** You can use the Ping command to determine how long it takes to bounce a packet off of another site, which tells you its Internet distance in network terms. For example, a web site hosted on your neighbor's computer next door with a different Internet service provider might go through more routers and be farther away in network distance than a site on the other side of the ocean with a direct connection to the Internet backbone.

If a site seems slow, you can compare ping distances to other Internet sites to determine whether it is the site, the network, or your system that is slow. You can also compare ping times to get an idea of which sites have the fastest network access and would be most efficient for downloading, chat, and other applications.

PING and How It Works

By Mark E. Donaldson

- **Domain IP address.** You can use the Ping command to probe either a domain name or an IP address. If you ping a domain name, it helpfully displays the corresponding IP address in the response.

Mike Muuss originally developed the ping command for the Unix system, with the options summarized below:

```
ping [-q] [-v] [-R] [-c Count] [-i Wait] [-s PacketSize] Host
```

Option	Example	Definition
ping -c count	ping -c 10	Specify the number of echo requests to send.
Ping -d	ping -d	Set the SO_DEBUG option.
Ping -f	ping -f	Flood ping. Sends another echo request immediately after receiving a reply to the last one. Only the super-user can use this option.
Ping host	ping 121.4.3.2	Specify the host name (or IP address) of computer to ping
ping -i wait	ping -i 2	Wait time. The number of seconds to wait between each ping
ping -l preload	ping -l 4	Sends "preload" packets one after another.
Ping -n	ping -n	Numeric output, without host to symbolic name lookup.
Ping -p pattern	ping -p ff00	Ping Pattern. The example sends two bytes, one filled with ones, and one with zeros.
Ping -q	ping -q	Quiet output. Only summary lines at startup and completion
ping -r	ping -r	Direct Ping. Send to a host directly, without using routing tables. Returns an error if the host is not on a directly attached network.
Ping -R	Ping -R	Record Route. Turns on route recording for the Echo Request packets, and display the route buffer on returned packets (ignored by many routers).
ping -s PacketSize	ping -s 10	Sets the packet size in number of bytes, which will result in a total packet size of PacketSize plus 8 extra bytes for the ICMP header
ping -v	ping -v	Verbose Output. Lists individual ICMP packets, as well as Echo Responses

Depending on the operating system, the results of the ping may be displayed somewhat differently.

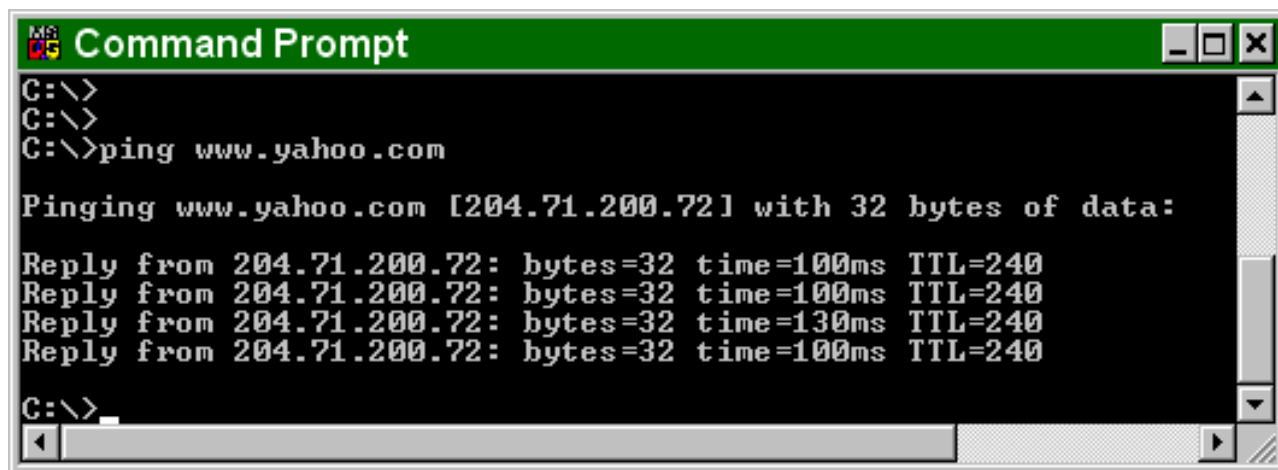
Here are the results of the command in GNU/Linux:

PING and How It Works

By Mark E. Donaldson

```
ping www.commentcamarche.net
PING www.commentcamarche.net (163.5.255.85): 56 data bytes
64 bytes from 163.5.255.85: icmp_seq=0 ttl=56 time=7.7 ms
64 bytes from 163.5.255.85: icmp_seq=1 ttl=56 time=6.0 ms
64 bytes from 163.5.255.85: icmp_seq=2 ttl=56 time=5.5 ms
64 bytes from 163.5.255.85: icmp_seq=3 ttl=56 time=6.0 ms
64 bytes from 163.5.255.85: icmp_seq=4 ttl=56 time=5.3 ms
64 bytes from 163.5.255.85: icmp_seq=5 ttl=56 time=5.6 ms
64 bytes from 163.5.255.85: icmp_seq=6 ttl=56 time=7.0 ms
64 bytes from 163.5.255.85: icmp_seq=7 ttl=56 time=6.0 ms
--- www.commentcamarche.net ping statistics ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 5.3/6.1/7.7 ms
```

You can run the ping command on a Windows computer by opening an MSDOS window and then typing "ping" followed by the domain name or IP address of the computer you wish to ping. You can list the available options for the Windows ping command with "ping -?".



```
MS-DOS Command Prompt
C:\>
C:\>
C:\>ping www.yahoo.com

Pinging www.yahoo.com [204.71.200.72] with 32 bytes of data:

Reply from 204.71.200.72: bytes=32 time=100ms TTL=240
Reply from 204.71.200.72: bytes=32 time=100ms TTL=240
Reply from 204.71.200.72: bytes=32 time=130ms TTL=240
Reply from 204.71.200.72: bytes=32 time=100ms TTL=240

C:\>
```

Here are the results of the command in Windows:

```
ping www.commentcamarche.net
Pinging www.commentcamarche.net [163.5.255.85] with 32 bytes of data:
Reply from 163.5.255.85: bytes=32 time=34 ms TTL=54
Reply from 163.5.255.85: bytes=32 time=37 ms TTL=54
Reply from 163.5.255.85: bytes=32 time=32 ms TTL=54
Reply from 163.5.255.85: bytes=33 time=32 ms TTL=54
Ping statistics for 163.5.255.85:
Packets: sent = 4, received = 4, lost = 0 (loss 0%),
Approximate round trip times in milli-seconds:
Minimum = 32ms, Maximum = 37ms, Average = 34ms
```

The basic ping command syntax is "ping hostname". For example, "ping cisco.net" from DOS prompt and the output might look like:

```
C:\Documents and Settings\DOS>ping www.cisco.net

Pinging www.cisco.net [71.18.254.xxx] with 32 bytes of data:
```

PING and How It Works

By Mark E. Donaldson

```
Reply from 71.18.254.xxx: bytes=32 time=49ms TTL=49
Reply from 71.18.254.xxx: bytes=32 time=49ms TTL=49
Reply from 71.18.254.xxx: bytes=32 time=49ms TTL=48
Reply from 71.18.254.xxx: bytes=32 time=49ms TTL=48
```

```
Ping statistics for 71.18.254.xxx:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 49ms, Maximum = 49ms, Average = 49ms
```

```
C:\Documents and Settings\DOS>
```

If ICMP is blocked by network admin, you will see below.

```
C:\Documents and Settings\DOS>ping www.cisconet.com
```

```
Pinging www.cisconet.com [71.18.254.xxx] with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 71.18.254.xxx:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

TTL reply

Ping sends an ICMP echo request packet that ICMP type is 8, code 0. (with the TTL value, default 128). Ping expects back an ICMP 'echo reply' packet that ICMP type is 11, code 0. The round trip time is displayed in millisecond.

TTL Expired in Transit/TTL Time exceed

Most devices initialize 128 or higher TTL value of outgoing IP Packets. Outside of devices that are far away than TTL hop, those devices are not able to communicate with origin. For example, if you are 17 hops away from website www.cisconet.com, set TTL 12 when you ping out to the site. the IP Packets will not reach the site. B/C TTL will be 'expire in transmit' before they reach the site.

Simply, you can tested it. Do traceroute to www.yahoo.com from your dos prompt.

```
C:\Documents and Settings\chris.yoon> tracert www.yahoo.com
```

```
Tracing route to www.yahoo-ht3.akadns.net [69.147.114.210]
over a maximum of 30 hops:
```

```
 1 <1 ms <1 ms <1 ms asqlr90-vlan215.mscil.com [154.139.198.130]
 2 <1 ms <1 ms <1 ms asqlr1-vlan64.mscil.com [154.139.254.141]
 3 <1 ms <1 ms <1 ms asqar1-vlan30.mscil.com [154.139.255.1]
 4 <1 ms <1 ms <1 ms asqir2-vlan49.mscil.com [166.141.0.39]
 5 <1 ms <1 ms <1 ms asqir1-vlan22.mscilink.com [192.135.72.201]
 6 <1 ms <1 ms <1 ms GigiEthernet1-0.ALT.NET [137.39.253.177]
 7 <1 ms <1 ms <1 ms 169.at-6-0-0.ALT.NET [152.163.34.182]
 8 3 ms 3 ms 3 ms 0.so-0-0-0.ALT.NET [152.163.136.209]
 9 4 ms 3 ms 3 ms 0.ge-7-1-0.ALT.NET [152.163.141.161]
10 4 ms 4 ms 4 ms telia-gw.n54ny.ip.att.net [192.205.32.49]
11 5 ms 5 ms 5 ms tbr1.wswdc.ip.att.net [12.123.8.98]
```

PING and How It Works

By Mark E. Donaldson

```
12 5 ms 4 ms 4 ms 12.122.113.17
13 5 ms 5 ms 5 ms 12.86.111.22
14 6 ms 6 ms 6 ms ge-3-1-0-pl70.msrr2.rel.yahoo.com [216.115.108.69
]
15 5 ms 5 ms 6 ms gil-23.bas-a2.re3.yahoo.com [66.196.112.55]
16 5 ms 5 ms 5 ms fl.www.vip.re3.yahoo.com [69.147.114.210]
```

Trace complete.

Total 16 hop to reach www.yahoo.com.

From DOS prompt, type ping -i 5 www.yahoo.com (it manually set TTL 5 on ICMP packet)

```
C:\Documents and Settings\DOS>ping -i 5 www.yahoo.com
```

Pinging www.yahoo-ht3.akadns.net [209.191.93.52] with 32 bytes of data:

```
Reply from 192.135.72.201: TTL expired in transit.
Reply from 192.135.72.201: TTL expired in transit.
Reply from 192.135.72.201: TTL expired in transit.
Reply from 192.135.72.201: TTL expired in transit.
```

Ping statistics for 209.191.93.52:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Documents and Settings\DOS>
```

As you can see above result, hop 5 192.135.72.201 device is responded to you. Of cause TTL expired in transit, b/c 192.135.72.201 is not final destination. So won't get echo reply.

How to Discover your TTL on your device

To discover the default TTL value of your device, 'ping localhost' and examine the TTL reply value. For older Windows machines this value is 32. For newer Windows machines, this value is 128.

```
C:\Documents and Settings\DOS>ping localhost
```

Pinging localhost [127.0.0.1] with 32 bytes of data:

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

Ping statistics for 127.0.0.1:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PING and How It Works

By Mark E. Donaldson

The table below lists possible ICMP-type values.

ICMP Type	Literal
0	echo-reply
3	destination unreachable code 0 = net unreachable 1 = host unreachable 2 = protocol unreachable 3 = port unreachable 4 = fragmentation needed and DF set 5 = source route failed
4	source-quench
5	redirect code 0 = redirect datagrams for the network 1 = redirect datagrams for the host 2 = redirect datagrams for the type of service and network 3 = redirect datagrams for the type of service and host
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded code 0 = time to live exceeded in transit 1 = fragment reassembly time exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

The below chart shown possible output characters from the ping :

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
Q	Source quench (destination too busy).
M	Could not fragment.
?	Unknown packet type.
&	Packet lifetime exceeded.

PING and How It Works

By Mark E. Donaldson

Thus, the ping command's output gives:

- The IP address which corresponds to the name of the remote machine;
- The ICMP sequence number;
- The packet's time to live (TTL). The time to live (TTL) field shows how many routers the packet went through as it travelled between the two machines. Each IP packet has a TTL field with a relatively high value. Each time it goes through a router, the value is reduced. If this number ever reaches zero, the router interprets this to mean that the packet is going around in circles, and terminates it;
- The round-trip delay field corresponds to the length of time in milliseconds of a round trip between the source and target machines. As a general rule, a packet must have a delay no longer than 200 ms;
- The number of lost packets.

One network device sends a request for a reply to another device and records the time the request was sent. The device receiving the request sends a packet back. When the reply is received, the round-trip time for packet propagation can be calculated. The receipt of a reply indicates a working connection. This elapsed time provides an indication of the length of the path. Consistency among repeated queries gives an indication of the quality of the connection. With the above in mind, ping answers two basic questions: "one, do I have a connection?" Two, "how good is that connection?"

Clearly, for the program to work, the networking protocol must support this query/response mechanism. The ping program is based on Internet Control Message Protocol (ICMP), part of the TCP/IP protocol. ICMP was designed to pass information about network performance between network devices and exchange error messages which supports a wide variety of message types, including query/response mechanism.

The normal operation of ping relies on two specific ICMP messages, ECHO_REQUEST and ECHO_REPLY, but it may respond to ICMP messages other than ECHO_REPLY when appropriate. In theory, all TCP/IP-based network equipment should respond to an ECHO_REQUEST by returning the packet to the source, but this is not always the case.

Interpreting Results

In different flavors of ping, results vary. However, for each packet we are given the size and source of each packet, an ICMP sequence number, a Time-To-Live (TTL) counter, and the round-trip times. Of course, the sequence number and round trip time are the most revealing when evaluating basic connectivity.

When each ECHO_REQUEST packet is sent, the time the packet is sent is recorded in the packet. This is copied into the corresponding ECHO_REPLY packet by the remote host. When an ECHO_REPLY packet is received, the elapsed time is calculated by comparing the current time to the time recorded in the packet, i.e., the time the packet was sent. This difference, the elapsed time, is reported along with ECHO_REPLY packet is received that matches a particular sequence number, that packet is resumed lost. The size and the variability of elapsed times will depend on the number and speed of intermediate links as well as the congestion on those links.

It may seem that TTL field could be used to estimate the number of hops on a path. Unfortunately,

PING and How It Works

By Mark E. Donaldson

this is problematic. When a packet is sent, the TTL field is initialized and is subsequently decremented by each router along the path. If it reaches zero, the packet is discarded. This imposes a finite lifetime on all packets ensuring that, in the event of a routing loop, the packet won't remain on the network indefinitely. Unfortunately, the TTL field may or may not be reset at the remote machine and, if reset, there is little consistency in what it is set to. Thus, you need to know very system-specific information to use the TTL field to estimate the number of hops on a path.

Options

- -c: allow you to specify the number of packets you want to send.
- -f: used to flood packets onto network. This option is to send as fast as the receiving host can handle them which is useful for stress testing a link or to get some indication of the comparative performance of interfaces. This is restricted to root.
- -l: used to flood packets onto network. It takes a count and sends out that many packets as fast as possible which eventually falls back to normal mode. This could be used to see how the router handles a flood of packets. This is restricted to root.
- -i: allows the user to specify the amount of time in seconds to wait between sending consecutive packets.
- -n: restricts output to numeric form which is useful if you have DNS problems.
- -v: used for verbose output.
- -q, -Q: used for quiet output.
- -s: specifies how much data to send. If set too small, less than 8, there won't be space in the packet for a time-stamp. Setting the packet size can help in diagnosing a problem caused by path Maximum Transmission Unit (MTU) settings (the largest frame size that can be sent on the path) or fragmentation problems. (Fragmentation is dividing data among multiple frames when a single packet is too large to cross a link. It is handled by the IP portion of the protocol stack.) The general approach is to increase packet sizes up to the maximum allowed to see if at some point you have problems. When this option isn't used, ping defaults to 64 bytes, which may be too small a packet to reveal some problems. Also, remember that ping does not count the IP or ICMP header in the specified length so that your packets will be 28 bytes larger than you specify.

You could conceivably see MTU problems with protocols, such as PPP, that use escaped characters as well. With escaped characters, a single character may be replaced by two characters. The expansion of escaped characters increases the size of the data frame and can cause problems with MTU restrictions or fragmentation.

-p: allows you to specify a pattern for the data included within the packet after the timestamp.

The above are not the entire list of options. As such, be sure to consult the documentation if things don't work as expected.

Problems with Ping

The program does not exist in isolation, but depends on the proper functioning of other elements of the network. Ping usually depends upon ARP and DNS. As previously mentioned, if you are using a hostname rather than an IP address as destination, the name of the host will have to be resolved

PING and How It Works

By Mark E. Donaldson

before ping can send any packets. You can bypass DNS by using IP address.

It is also necessary to discover the host's link level address for each host along the path to the destination. Although this is rarely a problem, should ARP resolution fail, then ping will fail. You could avoid this problem, in part; by using start ARP entries to ensure that the ARP table is correct. A more common problem is that the time reported by ping for the first packet sent will often be distorted since it reflects both transit times and ARP resolution times. On some networks, the first packet will often be lost. You can avoid this problem by sending more than one packet and ignoring the results for the first packet.

Sample Ping Packet Decode

The purpose of this topic is to partially decode a ICMP Echo or "Ping" packet as it appears on an Ethernet network.

Packet Representation On The Network

The following is a HEX dump of a simple ICMP echo or "ping" packet:

```
000000: 00 A0 CC 63 08 1B 00 40 : 95 49 03 5F 08 00 45 00 ...c...@.I...E.
000010: 00 3C 82 47 00 00 20 01 : 94 C9 C0 A8 01 20 C0 A8 .<.G.. ..... ..
000020: 01 40 08 00 48 5C 01 00 : 04 00 61 62 63 64 65 66 .@..H\....abcdef
000030: 67 68 69 6A 6B 6C 6D 6E : 6F 70 71 72 73 74 75 76 ghijklmnopqrstuv
000040: 77 61 62 63 64 65 66 67 : 68 69 wabcdefghijklmnopghijklm
```

The ping was initiated with the command:

```
C:> ping 192.168.1.64
```

and sent the ICMP echo request with the default of 32 bytes of data. The total length of the ping packet is 74 bytes.

The packet can be broken into the following protocol elements:

- Ethernet Header
- IP Datagram
- IP Header
- IP Data

Ethernet Header

The network media is Ethernet. This means that the first 14 bytes are the Ethernet Header:

```
000000: 00 A0 CC 63 08 1B 00 40 : 95 49 03 5F 08 00 45 00 ...c...@.I...E.
000010: 00 3C 82 47 00 00 20 01 : 94 C9 C0 A8 01 20 C0 A8 .<.G.. ..... ..
000020: 01 40 08 00 48 5C 01 00 : 04 00 61 62 63 64 65 66 .@..H\....abcdef
000030: 67 68 69 6A 6B 6C 6D 6E : 6F 70 71 72 73 74 75 76 ghijklmnopqrstuv
000040: 77 61 62 63 64 65 66 67 : 68 69 wabcdefghijklmnopghijklm
```

The 14 byte Ethernet Header includes three fields:

- MAC Destination Address (0-5, 6 bytes)
- MAC Source Address (6-11, 6 bytes)
- Ethernet Type Field (12-13, 2 bytes)

PING and How It Works

By Mark E. Donaldson

IP Datagram

The remaining 60 bytes (14-73) constitute the IP datagram itself:

```
000000: 00 A0 CC 63 08 1B 00 40 : 95 49 03 5F 08 00 45 00 ...c...@.I...E.
000010: 00 3C 82 47 00 00 20 01 : 94 C9 C0 A8 01 20 C0 A8 .<.G.. ..
000020: 01 40 08 00 48 5C 01 00 : 04 00 61 62 63 64 65 66 .@..H\....abcdef
000030: 67 68 69 6A 6B 6C 6D 6E : 6F 70 71 72 73 74 75 76 ghijklmnopqrstuv
000040: 77 61 62 63 64 65 66 67 : 68 69 wabcdefghijklmnopghijklmno
```

IP Header

The IP datagram begins at byte 14, which means that the IP Header also starts at byte 14. The 0x45 value found there is interpreted to mean that the packet is an IPv4 packet and the IP Header length is five(5) 32-bit words (14-33):

```
000000: 00 A0 CC 63 08 1B 00 40 : 95 49 03 5F 08 00 45 00 ...c...@.I...E.
000010: 00 3C 82 47 00 00 20 01 : 94 C9 C0 A8 01 20 C0 A8 .<.G.. ..
000020: 01 40 08 00 48 5C 01 00 : 04 00 61 62 63 64 65 66 .@..H\....abcdef
000030: 67 68 69 6A 6B 6C 6D 6E : 6F 70 71 72 73 74 75 76 ghijklmnopqrstuv
000040: 77 61 62 63 64 65 66 67 : 68 69 wabcdefghijklmnopghijklmno
```

Here are decodes of a few key fields:

- IP Version (14, high nibble) - IPv4
- IP Header Length (14, low nibble) - Five (5) 32-bit Words
- Source IP Address (26-29, 4 bytes) - 192.168.1.32 (C0.A8.01.20)
- Destination IP Address (30-33, 4 bytes) - 192.168.1.64 (C0.A8.01.40)

IP Data

Forty (40) bytes of IP Data follow the IP Header (34-73):

```
000000: 00 A0 CC 63 08 1B 00 40 : 95 49 03 5F 08 00 45 00 ...c...@.I...E.
000010: 00 3C 82 47 00 00 20 01 : 94 C9 C0 A8 01 20 C0 A8 .<.G.. ..
000020: 01 40 08 00 48 5C 01 00 : 04 00 61 62 63 64 65 66 .@..H\....abcdef
000030: 67 68 69 6A 6B 6C 6D 6E : 6F 70 71 72 73 74 75 76 ghijklmnopqrstuv
000040: 77 61 62 63 64 65 66 67 : 68 69 wabcdefghijklmnopghijklmno
```

Of course, the IP Data in this case is, in fact, an ICMP Echo Request, including thirty-two (32) bytes of Echo Data (42-73).