Ping

From Wikipedia, the free encyclopedia

Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. The name comes from active sonar terminology.

Ping operates by sending Internet Control Message Protocol (ICMP) *echo request* packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception (*round-trip time*)[1] and records any packet loss. The results of the test are printed in the form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times, and sometimes the standard deviation of the mean.

Ping may be run using various options (command line switches) depending on the implementation that enable special operational modes, such as to specify the packet size used as the probe, automatic repeated operation for sending a specified count of probes, and time stamping options.

Ping may be abused as a simple form of denial-of-service attack in the form of a ping flood, in which the attacker overwhelms the victim with ICMP echo request packets.

Contents

History

The ping utility was authored by Mike Muuss in December 1983 as a tool to troubleshoot problems in an IP network. He named it after the sound that sonar makes, since its methodology is similar to sonar's echo location. [1][2]

The usefulness of *ping* in assisting the diagnosis, of Internet connectivity issues was impaired starting in 2003, when a number of Internet service providers began filtering out ICMP Type 8 (ICMP Echo Request) messages at their network boundaries.[*citation needed*] This was partly due to the increasing use of ping for target reconnaissance, for example by Internet worms such as Welchia that flood the Internet with ping requests in order to locate new computers to infect. Not only did the availability of ping responses leak information to an attacker, it added to the overall load on networks, causing problems for routers across the Internet.[*citation needed*]

However *host discovery* or *ping scanning* or *ping sweep* is still a part of network scanning tools like nmap, as it may give basic evidence about the existence of a remote machine.

Although RFC 1122 prescribes that any host must accept an echo-request and issue an echo-reply in return, this has been characterized as a security risk.[3]

ICMP packet

ICMP packet

	Bit 0 - 7	**Bit 8 - 15**	**Bit 16 - 23**	**Bit 24 - 31**
IP Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Payload (8+ bytes)	Type of message	Code	Checksum	
	Quench			
	Data (*optional*)			

Generic composition of an ICMP packet[4]

- Header (in blue):
    - *Protocol* set to 1 and *Type of Service* set to 0.
- Payload (in red):
    - Type of ICMP message (8 bits)
    - Code (8 bits)
    - Checksum (16 bits), calculated with the ICMP part of the packet (the header is not used). It is the 16-bit one's complement of the one's complement sum of the ICMP message starting with the Type field[5]
    - The ICMP 'Quench' (32 bits) field, which in this case (ICMP echo request and replies), will be composed of identifier (16 bits) and sequence number (16 bits).
    - Data load for the different kind of answers (Can be an arbitrary length, left to implementation detail. However must be less than the maximum MTU of the network[*citation needed*]).
- Data Transportation

Sample ping test

The following is the output of running ping with the target `www.example.com` for five probes.

```
# ping -c 5 www.example.com
PING www.example.com (192.0.43.10) 56(84) bytes of data.
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=1 ttl=250 time=80.5 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=2 ttl=250 time=80.4 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=3 ttl=250 time=80.3 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=4 ttl=250 time=80.3 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=5 ttl=250 time=80.4 ms

--- www.example.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 80.393/80.444/80.521/0.187 ms
```

The utility summarizes its results after completing the ping probes. The shortest round trip time was 80.393 ms, the average was 80.444 ms, and the maximum value was 80.521 ms. The measurement had a standard deviation of 0.187 ms.

Message format

Echo request

The *echo request* is an ICMP message whose data is expected to be received back in an *echo reply* ("ping"). The host must respond to all echo requests with an echo reply containing the exact data received in the request message.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type = 8								Code = 0								Header Checksum															
Identifier																Sequence Number															
Data :::																															

- The Identifier and Sequence Number can be used by the client to match the reply with the request that caused the reply. In practice, most Linux systems use a unique identifier for every ping process, and sequence number is an increasing number within that process. Windows uses a fixed identifier, which varies between Windows versions, and a sequence number that is only reset at boot time.
- The data received by the Echo Request must be entirely included in the Echo Reply.

Echo reply

The *echo reply* is an ICMP message generated in response to an echo request, and is mandatory for all hosts and routers.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type = 0								Code = 0								Header Checksum															
Identifier																Sequence Number															
Data :::																															

- *Type* and *code* must be set to 0.
- The *identifier* and *sequence number* can be used by the client to determine which echo requests are associated with the echo replies.
- The data received in the echo request must be entirely included in the echo reply.

Possible reply messages include !H, !N, or !P (host, network or protocol unreachable) !S (source route failed) !F (fragmentation needed) !U or !W (destination network/host unknown) !I (source host is isolated) !A (communication with destination network administratively prohibited) !Z (communication with destination host administratively prohibited) !Q (for this ToS the destination network is unreachable) !T (for this ToS the destination host is unreachable) !X (communication administratively prohibited) !V (host precedence violation) !C (precedence cutoff in effect) !<num> (ICMP unreachable code <num>)

Other replies

In case of error, destination host or intermediate router will send back an ICMP error message, i.e. host unreachable or TTL exceeded in transit. In addition these messages include the first 8 bytes of original message (in this case header of ICMP echo request, including quench value), so ping utility can match it to originating query.[*citation needed*]

Payload

The payload of the packet is generally filled with ASCII characters, as the output of the tcpdump utility shows:

```
16:24:47.966461 IP (tos 0x0, ttl 128, id 15103, offset 0, flags [none],
proto: ICMP (1), length: 60) 192.168.146.22 > 192.168.144.5: ICMP echo request,
id 1, seq 38, length 40
       0x0000:  4500 003c 3aff 0000 8001 5c55 c0a8 9216  E..<:.....\U....
       0x0010:  c0a8 9005 0800 4d35 0001 0026 6162 6364  ......M5...&abcd
       0x0020:  6566 6768 696a 6b6c 6d6e 6f70 7172 7374  efghijklmnopqrst
       0x0030:  7576 7761 6263 6465 6667 6869            uvwabcdefghi
```

The payload includes a timestamp of when the message was sent, as well a sequence number. This allows ping to compute the round trip time in a stateless manner without needing to record when packets were sent. In cases of no answer and no error message, most implementations of ping display nothing, or periodically print notifications about timing out.[*citation needed*]

Other types of pinging

The term *ping* is commonly used to describe the transmission of any message or signal for the purpose of locating or testing network services or features. For example, a ping may be sent using the User Datagram Protocol (UDP) to a device located behind a network address translator (NAT) to keep the port binding on the NAT from timing out and removing the mapping. Other examples are short or empty instant messages, emails, voice mails, or missed-call notification to indicate availability.[*citation needed*]

In various network multi-player games, a video game ping performs a similar function as the ping program for Internet traffic. The game server measures the time required for a game packet to reach a client and a response to be received. This round-trip time is usually reported as the player's *ping*.[*citation needed*] It is an effective measurement of the player's latency, with lower ping times being desirable. This style of ping typically does not use ICMP packets.

See also

- Keepalive
- List of DOS commands
- List of Unix utilities
- Traceroute
- Ping of death
- Smurf attack

References

1. ^ [a] [b] Mike Muuss. "The Story of the PING Program" (http://www.webcitation.org/5saCKBpgH) . Adelphi, MD, USA: U.S. Army Research Laboratory. Archived from the original (http://ftp.arl.mil/~mike/ping.html) on 08 September 2010. http://www.webcitation.org/5saCKBpgH. Retrieved 08 September 2010. "I named it after the sound that a sonar makes, inspired by the whole principle of echo-location."
2. ^ Salus, Peter (1994). *A Quarter Century of UNIX*. Addison-Wesley. ISBN 0201547775.
3. ^ "Shields Up, Firewall Test. You get a warning about the dangers of ping if your computer answers ping request" (https://www.grc.com/x/ne.dll?bh0bkyd2) . https://www.grc.com/x/ne.dll?bh0bkyd2. Retrieved 4 June 2010.
4. ^ RFC 792
5. ^ "RFC Sourcebook's page on ICMP" (http://www.networksorcery.com/enp/protocol/icmp.htm#ICMP%20Header%20Checksum) . http://www.networksorcery.com/enp/protocol/icmp.htm#ICMP%20Header%20Checksum. Retrieved 20 December 2010.

External links

- `ping(8) (http://linux.die.net/man/8/ping)` : send ICMP ECHO_REQUEST to network hosts – Linux Administration and Privileged Commands Manual

Retrieved from "http://en.wikipedia.org/w/index.php?title=Ping&oldid=467675948"

Categories: MS-DOS/Windows Command Prompt commands | Network analyzers | Open source network management software | Internet Protocol based network software | Unix network-related software | Windows communication and services | Windows administration

- This page was last modified on 25 December 2011 at 22:58.
-