Increasing the payload of ICMP error messages

draft-gont-icmp-payload-00.txt

Abstract

The original ICMP specification states that when a packet elicits an ICMP error message, the IP header plus the next 64 bits of the original datagram must be returned in the payload of the ICMP error message. This imposes a constraint on the design of transport-layer protocols, which are forced to include all the relevant information needed to identify an instance of communication in the first 64 bits.
of their protocol header. It also limits the amount of data from the original packet available to the transport-layer when acting on the ICMP error message. Including only the first 64 bits of the original datagram’s payload may also not be enough to demultiplex ICMP error messages if IP is being used to tunnel some other network-layer protocol. This document proposes to increase the amount of data of the original datagram to be included in the payload of ICMP error messages.

1. Introduction

The Internet Control Message Protocol (ICMP) [1] is used in the Internet Architecture to perform the fault isolation function, that is, the group of actions that hosts and routers take to determine that there is some network failure [4].

The original ICMP specification [1] states that, whenever a packet elicits an ICMP error message, the internet header plus the first 64 bits of the original datagram’s data must be included in the payload of the ICMP error message. These data are used by the receiving host to match the error message to the instance of communication that elicited it.

This limit on the amount information returned in the payload of ICMP error messages has two drawbacks:

- It imposes a constraint on the design of transport-layer protocols, which are forced to include all the relevant information needed to identify a communication instance in the first 64 bits of their protocol header.

- It limits the amount of data the transport-protocol has available to perform, for example, security checks on the returned datagram.

- If IP [5] is being used for tunneling purposes, including just the first 8 bytes of the payload of the original datagram may not be enough information to demultiplex the ICMP error message.

As discussed in [1] and [6], in order to allow ICMP error messages to be demultiplexed, transport protocols are forced to include in the first 64 bits of their headers all the information needed to identify a communication instance. Thus, this limit somehow constrains the design of transport protocols.

There are a number of scenarios in which a larger amount of data from the original datagram may be needed, or, at least, desirable. For example, additional data from the original datagram could be used to perform security checks on the received ICMP error message [7].
Also, in case IP is being used to tunnel some other protocol, the first 64 bits of the original datagram’s payload may not provide enough information to the demultiplex the ICMP error message.

Even when the Host Requirements RFC [2] states that more than 8 octects of the original datagram’s payload MAY be included in the payload of an ICMP error message, it does not require any specific amount of data, and thus does not remove the constraints discussed above.

This document proposes a modification to the original ICMP specification to increase the amount of data of the original packet to be included in the payload of ICMP error messages.

2. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [3].

3. Specification

When a host or router sends an ICMP error message, it MUST include in the payload of the ICMP error message as many bytes of the original datagram as possible. However, the resulting IP datagram MUST NOT be greater than 576 bytes.

It must be noted that 576 is the minimum reassembly buffer size [2].

4. Security Considerations

This document proposes a minor modification to the original ICMP specification [1], to increase the amount of data of the original packet to be included in the payload of ICMP error messages. This modification does not raise any new security implications.

5. Acknowledgements

The author would like to thank Guillermo Gont and Michael Kerrisk for providing many valuable comments.

6. References

6.1 Normative References


6.2 Informative References


Author’s Address

Fernando Gont
Universidad Tecnologica Nacional
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires  1706
Argentina

Phone: +54 11 4650 8472
EMail: fernando@gont.com.ar