INTERNET-DRAFT
"Internet Protocol Five Fields - Internet Control Message Protocol",
Alexey Eromenko, 2016-01-18,
<draft-eromenko-ipff-icmp-03.txt>
expiration date: 2016-07-18

Intended status: Standards Track

A.Eromenko
January 2016

INTERNET CONTROL MESSAGE PROTOCOL v5
(for Internet Protocol "Five Fields", aka IPFF-ICMPv5)

PROTOCOL SPECIFICATION draft

Abstract

This document describes the format of a set of control messages used in ICMPv5 (Internet Control Message Protocol). ICMPv5 is the Internet Control Message Protocol for Internet Protocol Five Fields (IPFF).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

Summary of Message Types

Error messages:
- 1 Destination Unreachable
- 2 Packet Too Big
- 3 Hops Exceeded
- 4 Parameter Problem
- 5 Redirect

Other messages:
- 128 Echo Request
- 129 Echo Reply

Introduction

The Internet Protocol (IP) is used for host-to-host packet service in a system of interconnected networks called the Internet. The network connecting devices are called Routers. These routers communicate between themselves for control purposes via various routing protocols. Occasionally a router or destination host will communicate with a source host, for example, to report an error in packet processing. For such purposes this protocol, the Internet Control Message Protocol (ICMP), is used. ICMP, uses the basic support of IP as if it were a higher level protocol, however, ICMP is actually an integral part of IP, and must be implemented by every IP module.

ICMP messages are sent in several situations: for example, when a packet cannot reach its destination, and when the router can direct the host to send traffic on a shorter route.

The Internet Protocol is not designed to be absolutely reliable. The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable. There are still no guarantees that a packet will be delivered or a control message will be returned. Some packets may still be undelivered without any report of their loss. The higher level protocols that use IP must implement their own reliability procedures if reliable communication is required.

The ICMP messages typically report errors in the processing of packets. To avoid the infinite regress of messages about messages etc., no ICMP error messages are sent about ICMP error messages.

Message Formats

ICMP messages are sent using the basic IP header. The first byte of the data portion of the packet is a ICMP type field; the value of this field determines the format of the remaining data. Any field labeled "unused" is reserved for later extensions and must be zero when sent, but receivers should not use these fields (except to include them in the checksum). Unless otherwise noted under the individual format descriptions, the values of the internet header fields are as follows:

Version

5

Payload Length

Length of this ICMP header.

Hops to Live

Hops to live; as this field is decremented at each machine in which the packet is processed, the value in this field should be at least as great as the number of routers which this packet will traverse.

Protocol

ICMP = 1

Source Address

The address of the router or host that composes the ICMP message. Unless otherwise noted, this can be any of a router's addresses.

Destination Address

The address of the router or host to which the message should be sent.

NOTE: Node SHOULD check any ICMP packet for 999 field limit. According to IP-FF addressing specification, fields values between 1000 and 1023 are invalid.

Source and Destination Ports or Flow Label

0

Type of Service

0

Message Checksum Calculation

The checksum is the 32-bit CRC32c checksum
of the entire ICMPv5 message, starting with the ICMPv5 message
type field, and prepended with a "pseudo-header" of IPFF header
fields, as specified in [IPFF]. The Protocol value
used in the pseudo-header is "1" (="ICMP").

For computing the checksum, the checksum field is set to zero.

Internet Header + 512 bits of Data Packet

The internet header plus the first 64 bits of the original
packet's data. This data is used by the host to match the
message to the appropriate process. If a higher level protocol
uses port numbers, they are assumed to be in the first 512 bits
of the original packet's data.

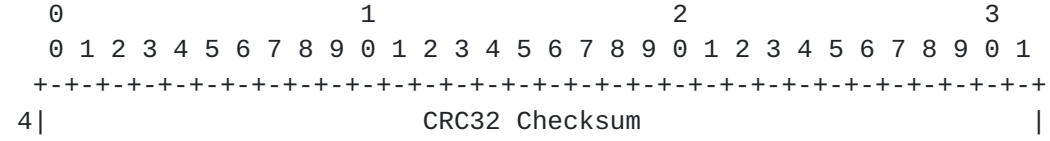
Design note: why 512 bits? Because it allows to cover the classic TCP
header in full (20 bytes x8 = 160 bits, plus most IP header options,
TCP options and then some user data);
It should be enough to cover most protocols.

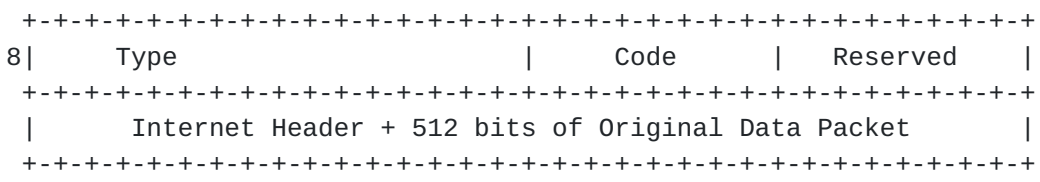
Destination Unreachable Message

Description

If, according to the information in the router's routing tables,
the network specified in the internet destination field of a
packet is unreachable, e.g., the distance to the network is
infinity, the router may send a destination unreachable message
to the internet source host of the packet. In addition, in some
networks, the router may be able to determine if the internet
destination host is unreachable. Routers in these networks may
send destination unreachable messages to the source host when the
destination host is unreachable.

If, in the destination host, the IP module cannot deliver the
packet because the indicated protocol module or process port is
not active, the destination host may send a destination
unreachable message to the source host.





IP Fields:

Destination Address

The source network and address from the original packet's data.

ICMP Fields:

Type

1

Code

0 = network unreachable;

1 = host unreachable;

2 = protocol unreachable;

3 = port unreachable;

4 = VRF table unreachable;

10 = communication with destination network
administratively prohibited

11 = communication with destination host
administratively prohibited

12 = communication with destination protocol or port
administratively prohibited

14 = Host Precedence Violation

Codes 0, 1 and 4 may be received from a router.
Codes 2 and 3 may be received from a host.
Codes 10-14 may be received from a firewall.

Reserved

Initialized to zero on transmission; ignored by receiver.

Short explanation of codes:

Network and host unreachable

When a router cannot find either target subnet,
or a particular host within that subnet.

Protocol unreachable

When the designated transport protocol is not supported.

Port unreachable

when the designated transport protocol (e.g., UDP) is unable to demultiplex the datagram but has no protocol mechanism to inform the sender.

Virtual Router Forwarding table unreachable

When a router receives a packet with VRF extension header, and lacks a specified routing table, or has VRF disabled; see [IPFF] VRF header extension for details.

Communication with destination administratively prohibited

It means that a firewall blocks this traffic by policy, and wants to inform the host.

Host Precedence Violation

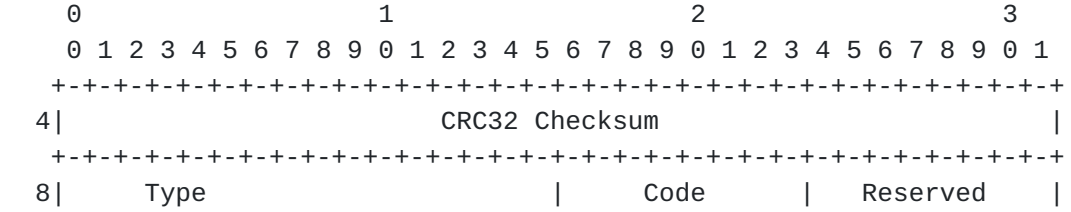
Sent by a first-hop router or firewall (the first router to handle a sent datagram) when the Precedence value in the Type Of Service field is not permitted.

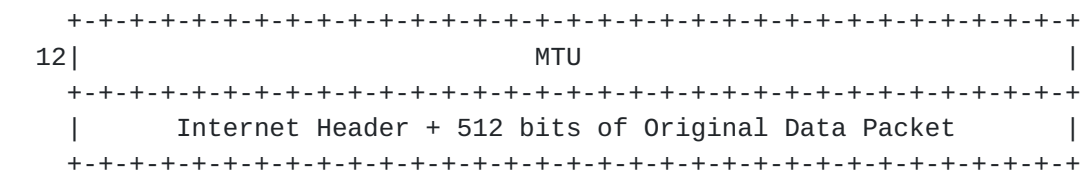
Packet Too Big Message

Description

A Packet Too Big MUST be sent by a router in response to a packet that it cannot forward because the packet is larger than the MTU of the outgoing link. The information in this message is used as part of the Path MTU Discovery process [PMTU].

Originating a Packet Too Big Message makes an exception to one of the rules as to when to originate an ICMPv5 error message. Unlike other messages, it is sent in response to a packet received with an IPFF multicast destination address, or unicast address.





IPFF Fields:

Destination Address

Copied from the Source Address field of the invoking packet.

ICMP Fields:

Type 2

Code 0

MTU The Maximum Transmission Unit of the next-hop link.

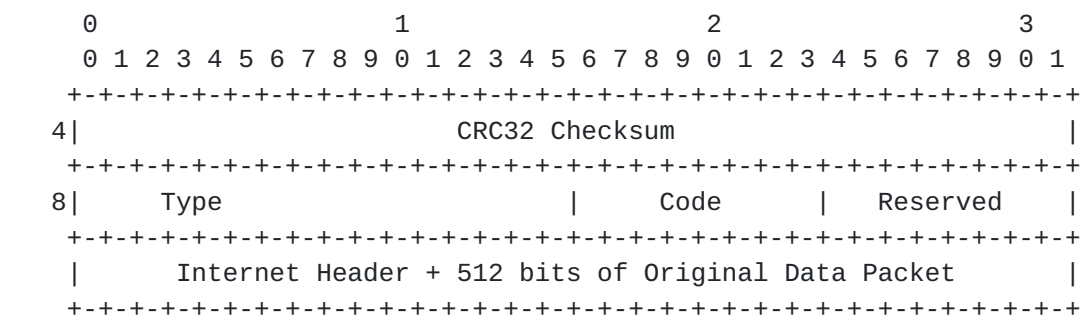
Upper Layer Notification

An incoming Packet Too Big message MUST be passed to the upper-layer process if the relevant process can be identified.

Hops Exceeded Message

Description

If the router processing a packet finds the hops to live field is zero it should discard the packet. The router may also notify the source host via the hops exceeded message.



IP Fields:

Destination Address

The source network and address from the original packet's data.

ICMP Fields:

Type 3

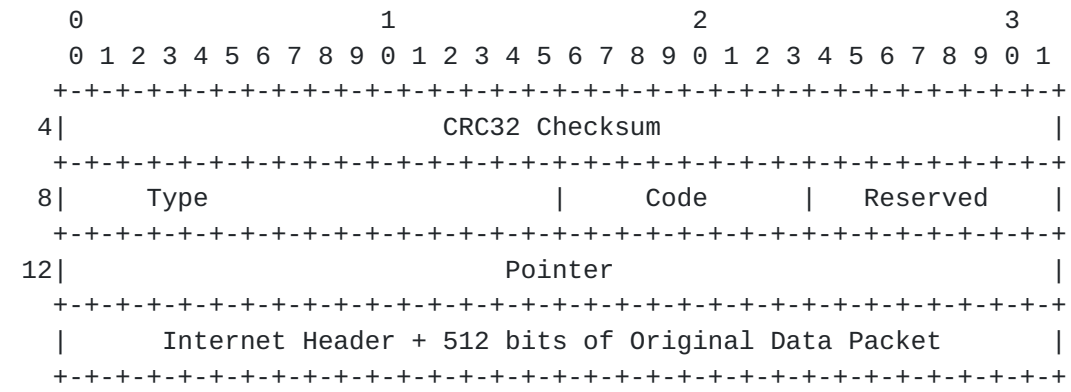
Code 0

Parameter Problem Message

Description

If an IPFF node processing a packet finds a problem with a field in the IPFF header or extension headers such that it cannot complete processing the packet, it MUST discard the packet and SHOULD originate an ICMP Parameter Problem message to the packet's source, indicating the type and location of the problem.

The pointer identifies the byte of the original packet's header where the error was detected.



IP Fields:

Destination Address

The source network and address from the original packet's data.

ICMP Fields:

Type

4

Code

0 = pointer indicates the error.
2 = Unrecognized IPFF option encountered

Code 2 is more informative subset of Code 0.
They may be received from a gateway or a host.

Pointer

Identifies the byte offset within the
invoking packet where the error was detected.

The pointer will point beyond the end of the ICMP
packet if the field in error is beyond what can fit
in the maximum size of an ICMP error message.

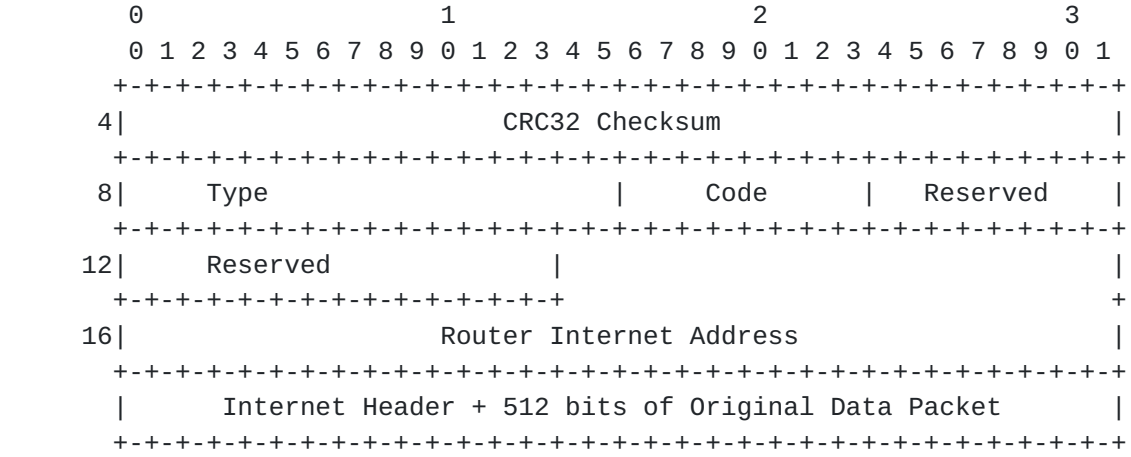
Redirect Message

Description

The router sends a redirect message to a host in the following situation. A router, R1, receives an internet packet from a host on a network to which the router is attached. The router, R1, checks its routing table and obtains the address of the next router, R2, on the route to the packet's internet destination network, X. If R2 and the host identified by the source address of the packet are on the same network, a redirect message is sent to the host. The redirect message advises the host to send its traffic for network X directly to router R2 as this is a shorter path to the destination. The router forwards the original packet's data to its internet destination.

For packets with the IP source route options and the router address in the destination address field, a redirect message is not sent even if there is a better route to the ultimate destination than the next address in the source route.

NOTE: Hops-to-live (HTL) for such packets must be set to 1. Routers should not forward this.



IP Fields:

Destination Address

The source network and address of the original packet's data.

ICMP Fields:

Type

5

Code

0 = Redirect packets for the Network.

1 = Redirect packets for the Host.

2 = Redirect packets for the Type of Service and Network.

3 = Redirect packets for the Type of Service and Host.

Codes 0, 1, 2, and 3 may be received from a router.

Router Internet Address

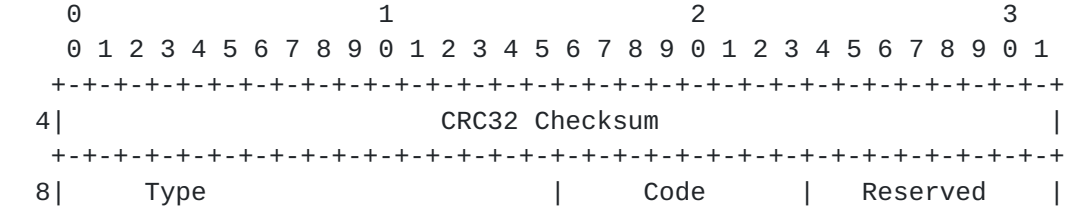
IP Address of the router to which traffic for the network specified in the internet destination network field of the original packet's data should be sent.

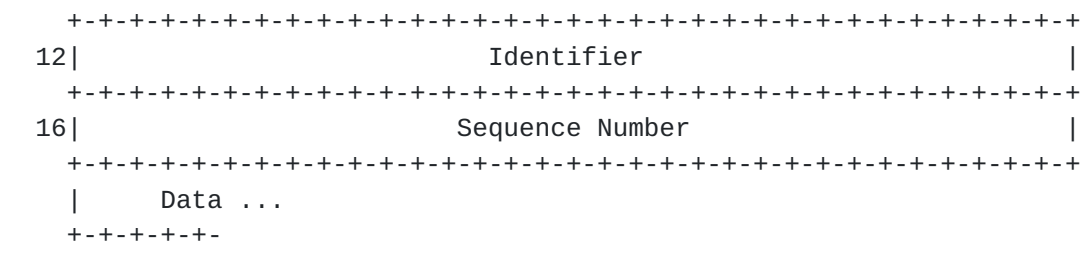
Echo or Echo Reply Message

Description

The data received in the echo message must be returned in the echo reply message. Commonly used via "ping" command to test connectivity.

The identifier and sequence number may be used by the echo sender to aid in matching the replies with the echo requests. For example, the identifier might be used like a port in TCP or UDP to identify a session, and the sequence number might be incremented on each echo request sent. The echoer returns these same values in the echo reply.





IP Fields:

Addresses

The address of the source in an echo message will be the destination of the echo reply message. To form an echo reply message, the source and destination addresses are simply reversed, and the checksum recomputed.

ICMP Fields:

Type

128 for echo message;

129 for echo reply message by host.

Code

0 for any request, or reply by host.

1 for reply by gateway.

Identifier

An identifier to aid in matching echos and replies, may be zero.

Sequence Number

A sequence number to aid in matching echos and replies, may be zero.

Design note: Identifier and Sequence Number fields were extended in IPFF, mainly to help with "ping" NAT traversal, especially at high-speeds.

References

[IPFF] = draft-eromenko-ipff.txt

Authors' Contacts

Alexey Eromenko

Israel

Skype: Fenix_NBK_
EMail: al4321@gmail.com
Facebook: https://www.facebook.com/technologov

Acknowledgements of prior art

Based on the hard work of people from DARPA, whom developed ICMP [RFC-792] and TCP/IP and "A. Conta", "S. Deering" and "M. Gupta", whom developed ICMPv6 RFC-4443 and "R. Braden", [RFC-1122].

INTERNET-DRAFT
Alexey
expiration date: 2016-07-18