

Network Working Group  
Internet-Draft  
Expires: August 22, 2002

M. Richardson  
SSW  
February 21, 2002

**An echo request/reply mechanism for ISAKMP  
draft-richardson-ipsec-ikeping-00.txt**

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on August 22, 2002.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">4</a>
<a href="#">2.</a>	Specification . . . . .	<a href="#">5</a>
<a href="#">2.1</a>	Format . . . . .	<a href="#">5</a>
<a href="#">2.1.1</a>	Cookies . . . . .	<a href="#">5</a>
<a href="#">2.1.2</a>	Next Payload . . . . .	<a href="#">5</a>
<a href="#">2.1.3</a>	Major Version . . . . .	<a href="#">6</a>
<a href="#">2.1.4</a>	Minor Version . . . . .	<a href="#">6</a>
<a href="#">2.1.5</a>	Exchange Type . . . . .	<a href="#">6</a>
<a href="#">2.1.6</a>	Flags . . . . .	<a href="#">6</a>
<a href="#">2.1.7</a>	Message ID . . . . .	<a href="#">6</a>
<a href="#">2.2</a>	Initiator . . . . .	<a href="#">6</a>
<a href="#">3.</a>	Security Considerations . . . . .	<a href="#">7</a>
	References . . . . .	<a href="#">8</a>
	Author's Address . . . . .	<a href="#">8</a>
	Full Copyright Statement . . . . .	<a href="#">9</a>

## Abstract

Bringing up IPsec gateways, clients and end systems is a hard task. One of the basic problems is determining if two peers can even communicate with each other. There are two typical blocks that can occur. They are at the transport and at the keying levels.

A failure for IP protocol 50 or 51 is a transport layer issue. This failure is not addressed here.

This document describes a diagnostic protocol for transport failures at the keying layer. Specifically it addresses determination of whether or not the ISAKMP port is open. Two new ISAKMP exchange types are defined, ECHOREQUEST and ECHOREPLY.

## **1. Introduction**

In complex network configurations, it is often the case that ISAKMP packets do not get through due to firewalls, network address translators, incompatible security settings, and sometimes even due to lack of actual network connectivity.

Increasingly paranoid network operators are turning off typical methods of determining reachability - the ICMP Echo Request ([[1](#)]) or "ping" packet. It is also not uncommon for a secure host to simply ignore ICMP echo requests.

For some time it has been well known that without access to log files at both ends of a IPsec tunnel the chances of successful configuration are low.

At the same time, people are building more complicated virtual private networks using IPsec. These are often cross-organizational. A single administrator seldom gets access to both sets of log files. When Opportunistic Encryption becomes more prevalent, this will be the norm rather than the exception.

Better diagnostics are necessary.

## 2. Specification

This document proposes two new ISAKMP exchange types. (See [2]).  
These would be:

ISAKMP\_XCHG\_ECHOREQUEST (value TBD-IANA) a request for an echo.

ISAKMP\_XCHG\_ECHOREPLY (value TBD-IANA) a reply to an echo request.

### 2.1 Format

These are minimal length ISAKMP packets, consisting of only the ISAKMP header with no payload.

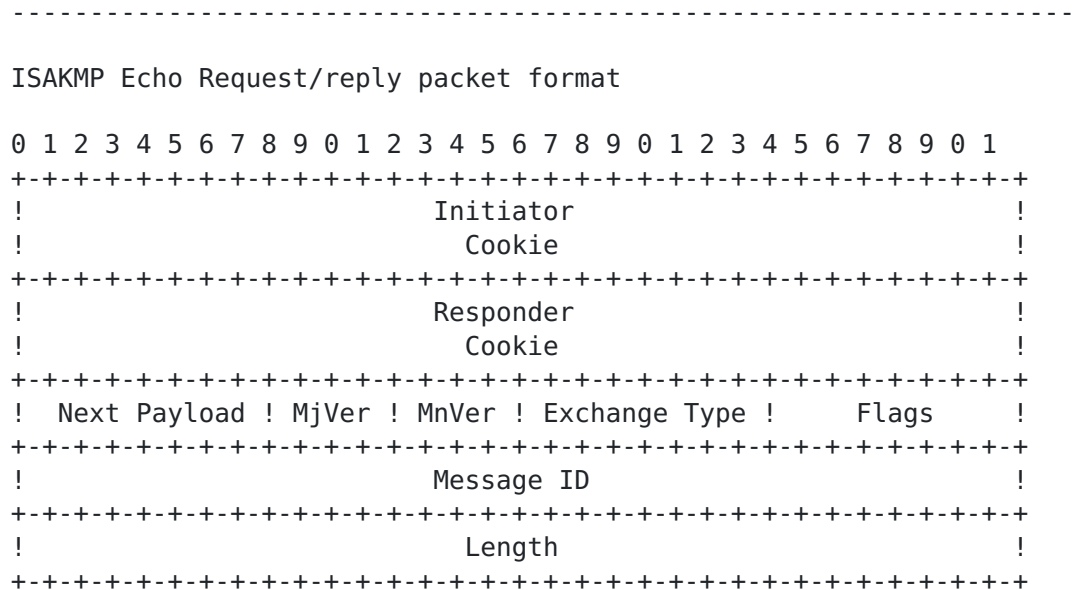


Figure 1: packet format

#### 2.1.1 Cookies

The cookie fields are arbitrarily set by the initiator and swapped by the recipient in the reply.

#### 2.1.2 Next Payload

Next payload is set to 0.

### **2.1.3 Major Version**

The Major version field is set to the maximum version supported by the end sending the packet.

### **2.1.4 Minor Version**

The Minor version field is set to the maximum version supported by the end sending the packet.

### **2.1.5 Exchange Type**

The Exchange type field is set ISAKMP\_XCHG\_ECHOREQUEST (value TBD-IANA) by the initiator of the echo request. It is set to ISAKMP\_XCHG\_ECHOREPLY (value TBD-IANA) by the responder.

### **2.1.6 Flags**

The Flags field is set to 0. There are no meaningful flags. There is no payload, and if there was, it would not be encrypted.

### **2.1.7 Message ID**

The message ID is set by the initiator, and simply repeated by the responder.

## **2.2 Initiator**

The initiator of an ISAKMP echo sends a properly formatted datagram under operator control. Often this will not be a full ISAKMP daemon instead a diagnostic utility, but this specification does not make any requirements here.

Any node which receives an ISAKMP echo request MAY log it. Repeated echo requests from the same originator SHOULD not cause excessive logging to occur.

A node MAY reply to an ISAKMP echo request with an ISAKMP echo reply. An implementation SHOULD rate limit the number of echo replies it sends to approximately 1 per second.

A node receiving an ISAKMP echo reply MAY log it. Repeated echo replies from the same originator SHOULD not cause excessive logging to occur.

### 3. Security Considerations

There is a concern that this protocol not be used to perform distributed denial attacks. If responder can be tricked into replying to a broadcast address, it could lead to an explosive multiplicative effect. This protocol is not susceptible to this because there are separate messages for request and reply.

In addition to the above observation, nodes are expected to rate limit all responses.

The responding node is asked to put its highest available ISAKMP version number in the reply. This is potentially useful information to an attacker, and implementations MAY choose to lie here. This is not recommended as there are other ways of determining this information.

## References

- [1] Postel, J., "Internet Control Message Protocol", STD 5, [RFC 792](#), September 1981.
- [2] Maughan, D., Schneider, M. and M. Schertler, "Internet Security Association and Key Management Protocol (ISAKMP)", [RFC 2408](#), November 1998.

## Author's Address

Michael C. Richardson  
Sandelman Software Works  
470 Dawson Avenue  
Ottawa, ON K1Z 5V7  
CA

EMail: [mcr@sandelman.ottawa.on.ca](mailto:mcr@sandelman.ottawa.on.ca)

URI: <http://www.sandelman.ottawa.on.ca/>



## Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.