Internet Draft
Expires in six months

R. Monsour, Hi/fn, Inc.
R. Pereira, TimeStep Corporation
A. Shacham, Cisco Systems

July 30, 1997

IP Payload Compression Protocol Architecture

<draft-ietf-ippcp-arch-00.txt>

Status of this Memo

Abstract

This memo describes an architecture for applying lossless compression to Internet Protocol datagrams. It defines several of the key architectural elements of a compression protocol and describes alternatives for each element.

Acknowledgments

The authors gratefully acknowledge the many sources of input who made this draft possible, including Rodney Thayer, Bob Moskowitz, Naganand Doraswamy, Thomas Narten and all those that participated in the early discussions and debates of these concepts. It is hoped that the continued focused effort of those involved in the IPCCP Working Group will result in the rapid development of a useful IP compression protocol.

Internet Draft draft-ietf-ippcp-arch-00.txt July 29, = 1997

Table of Contents

1. Introduction

This document is a submission to the IETF IP Payload Compression Protocol (IPCCP) Working Group. Comments are solicited and should be addressed to the working group mailing list = (ippcp@external.cisco.com)
or to the editor.

1.1. Background

The motivation for the development of the IP Payload Compression Protocol was initially driven by the use of the IP Security protocol and the negative effect that IP encryption has on data link layer compression techniques. Encrypted data is random in nature and not compressible. When an IP datagram is encrypted, compression methods used at lower protocol layers, e.g., the PPP Compression Control Protocol [RFC-1962], are rendered ineffective. If both compression and encryption are desired, compression must be performed first. Such

motivation drove the creation of a new working group, the IP Payload Compression Protocol working group, and the development of this document.

1.2. IP Payload Compression Overview

The IP payload compression architecture is designed to provide compression services for the IP Protocol. Two fundamental = requirements of such a compression protocol are: (1) that it supports the use of any lossless compression method, and (2) the two communicating = parties have a mechanism to negotiate the use of specific compression method and any related parameters.

This document describes the architectural alternatives available for supporting lossless compression services for IP datagrams. The following topics are discussed:

a) alternative approaches for integrating compression with IP Security
b) features of an IP compression protocol
c) negotiation and use of lossless compression techniques, both in the presence and absence of the IP Security protocol
d) requirements for a registration mechanism used for identifying compression methods for use with the protocol
e) a document roadmap to simplify access and understanding of the necessary specifications

1.3. Specification of Requirements

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 RFC2119 [RFC-2119].

2. Use of IP Compression with IPSec

2.1. General Compression Processing

The compression processing of IP datagrams has two phases, = compressing of outbound IP datagrams and decompressing of inbound datagrams.

The compression of outbound IP datagrams MUST be done before any IP security processing, such as encryption and authentication, and = before any fragmentation of the IP datagram. Similarly, the decompression = of inbound IP datagrams MUST be done after the reassembly of the IP datagrams, and after the completion of all IP security processing, such as authentication and decryption. Processing of inbound IP

datagrams MUST support both compressed and non-compressed IP datagrams.

A different compression algorithm may be negotiated in each direction of the communication channel, or only one direction may be = compressed.

2.2. Alternative Compression Protocol Approaches

Two recent Internet Drafts have been submitted by members of the working group, each offering a different approach to the application of lossless compression to IP datagram payloads. Note that in the description of both approaches, examples are provided in the more complex IP Security context. The simplification of the resulting packet formats for non-IPSec environments should be apparent from the examples.

2.2.1.T
he IP Encapsulation Approach

The first approach, what we=92ll call IP encapsulation, is described =
in
[Shacham]. This approach involves the following steps (Note: this is =
a
simplified view of the processing):

a) a complete IP datagram is treated as a payload and is compressed
b) a new IP header is prepended to the datagram to be compressed
c) subsequent IP security processing, if any, is applied to the new
datagram

The following is an example datagram structure which results when
using this approach in conjunction with ESP. This approach can be =
used
with AH as well as without any security processing of the datagram.