IP Header Compression over PPP

Status of this Memo

This document is an Internet-Draft. 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."

To learn the current status of any Internet-Draft, please check the "list-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this document is unlimited.

Abstract

This document describes an option for negotiating the use of header compression on IP datagrams transmitted over the Point-to-Point Protocol [RFC1661]. It defines extensions to the PPP Control Protocols for IPv4 and IPv6 [RFC1332, RFC2023]. Header compression may be applied to IPv4 and IPv6 datagrams in combination with TCP, UDP and RTP transport protocols as specified in [IPHC] and [CRTP].

[Note to IANA, to be removed before publication: The PPP protocol type assignments suggested in this document were selected from those unassigned in ftp://ftp.isi.edu/in-notes/iana/assignments/ppp-numbers on December 7, 1997. These selections were presented to the PPPext working group at IETF in Washington, DC on December 9, 1997 and were approved as being in the appropriate ranges for this protocol.]
1. Introduction

The IP Header Compression (IPHC) defined in [IPHC] may be used for compression of both IPv4 and IPv6 datagrams or packets encapsulated with multiple IP headers. IPHC is also capable of compressing both TCP and UDP transport protocol headers. The IP/UDP/RTP header compression defined in [CRTP] fits within the framework defined by IPHC so that it may also be applied to both IPv4 and IPv6 packets.

In order to establish compression of IP datagrams sent over a PPP link each end of the link must agree on a set of configuration parameters for the compression. The process of negotiating link parameters for network layer protocols is handled in PPP by a family of network control protocols (NCPs). Since there are separate NCPs for IPv4 and IPv6, this document defines configuration options to be used in both NCPs to negotiate parameters for the compression scheme.

IPHC relies on the link layer’s ability to indicate the types of datagrams carried in the link layer frames. In this document nine new types for the PPP Data Link Layer Protocol Field are defined along with their meaning.

In general, header compression schemes that use delta encoding of compressed packets require that the lower layer does not reorder packets between compressor and decompressor. IPHC uses delta encoding of compressed packets for TCP and RTP. The IPHC specification [IPHC] includes methods that allow link layers that may reorder packets to be used with IPHC. Since PPP does not reorder packets these mechanisms are disabled by default. When using reordering mechanisms such as multiclass multilink PPP [MCML], care must be taken so that packets that share the same compression context are not reordered.

2. Configuration Option

This document specifies a new compression protocol value for the IPCP IP-Compression-Protocol option as specified in [RFC1332]. The new value and the associated option format are described in section 2.1.

The option format is structured to allow future extensions to the IPHC scheme.

NOTE: The specification of link and network layer parameter negotiation for PPP [RFC1661], [RFC1331], [RFC1332] does not prohibit multiple instances of one configuration option but states that the specification of a configuration option must explicitly allow multiple instances. From the current specification of the IPCP IP-Compression-Protocol option it is one.
configuration option [RFC1332, p 6] it follows that it can only be used to select a single compression protocol at any given time.

NOTE:  [RFC1332] is not explicit about whether the option negotiates the capabilities of the receiver or of the sender. In keeping with current practice, we assume that the option describes the capabilities of the decompressor (receiving side) of the peer that sends the Config-Req.

2.1. Configuration Option Format

Both the network control protocol for IPv4, IPCP [RFC1332] and the IPv6 NCP, IPV6CP [RFC2023] may be used to negotiate IP Header Compression parameters for their respective protocols. The format of the configuration option is the same for both IPCP and IPV6CP.

Description

This NCP configuration option is used to negotiate parameters for IP Header Compression. The option format is summarized below. The fields are transmitted from left to right.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |    IP-Compression-Protocol    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           TCP_SPACE           |         NON_TCP_SPACE         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         F_MAX_PERIOD          |          F_MAX_TIME           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           MAX_HEADER          |          suboptions...        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type
2

Length
\geq 14

The length may be increased if the presence of additional parameters is indicated by additional suboptions.

IP-Compression-Protocol
0061 (hex)
TCP_SPACE
The TCP_SPACE field is two octets and indicates the maximum value of a context identifier in the space of context identifiers allocated for TCP.

Suggested value: 15

TCP_SPACE must be at least 0 and at most 255 (The value 0 implies having one context).

NON_TCP_SPACE
The NON_TCP_SPACE field is two octets and indicates the maximum value of a context identifier in the space of context identifiers allocated for non-TCP. These context identifiers are carried in COMPRESSED_NON_TCP, COMPRESSED_UDP and COMPRESSED_RTP packet headers.

Suggested value: 15

NON_TCP_SPACE must be at least 0 and at most 65535 (The value 0 implies having one context).

F_MAX_PERIOD
Maximum interval between full headers. No more than F_MAX_PERIOD COMPRESSED_NON_TCP headers may be sent between FULL_HEADER headers.

Suggested value: 256

A value of zero implies infinity, i.e. there is no limit to the number of consecutive COMPRESSED_NON_TCP headers.

F_MAX_TIME
Maximum time interval between full headers. COMPRESSED_NON_TCP headers may not be sent more than F_MAX_TIME seconds after sending the last FULL_HEADER header.

Suggested value: 5 seconds

A value of zero implies infinity.

MAX_HEADER
The largest header size in octets that may be compressed.

Suggested value: 168 octets

The value of MAX_HEADER should be large enough so that at least the outer network layer header can be compressed. To increase
compression efficiency `MAX_HEADER` should be set to a value large enough to cover common combinations of network and transport layer headers.

suboptions
The suboptions field consists of zero or more suboptions. Each suboption consists of a type field, a length field and zero or more parameter octets, as defined by the suboption type. The value of the length field indicates the length of the suboption in its entirety, including the lengths of the type and length fields.

```
0                   1                   2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|     Type      |    Length     |  Parameters...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

2.2 RTP-Compression Suboption

The RTP-Compression suboption is included in the NCP IP-Compression-Protocol option for IPHC if IP/UDP/RTP compression is to be enabled.

After successful negotiation of parameters for IP Header Compression the use of Protocol Identifiers `FULL_HEADER`, `COMPRESSED_TCP`, `COMPRESSED_TCP_NODELTA` and `COMPRESSED_NON_TCP` is enabled, regardless of the presence of an RTP-Compression suboption.

Description

Enable use of Protocol Identifiers `COMPRESSED_RTP`, `COMPRESSED_UDP` and `CONTEXT_STATE` as specified in [RFC].

```
0                   1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|     Type      |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Type

```
1
```

Length

```
2
```
3. Multiple Network Control Protocols

The IPHC protocol is able to compress both IPv6 and IPv4 datagrams. Both IPCP and IPV6CP are able to negotiate option parameter values for IPHC. These values apply to the compression of packets where the outer header is an IPv4 header and an IPv6 header, respectively.

3.1. Sharing Context Identifier Space

For the compression and decompression of IPv4 and IPv6 datagram headers the context identifier space is shared. While the parameter values are independently negotiated, sharing the context identifier spaces becomes more complex when the parameter values differ. Since the compressed packets share context identifier space, the compression engine must allocate context identifiers out of a common pool; for compressed packets, the decompressor has to examine the context state to determine what parameters to use for decompression.

Context identifier spaces are not shared between TCP and non-TCP/UDP/RTP. Doing so would require additional mechanisms to ensure that no error can occur when switching from using a context identifier for TCP to non-TCP.

4. Demultiplexing of Datagrams

The IPHC specification [IPHC] defines four header formats for different types of compressed headers. They are compressed TCP, compressed TCP with no delta encoding, compressed non-TCP with 8 bit CID and compressed non-TCP with 16 bit CID. The two non-TCP formats may be distinguished by their contents so both may use the same link-level identifier. A fifth header format, the full header is distinct from a regular header in that it carries additional information to establish shared context between the compressor and decompressor.

The specification of IP/UDP/RTP Header Compression [CRTP] defines four additional formats of compressed headers. They are for compressed UDP and compressed RTP (on top of UDP), both with either 8- or 16-bit CIDs. In addition, there is an explicit error message from the decompressor to the compressor.

The link layer must be able to indicate these header formats with distinct values. Nine PPP Data Link Layer Protocol Field values are specified below.
FULL_HEADER
The frame contains a full header as specified in [CRTP] Section 3.3.1. This is the same as the FULL_HEADER specified in [IPHC] Section 5.3.
Value: 0061 (hex)

COMPRESSED_TCP
The frame contains a datagram with a compressed header with the format as specified in [IPHC] Section 6a.
Value: 0063 (hex)

COMPRESSED_TCP_NODELTA
The frame contains a datagram with a compressed header with the format as specified in [IPHC] Section 6b.
Value: 2063 (hex)

COMPRESSED_NON_TCP
The frame contains a datagram with a compressed header with the format as specified in either Section 6c or Section 6d of [IPHC].
Value: 0065 (hex)

COMPRESSED_RTP_8
The frame contains a datagram with a compressed header with the format as specified in [CRTP] Section 3.3.2, using 8-bit CIDs.
Value: 0069 (hex)

COMPRESSED_RTP_16
The frame contains a datagram with a compressed header with the format as specified in [CRTP] Section 3.3.2, using 16-bit CIDs.
Value: 2069 (hex)

COMPRESSED_UDP_8
The frame contains a datagram with a compressed header with the format as specified in [CRTP] Section 3.3.3, using 8-bit CIDs.
Value: 0067 (hex)

COMPRESSED_UDP_16
The frame contains a datagram with a compressed header with the format as specified in [CRTP] Section 3.3.3, using 16-bit CIDs.
Value: 2067 (hex)

CONTEXT_STATE
The frame is a link-level message sent from the decompressor to the compressor as specified in [CRTP] Section 3.3.5.
Value: 2065 (hex)
5. References


6. Security Considerations

Negotiation of the option defined here imposes no additional security considerations beyond those that otherwise apply to PPP [RFC1661].

The use of header compression can, in rare cases, cause the mis-delivery of packets. If necessary, confidentiality of packet contents should be assured by encryption. Encryption applied at the IP layer (e.g., using IPSEC mechanisms) precludes header compression of the encrypted headers, though compression of the outer IP header and authentication/security headers is still possible as described in [IPHC]. For RTP packets, full header compression is possible if the RTP payload is encrypted by itself without encrypting the UDP or RTP headers, as described in [RFC1889]. This method is appropriate when the UDP and RTP header information need not be kept confidential.
7. Authors' Addresses

Mathias Engan
CDT/Dept of Computer Communication
Lulea University of Technology
S-971 87 Lulea, Sweden
Phone: +46 920 72288
Mobile: +46 70 522 8109
Fax: +46 920 72801
EMail: engan@cdt.luth.se

Stephen L. Casner
Precept Software, Inc.
1072 Arastradero Road
Palo Alto, CA 94304
United States
EMail: casner@precept.com

Carsten Bormann
Universitaet Bremen FB3 TZI
Postfach 330440
D-28334 Bremen, GERMANY
EMail: cabo@tzi.uni-bremen.de
Phone: +49.421.218-7024
Fax: +49.421.218-7000