A. Minaburo
P. Rawat
L. Toutain
J-M. Bonnin
GET/ENST Bretagne
E. Paik
KT

February 27, 2006

IP Tunneling Header Compression
draft-minaburo-hc-tunneling-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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/1id-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 31, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

The IP tunneling mechanisms are widely used in mobility (NEMO and Mobile IP), security (VPN) and IP transition. They use an IP encapsualation (at least 2 IP headers), which is very expensive for wireliss links. Header compression mechanisms can be used to reduce

this overhead, independent of the payload type.

This document defines the use of normal header compression mechanisms for the tunneled (inner) header together with a new header compression mechanism for the tunneling (outer) transport header to reduce the header size.

Table of Contents

1. Introduction

IP Tunneling [RFC 2003??] encapsulation has been used for many years by ISPs to offer VPNs with private addresses. Nowadays, IP in IP encapsulation is used to support mobility like in NEMO or Mobile IP, when mobile node or mobile router is not at their home networks. Another common use of IP tunneling is for migration to IPv6 and NAT traversal using UDP enscapuslation for IPv6 packets (e.g. using L2TP).

IP tunneling adds overhead due to double headers used between the two peers and the wireless nature of the communication. This leads to bad performance in wireless links where bandwidth is scarce. Many header compression algorithms have been studied to reduce the header size, but they give a low performance against errors in wireless links. Also, they focus only on the inner IP encapuslation leaving the outer part of the encapsulation without any compression.

This document defines a new header compression mechanism, tunneling compression protocol (TuCP) to compress the outer tunnel headers. And, explains the use of a header compression mechanism such as ROHC, ECRTP and CTCP to compress the ingress (inner) part of the tunneling encapsulation together with the tunneling compression protocol (TuCP). Also, a solution is provided for the problem that occurs due to the disordering of packets between two header compression endpoints. The normal header compression mechanisms do not support disordering of packets and have been defined to work in a point to point link where disordering does not takes place.

2. Header Compression and Tunneling Compression Protocol

2.1. Basics

IP Tunneling is the encapsulation of a packet within another packet, both of which supporting the same or different protocols as shown in Figure 1. IP tunneling involves different components: the tunneled protocol which gives the inner encapuslation and the tunneling or transport protocol that reperesents the outer encapsulation.

```
                Outer                  Inner
             Encapsulation          Encapsulation
   +---+---------------------+--------------------+----------+
   |   |Tunneling Header     | Tunneled Header    |          |      Without
   |IP |Any Tunnel Protocol  |  IP + Any upper    | Payload  |    Compression
   |   |                     | layer protocol     |          |
   +---+---------------------+--------------------+----------+
```

Figure 1: Tunneling and Tunneled Encapsualtion

As, tunnels are bi-directional, header compression mechanisms will be able to perform at both ends of the tunnel and use feedbacks. The tunneling encapsulation consists of an IP header followed by a combination of tunnel protocols such as GRE, UDP, L2TP, and PPP. The first IP header MUST not be compressed, because it ensures the delivery of the packet to the other end of the tunnel.

2.2. Tunneling Compression Profiles

Tunneling protocols add one or more additional headers to the tunneled header and are used to identify different tunnels. Tunneling can be applied at the same or at a different layer.

In the tunneling encapsulation (outer IP encapsulation), IP protocol will be used together with one or more protocols or without any protocol. These protocols can be UDP (User Datagram Protocol), L2TP (Layer 2 Tunnel Protocol), and PPP (Point to Point Protocol) etc. Figure 2. shows the generic tunnel headers. For the header compression of outer packet, four tunneling compression profiles have been defined:

Profile 0 no tunneling header

Profile 1 UDP

Profile 2 UDP/L2TP/PPP

Profile 3 L2TP/PPP Use when UDP is used for NAT traversal.

```
               Outer                   Inner
             Encapuslation          Encapsulation
   +---+---------------------+--------------------+----------+
   |   | Tunneling Header    |  Tunneled Header   |          |       With
   |IP |     TuCP            | Header Compression | Payload  |    Compression
   |   |                     |    Mechanism       |          |
   +---+---------------------+--------------------+----------+
```

Figure 2: Generic Tunnel Headers

2.3. General Packet Format

All the tunneling signalling (e.g. L2TP, Mobile IP) packets are not compressed and they are identified by two bits in the header format. Only user data packets will be compressed. Figure 3. shows the general compressed format packet. The first two bits are description type bits (D), which are used to identify the tunneling signalling from header compression (ROHC) negotiation packet and ROHC header compressed packets. TuCP (3 bits) bits are used to indetify the tunneling profile. Transfer Sequence Number is introduced to identify the disordering in the packet delivery.

```
           0                   1
           0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
           +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           :IP Header for egress tunneling :
           : encapsulation                 :
           +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           |TuCP | Transfer Seq. Number    |
           +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+    : Variable Length
           :TuCP hdr compression Hdr &     :
           :Hdr Compression Mech. Hdr or   :
           :Tunneling Signalling Hdr       :
           +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           :                               :
           :         Payload               :
           +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3: General Format Packet

D: Description Type Bits

00 Reserved

01 Tunneling Signalling Packets

10 Header Compression Mechanism Packets

11 Reserved

2.4. Transfer Sequence Number

Header compression mechanisms are designed to work over an ordered delivery transmission between the compressor and decompressor. When sending compressed packets in the IP tunneling, many hops will be crossed in different ways and ordered delivery may not be guaranteed. This document gives a solution that does not reduce the performance of header compression mechanisms and at the same time delivers packets in order. This is done by introducing a transfer sequence number in the general format packet as shown in Figure 3. The Transfer Sequence Number will give the decompressor, the transmission order in which packets have been sent. When, there is a disordering in the delivery of packets, before making decompression of an early arriving packet, the decompressor has to wait until the ordered delivery packet arrives or a timer expires. When the timer expires, missing packets are assumed to be lost.

The timer value is out of the scope of this draft, it will need to be studied depdending on the congestion in the network.

2.5. Overview of the Dual Header Compression

TuCP classifies the tunneling header fields into static and dynamic fields. First, TuCP sends both static and dynamic fields and then compressor sends only the dynamic fields. Section 3. gives a general classification of fields of different tunneling protocols. TuCP profiles can be used together with any header compression mechanism to reduce the header size. If we use a normal header compression mechanism within the complete tunneling encapsulation, we will need to modify the header compression mechanism to take into account tunneling. Also, the first IP header of the outer packet is not compressed because it is used by routers to forward the packet to the tunnel end-point.

The header compression can be done into two parts: the first part is the compression of the inner header packet with any header compression mechanism and the second part is the compression of the outer header packet with TuCP. This dual header compression can be used in NEMO networks and this solution can be extended for any tunneling encapsulation.

3. Tunneling Header Fields Pattern

This section gives a first approach for the pattern of the different fields of the tunneling protocols. All fields of different tunneling protocols can be classfied into static and dynamic fields. This section gives a general classification of fields of different tunneling protocols such as GRE, UDP, L2TP and PPP.

Field	Pattern
C flag	Static
Reserved flags	Static
Version	Static
Protocol Type	Static
Checksum	Dynamic
Reserved1	Static

Figure 4: GRE

Field	Pattern
Source Port	Static
Destination Port	Static
Datagram Length	Inferred
Checksum	Dynamic

Figure 5: UDP

Field	Pattern
T flag	Static
L flag	Static
S flag	Static
O flag	Static
P flag	Static
Version	Staitc
Length	Static
Tunnel ID	Static
Session ID	Static
Ns	Dynamic
Nr	Dynamic
Offset Size	Dynamic
Offset Pad	Static

Figure 6: L2TP

Field	Pattern
Address	Static
Control	Static
Protocol	Static
FCS	Dynamic

Figure 7: PPP

4. IANA Considerations

This document defines a new IP protocol to identify tunneling compression, which is described in section 3.

5. Security Considerations

This document by itself does not add any security risk to the use of header compression as they have already been defined in each mechanism.

6. References

6.1. Normative References

[BCP] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels, BCP 14", RFC 2119, March 1997.

[CTCP] Casner, S., Jacobson, V., and B. Thompson, "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links", RFC 2508, February 1999.

[ECRTP] Koren, T., Casner, S., Geevarghese, J., Thompson, B., and P. Ruddy, "Enhanced RTP (CRTP) for Links with High Delay, Packet Loss and Reordering", RFC 3545, July 2003.

[GRE] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation", RFC 2784, March 2000.

[L2TP] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and B. Palter, "Layer Two Tunneling Protcol", RFC 2661, August 1999.

[PPP] Simpson, W., "The Point-to-Point Protcol", RFC 1661, July 1994.

[RFC2131] Droms, R., ""Dynamic Host Configuration Protocol"", RFC 2131, March 1997.

[RFC2136] Vixie, P., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC3053] Durand, A., Fasano, P., Guardini, I., and D. Lento, "IPv6 Tunnel Broker", RFC 3053, January 2001.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Baisc Support Protocol", RFC 3963, January 2005.

[ROHC] Bromann, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L-E., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., and H. Zheng, ""Robust Header Compression

(ROHC): Framework and four profiles: RTP,UDP,ESP, and uncompressed"", RFC 3095, July 2001.

[UDP] Postel, J., ""User Datagram Protcol"", RFC 768, August 1980.

6.2. Informative References

[ENTANA] "IPv6 Enterprise Network Analysis", draft-ietf-v6ops-enst-analysis-03.txt (work in progress), July 2005.

[RFC4057] "IPv6 Enterprise Netwrok Scenariosn", RFC 4057, June 2005.

[TSP] Blanchet, M. and F. Parent, "Tunnel Setup Protocol", draft-blanchet-v6ops-tunnelbroker-tsp-03.tx (work in progress), March 2006.

Authors' Addresses

Ana Minaburo
GET/ENST Bretagne
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Fax: +33 2 99 12 70 30
Email: anacarolina.minaburo@enst-bretagne.fr

Priyanka Rawat
GET/ENST Bretagne
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Fax: +33 2 99 12 70 30
Email: Priyanka.Rawat@enst-bretagne.fr

Laurent Toutain
GET/ENST Bretagne
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Fax: +33 2 99 12 70 30
Email: Laurent.Toutain@enst-bretagne.fr

J-M Bonnin
GET/ENST Bretagne
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Fax: +33 2 99 12 70 30
Email: jm.bonnin@enst-bretagne.fr

Eun Kyoung Paik
KT
Portable Internet Team, Convergence Lab., KT
17 Woomyeon-dong, Seocho-gu
Seoul 137-792
Korea

Fax: +82 2 526 5200
Email: euna@kt.co.kr

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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