Network Working Group
Request for Comments: 5172
Obsoletes: 2472
Category: Standards Track

S. Varada, Ed.
Transwitch

March 2008

Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol

Status of This Memo

Abstract

The Point-to-Point Protocol (PPP) provides a standard method of encapsulating network-layer protocol information over point-to-point links. PPP also defines an extensible Link Control Protocol, and proposes a family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

The IPv6 Control Protocol (IPV6CP), which is an NCP for a PPP link, allows for the negotiation of desirable parameters for an IPv6 interface over PPP.

This document defines the IPv6 datagram compression option that can be negotiated by a node on the link through the IPV6CP.

Table of Contents

1. Introduction

PPP [1] has three main components:

1) A method for encapsulating datagrams over serial links.

2) A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.

3) A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

In order to establish communications over a point-to-point link, each end of the PPP link must first send LCP packets to configure and test the data link. After the link has been established and optional facilities have been negotiated as needed by the LCP, PPP must send NCP packets to choose and configure one or more network-layer protocols. Once each of the chosen network-layer protocols has been configured, datagrams from each network-layer protocol can be sent over the link. The link will remain configured for communications until explicit LCP or NCP packets close the link down, or until some external event occurs (power failure at the other end, carrier drop, etc.).

In the IPv6 over PPP specification [2], the NCP, or IPV6CP, for establishing and configuring IPv6 over PPP is defined. The same specification defines the Interface Identifier parameter, which can be used to generate link-local and globally unique IPv6 addresses, for negotiation.

In this specification, the compression parameter for use in IPv6 datagram compression is defined. Together with RFC 5072 [2], this document obsoletes RFC 2472 [13]. However, no protocol changes have been introduced over RFC 2472.

1.1. Specification of Requirements

In this document, several words are used to signify the requirements of the specification.

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 [3].

2. IPV6CP Configuration Options

IPV6CP Configuration Options allow negotiation of desirable IPv6 parameters. IPV6CP uses the same Configuration Option format as defined for LCP [1] but with a separate set of Options. If a Configuration Option is not included in a Configure-Request packet, the default value for that Configuration Option is assumed.

The only IPV6CP option defined in this document is the IPv6-Compression-Protocol. The Type field for this IPV6CP Option is as follows:

2 IPv6-Compression-Protocol

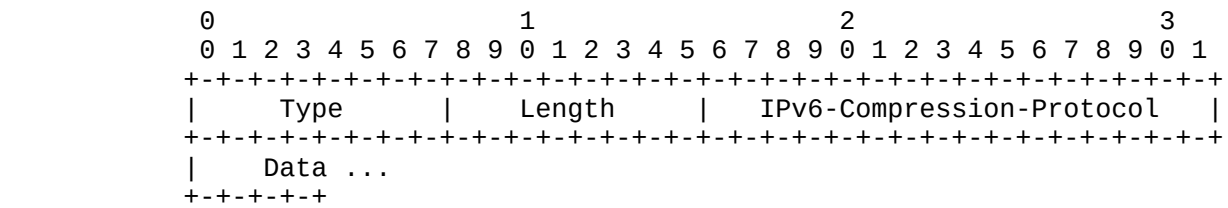
Note that the up-to-date values of the IPV6CP Option Type field are specified in the on-line database of "Assigned Numbers" maintained by IANA [7].

2.1. IPv6-Compression-Protocol

This Configuration Option provides a way to negotiate the use of a specific IPv6 packet compression protocol. The IPv6-Compression-Protocol Configuration Option is used to indicate the ability to receive compressed packets. Each end of the link MUST separately request this option if bidirectional compression is desired. By default, compression is not enabled.

IPv6 compression negotiated with this option is specific to IPv6 datagrams and is not to be confused with compression resulting from a compression method negotiated via the PPP Compression Control Protocol (CCP) [12], which potentially affects all datagrams.

A summary of the IPv6-Compression-Protocol Configuration Option format is shown below. The fields are transmitted from left to right.



Type

2

Length

>= 4

IPv6-Compression-Protocol

The IPv6-Compression-Protocol field is two octets and indicates the compression protocol desired. Values for this field are always the same as the PPP Data Link Layer Protocol field values for that same compression protocol.

IPv6-Compression-Protocol field values have been assigned in [4, 5] for IP Header Compression (0061), and in [6] for Robust Header Compression (ROHC) (0003). Other assignments can be made in documents that define specific compression algorithms.

Data

The Data field is zero or more octets and contains additional data as determined by the particular compression protocol.

The default (in the absence of negotiation of this option) is to have no IPv6 compression protocol enabled.

3. Security Considerations

Lack of proper link security, such as authentication, prior to data transfers may enable man-in-the middle attacks resulting in the loss of data integrity and confidentiality. The mechanisms that are appropriate for ensuring PPP link security are addressed below together with the reference to a generic threat model.

The mechanisms that are appropriate for ensuring PPP link security are: 1) Access Control Lists that apply filters on traffic received over the link for enforcing admission policy, 2) an authentication protocol that facilitates negotiations between peers [8] to select an authentication method (e.g., MD5 [9]) for validation of the peer, and 3) an encryption control protocol that facilitates negotiations between peers to select encryption algorithms (or crypto-suites) to ensure data confidentiality [10]).

There are certain threats associated with peer interactions on a PPP link even with one or more of the above security measures in place. For instance, using the MD5 authentication method [9] exposes one to replay attacks, in which an attacker could intercept and replay a station’s identity and password hash to get access to a network. The user of this specification is advised to refer to [8], which presents a generic threat model, for an understanding of the threats posed to

the security of a link. The reference [8] also gives a framework to specify requirements for the selection of an authentication method for a given application.

4. IANA Considerations

No specific action is needed for the assignment of a value for the Type field of IPv6 datagram compression option specified in this specification. The current assignment is up-to-date in the registry "PPP IPV6CP CONFIGURATION OPTIONS" for item IPv6-Compression-Protocol (2) at [7]. However, the RFC reference for that item has been changed to 5172.

No action is needed either for the assignment of the IPV6-Compression-Protocol values, as such values have already been defined by other documents listed in Section 2.1. Values for this field are always the same as the PPP Data Link Layer Protocol field values for that same compression protocol. As a result, future allocation of these values is governed by RFC 3818 [11] that requires IETF Consensus. Current values are in the registry "IPv6-Compression-Protocol Types". However, the RFC reference for that registry has been changed to 5172.

5. Management Considerations

From an operational point of view, the status of the negotiation and the compression algorithm on the link should be observable by an operator managing a network. There is no standard management interface that covers this at the time of the writing of this specification.

6. Acknowledgments

The editor is grateful to Jari Arkko for the direction provided on this document and James Carlson for helpful suggestions. Acknowledgments are also due to D. Haskin and E. Allen for the specification work done in RFC 2023 and RFC 2472.

7. References

7.1. Normative References

[1] Simpson, W., Ed., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[2] Varada, S., Ed., Haskin, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, September 2007.

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

[4] Degermark, M., Nordgren, B., and S. Pink, "IP Header Compression", RFC 2507, February 1999.

[5] Koren, T., Casner, S., and C. Bormann, "IP Header Compression over PPP", RFC 3544, July 2003.

[6] Bormann, C., "Robust Header Compression (ROHC) over PPP", RFC 3241, April 2002.

7.2. Informative References

[7] IANA, http://www.iana.org.

[8] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[9] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[10] Meyer, G., "The PPP Encryption Control Protocol (ECP)", RFC 1968, June 1996.

[11] Schryver, V., "IANA Considerations for the Point-to-Point Protocol (PPP)", BCP 88, RFC 3818, June 2004.

[12] Rand, D., "The PPP Compression Control Protocol(CCP)", RFC 1962, June 1996.

[13] Haskin, D. and E. Allen, "IP Version 6 over PPP", RFC 2472, December 1998.

Editor’s Address

Srihari Varada
TranSwitch Corporation
3 Enterprise Dr.
Shelton, CT 06484
US

Phone: +1 203 929 8810
EMail: varada@ieee.org

Full Copyright Statement

Intellectual Property