                   Point-to-Point Protocol (PPP) Vendor Protocol

Status of this Memo

Copyright Notice

Abstract

   The Point-to-Point Protocol (PPP) defines a Link Control Protocol
   (LCP) and a method for negotiating the use of multi-protocol traffic
   over point-to-point links. The PPP Vendor Extensions document adds
   vendor-specific general-purpose Configuration Option and Code
   numbers. This document extends these features to cover vendor-
   specific Network, Authentication, and Control Protocols.

1. Introduction

   PPP's [1] Vendor Extensions [3] defines a general-purpose mechanism
   for the negotiation of various vendor-proprietary options and
   extensions to the kinds of control messages that may be sent via the
   Code field.

   Some implementors may want to define proprietary network and control
   protocols in addition to the already-described features. While it
   would be possible for such an implementor to use the existing LCP
   Vendor-Specific Option to enable the use of the proprietary protocol,
   this staged negotiation (enable via LCP, then negotiate via some
   locally-assigned protocol number) suffers from at least three
   problems:

First, because it would be in LCP, the negotiation of the use of the
protocol would begin before identification and authentication of the
peer had been done. This complicates the security analysis of the
feature and constrains the way in which the protocol might be
deployed.

Second, where compulsory tunneling is in use, the system performing
the initial LCP negotiation may be unrelated to the system that uses
the proprietary protocol. In such a scenario, enabling the protocol
at LCP time would require either LCP renegotiation or support of the
proprietary protocol in the initial negotiator, both of which raise
deployment problems.

Third, the fact that any protocol negotiated via such a mechanism
would necessarily use a protocol number that is not assigned by IANA
complicates matters for diagnostic tools used to monitor the
datastream. Having a fixed number allows these tools to display such
protocols in a reasonable, albeit limited, format.

A cleaner solution is thus to define a set of vendor-specific
protocols, one in each of the four protocol number ranges defined by
[1]. This specification reserves the following values:

```
Value (in hex)   Protocol Name
005b             Vendor-Specific Network Protocol (VSNP)
405b             Vendor-Specific Protocol (VSP)
805b             Vendor-Specific Network Control Protocol (VSNCP)
c05b             Vendor-Specific Authentication Protocol (VSAP)
```

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 BCP 14, RFC 2119 [2].

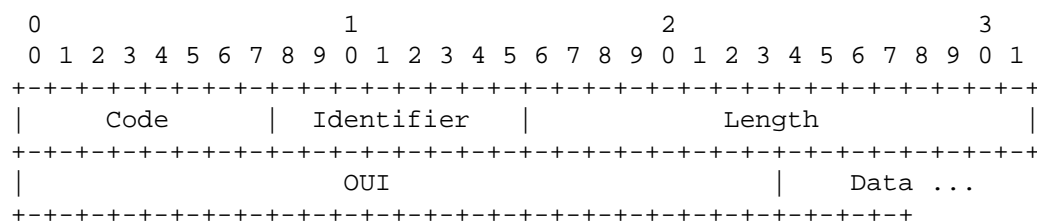2. PPP Vendor-Specific Network Control Protocol (VSNCP)

The Vendor-Specific Network Control Protocol (VSNCP) is responsible
for negotiating the use of the Vendor-Specific Network Protocol
(VSNP). VSNCP uses the same packet exchange and option negotiation
mechanism as LCP, but with a different set of options.

VSNCP packets MUST NOT be exchanged until PPP has reached the
Network-Layer Protocol phase. Any VSNCP packets received when not in
that phase MUST be silently ignored. If a VSNCP packet with an
unrecognized OUI is received, an LCP Protocol-Reject SHOULD be sent
in response.

The network layer data, carried in VSNP packets, MUST NOT be sent
unless VSNCP is in Opened state. If a VSNP packet is received when
VSNCP is not in Opened state and LCP is Opened, the implementation
MAY respond using LCP Protocol-Reject.

2.1. VSNCP Packet Format

Exactly one VSNCP packet is carried in the PPP Information field,
with the PPP Protocol field set to hex 805b (VSNCP). A summary of
the VSNCP packet format is shown below. The fields are transmitted
from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      OUI                      |  Data ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

   Only LCP Code values 1 through 7 (Configure-Request, Configure-
   Ack, Configure-Nak, Configure-Reject, Terminate-Request,
   Terminate-Ack, and Code-Reject) are used. All other codes SHOULD
   result in a VSNCP Code-Reject reply.

Identifier and Length

   These are as documented for LCP.

OUI

   This three-octet field contains the vendor's Organizationally
   Unique Identifier. The bits within the octet are in canonical
   order, and the most significant octet is transmitted first. See
   Section 5 below for more information on OUI values.

Data

   This field contains data in the same format as for the
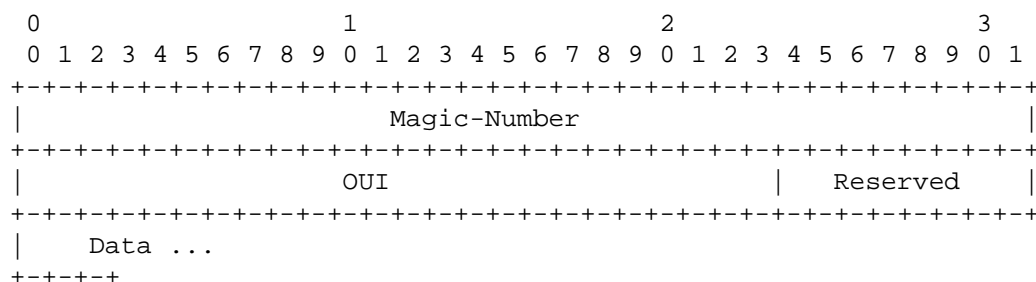   corresponding LCP Code numbers.

2.2. VSNP Packet Format

   When VSNCP is in Opened state, VSNP packets may be sent by setting
   the PPP Protocol field to hex 005b (VSNP) and placing the vendor-
   specific data in the PPP Information field. No restrictions are
   placed on this data.

3. PPP Vendor-Specific Protocol (VSP)

   The Vendor-Specific Protocol (VSP) is intended for use in situations
   where the implementation of a complete Network Layer Protocol is
   unnecessary, or where per-link signaling is required (see Section 7
   below).

   VSP packets MUST NOT be sent until PPP has reached either Network-
   Layer Protocol or Authentication phase. VSP packets received before
   those phases MUST be silently ignored. Once the proper phase has
   been reached, a VSP packet containing an unrecognized OUI value
   SHOULD be returned using LCP Protocol-Reject.

   Exactly one VSP packet is carried in the PPP Information field, with
   the PPP Protocol field set to 405b (VSP). A summary of the VSP
   packet format is shown below. The fields are transmitted from left
   to right.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         Magic-Number                          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         OUI                   |   Reserved    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    Data ...
   +-+-+-+
```

   Magic-Number

      The four-octet Magic-Number field is used to detect looped-back
      links. If the Magic-Number Option was not negotiated by LCP, then
      this field MUST be set to 0. Implementation of the LCP Magic-
      Number Option is RECOMMENDED.

   OUI

      This three-octet field contains the vendor's Organizationally
      Unique Identifier. The bits within the octet are in canonical
      order, and the most significant octet is transmitted first. See
      Section 5 below for more information on OUI values.

   Reserved

      Reserved for future definition. Must be zero on transmit and
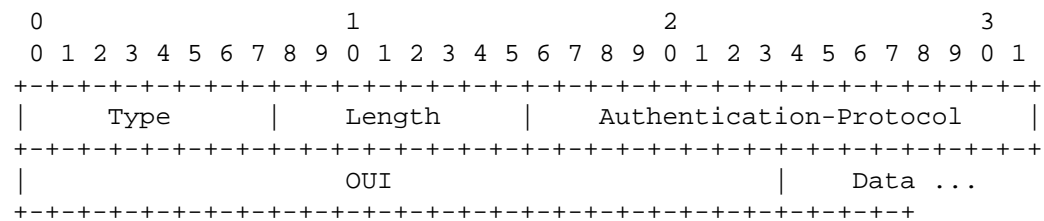   ignored on reception.

   Data

      Vendor-specific data.

4. PPP Vendor-Specific Authentication Protocol (VSAP)

   The Vendor-Specific Authentication Protocol (VSAP) is used in two
   ways. First, it is used with the LCP Authentication Option in order
   to negotiate the use of a vendor-specific authentication protocol to
   be used during the PPP Authentication phase. Second, it is used in
   the PPP Protocol field to carry those proprietary authentication
   messages during the PPP Authentication phase.

4.1. VSAP Authentication Option Format

   This option is used in LCP Configure-Request, -Ack, -Nak, and -Reject
   messages.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Length    |     Authentication-Protocol   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      OUI                      |    Data ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Type

      3

   Length

      >=7

   Authentication-Protocol

      The hex value c05b, in Network Byte Order.

   OUI

      This three-octet field contains the vendor's Organizationally
      Unique Identifier. The bits within the octet are in canonical
      order, and the most significant octet is transmitted first. See
      Section 5 below for more information on OUI values.

   Data

      This optional field contains options or other information specific
      to the operation of the vendor-specific authentication protocol.

4.2. VSAP Authentication Data Format

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Code      |  Identifier   |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    Data ...
   +-+-+-+-+
```

   The Identifier and Length fields are as for LCP. The Code and Data
   fields and the processing of the messages are defined by the vendor-
   specific protocol.

   However, it is RECOMMENDED that vendor-specific protocols use Code 3
   for "Success" and Code 4 for "Failure," as with [4] and [5], in order
   to simplify the design of network monitoring equipment.

5. Organizationally Unique Identifiers

   The three-octet Organizationally Unique Identifier (OUI) used in the
   messages described in this document identifies an organization
   ("vendor") that defines the meaning of the message. This OUI is
   based on IEEE 802 vendor assignments.

   Vendors that desire to use their IEEE 802 OUI for a PPP Vendor
   Protocol SHOULD also register the assigned OUI with IANA for the
   benefit of the community.

   A vendor that does not otherwise need an IEEE-assigned OUI can
   request a PPP-specific OUI from the IANA. This OUI shall be assigned
   from the CF0000 series. This procedure is defined for vendors that
   are not able to use IEEE assignments, such as software-only vendors.

6. Multiple Vendor-Specific Protocols

   Vendors are encouraged to define their protocols to allow for future
   expansion, where necessary. For example, it may be appropriate for a
   VSNP to include a locally-defined selector field to distinguish among
   multiple proprietary protocols carried via this mechanism, and
   appropriate Configuration Options in VSNCP to enable and disable
   these sub-protocols. Because the requirements of such a selector are
   known only to the vendor defining such protocols, they are not
   described further in this document.

   An implementation MAY also support more than one vendor-specific
   protocol, distinguished by OUI. In this case, the implementation
   MUST also treat LCP Protocol-Reject specially by examining the OUI
   field in the rejected message and disabling only the protocol to
   which it refers, rather than all use of the vendor-specific protocol
   number. Note that such an implementation is compatible with a simple
   implementation that supports only one OUI: that implementation will
   respond with LCP Protocol-Reject for unrecognized OUIs and otherwise
   leave the negotiation state unmodified.

   An OUI-distinguished mechanism is expected to be used only in the
   case of cooperating vendors. Vendors are encouraged to use just a
   single OUI for all protocols defined by that vendor, if possible.

7. Multilink, Compression, and Encryption Considerations

   The Vendor-Specific Network Protocol (VSNP) is defined to operate at
   the bundle level if Multilink PPP [6] is in use, and also above any
   Compression Protocols [7] and Encryption Protocols [8] in use.

   The Vendor-Specific Protocol (VSP) is defined to operate at the per-
   link level if Multilink PPP is in use, and MUST NOT be subjected to
   data compression. If a per-link encryption protocol is in use, then
   VSP packets MUST be encrypted.

   Note that because VSP is defined at the per-link level, bundle level
   encryption does not affect VSP.

8. Security Considerations

   The security of any vendor-specific authentication protocol is
   subject to the provisions of that proprietary mechanism.
   Implementations that wish to avoid security problems associated with
   such protocols SHOULD send LCP Configure-Nak in response to an LCP
   Configure-Request specifying VSAP, or MAY terminate operation.

When operating with PPP encryption, but without Multilink PPP, VSP
packets are sent in the clear. Implementations that require PPP
encryption as part of a security mechanism should consider whether to
employ per-link encryption or forego use of VSP in favor of VSNP.

The security of vendor-specific networking protocols is likewise
subject to the security mechanisms defined by those protocols.
Independent analysis of the security of any such protocol is
RECOMMENDED.

9. IANA Considerations

IANA has assigned four similarly-numbered PPP Protocol field values,
005b, 405b, 805b, and c05b, as described in Section 1 of this
document.

As described in Section 5 above and in [3], the IANA also maintains a
CF0000 series block of non-IEEE OUIs that may be allocated for
vendors that do not otherwise need an IEEE-assigned OUI.

10. References

10.1. Normative References

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

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

10.2. Informative References

   [3] Simpson, W., "PPP Vendor Extensions", RFC 2153, May 1997.

   [4] Simpson, W., "PPP Challenge Handshake Authentication Protocol
        (CHAP)", RFC 1994, August 1996.

   [5] Blunk, L. and J. Vollbrecht, "PPP Extensible Authentication
        Protocol (EAP)", RFC 2284, March 1998.

   [6] Sklower, K., Lloyd, B., McGregor, G., Carr, D. and T. Coradetti,
        "The PPP Multilink Protocol (MP)", RFC 1990, August 1996.

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

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

11. Acknowledgments

   The authors thank Karl Fox and Thomas Narten for their comments and
   help in preparing this document.

   Some of the language and phrasing has been borrowed from RFC 1332,
   written by Glenn McGregor, and RFC 2153, written by William Allen
   Simpson.

12. Authors

   Questions about this document should be addressed to the IETF pppext
   working group or the authors listed below.

   James Carlson
   Sun Microsystems
   1 Network Drive MS UBUR02-212
   Burlington MA 01803-2757

   Phone: +1 781 442 2084
   Fax: +1 781 442 1677
   EMail: james.d.carlson@sun.com

   Richard Winslow
   L-3 Communications Systems - East
   1 Federal Street A&E-2NE
   Camden, NJ 08102

   EMail: richard.winslow@l-3com.com

13. Full Copyright Statement