            Layer 2 Tunneling Protocol (L2TP) Active Discovery Relay
                      for PPP over Ethernet (PPPoE)

Status of this Memo

   This memo provides information for the Internet community. It does
   not specify an Internet standard of any kind. Distribution of this
   memo is unlimited.

Copyright Notice

Abstract

   The Point-to-Point Protocol (PPP) provides a standard method for
   transporting multi-protocol datagrams over point-to-point links.
   Layer Two Tunneling Protocol (L2TP), facilitates the tunneling of PPP
   packets across an intervening packet-switched network. And yet a
   third protocol, PPP over Ethernet (PPPoE) describes how to build PPP
   sessions and to encapsulate PPP packets over Ethernet.

   L2TP Active Discovery Relay for PPPoE describes a method to relay
   Active Discovery and Service Selection functionality from PPPoE over
   the reliable control channel within L2TP. Two new L2TP control
   message types and associated PPPoE-specific Attribute Value Pairs
   (AVPs) for L2TP are defined. This relay mechanism provides enhanced
   integration of a specific feature in the PPPoE tunneling protocol
   with L2TP.

Table of Contents

1. Introduction

   PPPoE [1] is often deployed in conjunction with L2TP [2] to carry PPP
   [3] frames over a network beyond the reach of the local Ethernet
   network to which a PPPoE Host is connected. For example, PPP frames
   tunneled within PPPoE may be received by an L2TP Access Concentrator
   (LAC) and then tunneled to any L2TP Network Server (LNS) reachable
   via an IP network.

   In addition to tunneling PPP over Ethernet, PPPoE defines a simple
   method for discovering services offered by PPPoE Access Concentrators
   (PPPoE AC) reachable via Ethernet from the PPPoE Host. Since the
   packets used in this exchange are not carried over PPP, they are not
   tunneled with the PPP packets over L2TP, thus the discovery
   negotiation cannot extend past the LAC without adding functionality.

   This document describes a simple method for relaying PPPoE Active
   Discovery (PAD) messages over L2TP by extracting the PAD messages and
   sending them over the L2TP control channel. After the completion of
   setup through the processing of PAD messages, PPP packets arriving
   via PPPoE are then tunneled over L2TP in the usual manner as defined
   in L2TP [2]. Thus, there are no data plane changes required at the
   LAC or LNS to support this feature. Also, by utilizing the L2TP
   control channel, the PPPoE discovery mechanism is transported to the
   LNS reliably, before creation of any L2TP sessions, and may take
   advantage of any special treatment applied to control messages in
   transit or upon receipt.

2. Protocol Operation

   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 RFC 2119 [4].

When PPPoE PAD messages are received at a PPPoE Access Concentrator,
the messages are passed over the L2TP control connection via a newly
defined Service Relay Request Message (SRRQ) on an established tunnel
(Section 3.1). When received, the PPPoE PAD message is processed at
the L2TP node, or relayed to another L2TP node or PPPoE Access
Concentrator. PPPoE PAD messages sent as replies are handled in a
similar manner over a newly defined Service Relay Reply Message
(SRRP) (Section 3.2).

2.1. PPPoE Active Discovery Stage

When a PPPoE Active Discovery Initiation packet (PADI) is received by
an L2TP LAC that is providing PPPoE Service Relay, the PADI MUST be
packaged in its entirety (including the Ethernet MAC header) within
the PPPoE Relay AVP and transmitted over established L2TP Control
Connection(s) associated with the interface on which the PADI
arrived.

The PPPoE Relay AVP is sent via the Service Relay Request Message
(SRRQ) defined in Section 3. The SRRQ message MUST NOT be sent to an
L2TP node which did not include the PPPoE Service Relay Response
Capability AVP during control connection establishment. If no
acceptable control connection is available or cannot be created,
PPPoE PAD operation MUST be handled locally by some means (including
intentionally ignoring the PPPoE PAD message, though this must be a
deliberate act).

It is a matter of local policy as to which control connections will
be established for relay and associated with a given interface, and
when the Control Connections will be established. For instance, an
implementation may "nail up" a control connection to a particular
L2TP destination and associate the connection with an interface over
which PPPoE PADI packets will arrive. Alternatively, an
implementation might dynamically establish a Control Connection to a
predetermined destination upon receipt of a PADI, or upon receipt of
a PADI from a particular source.

Upon receipt of the SRRQ, the included PPPoE PADI message MUST be
processed as described in [3], be relayed to another L2TP control
connection, or be relayed to another PPPoE AC.

After processing of a PADI, any resultant PPPoE Active Discovery
Offer packet (PADO) MUST be encapsulated in a PPPoE Relay AVP and
delivered via the Service Relay Reply Message (SRRP) to the sender of
the SRRQ.

Upon receipt of an SRRP message with relayed PADO, a LAC MUST send
the encapsulated PADO message to the corresponding PPPoE Host. The
source MAC address of the PADO message MUST be one which the LAC will
respond to, perhaps requiring substitution of its own MAC address.

In each exchange above, the PPPoE Host-Uniq TAG or AC-Cookie TAG MUST
be used as described in Section 2.3.

Following is an example of the PAD exchange between a PPPoE Host, LAC
and LNS up to this point, assuming the L2TP Control Connection has
already been established. Examples that include AC-Cookie TAG and
Host-Uniq TAG operation are included in the Appendix.

```
     PPPoE Host            LAC              Tunnel Switch            LNS

              PADI ->
                        SRRQ (w/PADI) ->      SRRQ (w/PADI) ->
                        <- SRRP (w/PADO)      <- SRRP (w/PADO)
              <- PADO
```

2.2. Session Establishment and Teardown

When a LAC that is providing the PPPoE Service Relay feature receives
a valid PPPoE Active Discovery Request packet (PADR), the LAC MUST
treat this as an action for creation of a Incoming Call Request
(ICRQ) as defined in [2]. The resultant ICRQ message MUST contain
the PPPoE Relay AVP containing the PADR in its entirety.

Upon receipt of an L2TP ICRQ message, the LNS parses the PADR message
as described in [3]. If this is an acceptable PPPoE service
connection (e.g., the Service-Name-Error TAG would not be included in
a PPPoE Active Discovery Session-confirmation packet (PADS)
response), the L2TP Incoming-Call-Reply (ICRP) message that is sent
to the LAC includes the resultant PPPoE PADS encapsulated within the
PPPoE Relay AVP. If the service is unacceptable, the PADS with a
Service-Name-Error Tag is delivered via the Relay Session AVP within
a Call-Disconnect-Notify (CDN) message, which also tears down the
L2TP session. The PPPoE PADS SESSION_ID in the PPPoE Relay AVP MUST
always be zero as it will be selected and filled in by the LAC.

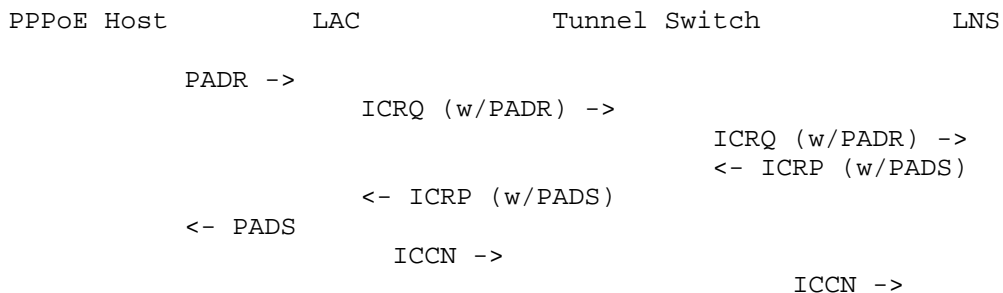Upon receipt of an ICRP with the PPPoE Relay AVP, the LAC parses the
PADS from the AVP, inserts a valid PPPoE SESSION_ID, and responds to
the PPPoE Host with the PADS. The MAC address of the PADS MUST be
the same one was utilized during the PADI/PADO exchange described
above. The LAC also completes the L2TP session establishment by
sending an Incoming-Call-Connected (ICCN) to the LNS and binds the

L2TP session with the PPPoE session. PPP data packets may now flow
between the PPPoE session and the L2TP session in the traditional
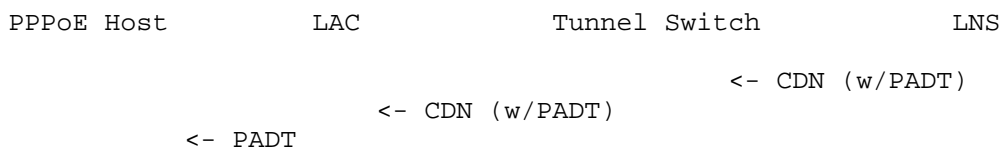manner.

If the L2TP session is torn down for any reason, the LAC MUST send a
PPPoE Active Discovery Terminate packet (PADT) to the host to
indicate that the connection has been terminated. This PADT MAY be
received from the LNS via the PPPoE Relay AVP within a CDN message if
this was a graceful shutdown initiated by the PPPoE subsystem at the
LNS. As with the PADS, the SESSION_ID in the PADT message is zero
until filled in with the proper SESSION_ID at the LAC.

If the LAC receives a PADT from the PPPoE Host, the L2TP session MUST
be shut down via the standard procedures defined in [2]. The PADT
MUST be sent in the CDN message to the LNS via the PPPoE Relay AVP.
If the PPPoE system at the LNS disconnects the session, a PADT SHOULD
be sent in the CDN. In the event that the LAC receives a disconnect
from L2TP and did not receive a PADT, it MUST generate a properly
formatted PADT and send it to the PPPoE Host as described in [3].

Session Establishment

  PPPoE Host   LAC   Tunnel Switch   LNS

          PADR ->
                      ICRQ (w/PADR) ->
                                            ICRQ (w/PADR) ->
                                            <- ICRP (w/PADS)
                      <- ICRP (w/PADS)
          <- PADS
                        ICCN ->
                                              ICCN ->

Session Teardown (LNS Initiated)

  PPPoE Host   LAC   Tunnel Switch   LNS

                                            <- CDN (w/PADT)
                      <- CDN (w/PADT)
          <- PADT

Session Teardown (Host Initiated)

  PPPoE Host   LAC   Tunnel Switch   LNS

          PADT ->
                      CDN (w/PADT) ->
                                            CDN (w/PADT) ->
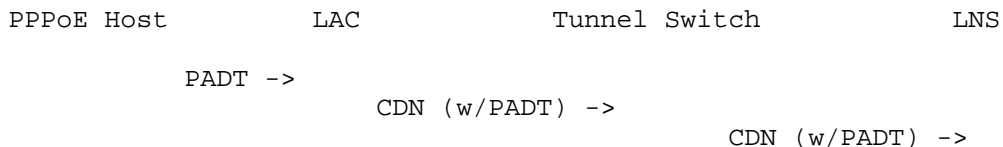
2.3. PPPoE PAD Message Exchange Coherency

   PPPoE PAD messages will arrive from multiple ethernet interfaces and
   be relayed across multiple L2TP control connections. In order to
   track which PAD messages must be sent where, we utilize the Host-Uniq
   TAG and AC-Cookie TAG. Each are used in the same manner, depending
   on which PAD message is being sent or replied to. Both take
   advantage of the fact that any PAD message sent as a reply to another
   PAD message MUST echo these TAGs in their entirety [3].

   For purposes of this discussion, it is useful to define two
   "directions" which PAD messages will traverse during a relayed PPPoE
   PAD message exchange. Thus, for the following example,

                  "Upstream" ----------------------->

            PPPoE Host ------ LAC ----- Tunnel Switch ------ LNS
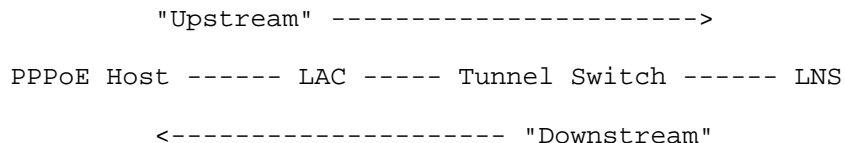
                  <-------------------- "Downstream"

   PAD messages being sent from the PPPoE Host, through the LAC, Tunnel
   Switch, and LNS, are defined to be traversing "Upstream." PAD
   messages being sent in the opposite direction are defined to be
   traversing "Downstream."

   Consider further, the following observation for this example:

   PAD messages that are sent Upstream: PADI, PADR, PADT
   PAD messages that are sent Downstream: PADO, PADS, PADT

   Also, there is a request/response connection between the PADI and
   PADO which must be linked with some common value. Similarly, there
   is a request/response connection between PADO and PADR. The PADS is
   sent on its own with no response, but must be delivered to the sender
   of the PADR. The PADT must be sent with the same SESSION_ID as
   established in the PADS.

   The goal for PAD message exchange coherency is to ensure that the
   connections between the PADI/PADO, PADO/PADR, and PADR/PADS and
   PADS/PADT all remain intact as the PAD messages are relayed from node
   to node.

   The basic mechanism for ensuring this for PADI, PADO, and PADR
   messages is the AC-Cookie TAG and Host-Uniq TAG. Both of these TAGs
   are defined as arbitrary data which must be echoed in any message
   sent as a response to another message. This is the key to tying
   these PAD messages together at each hop. The following two rules
   makes this possible:

For PAD messages that are sent Upstream, a new Host-Uniq TAG MUST
be inserted at each relaying node before the PAD message is
forwarded. There SHOULD be at most one Host-Uniq TAG per PAD
message.

For PAD messages being sent Downstream, a new AC-Cookie TAG MUST
be inserted at each relaying node before the PAD message is
forwarded. There SHOULD be at most one AC-Cookie TAG per PAD
message. Additionally, for an LNS receiving multiple PAD messages
from upstream, there SHOULD be at most one PAD message forwarded
downstream per received SRRP Message. In other words, there
SHOULD be exactly one PPPoE Relay AVP per L2TP SRRP Message.

The exception here is the PADS, which cannot carry an AC-Cookie TAG
(and, thankfully, doesn't need to), and the PADT. We will discuss
these later in this section. Using the above rules, PADI, PADO, and
PADR messages may be relayed through an arbitrary number of nodes,
each inserting its own value to link a message response that it might
receive.

In order to implement this exchange without tying up resources at
each L2TP node, it is desirable to not require ephemeral state at
each node waiting for a message response from each forwarded PAD
message. This is achievable if one is willing to be very intelligent
about the values that will be sent in the PPPoE TAGs used for message
coherency. Given that the TAGs are of arbitrary size and composition
and are always echoed in their entirety, one may use the information
here to map any next relay hop information. For example, the L2TP
Tunnel ID (Control Connection ID) could be encoded in the TAG in
order to identify where to relay the message when it arrives. If one
chooses this method, the encoding MUST incorporate some method of
encryption and authentication of the value. Note that this is a
relatively simple proposition given that it is only the source of the
encrypted and data that will ever need to decrypt and authenticate
the value upon receipt (thus, no key exchanges are necessary, and any
of a myriad of algorithms may be chosen). Note that individual TAGs
MUST never exceed 255 octets in length, and the length of an entire
PPPoE message MUST never exceed the maximum segment size of the
underlying ethernet. In the event that a TAG exceeds 255 octets in
length, a compression scheme which may include storage of state at an
L2TP node may be necessary before constructing a new TAG.

The PADS and PADT messages do not rely on the AC-Cookie TAG or Host-
Uniq TAG for directing to the proper node. As described in Section
2.2, the L2TP session is created upon receipt of a valid PADR at the
L2TP LAC. Since the PADS is sent as an AVP on this message exchange,

its coherency may be secured via the L2TP session itself. Similarly
for the PADT, as it is carried in the L2TP disconnect message (CDN)
for the L2TP session.

Clients are supposed to treat an AC-Cookie TAG as an opaque object.
They differentiate PADOs only by MAC address, Service-Name TAG(s) and
by AC-Name TAG(s). If an LAC sends multiple PADOs, they should
contain different AC-Name TAGs.

Furthermore, a node performing PPPoE L2TP Relay (such as an LAC)
SHOULD attempt to distinguish or rate limit retransmitted PADx
messages (perhaps via the source MAC address and/or arriving
interface of the message) in order to limit the overloading of L2TP.
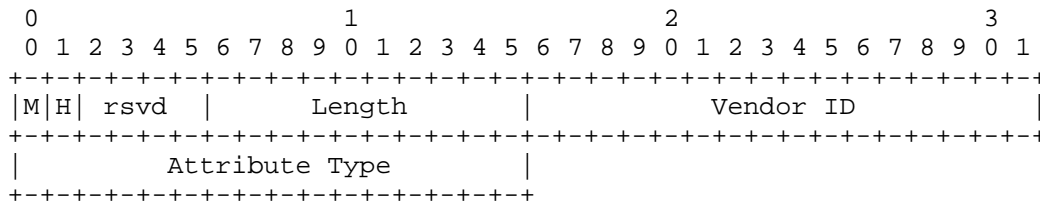
Examples of this operation for a number of scenarios and
considerations for certain deployment situations may be found in the
Appendix of this document.

2.4. PPPoE Service Relay Capabilities Negotiation

If the extensions defined in this document are present and configured
for operation on a given Control Connection, the AVPs listed in this
section MUST be present in the Start-Control-Connection-Request
(SCCRQ) or Start-Control-Connection-Reply (SCCRP) messages during
control connection setup.

2.4.1. PPPoE Service Relay Response Capability AVP

The PPPoE Service Relay Response Capability AVP, Attribute Type 56,
indicates to an L2TP peer that the PPPoE Service Relay (SRRQ, SRRP)
messages and the PPPoE Relay AVP will be processed and responded to
when received.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|M|H| rsvd  |      Length       |           Vendor ID           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Attribute Type         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The Vendor ID is the IETF Vendor ID of 0.

This AVP MAY be hidden (the H bit MAY be 0 or 1).

The M bit for this AVP may be set to 0 or 1. If the sender of this
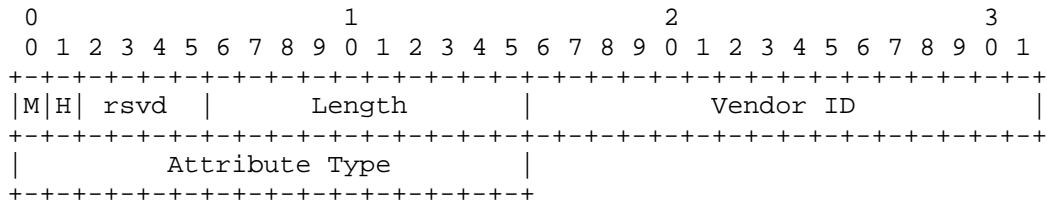AVP does not wish to establish a connection to a peer which does not

   understand this L2TP extension, it SHOULD set the M bit to 1,
   otherwise it MUST be set to 0.

   The Length of this AVP is 6.

   The AVP may be present in the following messages: SCCRQ, SCCRP

2.4.2. PPPoE Service Relay Forward Capability AVP

   The PPPoE Service Relay Forward Capability AVP, Attribute Type 57,
   indicates to an L2TP peer that PPPoE Service Relay (SRRQ, SRRP)
   messages and the PPPoE Relay AVP may be sent by this L2TP peer.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |M|H| rsvd  |     Length        |          Vendor ID            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        Attribute Type         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   The Vendor ID is the IETF Vendor ID of 0.

   This AVP MAY be hidden (the H bit MAY be 0 or 1).

   The M bit for this AVP may be set to 0 or 1. If the sender of this
   AVP does not wish to establish a connection to a peer which does not
   understand this L2TP extension, it SHOULD set the M bit to 1,
   otherwise it MUST be set to 0.

   The Length of this AVP is 6.

   The AVP may be present in the following messages: SCCRQ, SCCRP

3. L2TP Service Relay Messages

   This section identifies two new L2TP messages used to deliver PPPoE
   PADI and PADO messages.

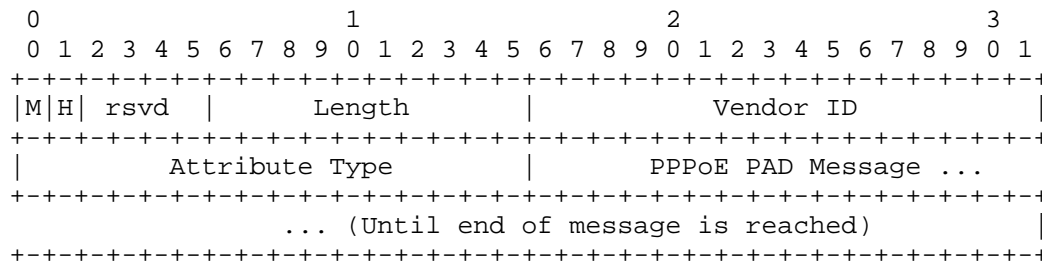3.1. Service Relay Request Message (SRRQ)

   The Service Relay Request Message (SRRQ), Message Type 18, is sent by
   an LAC to relay requests for services. This document defines one new
   AVP that may be present to request service in section 2. Further
   service relay mechanisms may also use this message in a similar
   context. Discussion of other service relay mechanisms are outside
   the scope of this document.

3.2. Service Relay Reply Message (SRRP)

   The Service Relay Reply Message (SRRP), Message Type 19, is sent by
   an LAC to relay responses of requests for services. This document
   defines one new AVP that may be present as a response to a request
   for service in section 2. Further service relay mechanisms may also
   use this message in a similar context. Discussion of other service
   relay mechanisms are outside the scope of this document.

4. PPPoE Relay AVP

   The PPPoE Relay AVP, Attribute Type 55, carries the entire PADI,
   PADO, PADR, PADS and PADT messages within, including Ethernet MAC
   source and destination addresses. This is the only AVP necessary for
   relay of all PAD messages via L2TP.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |M|H| rsvd  |      Length       |           Vendor ID           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Attribute Type        |       PPPoE PAD Message ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                ... (Until end of message is reached)         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   The Vendor ID is the IETF Vendor ID of 0.

   This AVP MAY be hidden (the H bit MAY be 0 or 1).

   The M bit for this AVP may be set to 0 or 1. If the sender of this
   AVP does not wish to establish a connection to a peer which does not
   understand this L2TP extension, it SHOULD set the M bit to 1,
   otherwise it MUST be set to 0.

   The Length of this AVP is 6 plus the length of the PPPoE PAD Message.

   The AVP may be present in the following messages: SRRQ, SRRP, ICRQ,
   ICRP, ICCN, and CDN.

5. Security Considerations

   PPPoE has a number of known security weaknesses that are not
   described here. For example, an intruder between a PPPoE Host and a
   PPPoE AC who can observe or modify PPPoE Active Discovery traffic has
   numerous opportunities for denial of service and other attacks. The
   use of the L2TP extensions described here makes it possible to tunnel
   PPPoE discovery packets between the LAC and LNS, extending the path

which the PPPoE Active Discovery packets are transported. There are
two possible implications of this. First, the tunneled packets may
now be observable by an intruder having access to traffic along the
L2TP tunnel path. This MAY make information regarding service
offerings or host identity easier to obtain to a rogue party given
that it is being sent over a wider variety of media, and presumably
over a longer distance and/or more hops or administrative domains.
Whether this information could be used for malicious purposes depends
on the information contained within, but it is conceivable that this
could be sensitive information, and this mechanism increases the
possibility that this information would be presented to an
interloper. Second, it may also be possible for an intruder to
modify PPPoE Active Discovery traffic while it is being carried
within L2TP control messages.

There are at least two methods defined to help thwart this inspection
or modification by an unauthorized individual. One of the two MUST
be used if the service discovery information is considered to be
sensitive and is traversing an untrusted network. The first
suggested method is AVP hiding described in [2]. This may be used to
hide the contents of the packets in transit, though offers no
integrity protection against modification of data in the AVP. The
second and more secure method is protecting L2TP with IPsec as
defined in [6].

6. IANA Considerations

   This document requires three new "AVP Attribute" (attribute type)
   numbers to be assigned through IETF Consensus [5] as indicated in
   Section 10.1 of [2].

      1. PPPoE Relay AVP (section 4.0)
      2. PPPoE Relay Response Capability AVP (section 2.4.1)
      3. PPPoE Relay Forward Capability AVP (section 2.4.2)

   This document requires two new "Message Type" numbers to be assigned
   through IETF Consensus [5] as indicated in Section 10.2 of [2].

      1. Service Relay Request Message (SRRQ) (Section 3.1)
      2. Service Relay Reply Message (SRRP) (Section 3.2)

   There are no additional requirements on IANA to manage numbers in
   this document or assign any other numbers.

7. Acknowledgements

   Thanks to Vinay Shankarkumar for valuable review, comment, and
   implementation.

   Thanks to David Skoll and a number of others on pppoe@ipsec.org for
   providing very helpful discussion about their PPPoE implementations.

   Thanks to Ross Wheeler, Louis Mamakos, and David Carrel for providing
   valuable clarifications of PPPoE [1] while designing this protocol.

8. References

8.1. Normative References

   [1] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D. and R.
       Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)",
       RFC 2516, February 1999.

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

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

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

   [5] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA
       Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

8.2. Informative References

   [6] Patel, B., Aboba, B., Dixon, W., Zorn, G. and S. Booth, "Securing
       L2TP Using IPsec," RFC 3193, November 2001.

Appendix A: PPPoE Relay in Point to Multipoint Environments

   The PPPoE PADI message in its native form, is sent as a broadcast
   message on an Ethernet link. Thus, more than one AC concentrator
   could conceivably receive and respond to this message. Similarly, a

   PPPoE interface could be associated with more than one L2TP Control
   Connection, in order to query multiple LNSs with potentially varying
   service profiles, as well as to load balance requests.

   As the PADI message is propagated, one may choose to replicate the
   message to multiple Control Connections in order to mimic the
   behavior of the PADI being sent on an ethernet link with multiple ACs
   attached. If the number of replicated nodes is large, and the number
   of hops deep, then an unmanageable "fan-out" of PADI propagation may
   occur. Thus, care should be taken here to only replicate messages to
   multiple Control Connections when it is absolutely necessary.

   The only case where it is seems necessary to replicate messages to
   multiple destinations is in the case where each destination is known
   to have varying service policies that all need to be advertised to a
   PPPoE Host for its gathering and selection. At the time of this
   writing, the authors know of no PPPoE Host implementations that take
   advantage of this ability (instead, responding to only a single PPPoE
   PADO). This, of course, is subject to change if and when PPPoE
   implementations are advanced to this stage.

   In cases where multiple Control Connections may exist to multiple
   LNSs for load balancing purposes, L2TP Service Relay should take
   measures to try one Control Connection at a time, rather than
   broadcasting to all Control Connections simultaneously.

Appendix B: PAD Message Exchange Coherency Examples

   Example 1: "PPPoE Relay With Multiple LNSs"

                         ,--- LNS1
                        /
           Host --- LAC
                        \
                         '--- LNS2
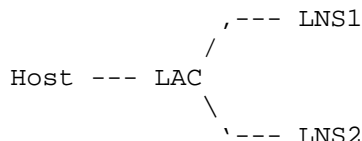
   This example assumes that there is good reason to send a copy of the
   PADI to both LNSs (e.g., each LNS may have a different service
   profile to offer).

1) a. Host sends PADI via broadcast MAC address to LAC

   b. LAC replicates the PADI message and forwards a copy to LNS1
      Host-Uniq = R1 (assigned)

   c. LAC replicates the PADI message and forwards a copy to LNS2
      Host-Uniq = R2 (assigned)

2) a. LNS1 responds with PADO to LAC
      Host-Uniq = R1 (echoed)
      AC-Cookie = C1 (assigned)

   b. LNS1 responds with PADO to LAC
      Host-Uniq = R2 (echoed)
      AC-Cookie = C2 (assigned)

   c. LAC forwards both PADO messages to Host with source MAC set to
      MAC address of LAC. PADO from (2a) is assigned new AC-Cookie
      C1' and PADO from (2b) is given AC-Cookie C2'

3) a. Host sends PADR to MAC address of LAC (choosing one)
      AC-Cookie = C1' (echoed)

   b. LAC knows to forward PADR to LNS1 based on C1'
      AC-Cookie = C1 (echoed)

4) Session Establishment at the LAC commences, with further PAD
   messages carried within the context of the L2TP session itself.
   No need to inspect the AC-Cookie TAG or Host-Uniq TAG from this
   point forward in order to direct messages properly.

   Example 2: "PPPoE Relay With L2TP Tunnel-Switching"

          Host --- LAC ---- LNS1 ---- LNS2

1) a. Host sends PADI to LAC.

   b. LAC sends PADI to LNS1
      Host-Uniq = R1 (assigned)

   c. LNS1 sends PADI to LNS2
      Host-Uniq = R2 (assigned)

2) a. LNS2 responds to LNS1 with PADO
      Host-Uniq = R2 (echoed)
      AC-Cookie = C1 (assigned)

   b. LNS1 relays PADO to LAC
      Host-Uniq = R1 (echoed)
      AC-Cookie = C1' (assigned)

   c. LAC sends PADO to Host
      AC-Cookie = C1'' (assigned)

3) a. Host sends PADR to MAC address of LAC
      AC-Cookie = C1'' (echoed)

   b. LAC sends PADR to LNS1
      AC-Cookie = C1' (echoed)

   c. LNS1 sends PADR to LNS2
      AC-Cookie = C1 (echoed)

4) Session Establishment at the LAC, LNS1 and LNS2 commences, with
   further PAD messages carried within the context of the L2TP
   session itself. No need to inspect the AC-Cookie TAG or Host-Uniq
   TAG from this point forward in order to direct messages properly.

   Example 3: "PPPoE Relay With Multiple PPPoE ACs"

```
                            ,--- AC1
                           /
        Host --- LAC ---- LNS
                           \
                            '--- AC2
```
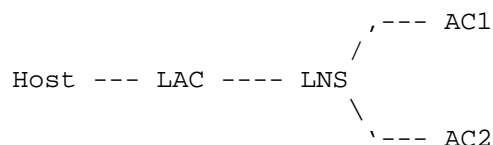
   In this example, AC1 and AC2 are PPPoE access concentrators on a
   broadcast domain. Sequence of operation is as follows.

1) a. Host sends PADI to LAC.

   b. LAC sends PADI to LNS
      Host-Uniq = R1 (assigned)

   c. LNS broadcasts PADI to AC1 and AC2
      Host-Uniq = R2 (assigned)

2) a. AC1 sends PADO to LNS
      Host-Uniq = R2 (echoed)
      AC-Cookie = C1 (assigned)

   b. AC2 sends PADO to LNS
      Host-Uniq = R2 (echoed)
      AC-Cookie = C2 (assigned)

       c. LNS sends two PADOs to LAC
          Host-Uniq = R1 (echoed)
          AC-Cookie (assigned) = C1' and C2', respectively

       d. LAC sends two PADOs to Host
          Host-Uniq = R1
          AC-Cookie (assigned) = C1'' and C2'', respectively

    3) a. Host sends PADR with to LAC to select service from AC2.
          AC-Cookie = C2'' (echoed)

       b. LAC sends PADR to LNS   AC-Cookie = C2' (echoed)

       c. LAC sends PADR to AC2
          AC-Cookie = C1 (echoed)

    4) Session Establishment at the LAC, LNS and AC2 commences, with
       further PAD messages carried within the context of the L2TP
       session or PPPoE session itself. No need to inspect
       the AC-Cookie TAG or Host-Uniq TAG from this point forward in
       order to direct messages properly.

Authors' Addresses

    W. Mark Townsley
    cisco Systems
    7025 Kit Creek Road
    Research Triangle Park, NC 27709

    EMail: mark@townsley.net

    Ron da Silva
    AOL Time Warner
    12100 Sunrise Valley Dr
    Reston, VA 20191

    EMail: rdasilva@va.rr.com