PPP Extensions Working Group
Internet Draft
Expires 30 Sep. 1997

Avri Doria
Xing Chen
General DataComm
25 March 1997

Proposal for a PPP Network Layer Entity Selection Protocol
<draft-ietf-pppext-nles-00.txt>

Status of this Memo

Abstract

With the introduction of xDSL services into public telecommunications networks, direct access (in contrast to dial-up access) will start to be used as an access method for data as well as other services. PPP has been very successful in providing connections for IP as well as other protocols in the dial-up access network. With the advent of direct access, changes will be need to be made for identifying the target hosts, as it will no longer be possible to rely on the telephone number that is dialed prior to initiating the PPP session. This proposal indicates one method for adapting PPP to the new requirements.

1. Overview

Whether it is for business reasons, or, in the US, because of the Telecommunications Act of 1996, local exchange carriers (LECs), competitive access providers (CAPs) and Internet service providers (ISPs) are all vying for the same markets. Many of the proposed access models include shifting away from POTS (plain old telephone service) to xDSL. This will allow the LECs to offer high end broadband access, with at least partial PPP termination, in the central office with trunking of IP and other traffic over ATM, Frame Relay or Sonet connections.

Currently there are two ways to provide PPP access in a direct access network; by using hard wired connections or by using hard state connections. Both of these are unsatisfactory solutions, however, and the LECs are already searching for equipment which allows a direct access customer to switch service providers without needing to also change a hard provisioning.

The normal procedure in PPP, is for the PPP termination point to be identified prior to making the connection; for example, the phone number is dialed, or the DLCI is assigned. In a direct access scenario, the customers will have a permanent connection to the central office where the copper loop is terminated. There is currently no means of dynamically defining the service provider prior to making a connection. Several different scenarios were investigated:

(1) Add a protocol before LCP to define the service provider requested.

This was rejected because the nature of the connection will not change when switching from one service provider to another. While running the LCP connection phase may not be that expensive, it did seem like a a wasted step. Additionally, this would require another protocol which did not seem to fit in the PPP model.

(2) Add the system identification information to the RADIUS protocol.

This was considered, but rejected because of the essential nature of the decision being made. The system to be accessed must be defined before the correct network access server can be selected. It was suggested that the system identifier could be included in one of the RADIUS protocol fields. This becomes difficult when we start to consider different types of addressing that might be used; for example, IP addressing, E.164 addressing, NANP addressing (telephone numbers as in the dial-up case). These have differing forms and lengths and will need to be identified in any protocol used to carry them.

(3) Add the target service to the authentication name when using L2TP.

This was rejected for similar reasons to those outlined above. It was also rejected because a general mechanism is required, that is, one which does not require tunneling. It is very possible that the LECs will be offering virtual collocation services which use the RADIUS model for authentication and accounting. In this case a model which relies on tunneling would not be effective.

(4) Include a connection phase LCP option to identify the service provider desired. It was suggested that this could either be defined as a standard or as a proprietary solution.

This was rejected for several reasons. Partially it was for the same reason suggested above, the connection will not change and there is no reason to renegotiate a connection that is already established. Additionally, it is felt that this may not be an appropriate task for a link establishment phase. Finally, it was felt that this service would be too wide spread for a vendor specific solution.

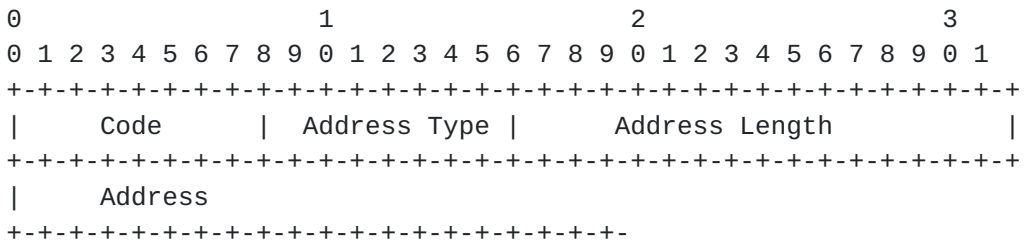
For the reasons outlined above, this draft proposes a new LCP protocol which can be optionally run after the LCP connection phase has completed, but before any authentication protocols are run. This Network Layer Entity Selection Protocol (NLES) is defined in this draft.

2. Description of NLES

After the LCP has completed but before any of the authentication protocols were run, the NLES will be run. This would be PPP protocol number cXXX (a number has yet to be applied for from IANA).

The message format will be as follows. It follows the Internet Protocol convention for packet description.

2.1. NLES Packet format



2.2. NLES Codes

The PPP NLES protocol will support 4 message codes.

Code	Function
1	NLES-Request
2	NLES-Ack
3	NLES-Nak
4	NLES-Reject

Code 1
In the NLES request, the sender would declare the addressing mode to be used and request a certain address. The reply could be:

Code 2
In this case, the original message would be returned with the code changed to indicate success.

Code 3
In this case, the message would be changed to include a preferred address type and address. This type of message could be used to do a query of a service provider if that service provider wished to provide service on different servers depending on some particular policy.

Code 4
In this case the message would be returned with the code changed to indicate failure.

2.3. NLES Address Types

The PPP NLES address types are:

Type	Description	Size
1	E.164 encoded in BCD format	8
2	NANP - North American Number Plan	5
3	IP Version 4	4
4	IP Version 6	16

3. Security Considerations

Security issues are not considered in this draft.

4. References

TBD

5. Contacts

Chair's Address

The working group can be contacted via the current chair:

Karl F. Fox
Ascend Communications
3518 Riverside Dr., Suite 101
Columbus, OH USA 43221

Authors' Addresses

Questions about this draft can be directed to:

Avri Doria
Boston Research Center
General DataComm Inc.
5 Mount Royal Ave
Marlborough MA USA 01752

(508) 624 6723
avri@gdc.com

Xing Chen
Technology Research Center
General DataComm Inc
Park Road Extension
P.O. Box 1299
Middlebury, CT 06762-1299

(203) 758 1811
xchen@gdc.com