ADD Working Group D. Liu
Internet-Draft Jinan University
Intended status: Informational Z. Yan
Expires: 21 January 2026 CNNIC
G. Geng
Y. Zhang
Jinan University
20 July 2025

PPP IPCP Extensions for Encrypted DNS Server Negotiation
draft-liu-add-ppp-edns-negotiation-00

Abstract

This document defines extensions to the Point-to-Point Protocol (PPP) Internet Protocol Control Protocol (IPCP) for negotiating encrypted DNS resolver configurations. These extensions allow PPP peers to exchange information about encrypted DNS servers supporting protocols such as DNS over TLS (DoT), DNS over HTTPS (DoH), and DNS over QUIC (DoQ). The design maintains backward compatibility with RFC 1877 while addressing modern security requirements.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Point-to-Point Protocol (PPP) [RFC1661] and its Ethernet adaptation, PPPoE ([RFC2516]) remain foundational technologies for authenticated network access, particularly in broadband and enterprise environments.

PPP is widely used in scenarios such as:

* ISP broadband access (e.g., PPPoE for DSL/fiber authentication)

* Industrial control networks (serial PPP for SCADA/PLC communications)

* Cellular backhaul (PPP over GTP in 4G/5G user-plane data)

* Secure tunneling (PPP inside L2TP/IPsec or MPLS VPNs)

Despite the rise of DHCP and IPv6 RA for configuration, PPP persists due to its fine-grained access control, negotiation flexibility, and compatibility with legacy systems. However, traditional PPP IPCP extensions ([RFC1877]) only support plaintext DNS, exposing queries to surveillance and manipulation — a critical gap in an era where encrypted DNS (DoT [RFC7858], DoH [RFC8484], DoQ [RFC9250]) is essential for privacy and security.

This document extends PPP IPCP to negotiate encrypted DNS resolvers, enabling:

* *Secure DNS by default*: Clients automatically adopt encrypted transports (e.g., DoT on port 853) without manual configuration.

* *Operator-managed trust*: ISPs can enforce authenticated DNS resolvers (via ADNs and certificate fingerprints) to prevent bypassing.

* *Backward compatibility*: Coexists with RFC 1877 options, allowing fallback to plaintext DNS if needed.

By integrating encrypted DNS negotiation into PPP, this specification bridges the gap between legacy access protocols and modern security requirements, ensuring confidentiality and integrity for DNS queries across diverse deployment scenarios — from home broadband to critical infrastructure.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174].

2. Additional IPCP Configuration Options

This document defines three new IPCP Configuration Options:

Type	Name	Description
133	Primary Encrypted DNS	Primary encrypted DNS server
134	Secondary Encrypted DNS	Secondary encrypted DNS server
135	DNS Encryption Parameters	Additional encryption parameters

Table 1

2.1. Primary Encrypted DNS Server Option

This option provides the primary encrypted DNS resolver configuration.

```
 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     |   Protocol    |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          ADN Length           |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
~                 Authentication Domain Name (ADN)              ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Port Number          |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
~                Additional Parameters (Optional)               ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Primary Encrypted DNS Option Format

Fields:

* Type: 133
* Length: 6
* Protocol: 1=DoT, 2=DoH, 3=DoQ
* Reserved: MUST be 0
* ADN Length: Length of ADN field

* ADN: Resolver FQDN (RFC 1035 format)

* Port Number: Defaults to 853 (DoT/DoQ) or 443 (DoH) if 0

2.2. Secondary Encrypted DNS Server Option

This option provides a fallback encrypted DNS resolver configuration when the primary server is unavailable. It follows the same structure as the Primary Encrypted DNS Server Option (Section 2.1) but uses a distinct type code.

* Type: 134

2.3. DNS Encryption Parameters Option

This option provides supplemental configuration parameters required for specific encrypted DNS protocols. It enables negotiation of advanced settings that cannot be conveyed in the primary/secondary options alone.

```
 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     |    Param Type | Param Length  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                       Parameter Value                       ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: DNS Encryption Parameters Option Format

Fields:

* Type: 135

* Length: 3

* Param Type (1 octet):

* 0x01 ALPN Protocols

* 0x02 DoH Path Template

* 0x03 Certificate Fingerprint

* 0x040xFF Reserved

* Param Length: Length of Parameter Value

* Parameter Value: Protocol-specific data

Defined Parameters:

1. *1. ALPN Protocols (Type 0x01)* Value: comma-separated list of ALPN identifiers. Example: “dot,h2” for DoT and HTTP/2.

2. *2. DoH Path Template (Type 0x02)* Value: URI path for DoH requests (UTF-8). Example: “/dns-query”.

3. *3. Certificate Fingerprint (Type 0x03)* Value: hash algorithm (1 octet) + hash bytes.
Algorithms: 0x01 = SHA-256, 0x02 = SHA-384.

3. Negotiation Process

This section specifies the state machine and processing rules for encrypted DNS option negotiation. The procedure follows standard IPCP negotiation defined in [RFC1332], with additional validation specific to encrypted DNS parameters.

3.1. Client Request Behavior

1. The client MAY include Option 133 and/or 134 in Configure-Request

2. To request configuration:

* Set ADN Length = 0

* Set Port Number = 0

* Omit ADN field

3. The client MAY include Option 135 to request specific parameters

3.2. Server Response Behavior

1. If server supports encrypted DNS:

* For valid requests: Respond with Configure-Ack

* For invalid/empty requests: Respond with Configure-Nak containing valid configuration

2. If server doesn’t support encrypted DNS:

* Respond with Configure-Reject

3.3. Configuration Priority

When both Options 129 (RFC 1877) and 133 are present:

1. Clients SHOULD prefer encrypted DNS (Option 133/134)

2. Clients MAY fall back to plaintext DNS if encrypted connection fails

4. Security Considerations

4.1. Authentication

* Clients MUST validate the server’s TLS certificate against the provided ADN

* When Option 135 (Certificate Fingerprint) is provided, clients SHOULD verify the certificate fingerprint

4.2. Privacy Protection

* While the options themselves may be transmitted in cleartext, they enable encrypted DNS transport

* Implementations SHOULD use PPP encryption (e.g., MPPE) when available

4.3. Downgrade Attacks

* Active attackers may remove encrypted DNS options from IPCP negotiation

* Clients SHOULD maintain a history of successful encrypted DNS usage and warn when unexpectedly unavailable

5. IANA Considerations

This document has no IANA actions.

6. Acknowledgments

This work is supported by the National Key Research and Development Program of China (No. 2023YFB3105700).

7. References

7.1. Normative References

[RFC1661] IETF, "The Point-to-Point Protocol (PPP)", RFC 1661, July 1994, <https://www.rfc-editor.org/rfc/rfc1661>.

[RFC1332] IETF, "PPP Internet Control Protocol", RFC 1332, May 1992, <https://www.rfc-editor.org/rfc/rfc1332>.

[RFC2119] IETF, "Key words for use in RFCs", RFC 2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] IETF, "Ambiguity of Uppercase", RFC 8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC7858] IETF, "Specification for DNS over TLS", RFC 7858, May 2016, <https://www.rfc-editor.org/rfc/rfc7858>.

[RFC8484] IETF, "DNS Queries over HTTPS", RFC 8484, October 2018, <https://www.rfc-editor.org/rfc/rfc8484>.

[RFC9250] IETF, "DNS over Dedicated QUIC", RFC 9250, May 2022, <https://www.rfc-editor.org/rfc/rfc9250>.

[RFC2516] IETF, "PPP over Ethernet", RFC 2516, February 1999, <https://www.rfc-editor.org/rfc/rfc2516>.

7.2. Informative References

[RFC1877] IETF, "PPP IPCP Extensions for Name Server Addresses", RFC 1877, December 1995, <https://www.rfc-editor.org/rfc/rfc1877>.

[RFC9460] IETF, "Service Binding via DNS", RFC 9460, November 2023, <https://www.rfc-editor.org/rfc/rfc9460>.

Appendix A. Example Negotiations

A.1. Basic DoT Configuration

```
Client: Configure-Request
  Option 133:
    Type: 133, Length: 10, Protocol: 1 (DoT),
    ADN Len: 0, Port: 0

Server: Configure-Nak
  Option 133:
    Type: 133, Length: 22, Protocol: 1 (DoT),
    ADN Len: 14, ADN: "dot.example.com",
    Port: 853
```

A.2. DoH with Custom Path

```
Client: Configure-Request
  Option 133:
    Type: 133, Length: 10, Protocol: 2 (DoH),
    ADN Len: 0, Port: 0
  Option 135:
    Type: 135, Length: 8,
    Param Type: 2 (DoH Path), Value: "/dns-query"

Server: Configure-Ack
  Option 133:
    Type: 133, Length: 22, Protocol: 2 (DoH),
    ADN Len: 14, ADN: "doh.example.com",
    Port: 443
  Option 135:
    Type: 135, Length: 8,
    Param Type: 2 (DoH Path), Value: "/dns-query"
```

A.3. DoQ with Certificate Pinning

```
Server: Configure-Request
  Option 133:
    Type: 133, Length: 30, Protocol: 3 (DoQ),
    ADN Len: 14, ADN: "doq.example.com",
    Port: 853
  Option 135:
    Type: 135, Length: 35,
    Param Type: 3 (Cert Fingerprint),
    Value: Alg=1 (SHA-256), Fingerprint=<32 bytes>

Client: Configure-Ack
```

Authors’ Addresses

Dongjie Liu
Jinan University

Email: dongjieliu8917@gmail.com

Zhiwei Yan
CNNIC
Email: yanzhiwei@cnnic.cn

Guanggang Geng
Jinan University
Email: guanggang.geng@gmail.com

Yinyan Zhang
Jinan University
Email: csyyzhang@gmail.com