Stream:	Internet Engineering Task Force (IETF)		
RFC:	8822		
Category:	Informational		
Published:	April 2021		
ISSN:	2070-1721		
Authors:	D. Allan, Ed. *Ericsson*	D. Eastlake 3rd *Futurewei Technologies*	D. Woolley *Telstra Corporation*

RFC 8822
5G Wireless Wireline Convergence User Plane Encapsulation (5WE)

Abstract

As part of providing wireline access to the 5G Core (5GC), deployed wireline networks carry user data between 5G residential gateways and the 5G Access Gateway Function (AGF). The encapsulation method specified in this document supports the multiplexing of traffic for multiple PDU sessions within a VLAN-delineated access circuit, permits legacy equipment in the data path to inspect certain packet fields, carries 5G QoS information associated with the packet data, and provides efficient encoding. It achieves this by specific points of similarity with the Point-to-Point Protocol over Ethernet (PPPoE) data packet encapsulation (RFC 2516).

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8822.

Copyright Notice

Table of Contents

1. Introduction

Converged 5G ("fifth generation") wireline networks carry user data between 5G residential gateways (5G-RGs) and the 5G Access Gateway Function (identified as a Wireline-AGF (W-AGF) by 3GPP in [TS23316]) across deployed access networks based on Broadband Forum [TR101] and [TR178]. This form of wireline access is considered to be trusted non-3GPP access by the 5G system.

The transport encapsulation used needs to meet a variety of requirements, including the following:

- The ability to multiplex multiple logical connections (Protocol Data Unit (PDU) sessions as defined by 3GPP) within a VLAN-identified point-to-point logical circuit between a 5G-RG and a W-AGF.
- To allow unmodified legacy equipment in the data path to identify the encapsulation and inspect specific fields in the payload. Some access nodes in the data path between the 5G-RG and the W-AGF (such as digital subscriber loop access multiplexers (DSLAMs) and optical line terminations (OLTs)) currently inspect packets identified by specific Ethertypes to identify protocols such as the Point-to-Point Protocol over Ethernet (PPPoE), IP, ARP, and IGMP. This may be for the purpose of enhanced QoS, the policing of identifiers, and other

applications. Some deployments are dependent upon this inspection. Such devices are able to do this for PPPoE or IP-over-Ethernet (IPoE) packet encodings but would be unable to do so if a completely new encapsulation, or an existing encapsulation using a new Ethertype, were used.

- To carry per-packet 5G QoS information.
- An encapsulation that minimizes processing since fixed access residential gateways are sensitive to the complexity of packet processing. While not a strict requirement, this is an important consideration.

A data encapsulation that uses a common Ethertype and has certain fields appearing at the same offset as the PPPoE data encapsulation [RFC2516] can address these requirements. This data encapsulation is referred to as the 5G WWC user plane encapsulation or 5WE. Currently deployed access nodes do not police the VER, TYPE, or CODE fields of an RFC 2516 PPPoE header and only perform limited policing of stateful functions with respect to the procedures documented in RFC 2516. Therefore, these fields have a different definition for 5WE and are used to:

- Identify that the mode of operation for packets encapsulated in such a fashion uses 5G WWC session establishment based on non-access stratum (NAS, a logical control interface between user equipment (UE) and a 5th Generation Core Network (5GC) as specified by 3GPP) and life-cycle maintenance procedures as documented in [TS23502] and [TS23316] instead of legacy PPP/PPPoE session establishment procedures [RFC2516] (i.e., PADI discipline, LCP, NCP, etc.). In this scenario, "discovery" is performed by means outside the scope of this document.
- Permit the session ID field to be used to identify the 5G PDU session the encapsulated packet is part of.
- Communicate per-packet 5G QoS Flow Identifier (QFI) and Reflective QoS Indication (RQI) information from the 5GC to the 5G-RG.

This 5G-specific redesign of fields not inspected by deployed equipment results in an encapsulation uniquely applicable to the requirements for the communication of PDU session traffic between the subscriber premises and the 5G system over wireline networks. The 6-byte RFC 2516 data packet header followed by a 2-byte PPP protocol ID is also the most frugal of the encapsulations that are currently supported by legacy access equipment that could be adapted to meet these requirements.

This encapsulation is expected to be used in environments where RFC 2516 is deployed. Therefore, implementations **MUST** examine the version number:

- If the version number is 1 and PPPoE [RFC2516] is supported, process the frame further; else, silently discard it.
- If the version number is 2 and 5WE is supported, process the frame further; else, silently discard it.

In both cases, frames for the supported version number should have session IDs corresponding to established sessions for the respective protocol models. A 5WE frame with an unrecognized session ID **MUST** be silently discarded.

This encapsulation may have MTU issues when used for Ethernet multiplexing in networks where the underlying Ethernet payload is limited to 1500 bytes.

This encapsulation is not suitable for other network environments, e.g., general use over the public Internet.

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] when, and only when, they appear in all capitals, as shown here.

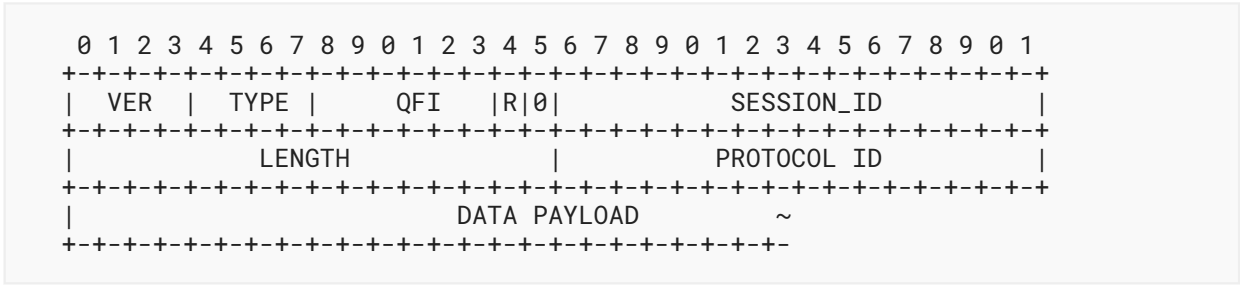
1.2. Acronyms

This document uses the following acronyms:

3GPP	3rd Generation Partnership Project
5WE	5G Wireless Wireline Convergence User Plane Encapsulation
5GC	5th Generation Core (network)
DSLAM	Digital Subscriber Loop Access Multiplexer
W-AGF	Wireline Access Gateway Function
IPoE	IP over Ethernet
NAS	Non-Access Stratum
OLT	Optical Line Termination
PDU	Protocol Data Unit
PPPoE	PPP over Ethernet
QFI	QoS Flow Identifier
QoS	Quality of Service
RG	Residential Gateway
RQI	Reflective QoS Indicator
WWC	Wireless Wireline Convergence

2. Data Encapsulation Format

The Ethernet payload [IEEE802] for PPPoE [RFC2516] is indicated by an Ethertype of 0x8864. The information following that Ethertype uses a value of 2 in the VER field for the repurposing of the PPPoE data encapsulation as the 5G WWC user plane encapsulation (5WE). The 5G WWC user plane encapsulation is structured as follows:



The description of each field is as follows:

VER: The version. It **MUST** be set to 0x02.

TYPE: The message type. It **MUST** be set to 0x01.

QFI: Encodes the 3GPP 5G QoS Flow Identifier [TS38415] to be used for mapping 5G QoS to IP DSCP/802.1 P-bits [IEEE802].

R: (Short for Reflective QoS Indication [TS38415]) Encodes the one-bit RQI. It is set by the network-side 5WE termination for downstream traffic and ignored by the network for upstream traffic.

0: Indicates the bit(s) that **MUST** be sent as zero and ignored on receipt.

SESSION_ID: A 16-bit unsigned integer in network byte order. It is used to distinguish different PDU sessions that are in the VLAN-delineated multiplex. A value of 0xffff is reserved for future use and **MUST NOT** be used.

LENGTH: The length in bytes of the data payload, including the initial Protocol ID. It is 16 bits in network byte order.

PROTOCOL ID: The 16-bit identifier of the data payload type encoded using values from the IANA "PPP DLL Protocol Numbers" registry <https://www.iana.org/assignments/ppp-numbers>.

The following values are valid in this field for 5G WWC use:

- 0x0021: IPv4
- 0x0031: Bridging PDU (Ethernet)
- 0x0057: IPv6

Packets received that do not contain one of the above protocol IDs are silently discarded.

DATA PAYLOAD: Encoded as per the protocol ID.

3. Security Considerations

5G NAS procedures used for session life-cycle maintenance employ ciphering and integrity protection [TS23502]. They can be considered a more secure session establishment discipline than existing RFC 2516 procedures, at least against on-path attackers. The design of the 5WE encapsulation will not circumvent existing anti-spoofing and other security procedures in deployed equipment. The existing access equipment will be able to identify fields that they normally process and police as per existing RFC 2516 traffic.

Therefore, the security of a fixed access network using 5WE will be equivalent or superior to current practice.

5WE-encapsulated traffic is used on what the 5GC considers to be trusted non-3GPP interfaces; therefore, it is not ciphered. 5WE is not suitable for use over an untrusted non-3GPP interface.

The security requirements of the 5G system are documented in [TS33501].

4. IANA Considerations

IANA has created the following registry on the "Point-to-Point (PPP) Protocol Field Assignments" page:

Registry Name: PPP Over Ethernet Versions

Registration Procedure: Specification Required

References: [RFC2516] [RFC8822]

VER	Description	Reference
0	Reserved	[RFC8822]
1	PPPoE	[RFC2516]
2	5G WWC User Plane Encapsulation	[RFC8822]
3-15	unassigned	

Table 1: PPP Over Ethernet Versions

IANA has added this document as an additional reference for Ethertype 0x8864 in the "Ether Types" registry on the IANA "IEEE 802 Numbers" page <https://www.iana.org/assignments/ieee-802-numbers>.

5. References

5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2516] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D., and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, DOI 10.17487/RFC2516, February 1999, <https://www.rfc-editor.org/info/rfc2516>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[TS23316] 3GPP, "Wireless and wireline convergence access support for the 5G System (5GS)", Release 16, TS 23.316, December 2018.

[TS23502] 3GPP, "Procedures for the 5G System (5GS)", Release 15, TS 23.502, December 2016.

[TS38415] 3GPP, "NG-RAN; PDU session user plane protocol", Release 15, TS 38.415, March 2018.

5.2. Informative References

[IEEE802] IEEE, "IEEE Standard for Local and Metropolitan Networks: Overview and Architecture", Std 802-2014, DOI 10.1109/IEEESTD.2014.6847097, June 2014, <https://doi.org/10.1109/IEEESTD.2014.6847097>.

[TR101] Broadband Forum, "Migration to Ethernet Based Broadband Aggregation", TR-101, issue 2, July 2011.

[TR178] Broadband Forum, "Multi-service Broadband Network Architecture and Nodal Requirements", TR-178, issue 1, September 2014.

[TS33501] 3GPP, "Security architecture and procedures for 5G System", Release 16, TS 33.501, December 2019.

Acknowledgements

This memo is a result of comprehensive discussions by the Broadband Forum's Wireline Wireless Convergence Work Area. The authors would also like to thank Joel Halpern and Dirk Von Hugo for their detailed review of this document.

Authors' Addresses

Dave Allan (EDITOR)
Ericsson
2455 Augustine Drive
San Jose, CA 95054
United States of America
Email: david.i.allan@ericsson.com

Donald E. Eastlake 3rd
Futurewei Technologies
2386 Panoramic Circle
Apopka, FL 32703
United States of America
Phone: +1-508-333-2270
Email: d3e3e3@gmail.com

David Woolley
Telstra Corporation
242 Exhibition St
Melbourne 3000
Australia
Email: david.woolley@team.telstra.com