

Transport Area Working Group

Internet-Draft

Updates: [6040](#), [2661](#), [2784](#), [3931](#), [4380](#)

(if approved)

Intended status: Standards Track

Expires: December 18, 2017

B. Briscoe

Simula Research Laboratory

June 16, 2017

**Propagating Explicit Congestion Notification Across IP Tunnel Headers
Separated by a Shim
draft-ietf-tsvwg-rfc6040update-shim-02**

Abstract

[RFC 6040](#) on "Tunnelling of Explicit Congestion Notification" made the rules for propagation of ECN consistent for all forms of IP in IP tunnel. This specification extends the scope of [RFC 6040](#) to include tunnels where two IP headers are separated by at least one shim header that is not sufficient on its own for packet forwarding. It surveys widely deployed IP tunnelling protocols separated by a shim and updates the specifications of those that do not mention ECN propagation (L2TPv2, L2TPv3, GRE and Teredo). The specification also updates [RFC 6040](#) with configuration requirements needed to make any legacy tunnel ingress safe.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 18, 2017.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology	3
3.	IP-in-IP Tunnels with Tightly Coupled Shim Headers	3
3.1.	Scope of RFC 6040	3
3.2.	Making a non-ECN Tunnel Ingress Safe by Configuration	4
3.3.	Specific Updates to Protocols under IETF Change Control	6
3.3.1.	L2TP (v2 and v3) ECN Extension	8
3.3.2.	GRE	10
3.3.3.	Teredo	11
4.	IANA Considerations	11
5.	Security Considerations	11
6.	Comments Solicited	11
7.	Acknowledgements	12
8.	References	12
8.1.	Normative References	12
8.2.	Informative References	13
	Author's Address	15

[1.](#) Introduction

[RFC 6040](#) on "Tunnelling of Explicit Congestion Notification" [[RFC6040](#)] made the rules for propagation of Explicit Congestion Notification (ECN [[RFC3168](#)]) consistent for all forms of IP in IP tunnel.

A common pattern for many tunnelling protocols is to encapsulate an inner IP header (v4 or v6) with shim header(s) then an outer IP header (v4 or v6). Some of these shim headers are designed as generic encapsulations, so they do not necessarily directly encapsulate an inner IP header. Instead they can encapsulate headers such as link-layer (L2) protocols that in turn often encapsulate IP.

To clear up confusion, this specification clarifies that the scope of [RFC 6040](#) includes any IP-in-IP tunnel, including those with shim header(s) and other encapsulations between the IP headers. Where necessary, it updates the specifications of the relevant

Briscoe

Expires December 18, 2017

[Page 2]

encapsulation protocols with the specific text necessary to comply with [RFC 6040](#).

This specification also updates [RFC 6040](#) to state how operators ought to configure a legacy tunnel ingress to avoid unsafe system configurations.

2. Terminology

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](#) [[RFC2119](#)] when, and only when, they appear in all capitals, as shown here.

This specification uses the terminology defined in [RFC 6040](#) [[RFC6040](#)].

3. IP-in-IP Tunnels with Tightly Coupled Shim Headers

3.1. Scope of [RFC 6040](#)

In many cases the shim header(s) and the outer IP header are always added (or removed) as part of the same process. We call this a tightly coupled shim header. Processing the shim and outer together is often necessary because the shim(s) are not sufficient for packet forwarding in their own right; not unless complemented by an outer header.

In some cases a tunnel adds an outer IP header and a tightly coupled shim header to an inner header that is not an IP header, but that in turn encapsulates an IP header (or might encapsulate an IP header). For instance an inner Ethernet (or other link layer) header might encapsulate an inner IP header as its payload. We call this a tightly coupled shim over an encapsulating header.

In [section 1.1 of RFC 6040](#) its scope was defined as:

"...ECN field processing at encapsulation and decapsulation for any IP-in-IP tunnelling, whether IPsec or non-IPsec tunnels. It applies irrespective of whether IPv4 or IPv6 is used for either the inner or outer headers. ..."

This specification updates [RFC 6040](#) by adding the following scoping text after the sentences quoted above:

It applies in cases where an outer IP header encapsulates an inner IP header either directly or indirectly by encapsulating other

headers that in turn encapsulate (or might encapsulate) an inner IP header.

Digging to arbitrary depths to find an inner IP header within an encapsulation is strictly a layering violation so it cannot be a required behaviour. Nonetheless, some tunnel endpoints already look within a L2 header for an IP header, for instance to map the Diffserv codepoint between an encapsulated IP header and an outer IP header [[RFC2983](#)]. In such cases at least, it should be feasible to also (independently) propagate the ECN field between the same IP headers. Thus, as long as the guidelines in section 6 of [[I-D.ietf-tsvwg-ecn-encap-guidelines](#)] are followed, access to the ECN field within an encapsulating header can be a useful and benign optimization. On the other hand, if a tunnel ingress is not willing to find an inner IP header, [Section 3.2](#) below specifies that it has to disable the ECN capability in the outer header by zeroing the ECN field.

[3.2.](#) Making a non-ECN Tunnel Ingress Safe by Configuration

Even when ECN propagation is not implemented or is not being used, it ought to be possible to render a tunnel ingress safe by configuration. The main safety concern is to disable the ECN capability in the outer IP header if the egress of the tunnel does not implement ECN logic to propagate any ECN markings into the packet forwarded beyond the tunnel. Otherwise the non-ECN egress could discard any ECN marking introduced within the tunnel, which would break all the ECN-based control loops that regulate the traffic load over the tunnel.

Therefore this specification updates [RFC 6040](#) by inserting the following text just before the last paragraph of [section 4.3](#):

When the implementation of a tunnel ingress does not support [[RFC6040](#)] or one of its compatible predecessors ([[RFC4301](#)] or the full functionality mode of [[RFC3168](#)]) and when the outer tunnel header is IP (v4 or v6), if possible, the operator MUST configure the ingress to zero the outer ECN field in any of the following cases:

- * if it is known that the tunnel egress does not support propagation of the ECN field ([RFC 6040](#), [RFC 4301](#) or the full functionality mode of [RFC 3168](#))
- * or if the behaviour of the egress is not known or an egress with unknown behaviour might be dynamically paired with the ingress.

- * or if an IP header might be encapsulated within a non-IP header that the tunnel ingress is encapsulating, but the ingress does not inspect within the encapsulation.

In order that the network operator can comply with the above safety rules, even if a tunnel ingress does not support [RFC 6040](#), [RFC 4301](#) or the full functionality mode of [RFC 3168](#), the implementation of the tunnel ingress:

- o MUST make propagation of the ECN field between inner and outer IP headers independent of any configuration of Diffserv codepoint propagation;
- o SHOULD zero the outer ECN field in its default configuration.

There might be concern that the above "MUST" makes compliant equipment non-compliant at a stroke. However, any equipment that is still treating the ToS octet (IPv4) or the Traffic Class octet (IPv6) as a single 8-bit field is already non-compliant, and has been since 1998 when the upper 6 bits were separated off for the Diffserv codepoint (DSCP) [[RFC2474](#)]. For instance, copying the ECN field as a side-effect of copying the DSCP is a seriously unsafe bug that risks breaking the feedback loops that regulate load on a tunnel.

Permanently zeroing the outer ECN field is safe, but it is not sufficient to claim compliance with [RFC 6040](#) because it does not meet the aim of introducing ECN support to tunnels (see [Section 4.3 of \[RFC6040\]](#)). Developers and network operators are encouraged to implement and deploy tunnel endpoints compliant with [RFC 6040](#) (as updated by the present specification) in order to provide the benefits of wider ECN deployment [[RFC8087](#)]. Nonetheless, propagation of ECN between IP headers, whether separated by shim headers or not, has to be OPTIONAL to implement and to use, because:

- o Legacy implementations of tunnels without any ECN support already exist
- o A network might be designed so that there is usually no bottleneck within the tunnel
- o If the tunnel endpoints would have to search within an L2 header to find an encapsulated IP header, it might not be worth the potential performance hit

3.3. Specific Updates to Protocols under IETF Change Control

There follows a list of specifications of encapsulations with tightly coupled shim header(s). The list is not necessarily exhaustive so, for the avoidance of doubt, [RFC 6040](#) applies to all tightly coupled shim headers whether or not they are listed here and whether or not the shim encapsulates an IP header or a different header that encapsulates (or might encapsulate) an IP header. The list is confined to standards track or widely deployed protocols.

- o PPTP (Point-to-Point Tunneling Protocol) [[RFC2637](#)];
- o L2TP (Layer 2 Tunnelling Protocol), specifically L2TPv2 [[RFC2661](#)] and L2TPv3 [[RFC3931](#)], which not only includes all the L2-specific specializations of L2TP, but also derivatives such as the Keyed IPv6 Tunnel [[RFC8159](#)];
- o GRE (Generic Routing Encapsulation) [[RFC2784](#)] and NVGRE (Network Virtualization using GRE) [[RFC7637](#)];
- o GTP (GPRS Tunnelling Protocol), specifically GTPv1 [[GTPv1](#)], GTP v1 User Plane [[GTPv1-U](#)], GTP v2 Control Plane [[GTPv2-C](#)];
- o Teredo [[RFC4380](#)];
- o CAPWAP (Control And Provisioning of Wireless Access Points) [[RFC5415](#)];
- o LISP (Locator/Identifier Separation Protocol) [[RFC6830](#)];
- o VXLAN (Virtual eXtensible Local Area Network) [[RFC7348](#)] and VXLAN-GPE [[I-D.ietf-nvo3-vxlan-gpe](#)];
- o Geneve [[I-D.ietf-nvo3-geneve](#)];
- o GUE (Generic UDP Encapsulation) [[I-D.ietf-intarea-gue](#)].

Some of the listed protocols enable encapsulation of a variety of network layer protocols as inner and/or outer. This specification applies in the cases where there is an inner and outer IP header as described in [Section 3.1](#). Otherwise [[I-D.ietf-tsvwg-ecn-encap-guidelines](#)] gives guidance on how to design propagation of ECN into other protocols that might encapsulate IP.

Where protocols in the above list are under IETF change control and they need to be updated to specify ECN propagation, update text is given in the following subsections. For those not under IETF control, it is RECOMMENDED that implementations of encapsulation and

decapsulation comply with [RFC 6040](#). It is also RECOMMENDED that their specifications are updated to add a requirement to comply with [RFC 6040](#) (as updated by the present document).

PPTP is not under the change control of the IETF, but it has been documented in an informational RFC [[RFC2637](#)]. However, there is no need for the present specification to update PPTP because L2TP has been developed as a standardized replacement.

NVGRE is not under the change control of the IETF, but it has been documented in an informational RFC [[RFC7637](#)]. NVGRE is a specific use-case of GRE (it re-purposes the key field from the initial specification of GRE [[RFC1701](#)] as a Virtual Subnet ID). Therefore the text that updates GRE in [Section 3.3.2](#) below is also intended to update NVGRE.

Although the definition of the various GTP shim headers is under the control of the 3GPP, it is hard to determine whether the 3GPP or the IETF controls standardization of the `_process_` of adding both a GTP and an IP header to an inner IP header. Nonetheless, the present specification is provided so that the 3GPP can refer to it from any of its own specifications of GTP and IP header processing.

The specification of CAPWAP already specifies [RFC 3168](#) ECN propagation and ECN capability negotiation. Without modification the CAPWAP specification already interworks with the backward compatible updates to [RFC 3168](#) in [RFC 6040](#).

LISP made the ECN propagation procedures in [RFC 3168](#) mandatory from the start. [RFC 3168](#) has since been updated by [RFC 6040](#), but the changes are backwards compatible so there is still no need for LISP tunnel endpoints to negotiate their ECN capabilities.

VXLAN is not under the change control of the IETF but it has been documented in an informational RFC. It is RECOMMENDED that VXLAN implementations comply with [RFC 6040](#) when the VXLAN header is inserted between (or removed from between) IP headers. And the authors of any future update to these specifications are encouraged to add a requirement to comply with [RFC 6040](#) as updated by the present specification.

VXLAN-GPE (Generic Protocol Extension) is on the IETF standards track. It is expected that it will specify ECN propagation before it is published as an RFC. {ToDo: Update this text once the VXLAN-GPE text has been updated.}

The specifications of Geneve and GUE already refer to [RFC 6040](#) for ECN encapsulation.

3.3.1. L2TP (v2 and v3) ECN Extension

The L2TP terminology used here is defined in [\[RFC2661\]](#) and [\[RFC3931\]](#).

L2TPv3 [\[RFC3931\]](#) is used as a shim header between any packet-switched network (PSN) header (e.g. IPv4, IPv6, MPLS) and many types of layer 2 (L2) header. The L2TPv3 shim header encapsulates an L2-specific sub-layer then an L2 header that is likely to contain an inner IP header (v4 or v6). Then this whole stack of headers can be encapsulated optionally within an outer UDP header then an outer PSN header that is typically IP (v4 or v6).

L2TPv2 is used as a shim header between any PSN header and a PPP header, which is in turn likely to encapsulate an IP header.

Even though these shims are rather fat (particularly in the case of L2TPv3), they still fit the definition of a tightly coupled shim header over an encapsulating header ([Section 3.1](#)), because all the headers encapsulating the L2 header are added (or removed) together. L2TPv2 and L2TPv3 are therefore within the scope of [RFC 6040](#), as updated by [Section 3.1](#) above.

L2TP maintainers are RECOMMENDED to implement the ECN extension to L2TPv2 and L2TPv3 defined in [Section 3.3.1.2](#) below, in order to provide the benefits of ECN [\[RFC8087\]](#), whenever a node within an L2TP tunnel becomes the bottleneck for an end-to-end traffic flow.

3.3.1.1. Safe Configuration of a 'Non-ECN' Ingress LCCE

The following text is appended to both [Section 5.3 of \[RFC2661\]](#) and [Section 4.5 of \[RFC3931\]](#) as an update to the base L2TPv2 and L2TPv3 specifications:

An LCCE that does not support the ECN Extension in [Section 3.3.1.2](#) of RFCXXXX MUST follow the configuration requirements in [Section 3.2](#) of RFCXXXX for when the outer PSN header is IP (v4 or v6). {RFCXXXX refers to the present document so it will need to be inserted by the RFC Editor}

In particular this means that an LCCE implementation that does not support the ECN Extension MUST propagate the ECN field between inner and outer IP headers independently of any configuration of the Diffserv extension of L2TP [\[RFC3308\]](#).

3.3.1.2. ECN Extension for L2TP (v2 or v3)

When the outer PSN header and the payload inside the L2 header are both IP (v4 or v6), to comply with [RFC 6040](#), an LCCE will follow the rules for propagation of the ECN field at ingress and egress in [Section 4 of RFC 6040](#) [[RFC6040](#)].

Before encapsulating any data packets, [RFC 6040](#) requires an ingress LCCE to check that the egress LCCE supports ECN propagation. If the egress supports ECN, the ingress LCCE can use the normal mode of encapsulation. Otherwise, the ingress LCCE has to use compatibility mode [[RFC6040](#)]. An LCCE can determine the remote LCCE's support for ECN either statically (by configuration) or by dynamic discovery during setup of each control connection between the LCCEs, using the Capability AVP defined in [Section 3.3.1.2.1](#) below.

Where the outer PSN header is some protocol other than IP that supports ECN, the appropriate ECN propagation specification will need to be followed, e.g. "Explicit Congestion Marking in MPLS" [[RFC5129](#)]. Where no specification exists for ECN propagation by a particular PSN, [[I-D.ietf-tsvwg-ecn-encap-guidelines](#)] gives general guidance on how to design ECN propagation into a protocol that encapsulates IP.

3.3.1.2.1. LCCE Capability AVP for ECN Capability Negotiation

The LCCE Capability Attribute Value Pair (AVP) defined here has Attribute Type ZZ. The Attribute Value field for this AVP is a bit-mask with the following 16-bit format:

```

      0                               1
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
      |X X X X X X X X X X X X X X X E|
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

```

This AVP MAY be present in the following message types: SCCRQ and SCCRP (Start-Control-Connection-Request and Start-Control-Connection-Reply). This AVP MAY be hidden (the H-bit set to 0 or 1) and is optional (M-bit not set). The length (before hiding) of this AVP MUST be 8 octets. The Vendor ID is the IETF Vendor ID of 0.

Bit 15 of the Value field of the LCCE Capability AVP is defined as the ECN Capability flag (E). When the ECN Capability flag is set to 1, it indicates that the sender supports ECN propagation. When the ECN Capability flag is cleared to zero, or when no LCCE Capability AVP is present, it indicates that the sender does not support ECN

propagation. All the other bits are reserved. They MUST be cleared to zero when sent and ignored when received or forwarded.

An LCCE initiating a control connection will send a Start-Control-Connection-Request (SCCRQ) containing an LCCE Capability AVP with the ECN Capability flag set to 1. If the tunnel terminator supports ECN, it will return a Start-Control-Connection-Reply (SCCRP) that also includes an LCCE Capability AVP with the ECN Capability flag set to 1. Then, for any sessions created by that control connection, both ends of the tunnel can use the normal mode of [RFC 6040](#) to propagate the ECN field when encapsulating data packets.

If, on the other hand, the tunnel terminator does not support ECN it will ignore the ECN flag in the LCCE Capability AVP and send an SCCRP to the tunnel initiator without a Capability AVP (or with a Capability AVP but with the ECN Capability flag cleared to zero). The tunnel initiator interprets the absence of the ECN Capability flag in the SCCRP as an indication that the tunnel terminator is incapable of supporting ECN. When encapsulating data packets for any sessions created by that control connection, the tunnel initiator will then use the compatibility mode of [RFC 6040](#) to clear the ECN field of the outer IP header to 0b00.

If the tunnel terminator does not support this ECN extension, the network operator is still expected to configure it to comply with the safety provisions set out in [Section 3.3.1.1](#) above, when it acts as an ingress LCCE.

[3.3.2](#). GRE

The GRE terminology used here is defined in [[RFC2784](#)]. GRE is often used as a tightly coupled shim header between IP headers. Sometimes the GRE shim header encapsulates an L2 header, which might in turn encapsulate an IP header. Therefore GRE is within the scope of [RFC 6040](#) as updated by [Section 3.1](#) above.

GRE tunnel endpoint maintainers are RECOMMENDED to support [[RFC6040](#)] as updated by the present specification, in order to provide the benefits of ECN [[RFC8087](#)] whenever a node within a GRE tunnel becomes the bottleneck for an end-to-end IP traffic flow tunnelled over GRE using IP as the delivery protocol (outer header).

GRE tunnels do not support dynamic configuration based on capability negotiation, so the ECN capability has to be manually configured, which is specified in [Section 4.3 of RFC 6040](#).

Where the delivery protocol is some protocol other than IP that supports ECN, the appropriate ECN propagation specification will need

to be followed, e.g Explicit Congestion Marking in MPLS [[RFC5129](#)]. Where no specification exists for ECN propagation by a particular PSN, [[I-D.ietf-tsvwg-ecn-encap-guidelines](#)] gives more general guidance on how to propagate ECN to and from protocols that encapsulate IP.

[3.3.2.1](#). Safe Configuration of a 'Non-ECN' GRE Ingress

The following text is appended to [Section 3 of \[RFC2784\]](#) as an update to the base GRE specification:

A GRE tunnel ingress that does not support [RFC 6040](#) or one of its compatible predecessors ([RFC 4301](#) or the full functionality mode of [RFC 3168](#)) MUST follow the configuration requirements in [Section 3.2](#) of RFCXXXX for when the outer delivery protocol is IP (v4 or v6). {RFCXXXX refers to the present document so it will need to be inserted by the RFC Editor}

[3.3.3](#). Teredo

{ToDo}

[4](#). IANA Considerations

IANA is requested to assign the following L2TP Control Message Attribute Value Pair:

+-----+	+-----+	+-----+
Attribute Type	Description	Reference
+-----+	+-----+	+-----+
ZZ	ECN Capability	RFCXXXX
+-----+	+-----+	+-----+

[TO BE REMOVED: This registration should take place at the following location: <https://www.iana.org/assignments/l2tp-parameters/l2tp-parameters.xhtml>]

[5](#). Security Considerations

The Security Considerations in [[RFC6040](#)] and [[I-D.ietf-tsvwg-ecn-encap-guidelines](#)] apply equally to the scope defined for the present specification.

[6](#). Comments Solicited

Comments and questions are encouraged and very welcome. They can be addressed to the IETF Transport Area working group mailing list <tsvwg@ietf.org>, and/or to the authors.

7. Acknowledgements

Thanks to Ing-jyh (Inton) Tsang for initial discussions on the need for ECN propagation in L2TP and its applicability. Thanks also to Carlos Pignataro, Tom Herbert and Ignacio Goyret for helpful advice and comments.

8. References

8.1. Normative References

- [I-D.ietf-tsvwg-ecn-encap-guidelines]
Briscoe, B., Kaippallimalil, J., and P. Thaler,
"Guidelines for Adding Congestion Notification to
Protocols that Encapsulate IP", [draft-ietf-tsvwg-ecn-encap-guidelines-08](#) (work in progress), March 2017.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", [BCP 14](#), [RFC 2119](#),
DOI 10.17487/RFC2119, March 1997,
<<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black,
"Definition of the Differentiated Services Field (DS
Field) in the IPv4 and IPv6 Headers", [RFC 2474](#),
DOI 10.17487/RFC2474, December 1998,
<<http://www.rfc-editor.org/info/rfc2474>>.
- [RFC2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn,
G., and B. Palter, "Layer Two Tunneling Protocol "L2TP"",
[RFC 2661](#), DOI 10.17487/RFC2661, August 1999,
<<http://www.rfc-editor.org/info/rfc2661>>.
- [RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P.
Traina, "Generic Routing Encapsulation (GRE)", [RFC 2784](#),
DOI 10.17487/RFC2784, March 2000,
<<http://www.rfc-editor.org/info/rfc2784>>.
- [RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition
of Explicit Congestion Notification (ECN) to IP",
[RFC 3168](#), DOI 10.17487/RFC3168, September 2001,
<<http://www.rfc-editor.org/info/rfc3168>>.
- [RFC3931] Lau, J., Ed., Townsley, M., Ed., and I. Goyret, Ed.,
"Layer Two Tunneling Protocol - Version 3 (L2TPv3)",
[RFC 3931](#), DOI 10.17487/RFC3931, March 2005,
<<http://www.rfc-editor.org/info/rfc3931>>.

- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), DOI 10.17487/RFC4301, December 2005, <<http://www.rfc-editor.org/info/rfc4301>>.
- [RFC4380] Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", [RFC 4380](#), DOI 10.17487/RFC4380, February 2006, <<http://www.rfc-editor.org/info/rfc4380>>.
- [RFC5129] Davie, B., Briscoe, B., and J. Tay, "Explicit Congestion Marking in MPLS", [RFC 5129](#), DOI 10.17487/RFC5129, January 2008, <<http://www.rfc-editor.org/info/rfc5129>>.
- [RFC6040] Briscoe, B., "Tunnelling of Explicit Congestion Notification", [RFC 6040](#), DOI 10.17487/RFC6040, November 2010, <<http://www.rfc-editor.org/info/rfc6040>>.

8.2. Informative References

- [GTPv1] 3GPP, "GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface", Technical Specification TS 29.060.
- [GTPv1-U] 3GPP, "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)", Technical Specification TS 29.281.
- [GTPv2-C] 3GPP, "Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)", Technical Specification TS 29.274.
- [I-D.ietf-intarea-gue]
Herbert, T., Yong, L., and O. Zia, "Generic UDP Encapsulation", [draft-ietf-intarea-gue-04](#) (work in progress), May 2017.
- [I-D.ietf-nvo3-geneve]
Gross, J., Ganga, I., and T. Sridhar, "Geneve: Generic Network Virtualization Encapsulation", [draft-ietf-nvo3-geneve-04](#) (work in progress), March 2017.
- [I-D.ietf-nvo3-vxlan-gpe]
Maino, F., Kreeger, L., and U. Elzur, "Generic Protocol Extension for VXLAN", [draft-ietf-nvo3-vxlan-gpe-04](#) (work in progress), April 2017.

- [RFC1701] Hanks, S., Li, T., Farinacci, D., and P. Traina, "Generic Routing Encapsulation (GRE)", [RFC 1701](#), DOI 10.17487/RFC1701, October 1994, <<http://www.rfc-editor.org/info/rfc1701>>.
- [RFC2637] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", [RFC 2637](#), DOI 10.17487/RFC2637, July 1999, <<http://www.rfc-editor.org/info/rfc2637>>.
- [RFC2983] Black, D., "Differentiated Services and Tunnels", [RFC 2983](#), DOI 10.17487/RFC2983, October 2000, <<http://www.rfc-editor.org/info/rfc2983>>.
- [RFC3308] Calhoun, P., Luo, W., McPherson, D., and K. Peirce, "Layer Two Tunneling Protocol (L2TP) Differentiated Services Extension", [RFC 3308](#), DOI 10.17487/RFC3308, November 2002, <<http://www.rfc-editor.org/info/rfc3308>>.
- [RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", [RFC 5415](#), DOI 10.17487/RFC5415, March 2009, <<http://www.rfc-editor.org/info/rfc5415>>.
- [RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", [RFC 6830](#), DOI 10.17487/RFC6830, January 2013, <<http://www.rfc-editor.org/info/rfc6830>>.
- [RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", [RFC 7348](#), DOI 10.17487/RFC7348, August 2014, <<http://www.rfc-editor.org/info/rfc7348>>.
- [RFC7637] Garg, P., Ed. and Y. Wang, Ed., "NVGRE: Network Virtualization Using Generic Routing Encapsulation", [RFC 7637](#), DOI 10.17487/RFC7637, September 2015, <<http://www.rfc-editor.org/info/rfc7637>>.
- [RFC8087] Fairhurst, G. and M. Welzl, "The Benefits of Using Explicit Congestion Notification (ECN)", [RFC 8087](#), DOI 10.17487/RFC8087, March 2017, <<http://www.rfc-editor.org/info/rfc8087>>.

[RFC8159] Konstantynowicz, M., Ed., Heron, G., Ed., Schatzmayr, R.,
and W. Henderickx, "Keyed IPv6 Tunnel", [RFC 8159](#),
DOI 10.17487/RFC8159, May 2017,
<<http://www.rfc-editor.org/info/rfc8159>>.

Author's Address

Bob Briscoe
Simula Research Laboratory
UK

EMail: ietf@bobbriscoe.net
URI: <http://bobbriscoe.net/>

