

Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: 1 October 2025

D. Eastlake
Independent
N. Cam-Winget
Cisco Systems
M. Umair
IPinfusion
30 March 2025

Security Considerations for Tenant ID and Similar Fields
draft-eastlake-secdispatch-tenantid-consid-06

Abstract

Many protocols provide for header fields to be added to a packet on ingress to a network domain and removed on egress from that domain. Examples of such fields are Tenant ID for multi-tenant networks, ingress port ID and/or type, and other identity or handling directive fields. These fields mean that a packet may be accompanied by supplemental information as it transits the network domain that would not be present with the packet or not be visible if it were simply forwarded in a traditional manner. A particular concern is that these fields may harm privacy by identifying, in greater detail, the packet source and intended traffic handling. This document provides Security Considerations for the inclusion of such fields with a packet.

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 <https://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 1 October 2025.

Copyright Notice

Copyright (c) 2025 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 (<https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

| | |
|---|----|
| 1. Introduction | 2 |
| 1.1. Meta-Data | 4 |
| 1.2. Terminology | 5 |
| 2. Threat Model | 5 |
| 3. Security Considerations | 6 |
| 3.1. Minimization | 7 |
| 3.2. Encryption | 7 |
| 3.2.1. Scope of Encryption | 8 |
| 3.2.2. Link Encryption | 9 |
| 3.2.3. Edge-to-Edge Encryption | 9 |
| 3.3. Obfuscation | 10 |
| 3.3.1. Field/Content Obfuscation | 10 |
| 3.3.2. Sequence Obfuscation | 10 |
| 3.4. Integrity and Authentication Considerations | 11 |
| 3.5. Covert Channel Considerations | 11 |
| 4. Examples of Applicable Fields | 12 |
| 4.1. Example Fields from Standards Track RFCs | 12 |
| 4.1.1. Service Function Chaining Network Service Header | 12 |
| 4.1.2. Geneve | 13 |
| 4.1.3. IP Header Fields | 13 |
| 4.2. Example Fields from Other RFCs | 14 |
| 4.2.1. VXLAN | 14 |
| 4.2.2. NVGRE | 15 |
| 5. IANA Considerations | 15 |
| 6. Normative References | 15 |
| 7. Informative References | 16 |
| Acknowledgements | 18 |
| Authors' Addresses | 18 |

1. Introduction

Many protocols provide for header fields to be added to a packet on ingress to a network domain and removed on egress from that domain as shown in Figure 1. Examples of such fields are Tenant ID for multi-tenant networks, ingress port ID and/or type, and other identity or handling directive fields. These fields mean that a packet may be accompanied by supplemental information as it transits the network

domain that would not be present with the packet or not be visible if it were simply forwarded in a traditional manner.

There are many such fields that have been specified. A few examples from IETF RFCs are given below in Section 4. This document provides Security Considerations [RFC3552] for the inclusion of such supplemental information with a packet.

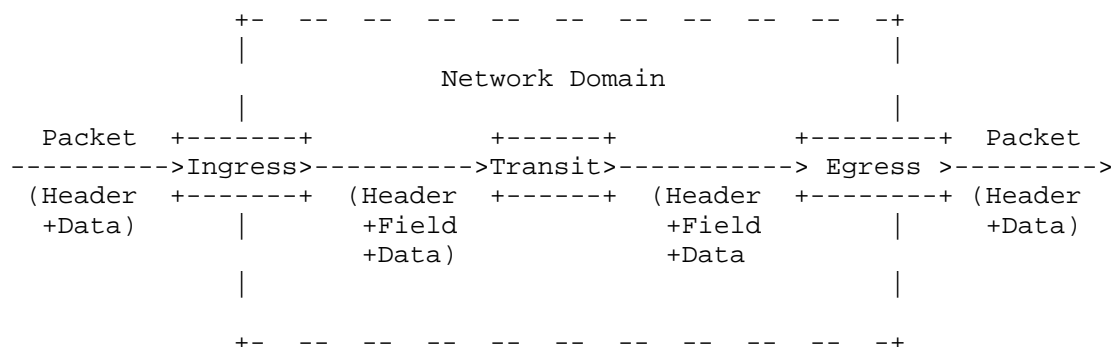


Figure 1: Example Network Domain

Figure 1 shows a simplified diagram. In a specific case, there may be zero or many transit nodes and, in the case of a multi-destination packet, there might be multiple paths from the ingress to multiple egress nodes. Also, there might be multiple fields added which are considered one logical field for the purposes of this document or an added information "field" might be encoded into an existing field or subpart of that field.

The primary security concern caused by the addition of such supplemental information is harm to the privacy of the packet source by distinguishing the packet's source and the packet's intended handling in detail. The granularity with which packet sources are distinguished can vary greatly. At their more specific, fields could distinguish one or combination of a single host computer, individual user, or specific process, application, or protocol instance within a host. At the less specific, only the identity of an adjacent Internet Service Provider might be revealed. For example, if VXLAN [RFC7348] is in use, the combination of the outer IP header source and destination IP addresses, which identify VXLAN Tunnel End Points (VTEPs), and the inner original header IP addresses, normally enable one to precisely identify a host/VM/Tenant. In addition to distinguishing packet sources with a finer granularity, supplemental information may enable multiple apparently different sources to be grouped as related and allow some information about the structure of complex sources to be deduced.

The supplemental information fields added or set by the ingress node may be derived from fields present in the packet which are normally forwarded, such as the "5-tuple" of IP Source and Destination Address, IP Source and Destination Port, and IP Protocol and/or additional header fields that would be transmitted with the packet. Reasons for adding a derived field include that the information it is derived from will not be available to transit nodes because it will be encrypted or it is too deep in the packet, that is, too far from the beginning of the packet.

In other cases, the field may be derived in whole or in part from information such as ingress port identity or a VLAN tag on the packet arriving via Ethernet and which would not normally be forwarded with the packet.

1.1. Meta-Data

The supplemental added information referred to above is an example of meta-data, which is additional data distinct from the content of messages. Meta-data is usually less sensitive than the content of messages. For example, consider messages between an individual and a doctor with a narrow medical specialty where there was no prior relationship between them. The existence and timing of such an exchange of messages could be quite revealing but clearly less so than the content of the messages which could reveal specific diagnosis and prognosis as well as the actual patient name which might be different from the messaging participant. While there are exceptions, in mandatory label systems, such as the USA government classification system for national security information with categories

Unclassified < Confidential < Secret < Top Secret,

a default rule of thumb is that the meta-data for a messages stream is one level less sensitive than the messages contents. For example, if there is a stream of messages whose content is classified as Secret, the message meta-data such as source and destination addresses, message timing and size, etc., would tend to be classified as Confidential. A counter-example would be the less common case where the content of a message was only moderately important but the mere existence and address of the source and/or destination is very sensitive.

A former head of the USA NSA and CIA has said, [Ferran] "We kill people based on meta-data".

1.2. Terminology

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.

The acronyms and terms below are used in this document. For further security term definitions, see [RFC4949].

AEAD - Authenticated Encryption with Additional Data.

ASCII - American Standard Code for Information Interchange [RFC0020].

ciphertext - Data that has been transformed by encryption so that its semantic information content is no longer intelligible or directly available (see Section 3.2) [RFC4949].

CPU - Central Processing Unit.

DSCP - Differentiated Services Code Point [RFC2474].

LAN - Local Area Network.

MAC - Media Access Control [IEEE802.1Q].

plaintext - Data that is input to an encryption process (see Section 3.2) [RFC4949].

QoS - Quality of Service.

TLV - Type, Length, Value.

VLAN - Virtual LAN [IEEE802.1Q].

VTEP - VXLAN Tunnel End Point.

2. Threat Model

The primary threats considered in this document due to the inclusion of meta data in packets are from surveillance and from the modification of such fields. Such surveillance or modification could be accomplished either on links within the network domain or by the subversion of one or more nodes.

Surveillance threatens loss of privacy to the users whose traffic is transiting the network domain because it permits packets to be associated with such users and their host or service provider with greater specificity. The additional information with packets may also reveal associations between users or aspects of the network domain structure and capabilities. And, to the extent that the additional information affects the treatment of the packet, unauthorized modification may disrupt network operation and interfere with the modified traffic or other traffic.

Note that, without suitable countermeasures, radio links are particularly subject to surveillance and to traffic modification through blocking the original version of a packet and injection of a modified copy.

Subversion of a transit or egress node enables surveillance and modification of all the traffic through that node. Subversion of an ingress node is a threat but not closely related to adding information to the packet. All the information that might be in or associated with the packet is available at the ingress node regardless of whether any of this is added to the packet being ingressed.

3. Security Considerations

This section provides Security Considerations for the inclusion in a packet of additional fields/information as discussed in this document. These considerations are equally applicable to IPv4 [RFC0791] and IPv6 [RFC8200]. They are grouped into the following topics:

- * Surveillance Oriented Considerations
 - o Minimization
 - o Encryption
 - o Obfuscation
- * Other Security Considerations
 - o Integrity and Authentication Considerations
 - o Covert Channel Considerations

The first three items above have a dominance relationship as follows:

Minimization > Encryption > Obfuscation

As further discussed below, where reasonably possible, the types of additional information discussed in this document SHOULD NOT be included with a packet. Where it is necessary to include the information, it SHOULD be encrypted where practical. Where encryption of the entire packet is prohibitive, the cleartext data that is not mutable in transit MUST be authenticated, for example through authenticated encryption with associated data (AEAD) mechanisms. In cases where it can be neither excluded nor encrypted, consideration should be given to obfuscating the information, even though that provides only weak protection.

3.1. Minimization

The simplest method to minimize the harm that can be caused by the threats described in Section 2 is to minimize the amount of additional information added to packets transiting the network domain. If some information will not be necessary for controlling the treatment of a packet or other network management functions, it SHOULD NOT be included. The exceptional cases where inclusion is reasonable are

1. transition scenarios, where information remains included for a brief time while mechanisms using the information are being removed or disabled, or included starting a brief time before mechanisms using the information are being installed or enabled, and
2. some debugging cases where the additional information would be temporarily helpful (but note that the mere addition of this information may change behavior and mask or cause erroneous behavior).

Minimization is the strongest method to defeat the security threats outlined in Section 2 and MUST always be considered so a determination can be made as to whether the benefits of including the information exceed the risks. Any data that does not appear with the packets cannot, due to its transit of or egress from the network domain, compromise the privacy/security of the packet source.

3.2. Encryption

Encryption is a powerful technique. With the use of appropriate cryptographic algorithms and key management, encryption converts easily understandable plaintext into cyphertext from which the original plaintext cannot be derived without knowledge of the key.

Use of encryption provides clear benefits but there also costs. The computational burden of encryption/decryption at line speed may increase the cost of CPU or port hardware, may increase latency, and requirements for key management and pseudorandom number generation [RFC4086] will impose some burden.

Even with strong encryption, surveillance can yield information such as outer addressing and control information and the size and number of packets transmitted. The analysis of such indications is commonly known as "traffic analysis". Padding and dummy packets can obscure some of this meta information about encrypted traffic but only at a significant expense in bandwidth consumed.

The subsections below discuss the scope of encryption, such as what part of a packet it can be applied to and whether it is at the link level or edge-to-edge. It is RECOMMENDED that both link level and edge-to-edge encryption be used unless careful consideration shows the costs to exceed the benefits in a particular case. If both are not being used, then it RECOMMENDED that one or the other be used with default preference for edge-to-edge encryption in wired networks and link encryption for radio networks. Some reasons for this default preference are that wired networks are typically higher speed and hardware security assist in a port is unusual and relatively expensive while the ease of access to traffic in radio networks has lead to the almost universal inclusion of hardware security in wireless chip sets such that the use of encryption and authentication on a radio link can be considered low or zero cost

3.2.1. Scope of Encryption

Encryption can be applied to various parts of a packet; enough addressing and service information must be present outside the encryption to get the packet through the one or more hops it needs to transit with the desired QoS to the point where it will be decrypted. Finally, there is usually some encryption control information such as a Key ID to facilitate key rollover and the like. Also, depending on the mode of operation, a packet sequence number or the like may be needed. When part of a packet is encrypted, authentication of unencrypted fields in the packet SHOULD be considered (see Section 3.4).

3.2.2. Link Encryption

Link encryption encrypts a packet as it is output from the ingress node or a transit node and decrypts it on input to the next node in the path, which will be a transit node or the egress node. This protects the information content of the packet from surveillance of the link. However, it is usual that some link layer addressing information, such as a MAC address, and control information is needed by the destination node and in some cases needed by devices within the link. For example, if routers are connected by a bridged LAN [IEEE802.1Q] proper handling of the packets between them may require that the packet be sent with a VLAN/priority tag. However, link layer encryption can normally encrypt network layer addressing and control information including IP addresses.

With link encryption, the packet will be decrypted inside the hop-by-hop destination node so any additional information within the packet will be exposed there and privacy can still be harmed or service selectively denied by a subverted transit or egress node.

Link encryption is common by default on radio links which are easily surveilled. For example, almost all Wi-Fi [IEEE802.11] chip sets have built in cryptographic hardware so standardized link encryption for Wi-Fi is usually thought of as "free" in that its use does not impose significant additional overhead or speed limitations.

An example more commonly used on wired networks, is the IEEE MACSEC [IEEE802.1AE] standard.

3.2.3. Edge-to-Edge Encryption

Encryption between the ingress node and the egress node provides protection from surveillance of all the links along that path as well as surveillance by the transit nodes used. However, such encryption cannot cover any fields that are needed to control the treatment of the packet along its path in the network domain or that cause it to be routed to and decrypted at its egress node (or possibly nodes in the case of multicast). Thus edge-to-edge encryption does not cover network layer addresses and control information or link layer addressing and control information.

While Link Encryption involves key setup only between adjacent nodes on the link, usually two nodes, strong Edge-to-Edge Encryption would require key setup for every pair of edge (ingress or egress) nodes that will be communicating traffic. This is potentially up to $N*(N-1)/2$ pairs if there are N edge nodes. And additional key set up and management may be required for multicast groups or the like.

3.3. Obfuscation

Obfuscation refers to weak methods of hiding the content of a field or packet or reducing the predictability of some sequence identifier field. The strongest obfuscation would be to use a random, possibly even time-varying, one-to-one mapping of the values in such fields but this imposes a burden of generating and storing such a mapping at nodes that set or access such a mapped field. It is more common to use weaker obfuscation as suggested below.

3.3.1. Field/Content Obfuscation

The first type of obfuscation of can be thought of as weak encryption that is unkeyed or uses a fixed key or a key sent with the message. There is, nevertheless, some benefit to its use. Roughly speaking, it protects against inadvertent disclosure but provides almost no protection against deliberate attack.

An interesting example of obfuscation is "masking" in The WebSocket Protocol [RFC6455]. For client to server data transfer the protocol requires that the payload be "masked" by taking a 4-byte mask value, repeating it as many times as necessary, and XORing it with the payload. Furthermore the mask value is required to be a random number different for each message derived from a strong source of entropy. However, this mask value is included as plain text with the payload so an entity that understands this masking can easily unmask the payload. In this case the obfuscation serves a particular security purpose as explained in [RFC6455] which provides further information.

As another example, someone debugging a network problem might do a capture of the packets on a link with a program that will display the packet data in hexadecimal and ASCII. This data might include personally identifying information or other sensitive information that could be immediately read if interpreted as ASCII. Such inadvertent disclosure could be avoided by an obfuscation as simple as XORing a fixed non-zero byte value with each data field byte.

3.3.2. Sequence Obfuscation

The second type of obfuscation involves, to the extent practical, avoiding easily predictable numbers for identifiers such as Tenant IDs, sequence numbers, interface (port) identifiers, IP addresses, source socket numbers, and the like. If successively allocated identifiers of this sort are easily predictable, it is, for example, much easier to forge packets that may be accepted as genuine. Instead of simply counting to determine a next value to use, something like the output of a linear feedback shift register could

be used.

For further discussion, see [RFC9416], "Security Considerations for Transient Numeric Identifiers Employed in Network Protocols", which, among other things, states the following: "Protocol specifications SHOULD NOT employ predictable transient numeric identifiers, except when such predictability is the result of their interoperability requirements." [RFC9414] and [RFC9415] may also be of interest.

3.4. Integrity and Authentication Considerations

Providing for the integrity and authentication of packets in the network domain is generally a good idea for reasons including the following:

1. To the extent that additional information with a packet affects network handling of that packet, it is important that the information is not corrupted or forged. Not only can the treatment of the packet be affected but if, for example, arbitrary numbers of high priority packets can be forged, overall performance of the network domain can be disrupted. Thus, integrity and authentication SHOULD be used.
2. Some modes of encryption (see Section 3.2) are sensitive to modified, dropped, or extra packets which may result in garbling the decryption of following genuine packets. Appropriate integrity and authentication SHOULD be used with flows that are so encrypted.

Where part of a packet is encrypted and authenticated, unencrypted parts may be authenticated using AEAD.

3.5. Covert Channel Considerations

The presence of additional information in a packet provides a place into which a node forwarding a packet can hide information and from which a subsequent node in the packet's path can retrieve information. The encryption of such additional information, which is desirable for reasons given above, can make detection of such tunneling to exfiltrate information hard to detect.

Many of the headers discussed in Section 4 which provide for the sort of additional information fields which are the primary focus of this document also have reserved fields. Most commonly the specification for these fields, which are reserved for later definition, state they must be sent as zero and ignored on receipt. Since their value is ignored by standards compliant nodes, such fields could be used for covert channel communications.

4. Examples of Applicable Fields

The subsections below give some examples of fields to which the Security Considerations material in Section 3 apply.

4.1. Example Fields from Standards Track RFCs

The following are examples of fields specified in Standards Track RFCs to which these Security Considerations would apply.

4.1.1. Service Function Chaining Network Service Header

The Service Function Header (SFC) Network Service Header (NSH) [RFC8300] provides for the inclusion of metadata with packets inside an SFC enabled domain as shown in Figure 2.

NSH Header:

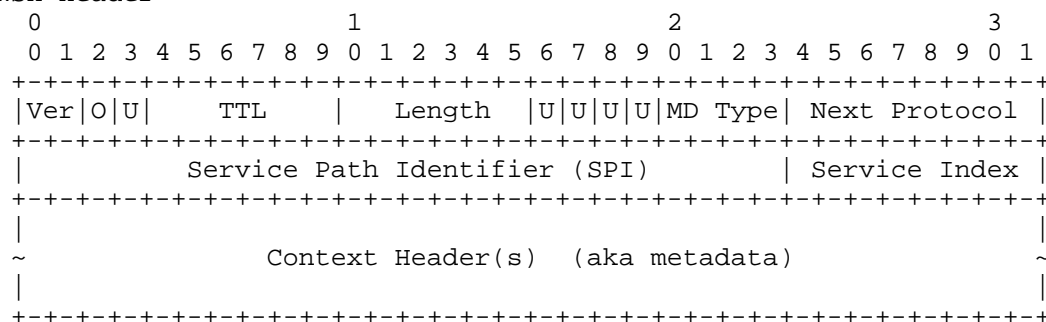


Figure 2: SFC NSH (from [RFC8300])

The MD Type field in the NSH header indicates the type of metadata field or fields in the "Context Headers" section of the NSH header. Such fields are appropriate for including additional information with a packet that would otherwise only be available at the ingress node. See, for example, the context headers specified in [RFC9263].

The NSH is used to encapsulate the traffic and requires an outer transport header as shown in Figure 3. This encapsulation is applied on ingress to the SFC enabled domain and removed on egress from that domain. If the transport encapsulation is, for example, IP, transport encapsulation fields may also be available to add information to the packet within the network domain (see Section 4.1.3).

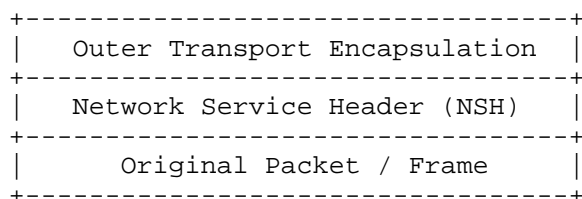


Figure 3: NSH Encapsulation (from [RFC8300])

4.1.2. Geneve

The Geneve (General Network Virtualization Encapsulation) [RFC8926] header provides for a Virtual Network Identifier which is equivalent to a Tenant ID, as shown in Figure 4. It also has a flexible provision for header options encoded at TLVs.

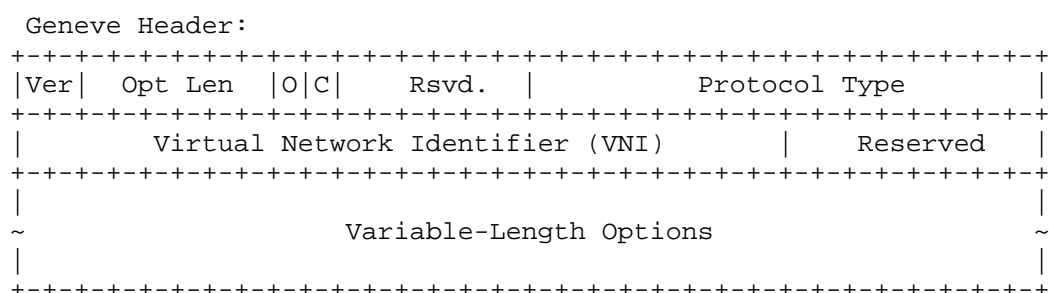


Figure 4: Geneve Header (from [RFC8926])

Geneve is used to encapsulate the traffic transiting the network domain with an IP transport encapsulation in a manner similar to the NSH Header as shown in Figure 3 and similar considerations apply.

4.1.3. IP Header Fields

There are a number of IPv4 [RFC0791] and IPv6 [RFC8200] header fields that can be used to encode supplemental information. Some of these fields are, in general, mutable, so they could change as a packet is propagated through a network; however, this document is restricted to considerations within a single network domain with coordinated management which can, in some cases, avoid changing such fields.

There is particular freedom to use IP fields where the traffic transiting the network domain is encapsulated in a manner that provides for a new outer IP header. For example, IP-in-IP or where the traffic is encapsulated in a tunnel header, such as VXLAN, NVGRE, SFC NSH, or Geneve, which is in turn encapsulated in an outer IP header.

DSCP/ToS - There is an 8-bit field in the IPv6 and IPv4 header. Two of these bits are commonly used for Explicit Congestion Notification (ECN, [RFC3168]) and the other six are commonly used to encode hop-by-hop behaviors [RFC2474]. In an outer IP header within a network domain with common management those six bits could be used as desired as could the ECN bits unless those bit are used to accumulate congestion information to be combined into an inner IP or similar header on domain egress.

Options - Both IPv4 and IPv6 provide for header options with IPv6 having provisions for more flexible and extensive options but these have proven hard to use in practice.

IPv6 Flow Label - In the IPv6 header, a 20-bit Flow Label field is available.

Addresses - Where an outer IP header is used within a network domain, not all of the IPv4 or generously sized IPv6 address fields are needed to direct transit traffic from ingress to egress. Thus other additional information could be encoded into the address field, perhaps in low order bits.

Sockets, Etc. - There are additional fields available in the commonly used UDP and TCP headers that could, in an outer IP encapsulation inside a network domain, be interpreted as holding other information.

4.2. Example Fields from Other RFCs

The following are examples of fields specified in RFCs that are not Standards Track to which the Security Considerations material in Section 3 apply.

4.2.1. VXLAN

VXLAN (Virtual eXtensible Local Area Network) is specified in [RFC7348] and the VXLAN header is shown in Figure 5.

VXLAN Header:

```

+-----+
|R|R|R|R|I|R|R|R|          Reserved          |
+-----+
|          VXLAN Network Identifier (VNI)      | Reserved |
+-----+

```

Figure 5: VXLAN Header (from [RFC7348])

The Virtual Network Identifier (VNI) is a tenant identifier in multi-tenant domains. It is intended to identify traffic that uses an overlay network for that tenant. In addition, the use of VXLAN involves encapsulation of the traffic being forwarded so there is an outer IP and UDP header with various fields that could be used for additional information (see Section 4.1.3).

4.2.2. NVGRE

NVGRE (Network Virtualization Using Generic Routing Encapsulation) is specified in [RFC7637] and the NVGRE header is shown in Figure 6.

NVGRE Header:

```

+-----+
|0| |1|0|   Reserved0       | Ver |   Protocol Type 0x6558   |
+-----+
|          Virtual Subnet ID (VSID)            |   FlowID   |
+-----+

```

Figure 6: NVGRE Header (from [RFC7637])

The Virtual Subnet ID (VSID) is a tenant identifier in multi-tenant domains. It is intended to identify traffic that uses an overlay network for that tenant. In addition, the use of NVGRE involves encapsulation of the traffic being forwarded so there is an outer IP and UDP header with various fields that could be used for additional information (see Section 4.1.3).

5. IANA Considerations

This document requires no IANA actions.

6. Normative References

- [RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <<https://www.rfc-editor.org/info/rfc791>>.

- [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>>.
- [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>>.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.

7. Informative References

- [Ferran] Ferran, L., "'Ex-NSA Chief: 'We Kill People Based on Metadata'", May 2014, <<https://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata>>.
- [IEEE802.11] 802.11 WG, IEEE., "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2016, 7 December 2016.
- [IEEE802.1AE] 802.1 WG, IEEE., "Media Access Control (MAC) Security", IEEE Std 802.1AE-2018, 27 September 2018.
- [IEEE802.1Q] 802.1 WG, IEEE., "Bridges and Bridged Networks", IEEE Std 802.1Q-2014, 3 November 2014.
- [RFC0020] Cerf, V., "ASCII format for network interchange", STD 80, RFC 20, DOI 10.17487/RFC0020, October 1969, <<https://www.rfc-editor.org/info/rfc20>>.
- [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, <<https://www.rfc-editor.org/info/rfc2474>>.
- [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, <<https://www.rfc-editor.org/info/rfc3168>>.

- [RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <<https://www.rfc-editor.org/info/rfc3552>>.
- [RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <<https://www.rfc-editor.org/info/rfc4086>>.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/info/rfc4949>>.
- [RFC6455] Fette, I. and A. Melnikov, "The WebSocket Protocol", RFC 6455, DOI 10.17487/RFC6455, December 2011, <<https://www.rfc-editor.org/info/rfc6455>>.
- [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, <<https://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, <<https://www.rfc-editor.org/info/rfc7637>>.
- [RFC8300] Quinn, P., Ed., Elzur, U., Ed., and C. Pignataro, Ed., "Network Service Header (NSH)", RFC 8300, DOI 10.17487/RFC8300, January 2018, <<https://www.rfc-editor.org/info/rfc8300>>.
- [RFC8926] Gross, J., Ed., Ganga, I., Ed., and T. Sridhar, Ed., "Geneve: Generic Network Virtualization Encapsulation", RFC 8926, DOI 10.17487/RFC8926, November 2020, <<https://www.rfc-editor.org/info/rfc8926>>.
- [RFC9263] Wei, Y., Ed., Elzur, U., Majee, S., Pignataro, C., and D. Eastlake 3rd, "Network Service Header (NSH) Metadata Type 2 Variable-Length Context Headers", RFC 9263, DOI 10.17487/RFC9263, August 2022, <<https://www.rfc-editor.org/info/rfc9263>>.

- [RFC9414] Gont, F. and I. Arce, "Unfortunate History of Transient Numeric Identifiers", RFC 9414, DOI 10.17487/RFC9414, July 2023, <<https://www.rfc-editor.org/info/rfc9414>>.
- [RFC9415] Gont, F. and I. Arce, "On the Generation of Transient Numeric Identifiers", RFC 9415, DOI 10.17487/RFC9415, July 2023, <<https://www.rfc-editor.org/info/rfc9415>>.
- [RFC9416] Gont, F. and I. Arce, "Security Considerations for Transient Numeric Identifiers Employed in Network Protocols", BCP 72, RFC 9416, DOI 10.17487/RFC9416, July 2023, <<https://www.rfc-editor.org/info/rfc9416>>.

Acknowledgements

The suggestions and comments on this document from the following persons are gratefully acknowledged:

TBD

Authors' Addresses

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

Nancy Cam-Winget
Cisco Systems
3550 Cisco Way
San Jose, CA 95134
United States of America
Email: ncamwing@cisco.com

Mohammed Umair
IPinfusion
India
Email: mohammed.umair2@gmail.com