

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 25, 2017

T. Li
Peloton Technology
G. Salgueiro
Cisco Systems, Inc.
D. Farinacci
lispers.net
May 24, 2017

Transmission of IPv4 over IEEE 802.11 in OCB mode
draft-li-ipv4-over-80211ocb-01

Abstract

This document describes the transmission of IPv4 packets over IEEE 802.11-2012 networks when run Outside the Context of a BSS (802.11-OCB, earlier known as 802.11p).

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 November 25, 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

Internet-Draft

IPv4-over-80211ocb

May 2017

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.	Transmission of IPv4 over 802.11-OCB	3
3.1.	Frame Format	3
3.1.1.	Ethernet Adaptation Layer	5
3.2.	Maximum Transmission Unit (MTU)	6
3.3.	MAC Address Resolution	6
3.4.	IPv4 Addressing	7
4.	Security Considerations	7
4.1.	Design Considerations	7
4.2.	Privacy Considerations	7
4.3.	Certificate Considerations	8
4.4.	Other Considerations	9
5.	IANA Considerations	9
6.	Acknowledgments	9
7.	References	9
7.1.	Normative References	9
7.2.	Informative References	10
Appendix A.	IPv4 Packet in Flight	11
Authors' Addresses	12

[1.](#) Introduction

This document describes the transmission of IPv4 and ARP packets over IEEE 802.11-2012 networks when run Outside the Context of a BSS (802.11-OCB, earlier known as 802.11p), as documented in [[IEEE802.11-2012](#)]. IPv4 packets are encapsulated in a LLC SNAP layer and then the 802.11 MAC layer before transmission.

In the following text we use the term "802.11-OCB" to refer to IEEE 802.11-2012 when operated with the "OCBActivated" flag set. Previous versions of other documents also referred to this as 802.11p.

802.11-OCB networks are used frequently in vehicular communications and have specific safety related requirements that are not discussed here. Nothing in this document should be construed to contradict, contravene, or otherwise deter compliance with other safety requirements and regulations. Specifically, IPv4 is prohibited on

the 802.11-OCB 'Control Channel' (channel 178 at FCC/IEEE, and 180 at ETSI).

This document only describes the encapsulation of IPv4 packets. Other issues such as addressing, discovery, channel selection, and

transmission timing are out of scope for this document. IPv6 is out of scope for this document.

[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](#)].

LLC: The Logical Link Control layer from IEEE 802. Throughout this document, this also assumes the Subnetwork Access Protocol (SNAP) extension with an EtherType protocol on top of SNAP.

OCB: Outside the Context of a Basic Service Set identifier.

802.11-OCB: IEEE 802.11-2012 text flagged by "dot11OCBActivated". This means: IEEE 802.11e for quality of service; 802.11j-2004 for half-clocked operations; and 802.11p for operation in the 5.9 GHz band and in mode OCB.

[3.](#) Transmission of IPv4 over 802.11-OCB

IEEE 802.11-OCB specifies that packets should be framed with an LLC header and then one of the various 802.11-OCB headers. This document specifies how IPv4 and ARP are encapsulated over 802.11-OCB.

[3.1.](#) Frame Format

IP packets are transmitted over 802.11-OCB within the standard LLC encapsulation using the EtherType code 0x0800, as specified in [[RFC1042](#)] and [[RFC0894](#)].

IPv4 packets can be transmitted as "IEEE 802.11 Data" or alternatively as "IEEE 802.11 QoS Data". Thus, formatted frames may appear in either of these formats:

IPv4 packet
 Logical-Link Control
 IEEE 802.11 Data

IPv4 packet
 Logical-Link Control
 IEEE 802.11 QoS Data

This format is slightly different than standard Ethernet framing for IPv4, so implementations SHOULD provide an adaptation layer so that the network layer perceives traditional Ethernet encapsulation.

When transmitting an IPv4 packet, the value of the field "Type/Subtype" in the 802.11 Data header is 0x20 (Data, Data). The value

of the field "Type/Subtype" in the 802.11 QoS header is 0x28 (Data, QoS data). The 802.11 data header is

```

      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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           Frame Control           |           Duration           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     Receiver Address...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
... Receiver Address                | Transmitter Address...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
... Transmitter Address                |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     BSS Id...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
... BSS Id                          | Frag Number and Seq Number |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Within the two Frame Control octets, the bits are:

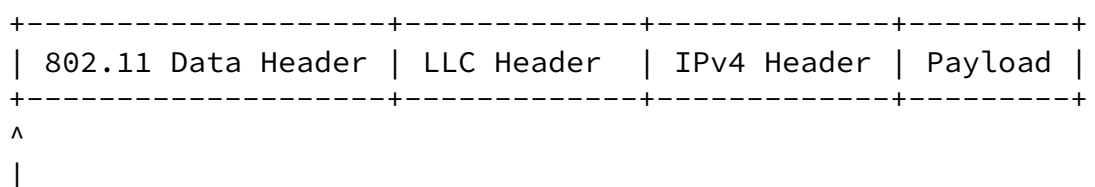
- o 2 bits: Protocol Version
- o 2 bits: Type
- o 4 bits: Subtype
- o 1 bit: To DS

- o 1 bit: From DS
- o 1 bit: More Frag
- o 1 bit: Retry
- o 1 bit: Power Mgmt
- o 1 bit: More Data
- o 1 bit: WEP
- o 1 bit: Order

[3.1.1.](#) Ethernet Adaptation Layer

In general, an adaptation layer is inserted between a MAC layer and the Networking layer to transform some parameters between the form expected by the IP stack and the form provided by the MAC layer. In this case, the goal is to transform the LLC encapsulation into traditional Ethernet encapsulation. This translated encapsulation is not sent over the 802.11-OCB network, but is instead presented by the device driver to the operating system. This allows 802.11-OCB interfaces to easily take advantage of all of the operating system facilities that exist for Ethernet already.

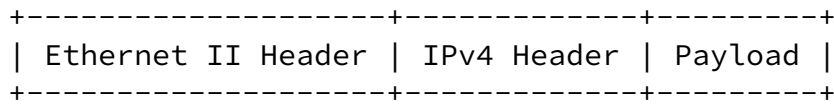
On packet reception, this layer takes the IEEE 802.11 Data Header and the Logical-Link Layer Control Header and produces an Ethernet II Header. At transmission, it performs the reverse operation.



802.11-to-Ethernet Adaptation Layer

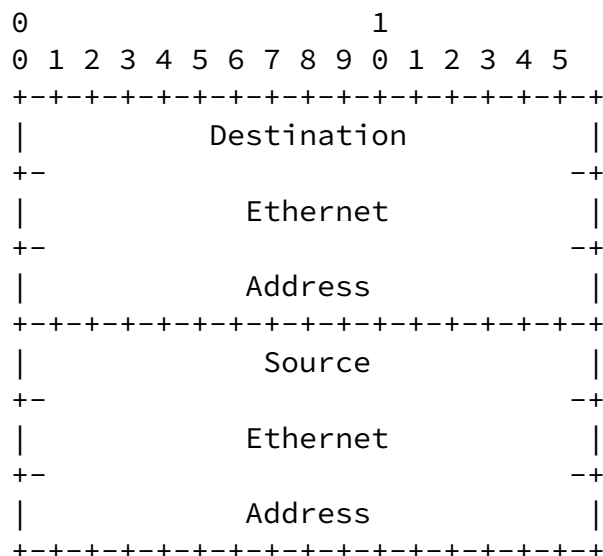
|

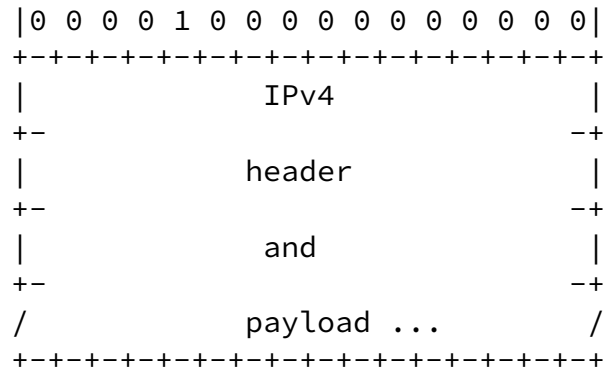
v



The Receiver and Transmitter Address fields in the 802.11 Data Header contain the same values as the Destination and the Source Address fields in the Ethernet II Header, respectively. The value of the Type field in the LLC Header is the same as the value of the Type field in the Ethernet II Header. The other fields in the Data and LLC Headers are not used by the IPv4 stack.

The result of the adaptation layer transformation is a typical IP over Ethernet frame:





3.2. Maximum Transmission Unit (MTU)

The MTU for IPv4 packets on 802.11-OCB is 1500 octets. It is the same value as IP packets on Ethernet links, as specified in [\[RFC0894\]](#). While the physical layer and link layer can support slightly larger packets, a different MTU value would cause frequent fragmentation, which would be suboptimal. [\[Fragmentation\]](#)

If a packet is fragmented by the IPv4 network layer before transmission on 802.11-OCB, the field "Sequence number" in the 802.11 Data header SHOULD increment for each fragment and the "Fragment number" field SHOULD remain 0. This is recommended because the link layer cannot do IP fragment reassembly or aid the final IPv4 recipient in any way. Further, the interaction between the network layer and the data link layer is a significant blurring of the layer boundary.

3.3. MAC Address Resolution

Address Resolution Protocol (ARP) [\[RFC0826\]](#) is used to determine the MAC address used for an IPv4 address, exactly as is done for Ethernet and Wi-Fi, with EtherType 0x0806.

3.4. IPv4 Addressing

This document does not make a recommendation on the IPv4 addressing strategy that is used on 802.11-OCB networks. A specific network is free to choose the addressing strategy that best suits its specific application. Known successful IPv4 unicast addressing strategies include, but are not limited to:

- o Static addressing
- o DHCP with network assigned addresses [[RFC2131](#)]
- o DHCP with private addressing and NAT [[RFC1918](#)] [[RFC3022](#)]
- o Link-local addressing [[RFC3927](#)]

Multicast addressing for IPv4 is as for Ethernet, as described in [[RFC1112](#)].

[4.](#) Security Considerations

[4.1.](#) Design Considerations

IEEE 802.11-OCB itself does not provide useful security guarantees. The link layer does not provide any authentication mechanism, leaving hosts just as exposed as they would be at a public Wi-Fi hot spot.

This section does not address safety-related applications, which are done on non-IP communications.

Because 802.11-OCB is specifically intended for mobile applications, privacy is a significant concern. 802.11-OCB already attempts to assist with privacy by having a station change its MAC address. This raises several issues discussed below.

[4.2.](#) Privacy Considerations

The L2 headers of IEEE 802.11-OCB and L3 headers of IPv4 are not encrypted, and expose the MAC address and IP address of both the source and destination. Adversaries could monitor the L2 or L3 headers, track the addresses, and through that track the position of a vehicles over time.

For hosts that have concerns about privacy, the obvious mitigation is to periodically use some form of MAC address randomization. We can assume that there will be "renumbering events" causing MAC addresses to change. A change of MAC address MUST induce a simultaneous change

of IPv4 address, to prevent linkage of the old and new MAC addresses

through continuous use of the same IP Addresses.

Unfortunately, the change of an IP address is very likely to cause disruption at the transport layer, breaking TCP connections at the renumbering event and disrupting any outstanding UDP transactions. For this reason, renumbering events **MUST** be coordinated between the transport, network, and link layers and **MUST** only happen when there are no active transport connections. For hosts that require a long-term continuous uptime, this will be problematic and hosts **MAY** choose to forgo renumbering events and sacrifice privacy.

MAC address randomization will not prevent tracking if the address stays constant for long intervals. Suppose for example that a vehicle only renumbers when leaving the owner's garage in the morning. It would be trivial to observe the "number of the day" at the known garage location, and to associate that with the vehicle's identity, thereby enabling tracking throughout the day. If renumbering events are too infrequent, they will not protect privacy, but if they are too frequent they will disrupt service. Careful, detailed communications between an implementations layers will be required to produce an optimal result.

Normally, hosts would be able to maintain transport connections across renumbering events by making use of multi-path TCP. [[RFC6824](#)] With multi-path TCP, a host can advertise multiple addresses to its correspondents, causing the correspondent to send packets to any of the addresses. If any of the addresses stops working, traffic continues to flow on the working addresses. However, in this situation, advertising multiple addresses would defeat the privacy goals.

[4.3.](#) Certificate Considerations

Because 802.11-OCB provides no link level security, some hosts **MAY** choose to implement cryptographic techniques to provide data privacy and authentication. The common approach to that today would be through the use of certificates and performing a key-exchange before commencing secure communications.

The challenge that this creates is that the key exchange needs to be performed prior to the exchange of other key information. Simply transmitting constant certificates in the clear is not optimal as that would violate the privacy requirements.

One approach to simply change certificates. To preserve privacy, a host **MUST** change its certificate any time it has a renumbering event.

Other approaches that allow for the private exchange of certificates are also possible and are an area for future study.

[4.4.](#) Other Considerations

At the IP layer, IPsec can be used to protect unicast communications. If no protection is used by the IP layer, upper layers should be cryptographically protected.

[5.](#) IANA Considerations

This document has no IANA actions.

[6.](#) Acknowledgments

The author would like to thank Alexandre Petrescu, Nabil Benamar, Jerome Haerri, Christian Huitema, Jong-Hyouk Lee, and Thierry Ernst for their work on [[I-D.petrescu-ipv6-over-80211p](#)] from which much of this text was taken.

[7.](#) References

[7.1.](#) Normative References

- [IEEE802.11-2012]
IEEE, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Standard freely available at <http://standards.ieee.org/findstds/standard/802.11-2012.html> retrieved on November 17th, 2016, March 2012.
- [RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", STD 37, [RFC 826](#), DOI 10.17487/RFC0826, November 1982, <<http://www.rfc-editor.org/info/rfc826>>.
- [RFC0894] Hornig, C., "A Standard for the Transmission of IP Datagrams over Ethernet Networks", STD 41, [RFC 894](#), DOI 10.17487/RFC0894, April 1984, <<http://www.rfc-editor.org/info/rfc894>>.
- [RFC1042] Postel, J. and J. Reynolds, "Standard for the transmission of IP datagrams over IEEE 802 networks", STD 43, [RFC 1042](#), DOI 10.17487/RFC1042, February 1988,

- [RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, [RFC 1112](#), DOI 10.17487/RFC1112, August 1989, <<http://www.rfc-editor.org/info/rfc1112>>.
- [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>>.
- [RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", [RFC 3927](#), DOI 10.17487/RFC3927, May 2005, <<http://www.rfc-editor.org/info/rfc3927>>.

7.2. Informative References

- [Fragmentation]
Kent, C. and J. Mogul, "Fragmentation considered harmful", ACM SIGCOMM Computer Communication Review Special twenty-fifth anniversary issue. Highlights from 25 years of the Computer Communication Review, Volume 25, Issue 1, January 1995.
- [I-D.petrescu-ipv6-over-80211p]
Petrescu, A., Benamar, N., Haerri, J., Huitema, C., Lee, J., Ernst, T., and T. Li, "Transmission of IPv6 Packets over IEEE 802.11 Outside the Context of a Basic Service Set (OCB)", [draft-petrescu-ipv6-over-80211p-06](#) (work in progress), November 2016.
- [RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", [BCP 5](#), [RFC 1918](#), DOI 10.17487/RFC1918, February 1996, <<http://www.rfc-editor.org/info/rfc1918>>.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), DOI 10.17487/RFC2131, March 1997, <<http://www.rfc-editor.org/info/rfc2131>>.

- [RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", [RFC 3022](#), DOI 10.17487/RFC3022, January 2001, <<http://www.rfc-editor.org/info/rfc3022>>.
- [RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", [RFC 6824](#), DOI 10.17487/RFC6824, January 2013, <<http://www.rfc-editor.org/info/rfc6824>>.

Li, et al.

Expires November 25, 2017

[Page 10]

Internet-Draft

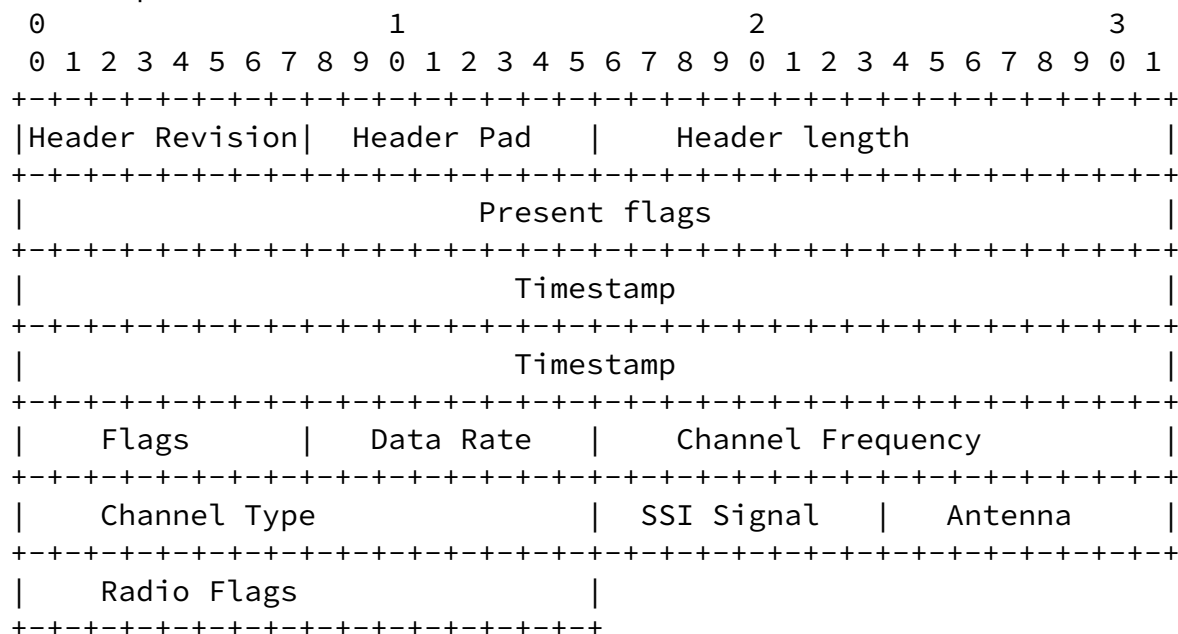
IPv4-over-80211ocb

May 2017

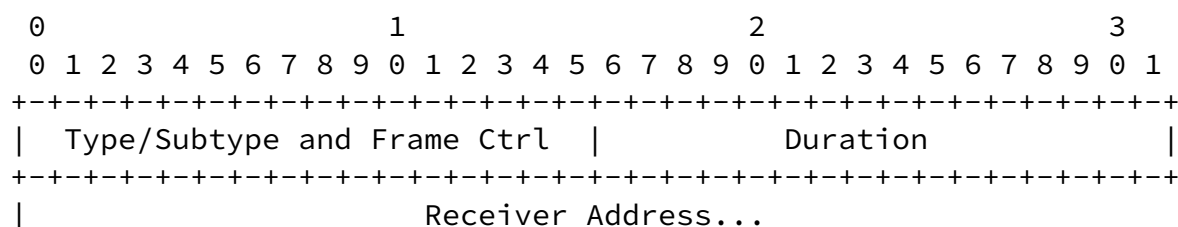
[Appendix A](#). IPv4 Packet in Flight

The following diagram shows an IPv4 packet with the IEEE 802.11 Data Header, Logical Link Control Header, IPv4 Header.

Radiotap Header v0



IEEE 802.11 Data Header



```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+
... Receiver Address          |          Destination Address...
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
... Destination Address          |
|          Transmitter Address...
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
... Transmitter Address          |          Source Address...
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
... Source Address          |
|          BSS Id...
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
... BSS Id          |   Frag Number and Seq Number   |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

Logical-Link Control Header

```

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
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|   DSAP   |I|   SSAP   |C| Control field | Org. code...
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
... Organizational Code          |          Type          |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

IPv4 Header

```

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
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|Version|  IHL  |Type of Service|          Total Length          |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|          Identification          |Flags|          Fragment Offset  |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Time to Live |   Protocol   |          Header Checksum          |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|          Source Address          |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|          Destination Address          |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|          Options          |          Padding          |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

Authors' Addresses

Tony Li
Peloton Technology
1060 La Avenida St.
Mountain View, California 94043
United States

Phone: +1 650 395 7356
Email: tony.li@tony.li

Gonzalo Salgueiro
Cisco Systems, Inc.
7025 Kit Creek Rd.
Research Triangle Park, NC 27709
USA

Phone: +1 919 392 3266
Email: gsalguei@cisco.com

Li, et al.

Expires November 25, 2017

[Page 12]

Internet-Draft

IPv4-over-80211ocb

May 2017

Dino Farinacci
lispers.net
San Jose, CA
USA

Email: farinacci@gmail.com

