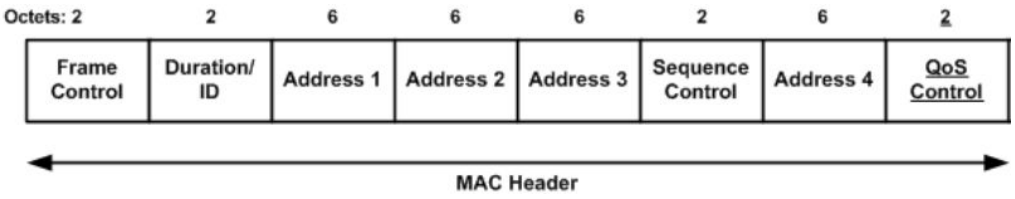
Use of MAC Header in Arada Systems Units

J. Astorga
D. Moreira
K. Wagemann

1. Introduction

The goal of the following document is to present a summary of the uses of the 802.11 MAC Header in ipv4 and ipv6 applications through wireless connection of two commercial V2X units of Arada Systems. An 802.11 MAC Header is defined by the following sections:



2. Messages

The messages are requests or replies from the ping network utility, on its IPv4 and IPv6 variations. All wireless communication was captured on an RSU Commando unit, which interacted with an OBU Classic unit. The communication was made through a WAVE link (IEEE 802.11p).

All of the messages shared the following fields: *version, type, subtype, flags, duration/id, BSS ID* and *QoS Control.* The structure of the messages is:

Frame Control Field
-Version: 0
-Type: Data frame (2)
-Subtype: Beacon (8)
-Flags:
DS status: To DS:0 From DS:0 (.... ..00)
More Fragments: This is the last fragment (.... .0..)
Retry: Frame is not being retransmitted (.... 0...)
PWR MGT: STA will stay up (...0 ....)
More Data: No data buffered (..0. ....)
Protected flag: Data is not protected (.0.. ....)
Order flag: Not strictly ordered (0... ....)

The combination of the type and subtype corresponds to the *QoS Data* MAC header. None of the messages used the *Address 3* section. That's because their type doesn't need to do so. The analyzed messages weren't fragmented so they are always the last fragment.

Duration/ID Field:

-0x0000 (Duration)

Contents of this field changes according to the type and subtype of the frame. In the case of type 2 subtype 8 unicast data frames (called simply QoS Data) with the subfield Ack Policy as No Ack, this field can have two values:

a) 0, if the frame is the TXOP's final fragment, or
b) The time required for the transmission of the next MPDU and its response if required.

In this case, as every message is sent in only one data frame, the frame is always the final fragment of the TXOP, therefore this field always contains 0, which corresponds with this what the message says.

Sequence Control Field:

- Fragment Number: 0 (.... .... 0000)
- Sequence Number: *X* (**** **** **** ….)

Fragment number indicates the number of each fragment of an MSDU, in the case of the captured packets is always set to 0, indicating that the packets aren't fragmented.

Sequence Number is a 12-bit field indicating the correlative sequence number of an MSDU. This field is variable between the messages.

Qos Control Field:

- TID: 0 (.... .... 0000)
- EOSP: Service period (.... ....0 ....)
- Ack Policy: No Ack (0x1) (.... .... .01. ....)
- Payload Type: MSDU (.... .... 0... ....)
- XOP Duration Requested: 0 (no TXOP requested) (0000 0000 ....)

Addresses:

-Receiver Address (RA) and Transmitter Address (TA)

These fields change according to which part of the ping is. The receiver address is always the address of the replier in a request message and the requester during a reply message. The case of the transmitter address is the opposite: it's always the address of the requester during a request message and the replier during a reply message.

-Basic Service Set Identifier (BSSID):

- Broadcast (ff:ff:ff:ff:ff:ff)

-Address 4:

The messages do not include this field on their structure.

2.1 RSU Commando doing ping to OBU Classic

Doing ping from RSU Commando (192.168.3.44) to OBU Classic (192.168.3.43). Captured in RSU Commando.

2.1.1 ICMP echo (ping) request

```
MAC Header: [88 00|00 00|00 f0 84 2c 6b da|00 26 ad 05 03 e7|
                ff ff ff ff ff ff|a0 0d|20 00]
```

IEEE 802.11 QoS Data, Flags: .....

Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8800
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x00
.... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.0.. .... = Protected flag: Data is not protected
0... .... = Order flag: Not strictly ordered
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: 00:f0:84:2c:6b:da (00:f0:84:2c:6b:da)
Transmitter address: Arada_05:03:e7 (00:26:ad:05:03:e7)
Destination address: 00:f0:84:2c:6b:da (00:f0:84:2c:6b:da)
Source address: Arada_05:03:e7 (00:26:ad:05:03:e7)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
.... 0000 = Fragment number: 0
0000 1101 1010 .... = Sequence number: 218
Qos Control: 0x0020
.... 0000 = TID: 0
[.... .... .000 = Priority: Best Effort (Best Effort) (0)]
....0 .... = EOSP: Service period
.... .01. .... = Ack Policy: No Ack (0x1)
.... 0... .... = Payload Type: MSDU

0000 0000 .... = TXOP Duration Requested: 0 (no TXOP requested)

2.1.2 ICMP echo (ping) reply

```
MAC Header: [88 00|00 00|00 26 ad 05 03 e7|00 f0 84 2c 6b da|
                ff ff ff ff ff ff|90 0f|20 00]
```

IEEE 802.11 QoS Data, Flags: .....

Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8800
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x00
.... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.0.. .... = Protected flag: Data is not protected
0... .... = Order flag: Not strictly ordered
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Arada_05:03:e7 (00:26:ad:05:03:e7)
Transmitter address: 00:f0:84:2c:6b:da (00:f0:84:2c:6b:da)
Destination address: Arada_05:03:e7 (00:26:ad:05:03:e7)
Source address: 00:f0:84:2c:6b:da (00:f0:84:2c:6b:da)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
.... 0000 = Fragment number: 0
0000 1111 1001 .... = Sequence number: 249
Qos Control: 0x0020
.... 0000 = TID: 0
[.... .... .000 = Priority: Best Effort (Best Effort) (0)]
....0 .... = EOSP: Service period
.... .01. .... = Ack Policy: No Ack (0x1)
.... 0... .... = Payload Type: MSDU
0000 0000 .... = TXOP Duration Requested: 0 (no TXOP requested)

2.2 RSU Commando doing ipv6 ping to OBU Classic

Doing pingv6 from RSU Commando (192.168.3.44) to OBU Classic (192.168.3.43). Captured in RSU Commando.

2.2.1 ICMPv6 echo (ping) request

```
MAC Header: [88 00|00 00| 00 bf e9 b3 4c 4e|00 26 ad 05 03 e7|
                ff ff ff ff ff ff|00 01|20 00]
```

IEEE 802.11 QoS Data, Flags: .....

Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8800
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x00
.... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.0.. .... = Protected flag: Data is not protected
0... .... = Order flag: Not strictly ordered
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: MS-NLB-VirtServer_e9:b3:4c:4e (00:bf:e9:b3:4c:4e)
Transmitter address: Arada_05:03:e7 (00:26:ad:05:03:e7)
Destination address: MS-NLB-VirtServer_e9:b3:4c:4e (00:bf:e9:b3:4c:4e)
Source address: Arada_05:03:e7 (00:26:ad:05:03:e7)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
.... 0000 = Fragment number: 0
0000 0001 0000 .... = Sequence number: 16
Qos Control: 0x0020
.... 0000 = TID: 0
[.... .... .000 = Priority: Best Effort (Best Effort) (0)]
....0 .... = EOSP: Service period
.... .01. .... = Ack Policy: No Ack (0x1)
.... 0... .... = Payload Type: MSDU
0000 0000 .... = TXOP Duration Requested: 0 (no TXOP requested)

2.2.2 ICMPv6 echo (ping) reply

IEEE 802.11 QoS Data, Flags: .....
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8800
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x00
.... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.0.. .... = Protected flag: Data is not protected
0... .... = Order flag: Not strictly ordered
.000 0000 0011 1100 = Duration: 60 microseconds
Receiver address: Arada_05:03:e7 (00:26:ad:05:03:e7)
Transmitter address: MS-NLB-VirtServer_e9:b3:4c:4e (00:bf:e9:b3:4c:4e)
Destination address: Arada_05:03:e7 (00:26:ad:05:03:e7)
Source address: MS-NLB-VirtServer_e9:b3:4c:4e (00:bf:e9:b3:4c:4e)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
.... 0000 = Fragment number: 0
0000 0001 0001 .... = Sequence number: 17
Qos Control: 0x0020
.... 0000 = TID: 0
[.... .... .000 = Priority: Best Effort (Best Effort) (0)]
....0 .... = EOSP: Service period
.... .01. .... = Ack Policy: No Ack (0x1)
.... 0... .... = Payload Type: MSDU
0000 0000 .... = TXOP Duration Requested: 0 (no TXOP requested)