IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| On A-MSDU addressing | | | | |
| Date: 2021-10-01 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Mark RISON | Samsung Cambridge Solution Centre | SJH, CB4 0DS, U.K. | +44 1223 434600 | at samsung (a global commercial entity) I'm the letter emme then dot rison |
| Mathy Vanhoef | KU Leuven / NYUAD | Leuven, Belgium |  | mathy.vanhoef at nyu.edu or at kuleuven.be |
| Mark Hamilton | Ruckus/CommScope | 350 W Java Drive  Sunnyvale, CA 94089 | +1-303-818-8472 | mark.hamilton@commscope.com |
| Jouni Malinen | Qualcomm, Inc. |  |  | jouni@qca.qualcomm.com |

Abstract

This submission discusses the addresses present in the context of A-MSDUs, and constraints thereon.

Green highlight indicates material agreed to in the group, yellow material to be discussed, red material rejected by the group and cyan material not to be overlooked. The “Final” view should be selected in Word.

Discussion:

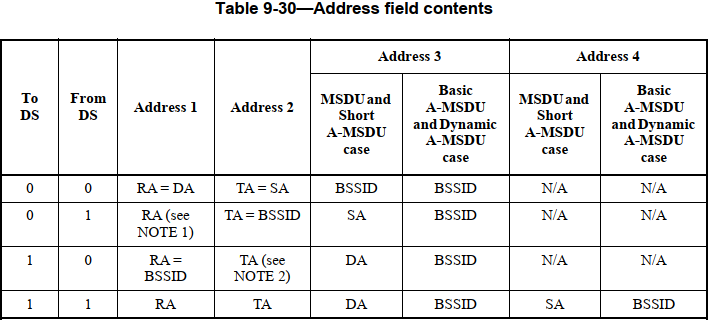
The MAC header addresses for an MPDU containing an A-MSDU are relatively well-defined:

In 10.11 A-MSDU operation:

In non-GLK transmissions, the Address 1 field in an MPDU carrying an A-MSDU shall be set to an individual address or to the GCR concealment address. In GLK transmissions by an AP, the Address 1 field may be set to a SYNRA. In GLK transmissions by a non-AP STA, the Address 1 field shall be set to an individual address.

The only thing that’s vague is the implicit restriction for GLK transmissions by an AP on the Address 1 field not being a group address other than a SYNRA. GLK STAs never send group addressed frames in the literal sense. The only time a GLK STA will send a group addressed frame is if it is an AP and the bridge controlling it has indicated that a frame should be sent to multiple peers, and when that happens the bridge will provide a specific list of those peers (because it is doing routing/loop-detection/pruning/etc.). That specific list is targeted with a specific SYNRA address, and that’s what the GLK AP will use. The SYNRA is logically a list of AIDs of the peers that should receive the frame, and the other peers will ignore it.

In 9.3.2.1.2 Address and BSSID fields:



However, there is really no reason to disallow a group-addressed MPDU containing an A-MSDU, as long as the MSDUs therein are also group-addressed (otherwise individually addressed packets are being sent as group addressed packets, which is suspect from a security viewpoint, given the differing security contexts of PTKs and GTKs). It is believed that some non-GCR and non-GLK implementations in the field already send such A-MSDUs. Note the existing GCR/GLK exemptions suggest that there is no issue with this per se.

So basically you can have unicast MSDUs in A-MSDU in unicast MPDU, groupcast MSDUs in A-MSDU in unicast MPDU (inc. for DMS and GLK, but not just those) or groupcast MSDUs in A-MSDU in group-addressed MPDU (inc. for non-GLK GCR and for GLK SYNRA, but not just that); just not unicast MSDUs in A-MSDU in group-addressed MPDU (except GLK, which might use this scenario -- this allows malicious insider attacks because everyone knows the GTK, so a malicious insider can forge a group-addressed MPDU containing a unicast MSDU that appears to come from someone else). A SYNRA is only used when transmitting A-MSDUs inside 4AFs, not with A-MSDUs inside 3AFs (see 10.65).

The A-MSDU subframe addresses are much less well-defined, and prompt various questions:

In 10.11 A-MSDU operation:

An A-MSDU contains only MSDUs whose DA parameter values map to a single RA value (see 9.3.2.2 (Aggregate MSDU (A-MSDU) format)). An A-MSDU contains only MSDUs whose SA parameter values map to a single TA value (see 9.3.2.2 (Aggregate MSDU (A-MSDU) format)).

What does “map to a single RA/TA value” (and similarly “map to the same RA/TA” and “map to the same Address 1/2 parameter values” below) mean? Can a set of group DAs “map to a single RA value”? Does the interpretation depend on whether the receiver is an AP or a non-AP STA in an infrastructure BSS or a peer TDLS STA or an IBSS/PBSS/MBSS STA?

In 9.3.2.2.2 Basic A-MSDU subframe format:

An A-MSDU contains only MSDUs whose DA and SA parameter values map to the same receiver address (RA) and transmitter address (TA) values. The rules for determining RA and TA are independent of whether the frame body carries an A-MSDU.

NOTE 1—It is possible to have different DA and SA parameter values in A-MSDU subframe headers of the same A-MSDU as long as they all map to the same Address 1 and Address 2 parameter values.

NOTE 3—It is possible to have different Mesh DA, Mesh SA, and Mesh Control in subframe headers of the same A-MSDU as long as they all map to the same Address 1 and Address 2 values.

What is “The rules for determining RA and TA are independent of whether the frame body carries an A-MSDU.” trying to say? Is it trying to say that the RA and TA are always the immediate 802.11 receiver(s) and transmitter addresses in all cases?

In 9.3.2.1.2 Address and BSSID fields:

NOTE 1—Address 1 field of a frame with To DS equal to 0 and From DS equal to 1 is equal to the DA, except when an individually addressed A-MSDU frame is used in DMS and S1G relay, in which case, the destination address of the frame is included in the DA field of the A-MSDU subframe (see 11.21.16 (Group addressed transmission service) and 10.54 (S1G relay operation)).

NOTE 2—Address 2 field of a frame with To DS equal to 1 and From DS equal to 0 is equal to the SA, except when an individually addressed A-MSDU frame is used in S1G relay, in which case, the source address of the frame is included in the SA field of the A-MSDU subframe (see 10.54 (S1G relay operation)).

This does seem to clarify the restrictions, but it’s not clear that there is normative text to back this up.

Really, the position needs to be set out normatively. The following is proposed, for an MPDU containing an A-MSDU:

* In a frame from an AP, and between IBSS, PBSS or mesh STAs, allow the RA in the MAC header to be a group address (not currently permitted except for GCR), but only if the DAs in all A-MSDU subframe headers are group addresses.
* In a frame not to an AP, including between IBSS STAs, but excluding between TDLS peer STAs, if the RA in the MAC header is an individual address, allow DAs in the A-MSDU subframe headers to be group addresses. Otherwise require the DAs to be the same as the RA in the MAC header. [In a frame to an AP the DAs can be any individual or group address.]
* In a frame not from an AP, including between TDLS peer STAs and between IBSS STAs, require all the SAs in the A-MSDU subframe headers to be the same as the (non-bandwidth-signalling) TA in the MAC header. [In a frame from an AP the SAs can be any individual address.]
* Except for GLK, DMG relay and S1G relay, where the SA and DA can be anything. [S1G: is this OK? This is per Figure 10-112—S1G relay architecture. But can the RA be a group address, when sent by an S1G relay AP? Assuming DMG relay is the same as S1G relay]

A statement should be added to indicate that the whole A-MSDU should be dropped if any A-MSDU subframe does not meet these conditions, since as described in <https://papers.mathyvanhoef.com/usenix2021.pdf> in §3, not doing so opens up vulnerabilities when SPP A-MSDUs are not used (see also [07/0397](https://mentor.ieee.org/802.11/dcn/07/11-07-0397-07-000n-msdu-protection.doc) on 11n/D3.0).

Other stuff for reference:

In 9.3.2.1.2 Address and BSSID fields:

The DA field contains the destination of the MSDU (or fragment thereof) or A-MSDU in the Frame Body field.

NOTE 1—A SYNRA is never the DA. When a GLK AP uses a SYNRA as the RA, the actual DA is carried in another field. See 10.65 (Addressing of GLK Data frame transmission).

The SA field contains the address of the MAC entity that initiated the MSDU (or fragment thereof) or A-MSDU in the Frame Body field.

When a Data frame carries an MSDU (or fragment thereof), the DA and SA values related to that MSDU are carried in the Address 1, Address 2, Address 3, and Address 4 fields (according to the setting of the To DS and From DS subfields) as defined in Table 9-30 (Address field contents).

When a Data frame carries a basic A-MSDU, the DA and SA values related to each MSDU carried by the A-MSDU are carried within the A-MSDU subframe header. Zero, one, or both of these fields are present in the Address 1 and Address 2 fields as indicated in Table 9-30 (Address field contents).

The RA field is the individual address of the STA that is the immediate intended receiver of the frame or the group address of the STAs that are the immediate intended receivers of the frame.

When a GLK AP Data frame is sent with a four-address MAC header with a groupcast RA, the RA is a SYNRA (see 10.65 (Addressing of GLK Data frame transmission)). A SYNRA is also used when the DA is not known by the corresponding IEEE 802.1Q bridge.

In 10.2.7 MAC data service:

A MAC not contained within an S1G relay performs address filtering on the Address 1 field in each MPDU contained in a PPDU and, for non-GLK non-AP STAs, on the DA of each MSDU within an A-MSDU. In the case of a non-GLK STA receiver, when the Address 1 field or DA field contains a group address, address filtering is performed by comparing the value in the Address 1 field or DA field to all values in the dot11GroupAddressesTable, and the STA also validates the BSSID to verify either that the group addressed frame originated from a STA in the BSS of which the receiving STA is a member, or that it contains the wildcard BSSID value, indicating a Data frame sent outside the context of a BSS (dot11OCBActivated is true in the transmitting STA). Address 1 filtering is as specified in 10.65 (Addressing of GLK Data frame transmission) when Address 1 is a SYNRA. A GLK AP does not perform any DA filtering for MPDUs received over a non-general link; all MSDUs so received are passed to the DS for further processing. A GLK STA does not perform DA filtering for MPDUs received over a general link; all MSDUs so received are passed to the GLK convergence function and from there to the bridge for further processing.

If the Address 1 field of an MPDU carrying an A-MSDU does not match any address at a receiving STA, then the entire A-MSDU is discarded.

Proposed changes:

In 10.11 A-MSDU operation:

An A-MSDU contains only MSDUs whose DA parameter values map to a single RA field value ~~(see 9.3.2.2 (Aggregate MSDU (A-MSDU) format)). An A-MSDU contains only MSDUs~~and whose SA parameter values map to a single TA field value (see 9.3.2.2 (Aggregate MSDU (A-MSDU) format)).

Specifically, for a frame containing an A-MSDU:

* The RA may be a group address if all of the following conditions are met:
  + the frame is from an AP or PCP, or between IBSS, PBSS or mesh STAs
  + the DAs in all A-MSDU subframe headers are group addresses, or the frame is transmitted under GLK
  + the frame is not transmitted under GLK, or the RA is a SYNRA

Otherwise, the RA shall be an individual address.

NOTE—STAs conformant with a previous revision of this standard might not accept a group addressed frame containing an A-MSDU, outside the context of a GCR concealment address or a GLK SYNRA, where supported.

* Each DA shall be the RA or (if not between TDLS peer STAs) a group address if none of the following conditions is met:
  + the frame is to an AP or associated PCP
  + the frame is transmitted under DMG relay or S1G relay operation
  + the frame is from a GLK STA
  + the frame is from a mesh STA

Otherwise, there is no restriction on each DA, except that the DA in the first A-MSDU subframe header shall not be AA-AA-03-00-00-00.

NOTE—The address AA-AA-03-00-00-00 is that which results from an attack in which an encrypted QoS Data frame not containing an A-MSDU (whose unencrypted frame body therefore starts with an LLC header followed by a SNAP header constructed per IETF RFC 1042) has the A-MSDU Present subfield changed to 1 by an attacker to cause it to appear to be a PP A-MSDU with multiple MSDUs (each preceded by an A-MSDU subframe header, which starts with the DA).

* Each SA shall be the nonbandwidth signaling TA if none of the following conditions is met:
  + the frame is from an AP or PCP
  + the frame is transmitted under DMG relay or S1G relay operation
  + the frame is from a GLK STA
  + the frame is from a mesh STA

Otherwise, each SA shall be an individual address.

NOTE 1—The DA and SA are contained in the Mesh DA and Mesh SA fields respectively in the case of Basic A-MSDU subframes transmitted in mesh Data frames, and in the DA and SA subfields respectively, where present, in other A-MSDU subframes.

NOTE 2—Frames not to an AP or associated PCP and frames not from an AP or PCP include frames transmitted between TDLS peer STAs or between IBSS, non-PCP PBSS or mesh STAs.

~~In non-GLK transmissions, the Address 1 field in an MPDU carrying an A-MSDU shall be set to an individual address or to the GCR concealment address. In GLK transmissions by an AP, the Address 1 field may be set to a SYNRA. In GLK transmissions by a non-AP STA, the Address 1 field shall be set to an individual address.~~

A STA that receives a frame containing an A-MSDU that violates these rules should discard it.666

666The check on the DA in the first A-MSDU subframe header is important to defend against attacks from malicious outsiders when SPP A-MSDUs are not being used. The other checks on the DAs and the checks on the SAs are important to defend against impersonation attacks from malicious insiders (which means there is no protection against malicious APs or PCPs, DMG or S1G relays, GLK STAs and mesh STAs). The lack of checks on the SA and DA in the case of mesh and relay operation presents an attack surface that is outside the scope of remediation in this standard. In the case of GLK, use of a SYNRA for an individually addressed MSDU with multiple links indicated in the station vector parameter also presents such an attack surface, which can be avoided by transmitting multiple individually addressed MPDUs instead (see 10.65).

In 9.3.2.1.2 Address and BSSID fields:

**Table 9-30—Address field contents for Data frames transmitted by nonmesh STAs**

NOTE 1—The Address 1 field of a frame with the To DS subfield equal to 0 and the From DS subfield equal to 1 is equal to the DA, except when a~~n individually addressed~~ frame containing an A-MSDU ~~frame~~ is used ~~in~~ (for DMS , DMG relay ~~and~~or S1G relay the frame is individually addressed; for GCR it is (group) addressed to the GCR concealment address), in which case~~,~~ the destination address of the ~~frame~~MSDU is ~~included~~indicated in the DA or Mesh DA field of the A-MSDU subframe (see 11.21.16 (Group addressed transmission service) ~~and~~, 10.11, 10.45 (DMG relay operation), 10.54 (S1G relay operation) and 10.65).

NOTE 2—The Address 2 field of a frame with the To DS subfield equal to 1 and the From DS subfield equal to 0 is equal to the SA, except when an individually addressed frame containing an A-MSDU ~~frame~~ is used in GLK, DMG relay or S1G relay, in which case~~,~~ the source address of the ~~frame~~MSDU is ~~included~~indicated in the SA or Mesh SA field of the A-MSDU subframe (see 10.11, 10.45 (DMG relay operation), 10.54 (S1G relay operation) and 10.65).

In 9.3.5 Frame addressing in an MBSS:

**Table 9-47—~~Valid a~~Address field ~~usage~~contents for ~~M~~mesh Data and Multihop Action frames**

In 9.3.2.2.1 General add at the end (the change tracking is w.r.t. material in 9.3.2.2.2 in D0.0; all this text needs to be added, except text with strikethrough):

An A-MSDU contains only MSDUs whose DA and SA parameter values (in the MA-UNITDATA.request primitive) map to the same receiver address (RA) and same transmitter address (TA) field values (see 10.11), respectively. ~~The rules for determining RA and TA are independent of whether the frame body carries an A-MSDU.~~

NOTE 1—The Address 1 (RA) and Address 2 (TA) fields in a Data frame identify the STA(s) receiving the frame and the STA transmitting the frame respectively, whether or not the frame body carries an A-MSDU and, if it does, whether or not the source or destination of the MSDUs are those STAs.

~~NOTE 1—It is possible to have different DA and SA parameter values in A-MSDU subframe headers of the same A-MSDU as long as they all map to the same Address 1 and Address 2 parameter values.~~

In 9.3.2.2.2 Basic A-MSDU subframe format:

The structure of a Basic A-MSDU subframe when not in a mesh Data frame is shown in Figure 9-69 (Basic A-MSDU subframe structure).

**Figure 9-69—Basic A-MSDU subframe structure when not in a mesh Data frame**

~~When mesh Data frames are aggregated, the A-MSDU subframe header includes Mesh DA, Mesh SA, Length, and Mesh Control.~~ The structure of a Basic A-MSDU subframe ~~structure for M~~when in a mesh Data frame is ~~defined~~shown in Figure 9-70 (A-MSDU subframe structure for Mesh Data).

**Figure 9-70—Basic A-MSDU subframe structure ~~for M~~when in a mesh Data frame**

~~NOTE 3—It is possible to have different Mesh DA, Mesh SA, and Mesh Control in subframe headers of the same A-MSDU as long as they all map to the same Address 1 and Address 2 values.~~

**References:**

802.11me/D0.0

<https://papers.mathyvanhoef.com/usenix2021.pdf> , with permanent bibliographical information taken from <https://www.usenix.org/conference/usenixsecurity21/presentation/vanhoef> :

@inproceedings {263830,  
author = {Mathy Vanhoef},  
title = {Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation},  
booktitle = {30th {USENIX} Security Symposium ({USENIX} Security 21)},  
year = {2021},  
isbn = {978-1-939133-24-3},  
pages = {161--178},  
url = {https://www.usenix.org/conference/usenixsecurity21/presentation/vanhoef},  
publisher = {{USENIX} Association},  
month = aug,  
}