IEEE 802 Privacy Threat Analysis

Brian Weis, Jerome Henry
Cisco Systems
01/15/17

1 Introduction

IEEE 802 standards are a set of protocols that provide network communication for frame-based data networks. Various protocol frame formats and data fields provide opportunity for active and passive attackers to observe or deduce Personally identifiable information (PII). The IEEE P802E standard will provide privacy recommendations related to IEEE 802 standards.

Note Well: This is a DRAFT threat analysis, subject to change as a result of further investigation and corrections due to the review process.

2 Scope

The scope of PII in P802E is defined to be “PII in our standards, PII that is directly derived from our standards (e.g. IP derived from MAC), and PII in other standards that we use”. Although PII is considered “personal”, PII is not limited to information about a person. PII extends to information about devices that a person uses (e.g., laptop, cellphone), which is termed Personal Correlated Information (PCI). However, attributes of a device only represent PII when relevant. For example, a MAC address may be considered PII when it is associated with a person, but not when it is associated with an intermediate network device.

[Clarify: not miscellenous defects in the protocol … certain id’ing info is explicitely for communicating from user to sp or to id a service instance and is not nec. Visiable at some points on route.]

3 Terms

The following terms are used in this document. Several are adapted from security terms defined in [RFC4949].

- **Active Attacker**. An adversary who emits frames as part of their attack in order to cause a target to emit PII.
- **Adversary**. A threat agent who is taking steps to fingerprint one or more targets. An adversary is assumed to have the capabilities of the Most Powerful Attacker Model [KMM]. In the context of this threat analysis the adversary is assumed to have the

Deleted: obtain PII

Deleted: from

capability to observe and manipulate Target and Respondent frames anywhere in a bridged network.

- **Fingerprint**.
- **Passive Attacker**. An adversary who observes frames but does not emit frames as part of the attack. A passive attacker is assumed to have full visibility to all network frames, as well as the ability to store copies of network frames for long-term analysis.
- **Personally Identifiable Information (PII)**. Any data that identifies an individual or from which identity or contact information of an individual can be derived.
- **Personal Correlated Information (PCI)**. Data gathered about a person by observing devices associated with that person.[Personal Device]
- **Respondent**. The network device to which a target is intending to communicate. In other words, the Target and Respondent MAC addresses comprise the Source MAC address and Destination MAC address on the frame (in either order). The term is used without regard to whether the network device actually responds to the target.
- **Target**. The person (or frames from a machine associated with a person) containing PII in which an adversary wishes to obtain.[fingerprinting]
- **Threat**. A potential for violation of privacy, the unauthorized disclosure of PII.
- **Threat Action**. The unauthorized disclosure of PII.
- **Threat Agent**. An entity that performs a threat action.
- **Universal Address**. A globally unique MAC address (see Clause 8.2 of [IEEE802]).

Formatted: Font:Not Bold

Deleted: ing

4 Goals of Adversaries

A number of actors are considered to be interested in exfilterating (i.e., observing and capturing) PII from IEEE 802 frames with various goals. Possible motivations of these actors include:

- **Surveillance**. Passive fingerprinting by adversaries, where the goal is to observe where/when a target has connected to a network. [for example] When the adversary can collect PII across many network links, this is referred to as Pervasive Surveillance. For a Pervasive Surveillance threat analysis, see RFC 7624 [RFC7424].
- **Probing**. Sourcing of packets sent to a target or it's respondent in order to cause it to reveal PII.[Tools?]
- **Modification**. Changing frames sent to/from a target in order to cause it to reveal PII.

Deleted: collection of PII

Deleted: replicate the

Deleted: ion

Deleted: of

5 IEEE 802 PII

This clause lists identified PII within the scope defined in Clause 2. Privacy threats to the PII are discussed. Mitigations to the threats are not addressed in this document.

5.1 IEEE 802 Common fields

All IEEE 802 protocol frames begin with a Destination MAC Address (DA) and a Source MAC Address (SA) (for example, see Figure 5). In order to simplify the analysis, these are considered independently and apply to all use cases. The analysis is written as if a Target is initiating frames, where the SA might possibly be PII. (Of course, for frames directed to the Target the DA would be considered PII.)

An SA is considered PII if it is associated with a Target (I.e., is considered a "personal device" as defined by the current P802E draft). Not every device emitting frames is considered a target. For example, a bridge within a network is not generally associated with a person [shared service device], and therefore would not be considered a Target. However, the SA associated with a residential gateway network device [example] is very much associated with its subscriber (i.e., a user or household of users), and thus would be considered a Target.

Threats:

1. When the target MAC address is a universal address, correlation of Target MAC address across multiple networks in time and space is possible. This includes cases where the MAC address is used as an SA or DA on the frame, or is included in a well-known

network header (e.g., an encapsulated Ethernet header, IEEE 802.1Q I-TAG, or in an IPv6 header).

2. Correlation of any Target MAC address can be used as an aid to
    a. Track location of the Target MAC address when it is mobile.
    b. Collect frames to and from the Target MAC address, to be used for further analysis. Further analysis might include the identification of MAC addresses that appear to be associated with an individual, or once it is associated with an individual to evaluate it to determine which individual.

Deleted: (?)

Correlation of a Target MAC address is not always a threat to privacy. An individual may authorize the correlation for his/her own benefit by, for example, explicitly “opting in” to the correlation after having been offered special treatment by the network owner (e.g., a business). However, when the correlation is not authorized it may be considered an attack.

5.2 IEEE 802.1

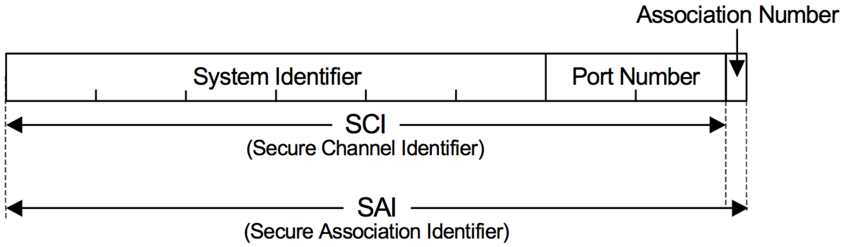
The following IEEE 802.1 protocol elements and management frames have been evaluated for privacy considerations.[1]

5.2.1 Encapsulated MAC address

Some IEEE 802.1 protocols include an encapsulated MAC address: IEEE 802.1Q Congestion Notification Message PDU, IEEE 802.1Q SRP StreamID, IEEE 802.1Q VSIID, IEEE 802.1AB Chassis ID, IEEE 802.1AB Port ID, IEEE 802.1X EAPOL-MKA SCI, and IEEE 802.1AE SecTag (System Identifier in Figure 1). Threats to MAC addresses listed in Clause 5.1 apply to these MAC addresses.

Additionally, a bridge may be considered to be Personal Correlated Information if it is located at a network edge associated with people (e.g., a residential gateway). The Bridge Address associated with the bridge is required to be a universal address, and it may be used to locate host addresses (e.g., those embedded in a Stream Identifier).

Figure 1. IEEE 802.1AE System Channel Identifier



5.2.2 Priority Code Point

A Priority Code Point (PCP) is found in several IEEE 802.1Q protocol elements: VLAN Tag (see Figure 2), Congestion Notification Message PDU, and the MSRP Structure. The PCP typically marks frames that should be prioritized because they have particular latency requirements (such as voice or video frames). In some cases, an adversary is looking for certain classes of traffic or endpoints that emit those classes of traffic

[1] This list does not include SNMP or Netconf, both of which are used to manage IEEE 802 devices. These are IP protocols rather than IEEE 802 management frames and their privacy threats are out of scope.

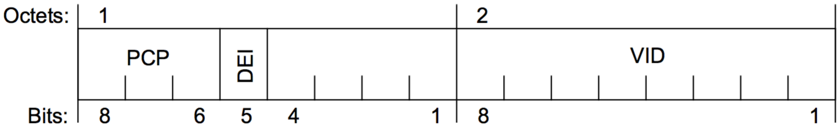
Threats:

1. Classes of Targets may be identified based on the PCP, if the adversary is aware of the PCP mappings. Some mappings are de-facto or actual standards. Identification of voice and video traffic are well known and can aid in the identification of classes of Targets.

5.2.3 VLAN Identifier (IEEE 802.1Q)

A VLAN Tag (Figure 2) is used within networks to mark a frame for a particular priority and/or provide an identifier used to classify the frame. A VLAN Identifier (VID) is often used to separate different types of traffic, such as traffic from different organizations or individuals with different roles in the organization. [List them]

Figure 2. VLAN TCI Format



Threats:

1. Classes of Targets (e.g., Organization, Role) may be identified based on the VID value, if the adversary is aware of the VID mappings. Such mappings are likely to be network specific, and less likely to be obvious to the adversary unless correlated with other traffic analysis. However, the adversary may ascertain the mappings with enough correlation analysis.

5.2.4 Congestion Notification Tag (IEEE 802.1Q)

An end station may add a Congestion Notification Tag (CN-TAG) to every frame it transmits from a congestion-controlled flow, which contains Flow Identifier (Clause 33.2.1 of [IEEE802.1Q]). The format of the Flow Identifier is not specified, but in order to be useful is likely to be persistent for a flow.

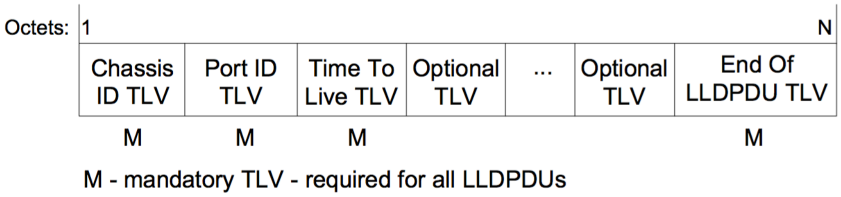
Threats:

1. A particular flow between a Target and Respondent may be identified based on a Flow Identifier, without the Adversary interpreting the value of the tag.
2. An Adversary with knowledge of how to interpret the tag may be able to correlate flows between a Target and one or more Respondents.

5.2.5 LLDP (IEEE 802.1AB)

Link Layer Discovery Protocol (LLDP) frames deliver information about a station as TLVs, which may be valuable to other peers on a network segment. The format of an LLDPDU is shown in Figure 8-1 of IEEE 802.1AB, reproduced as Figure 3.

Figure 3. LLDP PDU



LLDP frames are typically emitted by network infrastructure components, but can are also emitted from other non-consumer types of endpoint devices (e.g., PoE connected luminaires), and could be emitted from consumer devices.

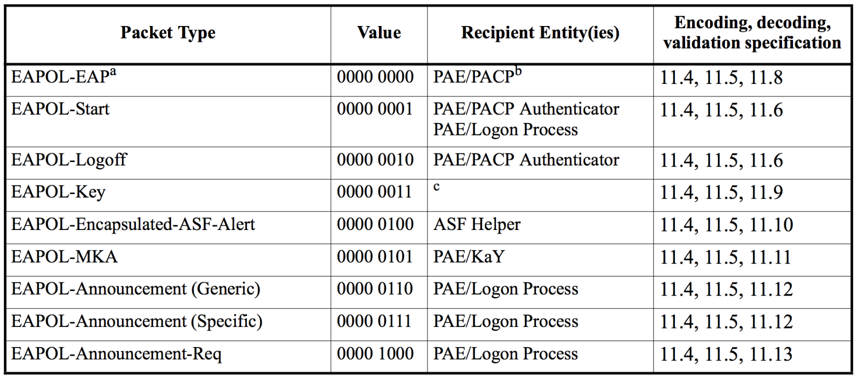
Threats:

1. A network address (MAC address or IP address) in a network address TLV can be used to identify a target.
2. A system name subTLV can bused used to identify a target by domain name.
3. A System Capabilities TLV can identify a class of target (e.g., Telephone, DOCSIS cable device) can be Personal Correlated Information.
4. Organizationally Specific TLVs may be defined to contain PII or Personal Correlated Information.

5.2.6 Port-Based Network Access Control (IEEE 802.1X)

Several types of management frames can be represented as EAP over LAN (EAPOL) frames, and are itemized in Table 11-3 of IEEE 802.1X, reproduced as Figure 4.

Figure 4. EAPOL Types



Packet Type	Value	Recipient Entity(ies)	Encoding, decoding, validation specification
EAPOL-EAP[a]	0000 0000	PAE/PACP[b]	11.4, 11.5, 11.8
EAPOL-Start	0000 0001	PAE/PACP Authenticator PAE/Logon Process	11.4, 11.5, 11.6
EAPOL-Logoff	0000 0010	PAE/PACP Authenticator	11.4, 11.5, 11.6
EAPOL-Key	0000 0011	[c]	11.4, 11.5, 11.9
EAPOL-Encapsulated-ASF-Alert	0000 0100	ASF Helper	11.4, 11.5, 11.10
EAPOL-MKA	0000 0101	PAE/KaY	11.4, 11.5, 11.11
EAPOL-Announcement (Generic)	0000 0110	PAE/Logon Process	11.4, 11.5, 11.12
EAPOL-Announcement (Specific)	0000 0111	PAE/Logon Process	11.4, 11.5, 11.12
EAPOL-Announcement-Req	0000 1000	PAE/Logon Process	11.4, 11.5, 11.13

Message types that could contain PII include:

- EAPOL-EAP. Provides an IEEE 802 framing around Extensible Authentication Protocol (EAP) [RFC3748] frames, which allow a station to authenticate itself to the network and be admitted [reword?]. Credentials can be user credentials, host credentials, or both.
- EAPOL-MKA. MACsec Key Agreement (MKA) determines session keys for MACsec. MKA identities ("Member Identifier") are not persistent. They also carry a MACsec SCI associated with the member.
- EAPOL Announcements. Announcements include capabilities for the station, including information describing a cached Secure Connectivity Association Key (CAK).

Deleted: access

Threats:

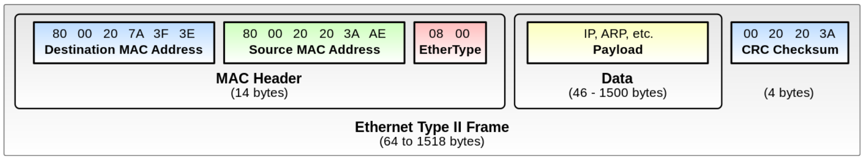
1. A passive adversary between the target and EAP authenticator can observe any information that an EAP method passes without confidentiality protection. This can be mitigated by using a "tunneled EAP" method (e.g., TEAP (RFC 7170)).
2. An active adversary between the target and EAP authenticator may be able to spoof a legitimate respondent in an EAP method to the point where the target presents its identity (e.g., the subject name in a client certificate).
3. A passive adversary in the broadcast domain of the target can observe Announcement data, and identify or deduce the class of target. The KMD or NID may

identity the organization; the set of announcement data presented may indicate the type of device.

5.3 IEEE 802.3

An IEEE 802.3 frame comprises an Ethernet frame, usually sent over an electrical or optical link. A high level representation is shown in Figure 5.

Figure 5. IEEE 802.3 frame[2]



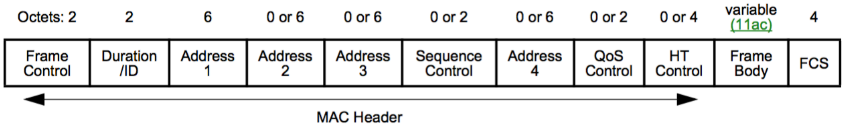
TBD

5.4 IEEE 802.11

5.4.1 IEEE 802.11 Common fields

In addition to the SA and DA MAC addresses specified in section 5.1, IEEE 802.11 uses the Transmitter Address (TA) and the Receiver Address (RA), to allow relay of frames through an intermediate device. The TA may be considered a target when associated with a personal device. Similarly, the RA may be considered a target when associated with a personal device.

All 802.11 frames include a common header displayed below.

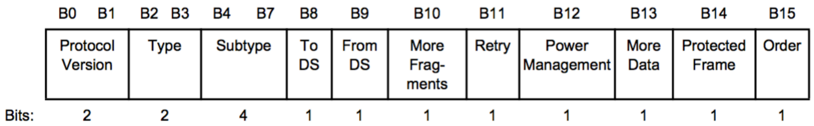


Octets: 2	2	6	0 or 6	0 or 6	0 or 2	0 or 6	0 or 2	0 or 4	variable (11ac)	4
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

Most fields are mandatory. Some fields, like QoS control, HT control and VHT (11ac) are optional and present only if the transmitter supports the relevant standard amendments. As such, these optional fields may be used to identify a specific device.

The Frame Control field is present in all IEEE 802.11 frames. Its structure is specific when 802.11 operates over the 60 GHz band, and is as follows for all other frequency bands:

[2] Image from https://en.wikipedia.org/wiki/Ethernet_frame#/media/File:Ethernet_Type_II_Frame_format.svg, and is marked as being in the Public Domain.



	B0 B1	B2 B3	B4 B7	B8	B9	B10	B11	B12	B13	B14	B15
	Protocol Version	Type	Subtype	To DS	From DS	More Frag-ments	Retry	Power Management	More Data	Protected Frame	Order
Bits:	2	2	4	1	1	1	1	1	1	1	1

Several sub-fields may be used to identify a transmitter:

- More Fragments: fragmenting is optional. Some driver implementations never use fragments, some others commonly do. This field can be used to fingerprint a transmitter.
- Power Management: APs usually do not sleep. Some client stations always implement power management, some others implement power management based on mode (connected to power source or not), some client stations never implement power management. Observing this bit and its pattern for a given source can be used to fingerprint a transmitter.

5.4.2 IEEE 802.11 Beacon frames

The following information elements are not generally implemented, and have not been analyzed: Frequency-Hopping (FH) Parameter Set; Point Coordination Function (PCF);

The beacon is sent by the access point. In many networks, information contained in the beacon will only identify the wireless infrastructure and will not contain useful PII. However, beacon information may be correlated to PII when the access point is associated to an individual, for example when implemented in a home or small store, a mifi, or in a peer to peer (e.g. IBSS) topology. Beacon frames advertises information about the network. Multiple fields are optional or contain optional elements destined to specify what features are supported. An adversary can observe the beacons and use the observed fields to fingerprint the transmitter. In particular, an adversary can use the beacon Timestamp, Beacon interval, Capability field, SSID, Supported rates and BSS Membership Selector, DSSS Parameter set, IBSS Parameter set, TIM, Power Constraint, Channel Switch, Quiet Element, IBSS DFS Element, TPC Report IE, ERP element , Extended Supported rates and BSS Membership Selector, RSN IE, BSS Load Element, EDCA Parameter Set, QOS Capability IE, AP Channel Report IE, BSS Average Access Delay, Antenna IE, BSS Available Admission Capacity, BSS AC Access Delay, Measurement Pilot Transmission, MBSSID IE, RM Enabled Capabilities, Mobility Domain IE, DSE registered location, Extended Channel Switch Announcement element, Supported Operating Classes element, HT Capabilities, HT Operations, 20/40 BSS Coexistence element, Overlapping BSS Scan Parameters element, Extended Capabilities IE, FMS Descriptor IE, QoS Traffic Capability, Time Advertisement IE, Internetworking IE, Advertisement Protocol IE, Roaming Consortium IE, Emergency Alert

Identifier, Mesh ID IE, Mesh Configuration IE, Mesh Awake Window IE, Beacon Timing IE, MCCAOP Advertisement Overview IE and MCCAOP Advertisement IE, and / or Mesh Channel Switch Parameters IE to fingerprint the transmitter.

An adversary can also emit a TPC request and observe the TPC response from the AP in the subsequent beacon and use this information to fingerprint the transmitter and its location.

Additionally, an adversary can emit a beacon containing an SSID string identical to that of another system. Attacker then attracts targets to the attacker’s device rather than the legitimate AP in order to collect PII from subsequent frames.

5.4.3 IEEE 802.11 DMG Beacon frames

The DMG (Direction Multi-gigabit) Beacon frame presents a structure similar to that of the Beacon frame, many of the same fields, and therefore the same threats. The DMG beacon frame also contains fields specific to the 60 GHz operations, such as sector sweep information element, clustering control information element, DMG capabilities, extended schedule, DMG operations element, DMG ATI, DMG BSS parameter change, multiband element of Awake Window element, DMG wakeup schedule, UPSIM element, non-transmitted BSSID capability element, SSID list element, PCP handover element, Next PCP list, and antenna sector ID pattern element, all elements that can be used fingerprint the emitting access point.

5.4.4 IEEE 802.11 Probe responses

The Probe response structure is very similar to that of the beacon, and the same elements can be used to fingerprint the transmitter.

However, Probe responses do not contain TIM fields, QoS capability, FMS descriptor, HCCA TXOP Update count and Future Channel guidance element.

5.4.5 IEEE 802.11 ATIM Frame

The following information elements are not generally implemented, and have not been analyzed: Frequency-Hopping (FH) Parameter Set; Point Coordination Function (PCF);

ATIM frames mark (in an IBSS) a station power management transitions. Its body is empty (power bit set to 0 or 1 in Control field), but its presence and rhythm can be used to uniquely fingerprint the emitting STA.

5.4.6 IEEE 802.11 Disassociation Frame

Disassociation frame contains a Reason code, one or several vendor specific elements, and optionally a Management MIC Element when Management Frame Protection is enabled and the frame is addressed to a group.
Several reason codes may be used to uniquely identify an AP, such as reason code 1 (unspecified) in response to targeted messages, reason 4 (timeout values), reason5 (too many STAs), reason 10 (unacceptable power capabilities), reason 11 (unacceptable supported channels), reason 13 (invalid element), reason 27 (lack of roaming agreement to service provider), reason code 28 (requested service not authorized in this location), reason code 32 (unspecified QoS reason), reason code 33 (not enough bandwidth), reason code 34 (missing acks, too many frames to ack but AP RF conditions prevent sending them), reason code 46 (peer initiated, authorized access limit reached), reason code 47 (AP initiated, due to external service requirements), reason code 53 (mesh max peers STA reached), reason code 56 (mesh max retries),reason code 57 (mesh confirm timeout), reason code 61 (mesh path error, no proxy information for target destination), reason code 62 (mesh path error, no forwarding information for target destination), reason code 63 (mesh path error destination unreachable, reason code 66 (mesh channel switch for unspecified reason), the presence of the Management MIC Element. All these elements can be used to uniquely identify the sender and its position in the infrastructure.

5.4.7 IEEE 802.11 Association Request Frame (Management frame)

Association request frames are typically sent by a STA attempting to join a BSS. As such, they describe in details the capabilities of the requesting station, present in elements such as the Capability Information element, Listen Interval Field, supported rates and BSS Membership selector element, extended supported rates and BSS Membership selector element, Power capability element, Supported channel element, QoS capability element, RM enabled capabilities element, Mobility Domain element, Supported Operating classes element, HT capabilities element, 20/40 Coexistence element, Extended Capabilities element, QoS traffic capability element, TIM broadcast request element, Internetworking element, multi band element, DMG capabilities element, Multiple MAC sublayers element, VHT capabilities element, Operating Mode Notification element and vendor specific element. These elements, individually and in combinations, provide multiple ways of uniquely identifying the requesting station.

5.4.8 IEEE 802.11 Association Response Frame (Management frame)

The association response is typically sent in response to the association request. As such it contains the capability of the BSS provider (typically an AP). Elements such as the Capabilities Information element, the supported rates and BSS Membership selector element, extended supported rates and BSS Membership selector element, the EDCA parameter set element, the RCPI element, the RSNI element, the RM Enabled capabilities element, the Mobility Domain element, the Fast BSS Transition element, the DSE registered location element, the Association comeback element, the HT capabilities element, the HT operations element, the 20/40 BSS Coexistence element, the Overlapping BSS Scan parameters, the Extended Capabilities element, the BSS Max Idle Period element, the TIM broadcast response element, the QoS map element, the QMF policy element, the multiband element, the DMG capability element, the DMG operation element, the Multiple MAC sublayer element, the Neighbor report element, the VHT capability element, the VHT operation element, the Operating mode notification element, the Future Channel Guidance element, and vendor specific elements can contain, individually or in combination, enough unique information for an adversary to uniquely identify the sender and its capabilities. Additionally, an adversary can also generate association request frames with various capabilities announced, and observe the response, including the status code, of the AP. With this process, the adversary can trigger the AP to provide extended information about the supported parameters, and uniquely identify the AP this way.

5.4.9 IEEE 802.11 Reassociation Request Frame (Management frame)

The structure of the reassociation request frame is similar to that of the association request frame. The reassociation request frame contains all the elements that can be found in the association request frame.

The reassociation request frame also contains additional elements, such as the current AP address, the Fast BSS Transition element, the Resource Information Container (RIC) element, the FMS request element and the DMS request elements, that can be used to further uniquely fingerprint the requesting station.

5.4.10 IEEE 802.11 Reassociation Response Frame (Management frame)

he reassociation response frame is similar in structure to the association response frame. All the elements of the association response frame are present in the reassociation response frame.

The reassociation response frame also contains additional elements, such as the Resource Information Container (RIC) element, the FMS request element, and the DMS request element, that can be used to further uniquely fingerprint the responding AP.

5.4.11 IEEE 802.11 Probe Request Frame (Management frame)

The probe request contains some elements identical to the Association request frame, including the Supported rates and BSS Membership selector element, the Extended Supported Rates and BSS membership selector element, the Supported Operating classes element, the HT capabilities element, the 20/40 BSS Coexistence element, the Extended Capabilities element, the Interworking element, the Multiband element, the DMG Capabilities element, the Multiple MAC Sublayers element, the VHT capabilities element, and the Vendor specific element. Their characteristics are identical for the association request and the probe request and can be used to uniquely identify the requesting station and its characteristics.

The probe request also includes elements such as the SSID element, the DSSS Parameter set, the SSID list, the Channel Usage element, the Mesh ID element, the Estimated Service Parameter Element and the Extended Request element, that can contain further information to uniquely fingerprint the requesting station.

5.4.12 IEEE 802.11 Authentication Frame (Management frame)

The authentication frame can be used as a request or a response (sequence number determines the frame position in the exchange choreography). An adversary can observe specific elements, such as the MDIE, FTE the RIC element, the multiband element and vendor specific element in both the station and AP messages, but also the RIC element, the Timeout interval, the Send Confirm element, the confirm element and neighbor report in the AP messages, and the Finite Cyclic group, the Finite Field element, the Anti clogging token, or the scalar element in the station messages, and use these elements to uniquely identify the sender. An adversary can also generate authentication messages, and observe the AP response. From the AP response, the adversary can deduce information about the AP feature support or uniquely fingerprint the AP.

5.4.13 IEEE 802.11 Deauthentication Frame (Management frame)

Deauthentication frames include reason codes. Reasons codes have been examined in a previous section and can be used to fingerprint the AP by listing AP supported features (or unsupported features). Deauthentication frames also include specific elements that can be further used to fingerprint the AP, such as the Management MIC element or vendor-specific elements.

5.4.14 IEEE 802.11 Action Frames (Management frame)

Action Frames form a large family of management frames, aiming at conveying specific information or instructions, in specific contexts or for specific capability information exchange. Besides containing information elements that can be used to identify the sender (such as vendor-specific element), they are by nature indicative of specific capabilities, specific context mandating a particular action, and as such can be used to uniquely identify the sender of the frame, and the responder. 802.11-revmc describes 162 types of individual action frames, among which 6 were found to be neutral (not providing unique information about the sender of the destination). All the others can be used by an adversary to uniquely identify the sender or receiver. In some cases, frames can be generated by an adversary to trigger a response and fingerprint the responder.

5.4.15 IEEE 802.11 Action no ACK Frames (Management frame)

Structure is similar to Action frame, with the exception that Action No Ack cannot contain Mesh Peering Exchange Element, or Management MIC Element. However, Action no Ack frames can also contain vendor-specific elements, and can be used to uniquely identify the emitter.

5.4.16 IEEE 802.11 Timing Advertisement Frame (Management frame)

Timing Advertisement frames are mandatory and therefore only sent by some APs. The frame also contains elements that can be used to uniquely identify the sending AP, such as the Capability Information element, the extended capability element, the power constraint element, the time advertisement element and vendor specific elements.

5.5 IEEE 802.15

TBD

5.5.1 IEEE 802.15 management frames

TBD

6 Acknowledgments

Mick Seaman provided invaluable input to the analysis of 802.1 frame types.

7 References

[IEEE802] Std. 802-2014. IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.

[IEEE802.11] Std. 802.11-2012, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[IEEE802.1AE] Std. 802.1AE-2006, IEEE Standard for Local and metropolitan area network – Media Access Control (MAC) Security.

[IEEE802.1Q] Std. 802.1Q-2014, IEEE Standard for Local and metropolitan area network – Bridges and Bridged Networks.

[IEEE802.1X] Std. 802.1X-2010, IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control.

[KMM] R. Kemmerer, C. Meadows, and J. Millen, "Three systems for cryptographic protocol analysis", *Journal of Cryptology* 7(2), 1994, 79-130.

[RFC3748] Extensible Authentication Protocol (EAP). B. Aboba, et. al., June 2004.

[RFC4949] Internet Security Glossary, Version 2, R. Shirey, August 2007.

[RFC7624] Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement. IAB.

[TUTORIAL] IEEE 802 Privacy Tutorial, https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0001-00-ecsg-ieee-802-privacy-tutorial.pdf

Appendix A Detailed Privacy Threat Analysis

An “asset/risk/threat analysis” is used to determine privacy risks and threats to objects identified as having privacy considerations

Table Label Definitions:

- **Risk**. A risk to that asset, which would affect privacy.
- **Threat**. A method by which an attacker could make use of the risk.
- **Threat Analysis**. A subjective analysis of threats.

A.1 IEEE 802 Destination MAC Address and Source MAC Address

Risk	Threat	Threat Analysis
Adversary observes target MAC address as DA or SA on the IEEE 802 frame	When the Adversary is close to the Target, it can monitor flows and detect changes to an SA	Adversary can detect the change from universal address to local address, or from one local address to a different local address.
	[Make more prominent the note that “sa or da” means “ target mac address”]	Bridging cannot detect the target MAC address change event, and may carry unnecessary state related to the address no longer in use. (Is this accurate? If so, is it a true threat?)[remove row]
	When target MAC address is associated with the Target, adversary observes and logs the target’s SA, correlates with other network accesses from this SA	When the target MAC address is a universal address, identification and correlation of Target MAC address across multiple networks in time and space is trivially possible.
Target MAC address Is embedded in the payload of the frame	Adversary observes and logs Target MAC address embedded in an IPv6 Source address	Same as above.
	Adversary observes and logs target MAC address located in an Ethernet frame that is tunneled within an Ethernet frame (e.g., MACinMAC defined in IEEE 802.1ah).[Now part of .1Q, found it?]	Same as above.

A.2 802.1 Threat Analyses

A.2.1 802.1Q Frames

Risk	Threat	Threat Analysis
Adversary observes Priority Code Point (PCP) in a VLAN TCI (Clause 9.6).	Adversary is aware that certain PCP values are associated with a certain class of Targets (e.g., VoIP)	An adversary aware of the PCP mappings may identify classes of Targets. Some mappings are de-facto or actual standards. Identification of voice and video traffic from a MAC address could indicate a Target.

Adversary observes VID in a VLAN TCI (Clause 9.6)	Adversary is aware that certain VID values refer to different classes of Targets. [Intro comment about classes of threats using routing/pcp data?] [verify “data packets out of scope”]	An adversary aware of the VID mappings may identify classes of Targets. Such mappings are likely to be network specific, and less likely to be obvious to the adversary. However, the adversary may ascertain the mappings with enough analysis.
Adversary observes the Flow Identifier in a CN-TAG. (Clause 33.2)	Adversary re-constructs a session based on the Flow Identifier. The format of Flow Identifier is unspecified, but it may have some consistent meaning deducible by the adversary.	Adversary can observe the session and identify the type of traffic.
	Adversary correlates flows with the same Flow Identifier.	Adversary identifies the target (or type of target) by correlating flows.
Adversary observes CN Message PDU.	Adversary observes the Congestion Point Identifier. (Clause 33.4.4)	Clause 33.4.5 notes that the CP identifier can be constructed as MAC address + priority. Both can be used to identify the identity of the station.
	Adversary observes the encapsulated priority. (Clause 33.4.7)	Priority mapping can be used to identify the type of traffic.
	Adversary observes Encapsulated destination MAC address. (Clause 33.4.8)	Encapsulated MAC address can be used to identify a target.
Adversary observes SRP StreamID (Clause 35.2.2.8.2)	Adversary observes the MAC address portion of the StreamID.	MAC address in the StreamID can be used to identify the presence of a Talker or Listener target within the bridged network.
		MAC address in the StreamID can be used to identify probable targets (e.g., audio/video endpoints).
	Adversary observes the Unique ID portion of the StreamID. [Add row for just StreamID]	StreamID correction can allow attacker to observe the frames of a single Talker stream and identify the type of traffic.
Adversary observes MSRP Structure (Clause 35.2.2.8.5)	Adversary observes PriorityAndRank in MSRP message.	An adversary aware of the PCP mappings may identify classes of Targets.
Adversary observes bridge address (Clause 8.13.8)	Adversary observes the bridge address of a target, which is required to be a universal address.	An adversary observing the bridge address of a personal bridge correlate may correlate the bridge address with host addresses behind the bridge if those host addresses are passed in frames with a SA of the bridge address.
Adversary observes VDB [EVB?] messages (Clause 41)	Adversary observes EVB frames containing VSIID values, which can be an IPv4, IPv6, or MAC address.	An adversary in the data center may use the VSIID to track the target. (VALIDATE)[Shared data center, at the hypervisor level]

Deleted: (VALIDATE)

Adversary observes CFM messages (Clauses 18 & 19)	Attacker observes a MA Endpoint (MEP) associated with an end station attachment to a LAN (Clause 19.2)	Can the MAC address used for discovery refer to a host or home gateway device? [yes] Can an attacker force a bridge to send CFM packets in order to find the location of a MAC Address in the network? [?] (VERIFY)
	Attacker observes a VID in a CFM message.	An adversary aware of the VID mappings may identify classes of Targets
Adversary observes SPSourceID (Clauses 27.10, 27.15)	Attacker observes autocreated group address with the local bit set based on the SPSourceID.	N/A. The group address is not PII (VERIFY)
Adversary observes PBBN Backbone Source MAC address or Destination address (Clause 26)	Attacker observers MAC Address of the provider bridge.	N/A. Provider bridges do not represent persons.

Deleted: . (VERIFY)

A.2.2 IEEE 802.1AB Frames

Risk	Threat	Threat Analysis
Adversary observes Chassis ID TLV	Adversary observes chassis ID subtype TLVs (e.g., MAC address, network address, interface name) (see Table 8-2)	MAC address can be used to identify a target.
		A network address (i.e., IP address) can be used to identify a target.
Adversary observes Port ID TLV	Adversary observes chassis ID subtype TLVs (e.g., MAC address, network address, interface name) (see Table 8-3)	MAC address can be used to identify a target.
		A network address (i.e., IP address) can be used to identify a target.
	Adversary observes port description subtype TLVs	N/A. Port description is usually an RFC 2863 ifDescr object, which is “name of the manufacturer, the product name and the version of the interface hardware/software” While it reveals information about the device type, it is less likely to identify a particular target.
Adversary observes a System Name TLV	Adversary observes a System name	A system name or description may be used to identify a target by owning organization. Name is typically an RFC 3418 sysName object, and “By convention, this is the node's fully-qualified domain name.”
Adversary observes a System Description TLV	Adversary observes System Description	N/A. System Description is usually an RFC 2863 ifDescr object (see above).
Adversary observes a System Capabilities TLV	Adversary observes System Capabilities	System capabilities (e.g., Telephone, DOCSIS cable device) may be used to identify a class of target.

Risk	Threat	Threat Analysis
Adversary observes Management Address TLV	Adversary observes subTLV types related to management address	An IP address or MAC management address can be used to identify a target.
Adversary observes Organizationally Specific TLVs	Adversary observes organization specific addresses	An organizational TLV containing identity information in a TLV could be used to identify a target.

A.2.3 IEEE 802.1X EAPOL Frames

Risk	Threat	Threat Analysis
Adversary observes EAPOL-EAP frames (and EAPOL-KEY frames containing an EAP method)	Adversary observes EAP messages and learns identity information therein.	EAP identity is observed. Some EAP methods may reveal additional identity or associated information. E.g., Client certificate may be sent before encryption, and the list of cipher suites in the EAP-TLS Client Hello message may reveal information about the type of target.
	Adversary spoofs EAP Authenticator to learn identity information.	For each EAP method, the adversary can perform the protocol through EAP method identity message.
Adversary observes EAPOL-Start frames	N/A. There is no Packet Body for the adversary to observe.	N/A
Adversary observes EAPOL-Logoff frames	N/A. There is no Packet Body for the adversary to observe.	N/A
Adversary observes EAPOL-Key key agreement frames	Adversary observes the Four-way handshake and other key agreement handshakes.	N/A. Key agreement messages are encrypted using a secret keys derived from EAP.
Adversary observes EAPOL-Encapsulated-ASF-Alert frames	N/A. This type is not generally deployed, and has not been analyzed.	N/A
Adversary observers EAPOL-MKA frames	Adversary observes SCI value, containing a MAC address of the target (possibly different from the SA).	The SCI may contain a universal address, when frames are emitted with a local address as the SA.
	Adversary observes KMD (If host is distributing it).	KMD may indicate organization or home location of the target.
	Adversary observes CA Key Name (CKN)	N/A. CKN value is not intended to include PII.
Adversary observes an Announcement (sent in any frame)	Attacker learns the set of Key Management Domain (KMD) and/or Network Identifier (NID) values the host is prepared to join.	KMD and/or NID may indicate organization or home location of the target.

A.2.4 IEEE 802.1AE frame

Risk	Threat	Threat Analysis
Adversary observes SecTag	Adversary observes the MAC address used in the MACsec SCI.	MAC address in the SCI can be used to identify a target, if SCI is different than the SA and DA on the frame. This is particularly a threat when the MACsec frame is encapsulated in a VLAN TCI across a provider network. [AEcg describes the use of a local address instead of a universal addresss. Still trivilally trackable. Also part of a known group (the CA)]

A.3 IEEE 802.3 frame

Risk	Threat	Threat Analysis
Adversary observes EtherType	Adversary observes which protocol (e.g., IPv4, IPv6) the target is sending to the respondent.	There is unlikely to be PII included in the EtherType. An infrequently used EtherType could indicate the target is a part of a distinct group of targets.
Adversary observes Payload	Adversary observes and logs PII included in the payload of the frame, including ARP with higher level PII).	PII in the Payload can be obscured using MACsec [IEEE802.1AE] and its amendments.
Adversary observes CRC	Adversary observes CRC value.	N/A. The CRC is a computed value and does not represent PII
Adversary observes the frame size and frequency of a protocol session. Protocol may be cleartext or encrypted.	Attacker applies analytic techniques to identify higher layer protocols.	Attacker may identify voice traffic, etc.

A.4 IEEE 802.11

A.4.1 Beacon Frame (Management frame)

Risk	Threat	Threat Analysis
Adversary observes Timestamp	Adversary observes inaccuracies between beacons.	Adversary can use this to fingerprint a particular AP.
Adversary observes Beacon interval	Adversary observes beaconing interval value.	Same as above.
	Adversary detects difference between announced interval and observed interval.	Same as above.
Adversary observes Capability field	Adversary observes set of announced capabilities	Same as above.
Adversary observes SSID	Adversary observers SSID value	Same as above.
	Adversary maps SSID to a target, class of target, or location.	Adversary can use this to identify a particular target.

Risk	Threat	Threat Analysis
Adversary emits an SSID	Adversary advertises the same SSID ("evil twin") in Beacon frame with a different SA.	Attacker attracts targets to the attacker's device rather than the legitimate AP in order to collect PII from subsequent frames.
	Adversary advertises the same SSID and SA ("evil twin") in Beacon frame.	Attacker spoofs the AP in order to collect PII from subsequent frames.
Adversary observes Supported rates and BSS Membership Selector	Adversary observes Support rate and BSS Selector values.	Adversary can use this to fingerprint a particular AP.
Adversary observes DSSS Parameter set	Adversary observes the DSSS Parameter set and identifies an unusual channel (e.g. channel 4)	Adversary can use this to identify a particular target.
Adversary observes the IBSS Parameter set	Adversary observes patterns in the (supposedly random) ATIM Window value in the IBSS Parameter set Information Element	Adversary can use this to fingerprint a particular station (acting as beacon source)
Adversary observes the TIM	Adversary observes the AID of STAs mentioned (or not mentioned) in the TIM	Adversary can use this to fingerprint a particular station
Adversary observes the Power Constraint	Adversary observes the optional Power Constraint IE	Adversary can use this to fingerprint a particular AP
Adversary observes the Channel Switch	Adversary observes the optional Channel Switch IE	Same as above
Adversary observes the Quiet Element	Adversary observes the optional Quiet IE	Same as above
Adversary observes the IBSS DFS Element	Adversary observes the DFS Owner and DFS Recovery map IE	Adversary can use this to identify members of the IBSS
	Adversary observes the channel map IE	Adversary can use this to identify a particular target
Adversary observes the TPC Report IE	Adversary observes the Power value in the TPC report IE	Adversary can use this to fingerprint a particular AP
Adversary emits a TPC Request and observes the TPC Report response (in subsequent beacon, probe response, Link Measurement Report or TPC report frames	Adversary observes the Power and Link Margin values in the TPC Report IE	Same as above
Adversary observes the ERP element	Adversary observes the Use Protection bit in the ERP Parameters IE	Adversary can use this to identify a target
	Adversary observes the Barker Preamble Mode in the ERP Parameter IR	Adversary can use this to fingerprint a particular AP
Adversary observes Extended Supported rates and BSS Membership Selector	Adversary observes the Extended Support rate and BSS Selector values.	Adversary can use this to fingerprint a particular AP.

Risk	Threat	Threat Analysis
Adversary observes the RSN IE	Adversary observes the authentication or pairwise cipher suite selectors, the single group data cipher suite selector, the RSN Capabilities field, the PMK identifier (PMKID) count, the PMKID list, and the single group management cipher suite selector.	Same as above
Adversary observes the BSS Load Element	Adversary compares the CU value reported by the AP to its own CU measurement	Same as above
	Adversary observes the Available Admission Capacity value	Same as above
Adversary observes the EDCA Parameter Set	Adversary observes the AIFSN, ECWmin/ECWmax and TXOP values	Same as above
Adversary observes the QOS Capability IE	Adversary observes the presence and values of the QoS Capability IE	Same as above
Adversary observes the AP Channel Report IE	Adversary observes the list of operating classes	Same as above
	Adversary observes the channel list	Same as above
Adversary observes the BSS Average Access Delay	Adversary observes the presence of the optional BSS Average Access Delay IE	Same as above
Adversary observes the Antenna IE	Adversary observes the presence of the optional Antenna IE	Same as above
	Adversary observes the value of the Antenna IE in beacons, probe responses, Location Track Notification frames or measurement report frames	Same as above
Adversary observes BSS Available Admission Capacity	Adversary observes the presence of the optional BSS Available Admission Capacity field	Same as above
	Adversary compares the values reported in the BSS Available Admission Capacity field to its own measurement for each AC	Same as above
Adversary observes BSS AC Access Delay	Adversary observes the presence of the optional BSS AC Access Delay field	Same as above
Adversary observes Measurement Pilot Transmission	Adversary observes the presence of the optional Measurement Pilot Transmission	Same as above
	The adversary observes the value of the Measurement Pilot interval, and the presence of the optional sub-elements	Same as above

Risk	Threat	Threat Analysis
Adversary observes the MBSSID IE	Adversary observes the MBSSID IE	Same as above
Adversary observes RM Enabled Capabilities	Adversary observes the values of the optional RM Enabled Capabilities IE	Same as above
Adversary observes Mobility Domain IE	Adversary observes the optional Mobility Domain IE and its value	Same as above. Also adversary can use to identify other APs in the same domain.
Adversary observes DSE registered location	Adversary observes the presence of the optional DSE registered location IE and its values	Adversary can use this to fingerprint a particular AP
Adversary observes the Extended Channel Switch Announcement element	Adversary observes the operating class and new channel number in the IE and deduces AP channel support and switching pattern	Same as above
Adversary observes the Supported Operating Classes element	Adversary observes the supported operating classes	Same as above
Adversary observes HT Capabilities	Adversary observes the HT Capabilities IE	Same as above
Adversary observes HT Operations	Adversary observes the HT Operations IE	Same as above
Adversary observes the 20/40 BSS Coexistence element	Adversary observes 20/40 BSS Coexistence element fields	Same as above
Adversary observes the Overlapping BSS Scan Parameters element	Adversary observes the fields in the Overlapping BSS Scan Parameters element	Same as above
Adversary observes the Extended Capabilities IE	Adversary observes the presence of the Extended Capabilities IE and its 47 possible and optional fields	Same as above
Adversary observes the FMS Descriptor IE	Adversary observes the presence and content of the optional Flexible Multicast Service IE	Same as above
Adversary observes the QoS Traffic Capability	Adversary observes the values of the QoS Traffic Capability IE	Same as above
Adversary observes the Time Advertisement IE	Adversary observes the Timer Advertisement values	Same as above
Adversary observes the Internetworking IE	Adversary observes the values of the Internetworking IE fields	Same as above
Adversary observes the Advertisement Protocol IE	Adversary observes the values in the Advertisement Protocol IE	Same as above
Adversary observes the Roaming Consortium IE	Adversary observes the values of the Roaming Consortium IE fields	Same as above
Adversary observes the Emergency Alert Identifier	Adversary observes the Emergency Alert Identifier IE values	Same as above
Adversary observes the Mesh ID IE	Adversary observes the value of the Mesh ID IE	Same as above, can also be used to identify the other APs in the same MBSS.

Comment [Office1]: Lists the various RM capabilities of the AP

Comment [Office2]: Geolocation of the AP, latitude, longitude, altitude etc.

Comment [JH3]: Supported channel width, block ack etc

Comment [JH4]: RIFS mode, dual beacon support in 40 Mhz etc

Comment [JH5]: What to do when 40 Mhz intolerant detected,

Comment [JH6]: Tells members of the BSS how to run OBSS scans

Comment [JH7]: Indicates if AP STA count is for AC_VO, AC_VI, both etc.

Comment [JH8]: specifies fields describing the source of time corresponding to a time standard, an external clock (external time source), an estimate of the offset between that time standard and the TSF timer, and an estimate of the standard deviation of the error in the offset estimate.

Comment [JH9]: Indicates private vs public network, personal de vice network etc.

Comment [JH10]: ANQP, proprietary etc

Comment [JH11]: Which SPs are supported

Comment [JH12]: Hash of the last Emergency Alert message, STAS use it to check if they have received that message already or should download it now

Risk	Threat	Threat Analysis
Adversary observes the Mesh Configuration IE	Adversary observes the values of the 7 different fields in the Mesh Configuration IE	Adversary can use this to fingerprint a particular AP
Adversary observes the Mesh Awake Window IE	Adversary observes if the Mesh Awake Window is present (optional) in regular beacons and the value of the window in the DTIM frames	Same as above
Adversary observes the Beacon Timing IE	Adversary observes the values in the beacon timing IE	Same as above
Adversary observes the MCCAOP Advertisement Overview IE and MCCAOP Advertisement IE	Adversary observes the optional mesh coordination function (MCF) controlled channel access opportunity IE	Same as above
Adversary observes the Mesh Channel Switch Parameters IE	Adversary observes the flags in the Mesh Channel Switch Parameters IE	Same as above
Adversary observes the QMF Policy Element	Adversary observes the subfields of the QoS Management Frame policy element	Same as above
Adversary observes the QLoad Report IE	Adversary observes the subfileds of the QLoad report IE	Same as above
Adversary observes the HCCA TXOP Update Count	Adversary observes the update count	Same as above
Adversary observes the Multi-band Element	Adversary observes the multiband element fields	Same as above
Adversary observes the VHT Capabilities element	Adversary observes the VHT capabilities element fields	Same as above
Adversary observes the VHT Operations element	Adversary observes the VHT Operation element fields	Same as above
Adversary observes the Transmit Power Envelope element	Adversary observes the Transmit Power Envelope element fields	Same as above
Adversary observes the Channel Switch Wrapper element	Adversary observes the fields of the Channel Switch Wrapper element	Same as above
Adversary observes Extended BSS Load Element	Adversary observes the Extended BSS Load element fields	Same as above
Adversary observes the Quiet Channel element	Adversary observes the Quiet Channel element	Same as above
Adversary observes the Operating Mode Notification Element	Adversary observes the Operating Mode Notification element	Same as above
Adversary observes the Reduced Neighbor Report	Adversary observes the Reduced Neighbor Report	Same as above
Adversary observes the TVHT element fields	Adversary observes the TVHT element fields	Same as above

Comment [JH13]: Path selection protocol, metric, congestion control mode etc

Comment [JH14]: Tells what is the TBTT of neighboring mesh APs, helps the receiver establish mesh peering with the neighbors

Comment [JH15]: Tells if reservations are accepted, and sends sort of TXOP values

Comment [JH16]: Who initiated the channel change (AP or other), can STA still send until jump, precedence value (random value)

Comment [JH17]: Used to exchange information about prioritization of management frames

Comment [JH18]: Informs about QoS traffic detected from neighboring BSSs

Comment [JH19]: Used to indicate when AP changes TXOP parameters in HCCA, requires HCCA TXOP negotiation parameter and HCCA

Comment [JH20]: Used to point to an alternate MAC address on another band when multiband is supported, optional, can indicate other band MAC

Comment [JH21]: 19 elements describing VHT operations

Comment [JH22]: width and center frequency

Comment [JH23]: 11ac, max power for 20, 40 80 160 Mhz

Comment [JH24]: 11ac, optional, tells what power and country value on new channel when channel switch happens

Comment [JH25]: 11ac, tells MUMIMO SS underutilization, 6 fields, can be used for vendor proprietary MUMIMO optimization

Comment [JH26]: 11ac tells if primary 80 or secondary 80 has to be quiet after channel jump. Quiet yes/no and 3 optional fields (Duration, count etc)

Comment [JH27]: 11ac, 80+80 or 160, number of SS Rx and Tx

Comment [JH28]: channel of neighboring APs

Comment [JH29]: describes support for TC whitespace channels

Risk	Threat	Threat Analysis
Adversary observes the Estimated Service Parameters element	Adversary observes the Estimated Service Parameters element fields	Same as above
Adversary observes the Future Channel Guidance element	Adversary observes the Future Channel Guidance element	Same as above
Adversary observes a Vendor specific element	Adversary observes an element specific to a vendor.	Same as above

Comment [JH30]: estimated throughput per AC, to be used to set uplink channel or P2P channel

Comment [JH31]: target channel in case of channel jump, along with power, primarily for mesh

Beacons IEs that are not seen as identifiers: FH Parameter set (not implemented today), CF Parameter Set (PCF is not implemented today), Country (common to all Aps), FH Parameters (not implemented today), FH Pattern Table (not implemented today), Extended Chanel Switch Announcement (support is mandatory).

A.4.2 DMG Beacon Frame (Management frame)

The DMG (Direction Multi-gigabit) Beacon frame presents a structure similar to that of the Beacon frame, and therefore the same threats. The following elements are identical:
Timestamp, Beacon interval, RSN, Multiple BSSID, SSID, IBSS Parameter Set, Country, BSS Load, EDCA Parameter Set, Power Constraint, Channel Switch Announcement, Neighbor Report, Quiet, QoS Capability, Extended Channel Switch Announcement, BSS Average Access Delay, RM Enabled Capabilities, Internetworking, Advertisement Protocol, Roaming Consortium, Vendor Specific.
The DMG Beacon frame also presents the following elements:

Risk	Threat	Threat Analysis
Adversary observes the Sector Sweep Information Element	Adversary observes the sector value (ID) in a given direction.	Adversary can use this to fingerprint a particular AP.
Adversary observes the Clustering Control Information Element	Adversary observes the cluster ID, cluster member role and cluster max member, and /or A-BFT responder address (depending on IE options)	Same as above.
Adversary observes the DMG Capabilities	Adversary observes the presence or absence of this optional element	Same as above.
Adversary observes the Extended Schedule	Adversary observes the presence or absence of this optional element and its values	Same as above
Adversary observes the DMG Operations Element	Adversary observes the presence or absence of this optional element and its values	Same as above
Adversary observes the DMG ATI	Adversary observes the presence or absence of this optional element and its values	Same as above
Adversary observes the DMG BSS Parameter change	Adversary observes the presence or absence of this optional element and its values	Same as above
Adversary observes the Multi band element	Adversary observes the presence or absence of this optional element and its values	Same as above
Adversary observes the Awake Window Element	Adversary observes the presence or absence of this optional element and its values	Same as above

Adversary observes the DMG Wakeup Schedule	Adversary observes the presence or absence of this optional element and its values	Same as above
Adversary observes the UPSIM Element	Adversary observes the presence or absence of this optional element and its values	Same as above
Adversary observes the Nontransmitted BSSID Capability Element	Adversary observes the presence or absence of this optional element and its values	Same as above
Adversary observes the SSID List element	Adversary observes the presence or absence of this optional element and its values	Same as above
Adversary observes the STA Availability element	Adversary observes the presence or absence of this optional element and its values	Same as above
Adversary observes the PCP Handover element	Adversary observes the presence or absence of this optional element and its values	Same as above
Adversary observes the Next PCP list	Adversary observes the presence or absence of this optional element and its values	Same as above
Adversary observes the Antenna sector ID pattern	Adversary observes the presence or absence of this optional element and its values in a given direction	Same as above

The following element was not considered a threat: DMG Parameters (common to all DMG APs)

A.4.3 Probe Response Frame (Management frame)

The structure of the Probe Response frame is similar to that of the Beacon frame. Most information elements are similar in both frames and convey the same type of information.

Risk	Threat	Threat Analysis
Adversary observes the Channel Usage (element ID 38)	Adversary observes the Channel Usage fields and channels suggested by the AP.	Adversary can use this to fingerprint a particular AP.
Adversary observes the Timezone (element ID 40)	Adversary observes the Timezone field and the local time announced by the AP.	Same as above.
Adversary observes the DMG Capabilities element (element ID 55)	Adversary observes the DMG Capabilities element fields.	Same as above.
Adversary observes the DMG Operation element (element ID 56)	Adversary observes the DMG Operation element	Same as above.
Adversary observes the Multiple MAC Sublayers element (element ID 57)	Adversary observes the Multiple MAC Sublayers element	Same as above.
Adversary observes the Antenna Sector ID Pattern element (element ID 58)	Adversary observes the Antenna Sector ID Pattern element	Same as above.

Comment [JH32]: recommends channels for P2P (DTLS) traffic)

Comment [JH33]: 8 fields describing direct multi gigabit operations (60 GHz)

Comment [JH34]: 8 other bits for 60 GHz operations

Comment [JH35]: describes the 60 GHz AP that has several Macs (i.e. 2.4 and 5 GHz)

Comment [JH36]: 4 fields describing 60 GHz combinations of 2 antennas

Adversary observes the Relay Capabilities (element ID 69)	Adversary observes what STA the AP can relay to, and what type of relay parameter is supported.	Same as above.
Adversary observes the Requested Elements (element ID – ‘last’)	The adversary observes which requested elements are provided.	Same as above.

Comment [JH37]: 7 fields describing mesh relay capabilities

However, the following fields are present in a beacon, but not present in a Probe Response:
9. Traffic Indication Map
21. Qos Capability
39. FMS Descriptor
55. HCCA TXOP Update Count
67. Future Channel Guidance

A.4.4 ATIM Frame (Management frame)

ATIM frames mark (in an IBSS) a station power management transitions. Its body is empty (power bit set to 0 or 1 in Control field), but its presence and rhythm can be used to uniquely fingerprint the emitting STA.

A.4.5 Disassociation Frame (Management frame)

Disassociation frame contains a Reason code, one or several vendor specific elements, and optionally a Management MIC Element when Management Frame Protection is enabled and the frame is addressed to a group.
Several reason codes may be used to uniquely identify an AP:

Risk	Threat	Threat Analysis
Adversary sends various forged frames and observes which frames (type, transmission quantity over time period) results in a disassociation frame from the AP, with a specific reason code	Adversary observes reason code 1 (unspecified) and deduces what parameters are not supported by the AP, or are vendor specific.	Adversary can use this to fingerprint a particular AP.
	Adversary observes reason code 4 (inactivity) and deduces AP timeout values	Same as above
	Adversary observes reason code 5 (too many STAs) and deduces AP max STA value	Same as above
	Adversary observes reason code 10 (unacceptable power capabilities) and deduces AP power capabilities values and ranges.	Same as above
	Adversary observes reason code 11 (unacceptable supported channels) and deduces AP supported channel ranges.	Same as above

Risk	Threat	Threat Analysis
	Adversary observes reason code 13 (invalid element) and deduces AP capabilities.	Same as above
	Adversary observes reason code 27 (lack of roaming agreement to service provider) and deduces AP specific service provider configuration.	Same as above
	Adversary observes reason code 28 (requested service not authorized in this location) and deduces AP local specific configuration.	Same as above
	Adversary observes reason code 32 (unspecified QoS reason) and deduces AP specific capabilities.	Same as above
	Adversary observes reason code 33 (not enough bandwidth) and deduces AP channel (wireless, wired) capabilities.	Same as above
	Adversary observes reason code 34 (missing acks, too many frames to ack but AP RF conditions prevent sending them) and deduces AP ACK max threshold.	Same as above
	Adversary observes reason code 46 (peer initiated, authorized access limit reached) and deduces AP local configuration.	Same as above
	Adversary observes reason code 47 (AP initiated, due to external service requirements) and deduces AP local configuration.	Same as above
	Adversary observes reason code 53 (mesh max peers STA reached) and deduces AP STA max capability.	Same as above
	Adversary observes reason code 56 (mesh max retries) and deduces AP mesh max Peering Open frames.	Same as above
	Adversary observes reason code 57 (mesh confirm timeout) and deduces AP max timeout value for mesh peering.	Same as above
	Adversary observes reason code 61 (mesh path error, no proxy information for target destination) and deduces AP routing / forwarding structure.	Same as above
	Adversary observes reason code 62 (mesh path error, no forwarding information for target destination) and deduces AP routing / forwarding structure.	Same as above

Risk	Threat	Threat Analysis
	Adversary observes reason code 63 (mesh path error destination unreachable) and deduces AP routing / forwarding structure.	Same as above
	Adversary observes reason code 66 (mesh channel switch for unspecified reason) and deduces AP local capabilities.	Same as above
Adversary observes MME	Adversary observes Management MIC Element and deduces that AP supports protected management frames.	Same as above.

The following reason codes were not considered as posing a specific risk for unique AP fingerprinting in the context of Disassociation frame (some reasons also do not apply to disassociation frames): 0 (reserved), 2 (invalid authentication), 3 (deauth because STA is leaving BSS), 6 (invalid class 2 frame), 7 (invalid class 3 frame), 8 (disassociation because STA is leaving BSS), 9 (STA is not authenticated), 12 (BSS transition management), 14 (MIC failure), 15 (4 way handshake timeout), 16 (GK handshake timeout), 17 (handshake element mismatch), 18 (invalid group cipher), 19 (invalid pairwise cipher), 20 (invalid AKMP), 21 (unsupported RSNE version), 22 (invalid RSNE capabilities), 23 (802.1X failed), 24 (cipher rejected), 25 (TDLS peer unreachable), 26 (TDLS unspecified reason), 29 (Bad cipher or AKM for target Service Provider), 31 (lack of bandwidth due to BSS operational mode change), 35 (exceeded TXOP), 36 (requesting STA is leaving), 37 (stream no longer used), 38 (Traffic stream not set), 39 (peer timeout), [40 to 44 do not exist], 45 (peer key mismatch), 48 (invalid FT frame count), 49 (invalid PMKID), 50 (invalid MDE), 51 (invalid FTE), 51 (mesh peering cancelled), 54 (mesh configuration policy violation), 55 (mesh peering close frame received), 58 (mesh invalid GTK), 59 (mesh inconsistent parameters), 60 (mesh invalid security capabilities), 64 (MAC address already exists in MBSS), 65 (channel switch due to regulatory requirements), [67 and up are reserved].

However, it must be noted that the reasons excluded above may be revealing due to vendor specific implementation (e.g. a given vendor may choose to return reason code 15, 4 way handshake timeout, for any handshake failure, i.e. reason code 13 to 22).

A.4.6 Association Request Frame (Management frame)

Risk	Threat	Threat Analysis
Adversary observes Capabilities Information element	Adversary observes the announced specific capabilities	Adversary can use this to fingerprint a particular station.
Adversary observes the Listen Interval Field	Adversary observes unusual interval values	Same as above.
Adversary observes the SSID field	Adversary observes sequence of SSID values	Same as above.
Adversary observes the supported rates and BSS Membership selector element	Adversary observes the supported announced rates (legacy, 11n and 11ac)	Same as above.
Adversary observes the Extended supported rates and BSS Membership selector element	Same as above	Same as above.

Comment [JH38]: short /long preamble, QoS, APSD etc

Risk	Threat	Threat Analysis
Adversary observes the Power capability element	Adversary observes the optional power capability element and the reported min and max values	Same as above.
Adversary observes the Supported channels element	Adversary observes the list of supported channels	Same as above.
Adversary observes the QoS capability element	Adversary observes the QOS elements supported by the STA	Same as above.
Adversary observes the RM Enabled Capabilities element	Adversary observes if the STA supports RM and which element are enabled	Same as above.
Adversary observes the Mobility Domain element	Adversary observes if STA supports Fast Transition through the presence of the MDIE (repeating AP announced MDIE in beacon / probe responses)	Same as above.
Adversary observes the Supported Operating Classes element	Adversary observes the classes supported by the STA in the local regulatory domain	Same as above.
Adversary observes the HT Capabilities element	Adversary observes the 802.11n parameters supported by the STA	Same as above.
Adversary observes the 20/40 BSS Coexistence element	Adversary observes the presence of the optional 20/40 BSS Coexistence element and its parameters	Same as above.
Adversary observes the Extended Capability element	Adversary observes the presence of this optional element and its advertised values	Same as above.
Adversary observes the QoS Traffic Capability element	Adversary observes the presence of the QoS traffic capability element	Same as above.
Adversary observes the TIM Broadcast Request element	Adversary observes that the STA requests TIM to be broadcasted at specific intervals	Same as above.
Adversary observes the Interworking element	Adversary observes the STA requesting the optional access to emergency services without prior authentication (unassociated 911)	Same as above.
Adversary observes the Multi-band element	Adversary observes the support for multiple bands	Same as above.
Adversary observes the DMG Capabilities element	Adversary observes the 802.11ad parameters supported by the STA	Same as above.
Adversary observes the Multiple MAC Sublayers element	Adversary observes the elements supported over multiple MAC, along with the MAC announced on the other band by the STA	Same as above.
Adversary observes the VHT capability element	Adversary observes the 802.11ac parameters announced as supported by the STA	Same as above.
Adversary observes the Operating Mode Notification element	Adversary observes the presence of the optional element and its parameters for 802.11ac (Rx, 80/160)	Same as above.

Risk	Threat	Threat Analysis
Adversary observes the vendor specific elements	Adversary observes the presence of vendor specific elements	Same as above.

The following fields were not considered as potential identifiers: RSN (element ID 8).

A.4.7 Association Response Frame (Management frame)

Risk	Threat	Threat Analysis
Adversary observes Capabilities Information element	Adversary observes the announced specific capabilities	Adversary can use this to fingerprint an AP.
Adversary observes the Status code	Adversary generates specific association requests, to observe the response from the AP and deduce AP capabilities. Status codes of interest include (one or several of) 2 (TDLS rejected, alternative TDLS wakeup schedule provided), 6 (unacceptable lifetime), 10 (cannot support all capabilities in the Capability information field), 17 (AP is unable to handle additional client STAs), 22 (association rejected because Spectrum management capability is required), 23 (association rejected because information in Power Capability element is unacceptable), 24 (Supported channels element is unacceptable), 27 (Association denied because the STA does not support HT features), 30 (refused temporarily, try again later), 31 (robust management frame policy violation), 32 (unspecified QoS failure), 33 (insufficient bandwidth to take one more QoS STA), 34 (association denied due to poor channel conditions or excessive frame loss), 38 (invalid parameters), 40 (invalid elements), 51 (listen interval is too large), 59 (GAS protocol not supported), 93 (AP out of memory), 99 (association rejected but multi band elements provided for alterative radio connection), 106 (association denied because information in the Spectrum management field is unacceptable), 104 (association denied because STAT does not support VHT features)	Same as above.

Comment [JH39]: short /long preamble, QoS, APSD etc

Risk	Threat	Threat Analysis
Adversary observes the supported rates and BSS Membership selector element	Adversary observes the supported announced rates (legacy, 11n and 11ac)	Same as above.
Adversary observes the Extended supported rates and BSS Membership selector element	Same as above	Same as above.
Adversary observes the EDCA parameter set element	Adversary observes specific QoS parameters announced by the AP.	Same as above.
Adversary observes the RCPI element	Adversary observes the presence of the optional RCPI element and the reported received power channel indicator value at which the AP heard the station	Same as above.
Adversary observes the RSNI element	Adversary observes the presence of the optional RSNI element and the reported RSN value at which the AP heard the station	Same as above.
Adversary observes the RM Enabled Capabilities element	Adversary observes if the AP supports RM and which element are enabled	Same as above.
Adversary observes the Mobility Domain element	Adversary observes if the AP supports Fast Transition through the presence of the MDIE (repeating AP announced MDIE in beacon / probe responses)	Same as above.
Adversary observes the Fast BSS Transition element	Adversary observes the presence of the optional Fast BSS transition element and the announced 11r parameters	Same as above
Adversary observes the DSE registered location element	Adversary observes the presence of the optional Dependent Station Enablement element, and the geographical location information reported for the AP location	Same as above.
Adversary observes the Association comeback element	Adversary observes the announced comeback timeout value.	Same as above
Adversary observes the HT Capabilities element	Adversary observes the 802.11n parameters supported by the AP	Same as above.
Adversary observes the HT operations element	Adversary observes the 802.11n parameters supported by the AP	Same as above.
Adversary observes the 20/40 BSS Coexistence element	Adversary observes the presence of the optional 20/40 BSS Coexistence element and its parameters	Same as above.
Adversary observes the Overlapping BSS Scan parameters	Adversary observes the presence of this optional element and the 6 parameters announced by the AP for STA OBSS scanning.	Same as above.

Risk	Threat	Threat Analysis
Adversary observes the Extended Capability element	Adversary observes the presence of this optional element and its advertised values	Same as above.
Adversary observes the BSS Max Idle period element	Adversary observes if AP supports this optional 802.11v feature and the timeout configured on the AP	Same as above.
Adversary observes the TIM broadcast response element.	Adversary observes if AP supports this feature and the interval announced by the AP.	Same as above.
Adversary observes the QoS Map element	Adversary observes the presence of this element and the DSCP to UP mapping announced by the AP	Same as above.
Adversary observes the QMF Policy element	Adversary observes the presence of QoS Management Frame element and the various UP announced for various management frames.	Same as above.
Adversary observes the Multi-band element	Adversary observes the support for multiple bands	Same as above.
Adversary observes the DMG Capabilities element	Adversary observes the 802.11ad parameters supported by the AP	Same as above.
Adversary observes the DMG Operations element	Adversary observes the 802.11ad parameters supported by the AP	Same as above.
Adversary observes the Multiple MAC Sublayers element	Adversary observes the elements supported over multiple MAC, along with the MAC announced on the other band by the AP	Same as above.
Adversary observes the Neighbor Report element	Adversary observes the presence of the Neighbor report when association is rejected with 'suggested BSS transition' reason code, and the suggested neighbor list.	Same as above
Adversary observes the VHT capability element	Adversary observes the 802.11ac parameters announced as supported by the AP	Same as above.
Adversary observes the VHT Operation element	Adversary observes the 802.11ac parameters announced as supported by the AP	Same as above.
Adversary observes the Operating Mode Notification element	Adversary observes the presence of the optional element and its parameters for 802.11ac (Rx, 80/160)	Same as above.
Adversary observes the Future Channel Guidance element	Adversary observes the presence of the Future Channel Guidance element, and the future channels announced by the AP in case of channel switch	Same as above.
Adversary observes the vendor specific elements	Adversary observes the presence of vendor specific elements	Same as above.

The following fields were not considered as identifiers for the association response: AID.

A.4.8 Reassociation Request Frame (Management frame)

The structure of the reassociation request frame is similar to that of the association request frame. The reassociation request frame contains all the elements that can be found in the association request frame.
The reassociation request frame also contains the following elements, that are not found in the association request frame:

Risk	Threat	Threat Analysis
Adversary observes the current AP address	The adversary observes information about the AP the client is roaming from, the AP the client is roaming to.	Adversary can use this to fingerprint a STA.
Adversary observes the Fast BSS Transition element	Adversary observes the STA support for 802.11r	Same as above.
Adversary observes the Resource Information Container (RIC) element	Adversary observes the presence of the optional RIC element	Same as above.
Adversary observes the FMS Request element	Adversary observes the presence of the optional Flexible Multicast Service request and the interval at which the station requests multicast to be delivered.	Same as above.
Adversary observes the DMS Request element	Adversary observes the presence of the optional Directed Multicast Service request and the interval at which the station requests multicast to be unicasted.	Same as above.

A.4.9 Reassociation Response Frame (Management frame)

The reassociation response frame is similar in structure to the association response frame. All the elements of the association response frame are present in the reassociation response frame. The following elements are present in the reassociation frame, but not in the association frame:

Risk	Threat	Threat Analysis
Adversary observes the Resource Information Container (RIC) element	Adversary observes the presence of the optional RIC element	Adversary can use this to fingerprint an AP.
Adversary observes the FMS Request element	Adversary observes the presence of the optional Flexible Multicast Service request and the interval at which the station requests multicast to be delivered.	Same as above.

Risk	Threat	Threat Analysis
Adversary observes the DMS Request element	Adversary observes the presence of the optional Directed Multicast Service request and the interval at which the station requests multicast to be unicasted.	Same as above.

The following element was not considered as identifying in the reassociation frame response: RSN (element ID 10).

A.4.10 Probe Request Frame (Management frame)

The probe request contains some elements identical to the Association request frame (4.5), including the Supported rates and BSS Membership selector element, the Extended Supported Rates and BSS membership selector element, the Supported Operating classes element, the HT capabilities element, the 20/40 BSS Coexistence element, the Extended Capabilities element, the Interworking element, the Multiband element, the DMG Capabilities element, the Multiple MAC Sublayers element, the VHT capabilities element, and the Vendor specific element. Their characteristics are identical for the association request and the probe request and analysis is not repeated here.

The probe request also includes the following elements, that are not included in the association request:

Risk	Threat	Threat Analysis
Adversary observes the SSID element	Adversary observes if the SSID element is broadcast or a list of specific strings	Adversary can use this to fingerprint a STA.
Adversary observes the DSS Parameter Set	Adversary observes if this optional element specifying the current channel is present.	Same as above.
Adversary observes the SSID list	Adversary observes the presence of this optional element, and the list of SSIDs for which the STA requests information (one probe for many SSIDs)	Same as above.
Adversary observes the Channel Usage element	Adversary observes the presence of this optional element, and the channel that the STA requests for TDLS communications	Same as above.
Adversary observes the Mesh ID element	Adversary observes the presence of this optional element, and the ID of the mesh network the station is part of.	Same as above. Can also be used to locate the STA.
Adversary observes the Estimated Service Parameter element	Adversary observes the presence of this optional element, and the estimated throughput that the STA calculates for traffic from the AP	Same as above. Can also be used to locate the STA.

Risk	Threat	Threat Analysis
Adversary observes the Extended request element	Adversary observes the presence of this optional element and the list of elements for which the STA would like information in the probe response.	Same as above.

A.4.11 Authentication Frame (Management frame)

Risk	Threat	Threat Analysis
Adversary observes the status code in AP response	Adversary generates valid authentication frames (Open system), and observes the responses from the AP with status code Not rejected with suggested BSS transition	Adversary can use this to fingerprint an AP.
	Adversary generates invalid or invalid authentication frames (Open System), and observes the responses from the AP with status code rejected with suggested BSS transition	Same as above.
	Adversary generates valid authentication frames (FT), and observes the responses from the AP with status code Not rejected with suggested BSS transition	Same as above.
	Adversary generates valid or invalid authentication frames (FT), and observes the responses from the AP with status code rejected with suggested BSS transition	Same as above.
	Adversary generates valid authentication frames (802.11s/Simultaneous Authentication of Equals / SAE), and observes the responses from the AP with status code Not rejected with suggested BSS transition	Same as above.
	Adversary generates valid or invalid authentication frames (SAE), and observes the responses from the AP with status code rejected with suggested BSS transition	Same as above.
Adversary observes the MDIE in AP response	Adversary observes the presence and value of the MDIE in the AP response	Same as above.
Adversary observes the MDIE in STA request	Adversary observes the presence and value of the MDIE in the STA request	Adversary can use this to fingerprint a STA

Risk	Threat	Threat Analysis
Adversary observes the FTE in STA request	Adversary observes the presence of the FT element	Same as above.
Adversary observes the FTE in AP response	Adversary observes the presence and value of the FT element (and suggested neighbors)	Adversary can use this to fingerprint an AP
Adversary observes the RIC element in AP response	Adversary observes the presence of 802.11r RIC element and value	Same as above.
Adversary observes the Timeout Interval in AP response	Adversary observes the presence of 802.11r reassociation deadline and value	Same as above.
Adversary observes the Finite Cyclic Group in STA request	Adversary observes the presence and value of the SAE Finite Cyclic Group	Adversary can use this to fingerprint a STA.
Adversary observes the Finite field element in STA request	Adversary observes the presence and value of the SAE Finite field element	Same as Above.
Adversary observes the Anti clogging token in STA request	Adversary observes the presence and value of the anti clogging token	Same as above.
Adversary observes the Scalar element in STA request	Adversary observes the presence and value of the Scalar element	Same as above.
Adversary observes the Send-Confirm element in AP response	Adversary observes the presence and value of the Send confirm element	Adversary can use this to fingerprint an AP.
Adversary observes the Confirm element in AP response	Adversary observes the presence and value of the confirm element	Same as above
Adversary observes the presence of the multi-band element	Adversary observes the presence and value of the multi band element	Adversary can use this to fingerprint the emitter (STA or AP)
Adversary observes the Neighbor report in AP response	Adversary observes the presence and value of the Neighbor report	Adversary can use this to fingerprint an AP.
Adversary observes the vendor specific element	Adversary observes the presence and value of vendor specific element(s)	Adversary can use this to fingerprint the emitter (STA or AP)

A.4.12 Deauthentication Frame (Management frame)

Deauthentication frames include reason codes. Reasons codes have been examined in section 4.4. Deauthentication frames specific elements include:

Risk	Threat	Threat Analysis
Adversary observes the Management MIC Element	Adversary observes the presence of Management MIC Element in AP deauthentication frames	Adversary can use this to fingerprint an AP.
Adversary observes vendor specific element(s)	Adversary observes the presence and value of vendor specific element(s)	Same as above.

A.4.13 Action Frame (Management frame)

Risk	Threat	Threat Analysis
Adversary observes the Management MIC Element	Adversary observes the presence of Management MIC Element in AP action frames	Adversary can use this to fingerprint an AP.
Adversary observes vendor specific element(s)	Adversary observes the presence and value of vendor specific element(s)	Same as above.
Adversary observes the Authenticated Mesh Peering Exchange Element	Adversary observes the presence of this optional element which indicates that a PMK exists between the sender and the recipient.	Same as above.

Specific action frames present specific risks:

Risk	Threat	Threat Analysis
Adversary observes the channel switch announcement field in the Spectrum Management Action frame	Adversary observes the channel indicated and switch time in the channel switch announcement	Adversary can use this to fingerprint an AP.
Adversary observes the Measurement request frame	Adversary observes the elements requested in the measurement request	Same as above. Adversary can also fingerprint the STA (when frame sent by STA)
Adversary observes Measurement Report frame	Adversary observes the elements reported in the report.	Same as above.
Adversary observes the TPC request frame	Adversary observes the elements requested in the transmit power control request	Same as above.
Adversary observes TPC Report frame	Adversary observes the elements reported in the report.	Same as above.
Adversary observes the Channel switch announcement action frame.	Adversary observes the channel in the announcement, the secondary channel offset and the optional mesh channel switch parameters, wide bandwidth channels switch element and new transmit power envelope element	Adversary can use this to fingerprint an AP.
Adversary observes the ADDTS Request or ADDTS Reserve Request QoS action frame	Adversary observes the flow described in the request	Adversary can use this to fingerprint a station.

Risk	Threat	Threat Analysis
Adversary observes ADDTS Response or ADDTS Reserve Response QoS action frame	Adversary observes the AP response	Adversary can use this to fingerprint an AP.
	Adversary triggers various ADDTS requests to observe AP response	Same as above.
Adversary observes the QoS Schedule QoS action frame	Adversary observes the Schedule values for data and polls frames	Same as above.
Adversary observes the DELTS QoS action frame	Adversary observes the flow marked for deletion.	Adversary can use this to fingerprint a STA.
Adversary observes the QoS map Configure Action frame	Adversary observes map reported in the action frame.	Adversary can use this to fingerprint an AP.
Adversary observes the Direct Link Setup (DLS) Request frame	Adversary observes the source and destination MAC addresses, DLS timeout value, supported rates, HT capabilities, VHT capabilities and/or AID in the request	Adversary can use this to fingerprint a STA.
Adversary observes DLS response	Adversary observes the same elements as in the request	Same as above.
Adversary observes the DLS teardown frame	Adversary observes source and destination MAC in the teardown frame	Same as above.
Adversary observes the ADDBA (block Ack) request	Adversary observes the BA parameters, timeout value, starting sequence control and optional Group Address, Multiband, TCLAS and extensions elements	Same as above.
Adversary observes the ADDBA response	Adversary observes the same elements as in the request	Same as above.
Adversary observes the DELBA Action frame	Adversary observes the parameter set, reason code, group address and optional multiband and TCLAS elements	Same as above.
Adversary observes Vendor specific action frames (any subtype of action frame classified as vendor specific)	Adversary observes the identifiers in the vendor specific action frame, along with the parameters	Adversary can use this to fingerprint the sender and recipient (AP or STA).
Adversary observes the radio measurement request frame	Adversary observes the repetition field and measured elements field	Adversary can use this to fingerprint the sender (AP or STA).
Adversary observes the radio measurement response	Adversary observes the measured elements	Adversary can use this to fingerprint the sender (AP or STA).
Adversary observes the neighbor report response frame	Adversary observes the reported channels, PHY types and optional location civic measurement and other optional elements	Adversary can use this to fingerprint the sender (AP or STA).

Risk	Threat	Threat Analysis
Adversary observes the Link Measurement Report frame	Adversary observes the transmit and receive antenna ID, the power values, channel and SNR values	Adversary can use this to fingerprint the sender (AP or STA).
Adversary observes The Public Action BSS Coexistence frame	Adversary observes 20/40 BSS coexistence and intolerant channel report elements	Same as above.
Adversary observes The Public Action Measurement Pilot frame	Adversary observes operating class, channel, measurement pilot interval and optional elements	Same as above.
Adversary observes The Public Action DSE Enablement frame	Adversary observes the requester and responder STA addresses and the enablement identifier (if present)	Same as above.
Adversary observes The Public Action DSE Deenablement frame	Adversary observes the requester and responder STA addresses	Same as above.
Adversary observes The Public Action DSE Registered Location Announcement frame	Adversary observes the coordinates present in the announcement	Same as above.
Adversary observes the Public Action Extended Channel switch announcement action frame.	Adversary observes the channel in the announcement, the secondary channel offset and the optional mesh channel switch parameters, wide bandwidth channels switch element and new transmit power envelope element	Adversary can use this to fingerprint an AP.
Adversary observes The Public Action DSE Measurement Request frame	Adversary observes requester and responder addresses, the operating class, channel number, measurement start time and duration	Adversary can use this to fingerprint the sender (AP or STA).
Adversary observes The Public Action DSE Measurement Report frame	Adversary observes requester and responder addresses, the operating class, channel number, measurement start time and duration and reported values	Same as above.
Adversary observes the Public Action DSE Power constraint frame	Adversary observes the requester and responder addresses, along with the local power constraint element and the reason code	Same as above.
Adversary observes the Public Action GAS initial request frame	Adversary observes the requested elements	Same as above.
Adversary observes the Public Action GAS	Adversary observes the query response elements	Same as above.
Adversary observes the Public Action GAS Comeback Request frame	Adversary observes the GAS comeback request coming from a supporting sta	Same as above.
Adversary observes the Public Action GAS comeback Response	Adversary observes the comeback delay, advertisement protocol element and the query response	Same as above.

Risk	Threat	Threat Analysis
	Adversary generates various GAS comeback requests and observes the responses	Same as above.
Adversary observes the Public Action TDLS Discovery Response frame	Adversary observes the capability, supported rates, extended supported rates, supported channels, RSNE, FTE, TPK key lifetime, operating classes, HT capabilities, 20/40 Coexistence element, link identifier, multiband and VHT elements, when present, and their values	Same as above.
Adversary observes the Public Action Location Track Notification frame	Adversary observes the location parameters elements and optional measurement report element values	Same as above.
Adversary observes the Public Action Quality of Service Management Policy Frame	Adversary observes the presence of the QMF Policy frame and its parameters	Adversary can use this to fingerprint an AP.
Adversary observes the Public Action Quality of Service Management Policy Change Frame	Adversary observes the presence of the QMF Policy Change frame and its parameters	Same as above.
Adversary observes the Public Action QLoad Request	Adversary observes the presence of the Qload request frame	Same as above.
Adversary observes the Public Action QLoad Response frame	Adversary observes the presence of the Qload response, along with the displayed element (traffic self, traffic shared, overlap, sharing policy, EDCA and HCCA parameters)	Same as above
	Adversary creates and sends QLoad request frames and observes the responses	Same as above
Adversary observes the Public Action Adversary observes the Public Action HCCA TXOP Advertisement frame	Adversary observes the presence of this frame and the possible reported TXOP reservations	Same as above
Adversary observes the Public Action HCCA TXOP Response frame	Adversary observes the presence of this frame and the schedule information for each TXOP reservation in the request	Same as above
Adversary observes the Public Action Public Key frame	Adversary observes the presence of this frame and the AP public key provided	Same as above.
Adversary observes the Public Action Channel Availability Query frame	Adversary observes the presence of this frame, and the requester / responder MAC addresses, the device class, identification and location information	Same as above.

Risk	**Threat**	**Threat Analysis**
Adversary observes the Public Action Channel Schedule Management frame	Adversary observes the presence of this frame, and the requester / responder MAC addresses, the channel schedule management code, the device identification information and schedule descriptor	Same as above.
Adversary observes the Public Action Contact Verification Signal frame	Adversary observes the presence of this frame and the WMS elements reported, such as channel, power, validity duration of the channel, channel bandwidth limits	Same as above.
Adversary observes the Public Action GDD Enablement Request frame	Adversary observes the presence of this frame and the device unique identifier in the frame	Same as above.
Adversary observes the Public Action GDD Enablement Response frame	Adversary observes the presence of this frame and the device unique identifier in the frame	Same as above.
Adversary observes the Public Action Network Channel Control Frame	Adversary observes presence of the frame and the requester / responder addresses, operating class, channel number and max transmit power values	Same as above.
Adversary observes the Public Action White Space Map (WSM) announcement frame	Adversary observes the presence of this frame and the map of available channels authorized	Same as above.
Adversary observes the Public Action Fine Timing Measurement request frame	Adversary observes the presence of the frame, the civic location information and measurement parameters	Same as above.
Adversary observes the Public Action Fine Timing Measurement frame	Adversary observes the presence of the frame, the civic location information, measurement parameters and optional synchronization information	Same as above.
Adversary observes the Public Action QAB request frame	Adversary observes the presence of the Quiet period request frame, the requester / responder MAC addresses, the target SSID, requested quiet period, offset and duration values	Same as above.
Adversary observes the Public Action QAB Response frame	Adversary observes the presence of the Quiet period response frame, the requester / responder MAC addresses, the target SSID, requested quiet period, offset and duration values	Same as above.
Adversary observes the FT Request frame	Adversary observes the presence of the FT request frame, the mobility domain, RSN and target AP addresses values	Adversary can use this information to fingerprint a station.

Risk	Threat	Threat Analysis
Adversary observes the FT response frame	Adversary observes the presence of this frame, mobility domain, RSN and status code values	Adversary can use this information to fingerprint an AP.
Adversary observes the FT Confirm frame	Adversary observes the presence of this frame, mobility domain, RSN and RIC values	Adversary can use this information to fingerprint a station.
Adversary observes the FT ACK frame	Adversary observes the presence of this frame, mobility domain, RSN, RIC and status code values	Adversary can use this information to fingerprint an AP.
Adversary observes the SA query or SA response frames	Adversary observes the presence of these frames	Adversary can use this information to fingerprint an AP or a STA.
Adversary observes the HT PSMP action frame	Adversary observes the presence of this frame, and the PSMP parameters for each PSMP station	Adversary can use this information to fingerprint an AP
Adversary observes the HT CSI frame	Adversary observes the presence of this frame and the CSI information reported (SNR for each chain, carrier and streams identifiers)	Adversary can use this information to fingerprint an AP or a STA
Adversary observes the HT Non compressed or the Compressed beam forming frame	Adversary observes the presence of this frame and the CSI information reported (SNR for each chain, carrier and streams identifiers)	Adversary can use this information to fingerprint an AP or a STA
Adversary observes the TDLS Setup request frame	Adversary observes the presence of the tunneled direct link sequence frame and the capability, supported rates and BSS membership, country, extended supported rate and BSS membership selector, supported channels, RSNE extended capabilities, QoS capabilities, FTE, timeout interval, supported operating classes, HT capabilities, 20/40 coexistence, link identifier, multiband, VHT capability and AID fields	Adversary can use this information to fingerprint a STA
Adversary observes the TDLS Setup response frame	Adversary observes the presence of the tunneled direct link sequence frame and the capability, supported rates and BSS membership, country, extended supported rate and BSS membership selector, supported channels, RSNE extended capabilities, QoS capabilities, FTE, timeout interval, supported operating classes, HT capabilities, 20/40 coexistence, link identifier, multiband, VHT capability, Operating mode notification and AID fields	Same as above.

Risk	Threat	Threat Analysis
Adversary observes the TDLS Setup Confirm frame	Adversary observes the presence of the tunneled direct link sequence frame and the RSNE, EDCA parameter set, FTE, timeout interval, HT operations, Link identifier, VHT Operation, and Operating mode notification fields	Same as above.
Adversary observes the TDLS Teardown frame	Adversary observes the presence of the tunneled direct link sequence frame, the link identifier and the optional FTE fields	Same as above.
Adversary observes the TDLS Peer Traffic Indication frame	Adversary observes the presence of the tunneled direct link sequence frame, the link identifier and the optional PTI control fields	Same as above.
Adversary observes the TDLS Channel Switch Request frame	Adversary observes the presence of the tunneled direct link sequence frame, the operating class, link identifier, channel switch timing, transmit power enveloped, and optional secondary channel offset, country and wide bandwidth channel switch fields	Same as above.
Adversary observes the TDLS Channel Switch Response frame	Adversary observes the presence of the tunneled direct link sequence frame, the link identifier and channel switch timing fields	Same as above.
Adversary observes the TDLS Peer PSM Request frame	Adversary observes the presence of the tunneled direct link sequence frame, the link identifier and wakeup schedule fields	Same as above.
Adversary observes the TDLS Peer PSM Response frame	Adversary observes the presence of the tunneled direct link sequence frame, and the link identifier field	Same as above.
Adversary observes the TDLS Discovery Request frame	Adversary observes the presence of the tunneled direct link sequence frame, and the link identifier and multiband fields	Same as above.
Adversary observes the WNM Event Request frame	Adversary observes the presence of the Wireless Network management frame, and the request events fields, such as vendor specific, WNM logs or peer to peer link fields	Adversary can use this information to fingerprint an AP or a STA.
Adversary observes the WNM Event Report frame	Adversary observes the presence of the Wireless Network management frame, and the report events fields, such as vendor specific, WNM logs or peer to peer link fields	Same as above.

Risk	Threat	Threat Analysis
Adversary observes the WNM Diagnostic Request frame	Adversary observes the presence of the Wireless Network management frame, and the requested diagnostic fields, such as configuration profile, association diagnostic, 802.1x authentication diagnostic or vendor specific fields.	Same as above.
Adversary observes the WNM Diagnostic Report frame	Adversary observes the presence of the Wireless Network management frame, and the reported diagnostic fields, such as configuration profile, association diagnostic, 802.1x authentication diagnostic or vendor specific fields.	Same as above.
Adversary observes the WNM Location Configuration Request frame	Adversary observes the presence of the Wireless Network management frame, and the requested fields, such as radio, location information, motion information, time of departure information and vendor specific fields	Same as above.
Adversary observes the WNM Location Configuration Response frame	Adversary observes the presence of the Wireless Network management frame, and the reported fields, such as radio, location information, motion information, time of departure information and vendor specific fields	Same as above.
Adversary observes the VNM BSS transition Management Query frame	Adversary observes the presence of the Wireless Network management frame, and the location indication channels, parameters, options and status of neighboring APs, along with vendor specific information	Adversary can use this information to fingerprint a STA.
Adversary observes the VNM BSS transition Management Request frame	Adversary observes the presence of the Wireless Network management frame, and the BSS transition candidate list fields	Adversary can use this information to fingerprint an AP.
Adversary observes the VNM BSS transition Management response frame	Adversary observes the presence of the Wireless Network management frame, and the BSS transition candidate list fields and optional target BSSID	Adversary can use this information to fingerprint a STA.
Adversary observes the VNM FMS request frame	Adversary observes the presence of the Wireless Network management Flexible Multicast Service frame, and the target addresses and ports for which FMS is requested	Adversary can use this information to fingerprint a STA.
Adversary observes the VNM FMS Response frame	Adversary observes the presence of the Wireless Network management Flexible Multicast Service frame, and the target addresses and ports for which FMS is granted (or declined)	Adversary can use this information to fingerprint an AP.

Risk	Threat	Threat Analysis
Adversary observes the VNM Interference request frame	Adversary observes the presence of the Wireless Network management frame, and the automatic report and report timeout values	Adversary can use this information to fingerprint an AP or a STA.
Adversary observes the VNM Interference report frame	Adversary observes the presence of the Wireless Network management frame, and the report period, interference accuracy and index and details (interval, burst length, duty cycle, frequency and bandwidth)	Same as above.
Adversary observes the VNM TFS Request frame	Adversary observes the presence of the Wireless Network management Traffic Filtering Service frame, and the traffic requested to be filtered, along with optional vendors specific elements	Adversary can use this information to fingerprint a STA.
Adversary observes the VNM TFS Response frame	Adversary observes the presence of the Wireless Network management Traffic Filtering Service frame, and the traffic identifier to be filtered, along with optional vendors specific elements	Adversary can use this information to fingerprint an AP.
Adversary observes the VNM TFS Notify frame	Adversary observes the presence of the Wireless Network management Traffic Filtering Service frame, and the number and list of traffic IDs to be filtered	Same as above.
Adversary observes the VNM TFS Notify Response frame	Adversary observes the presence of the Wireless Network management Traffic Filtering Service frame, and the number and list of traffic IDs to be filtered	Adversary can use this information to fingerprint a STA.
Adversary observes the VNM Sleep Mode request frame	Adversary observes the presence of the Wireless Network management Sleep mode frame, along with the sleep interval, and traffic IDs to be filtered during sleep	Same as above.
Adversary observes the VNM Sleep mode Response frame	Adversary observes the presence of the Wireless Network management Sleep mode response frame, along with traffic IDs to be filtered (or denied to be filtered) during sleep	Adversary can use this information to fingerprint an AP.
Adversary observes the VNM TIM broadcast request frame	Adversary observes the presence of the Wireless Network management frame, along with the interval requested by the STA for TIM broadcast	Adversary can use this information to fingerprint a STA
Adversary observes the VNM TIM broadcast response frame	Adversary observes the presence of the Wireless Network management frame, along with the interval (high rate, low rate, offset) accepted by the AP for TIM broadcast	Adversary can use this information to fingerprint an AP

Risk	Threat	Threat Analysis
Adversary observes the VNM QoS traffic capability update frame	Adversary observes the presence of the Wireless Network management frame, along with the UP reported as supported by the STA	Adversary can use this information to fingerprint a STA
Adversary observes the VNM Channel Usage Request frame	Adversary observes the presence of the Wireless Network management frame, and the channels for which usage is request	Adversary can use this information to fingerprint a STA
Adversary observes the VNM Channel Usage Response frame	Adversary observes the presence of the Wireless Network management frame, the channels for which usage is provided, along with optional power constraint, EDCA parameter sets and transmit power envelope fields	Adversary can use this information to fingerprint an AP
Adversary observes the VNM DMS Request frame	Adversary observes the presence of the Wireless Network management Directed Multicast Service frame, and the described traffic for which DMS is requested, along with optional subelements	Adversary can use this information to fingerprint a STA
Adversary observes the VNM DMS Response frame	Adversary observes the presence of the Wireless Network management Directed Multicast Service frame, and the described traffic for which DMS status is provided, along with optional subelements	Adversary can use this information to fingerprint an AP
Adversary observes the VNM Timing Measurement Request frame	Adversary observes the presence of the Wireless Network management frame, along with the interval at which the request is made	Adversary can use this information to fingerprint an AP or a STA
Adversary observes the VNM Notification Request frame	Adversary observes the presence of the Wireless Network management frame, along with the element notified, such as firmware update or vendor specific information	Adversary can use this information to fingerprint an AP or a STA
Adversary observes the VNM Notification Response frame	Adversary observes the presence of the Wireless Network management frame (status itself is not relevant)	Adversary can use this information to fingerprint an AP or a STA

Risk	Threat	Threat Analysis
Adversary observes the Mesh Peering Open frame	Adversary observes the presence of the frame, along with the advertised fields (capability, supported rates and BSS membership selectors, extended supported rates and BSS membership selectors, power capability, supported channels, RSN, mesh ID, mesh configuration, mesh peering management, ERP information, supported operating classes, HT capabilities, HT operations, 20/40 BSS coexistence elements, extended capabilities elements, internetworking, VHT capabilities, VHT operation, operating mode notification	Adversary can use this information to fingerprint an AP
Adversary observes the Mesh Peering Confirm frame	Adversary observes the presence of the frame, along with the advertised fields (capability, AID, supported rates and BSS membership selectors, extended supported rates and BSS membership selectors, RSN, mesh ID, mesh configuration, mesh peering management, HT capabilities, HT operations, 20/40 BSS coexistence elements, extended capabilities elements, VHT capabilities, VHT operation, operating mode notification	Same as above
Adversary observes the Mesh Peering Close frame	Adversary observes the presence of the frame, along with the mesh ID and mesh peering management fields	Same as above
Adversary observes the mesh group key inform frame	Adversary observes the presence of the frame, along with the peering exchange values	Same as above
Adversary observes the mesh group key acknowledge frame	Adversary observes the presence of the frame, along with the peering exchange values	Same as above
Adversary observes the mesh link metric report frame	Adversary observes the presence of the frame along with the metric reported for the link between both APs	Same as above
Adversary observes the mesh HWMP path selection frame	Adversary observes the presence of the frame, along with the path queried or reported in the Hybrid Wireless Mesh Protocol fields	Same as above
Adversary observes the mesh Gate announcement frame	Adversary observes the presence of the frame, along with the address of the gate announced by the sender	Same as above
Adversary observes the mesh Congestion Control Notification frame	Adversary observes the presence of the frame, along with the address of the node to which link is congested	Same as above

Risk	Threat	Threat Analysis
Adversary observes the mesh MCCA setup request frame	Adversary observes the presence of the mesh coordination function controlled channel access frame	Same as above
Adversary observes the mesh MCCA setup reply frame	Adversary observes the presence of the mesh coordination function controlled channel access frame	Same as above
Adversary observes the mesh MCCA Advertisement request frame	Adversary observes the presence of the mesh coordination function controlled channel access frame	Same as above
Adversary observes the mesh MCCA teardown frame	Adversary observes the presence of the mesh coordination function controlled channel access frame	Same as above
Adversary observes the mesh TBTT Adjustment request frame	Adversary observes the presence of the frame and intervals requested in the request	Same as above
Adversary observes the mesh TBTT Adjustment response frame	Adversary observes the presence of the frame and intervals indicated in the response	Same as above
Adversary observes the mesh Multihop Proxy Update frame	Adversary observes the presence of the frame and the addresses of the proxy mesh APs indicated in the update	Same as above
Adversary observes the Multihop Proxy Update Confirmation frame	Adversary observes the presence of the frame and the addresses of the proxy mesh APs acknowledged in the confirmation frame	Same as above
Adversary observes the Robust SCS Request frame	Adversary observes the presence of the frame and the Stream Classification request frame, along with the traffic identified in the fields and optional subelements	Adversary can use this information to fingerprint an AP or a STA
Adversary observes the Robust SCS Response frame	Adversary observes the presence of the frame and the status for the traffic identified in the fields and optional subelements	Same as above
Adversary observes the Robust Group Membership Request frame	Adversary observes the presence of the frame	Same as above
Adversary observes the Robust Group Membership Response frame	Adversary observes the presence of the frame and the group mac addresses reported in the response	Same as above
Adversary observes the DMG Power save configuration request frame	Adversary observes the presence of the frame and the optional schedule element	Same as above
Adversary observes the DMG Power save configuration response frame	Adversary observes the presence of the frame and the optional schedule element along with the optional antenna sector ID pattern element	Same as above

Risk	Threat	Threat Analysis
Adversary observes the DMG Information request frame	Adversary observes the presence of the frame and the elements requested	Same as above
Adversary observes the DMG Information response frame	Adversary observes the presence of the frame and the elements supported in the response	Same as above
Adversary observes the DMG handover request frame	Adversary observes the presence of the frame and timer after which handover is requested	Same as above
Adversary observes the DMG Information response frame	Adversary observes the presence of the frame (status code is not relevant)	Same as above
Adversary observes the DMG DTP Request frame	Adversary observes the presence of the Dynamic Tone Pairing frame	Same as above
Adversary observes the DMG DTP Report frame	Adversary observes the presence of the Dynamic Tone Pairing frame and the reported values for the link	Same as above
Adversary observes the DMG Relay Search request frame	Adversary observes the presence of the frame and the address for which a relay is searched	Same as above
Adversary observes the DMG Relay Search response frame	Adversary observes the presence of the frame and the number of relay capable STAs along with the information about these relays	Same as above
Adversary observes the DMG multi-relay channel measurement request frame	Adversary observes the presence of the frame	Same as above
Adversary observes the DMG multi-relay channel measurement report frame	Adversary observes the presence of the frame and the channels measured, along with the information about each measured channel	Same as above
Adversary observes the DMG RLS request frame	Adversary observes the presence of the frame, along with the address of the source, destination and destination for which relay link setup is requested	Same as above
Adversary observes the DMG RLS Response frame	Adversary observes the presence of the frame, along with the destination and relay status codes	Same as above
Adversary observes the DMG RLS Announcement frame	Adversary observes the presence of the frame, along with the destination ID for which RLS is announced	Same as above
Adversary observes the DMG RLS teardown frame	Adversary observes the presence of the frame, along with the relay and source AID for which RLS is tore down	Same as above
Adversary observes the DMG Relay ACK request frame	Adversary observes the presence of the frame	Same as above
Adversary observes the DMG Relay ACK response frame	Adversary observes the presence of the frame	Same as above

Risk	Threat	Threat Analysis
Adversary observes the DMG TPA Request frame	Adversary observes the presence of the Third Party Auditor frame along with the timing and sampling frequency offset values	Same as above
Adversary observes the DMG TPA Response frame	Adversary observes the presence of the Third Party Auditor frame and the dialog token	Same as above
Adversary observes the DMG TPA Report frame	Adversary observes the presence of the Third Party Auditor frame (status code is not relevant)	Same as above
Adversary observes the DMG ROC Request frame	Adversary observes the presence of the Relay Operation Change request and the relay operation type for which change is requested	Same as above
Adversary observes the DMG ROC Response frame	Adversary observes the presence of the Relay Operation Change frame (status code is not relevant)	Same as above
Adversary observes the FST Setup Request frame	Adversary observes the presence of the fast session transfer request frame, along with the optional multi-band, switching stream and awake window fields	Same as above
Adversary observes the FST Setup Response frame	Adversary observes the presence of the fast session transfer response frame, along with the optional multi-band, switching stream, timeout interval and awake window fields	Same as above
Adversary observes the FST Tear Down frame	Adversary observes the presence of the fast session transfer frame, along with the FSTS ID field.	Same as above
Adversary observes the FST ACK Request frame	Adversary observes the presence of the fast session transfer frame, along with the FSTS ID field.	Same as above
Adversary observes the FST ACK Response frame	Adversary observes the presence of the fast session transfer frame, along with the FSTS ID field.	Same as above
Adversary observes the FST On-channel tunnel Request frame	Adversary observes the presence of the fast session transfer frame, along with description of the MMPDU for which encapsulation is requested.	Same as above
Adversary observes the VHT Compressed Beamforming frame	Adversary observes the presence of the frame along with the compressed beamforming report values, and the MU exclusive beamforming report values	Same as above
Adversary observes the VHT Group ID Management frame	Adversary observes the presence of the frame along with the membership status and user position values	Adversary can use this information to fingerprint an AP
Adversary observes the VHT Operating mode notification frame	Adversary observes the presence of the frame and the channel width changes and SS changes reported	Adversary can use this information to fingerprint an AP or a STA

The following frames were not identified as threat: Radio Measurement Neighbor report, Radio Measurement Link Measurement Request, HT notify channel width, HT SM power save frame, set PCO frame (obsolete, never implemented), HT Antenna selection indices,

A.4.14 Action no Ack Frame (Management frame)

Structure is similar to Action frame, with the exception that Action No Ack only contain vendor-specific elements (no Mesh Peering Exchange Element, no Management MIC Element).

A.4.15 Timing Advertisement Frame (Management frame)

Risk	Threat	Threat Analysis
Adversary observes the Capability Information Element	Adversary observes the capabilities advertised in the Element	Adversary can use this to fingerprint an AP.
Adversary observes the Extended Capability Information Element	Adversary observes the capabilities advertised in the Element	Same as above.
Adversary observes the Power Constraint	Adversary observes the optional Power Constraint IE	Same as above
Adversary observes the Time Advertisement Element	Adversary observes time advertised, and / or observes the time drift from one advertisement to the net.	Same as above.
Adversary observes vendor specific element(s)	Adversary observes the presence and value of vendor specific element(s)	Same as above.

Element that was not seen a threat: Country value (common to all APs).