IEEE 802 Privacy Threat Analysis

Brian Weis
Cisco Systems
7/18/16

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 "fingerprint" devices associated with people, which is to analyze packets from a network device in order to observe or deduce Personally identifiable information (PII). The IEEE P802E standard will provide privacy recommendations related to IEEE 802 standards. This privacy threat analysis notes where fingerprinting is enabled in IEEE 802 standards, and is provided as a contribution to the development of these privacy recommendations.

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) that is considered a Personal Device. 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.

A reader might be surprised that IEEE 802 protocols could contain PII at all, since these protocols relate to the communication of a device on a Local Area or Metropolitan Area Network and for the most part does not directly identity a person. But the role of a network protocol is often to provide communication between a user of a network and a service instance. In order to provide this communication, some notion of user identity, or proxy for a user identity, must be maintained as protocol state in order to maintain a consistent and reliable service. For example, many protocols carry Priority Code Point (PCP) data, which has a purpose of ensuring certain classes of traffic will be afforded less delay than others within a network. However, by its very presence this marking also allows those classes of traffic to be more easily identified by an Adversary. This is not a fault of the network, but must be taken into account when identifying possible privacy threats.

This communication (and any contained PII) is not necessarily visible at some points along the route taken by the network protocol, but typically can be observed somewhere in the network. This threat analysis identifies protocol elements that can be considered PII, and possibly ways that they can be used for fingerprinting a person.

Note that an entity performing fingerprinting of network protocols is not necessary a threat to privacy. Only if the intent of the fingerprinting is to correlate the fingerprinting with a person (or class of persons) would this generally be considered a threat. For example, fingerprinting followed by a process anonymizing the PII network fields (e.g., with the goal of understanding network performance would not be considered a privacy threat).

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 capability to observe and manipulate Target and Respondent frames anywhere in a bridged network.
- **Fingerprinting**. The process correlating PII and/or other network attributes to identify a network identity. When the correlation is performed with the goal of identifying a target, the entity performing the fingerprinting is considered an adversary.
- **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 personal devices.
- **Personal Device**. A device associated with a person.
- **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**. A machine emitting network frames that can be associated with a person, and on which an Adversary can fingerprint.
- **Target MAC address.** The SA or DA in a network frame that is associated with a Target.
- **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]).

4 Tools 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 the device to reveal PII
- **Modification**. Changing frames sent to/from a target in order to cause it to reveal PII.

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, the term Target MAC Address is used, where either the SA of DA might possibly be PII. (Of course, for frames directed to the Target the DA would be considered PII.)

A Target MAC address is considered PII if it is 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 because it is a shared service device, and therefore the bridge would not be considered a Target. However, a bridge associated with a residential gateway network device 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.

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 Higher Layer LAN Protocols

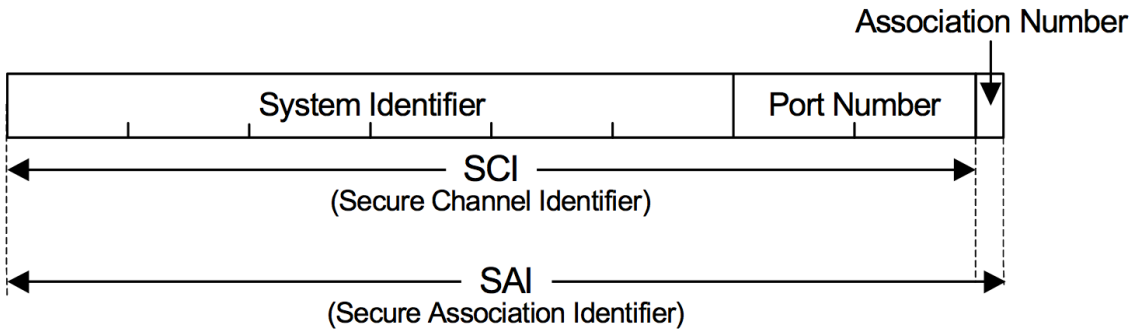
The following IEEE 802.1 protocol elements and management frames have been evaluated for privacy considerations.[1]

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 a Personal Device 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

Threats:

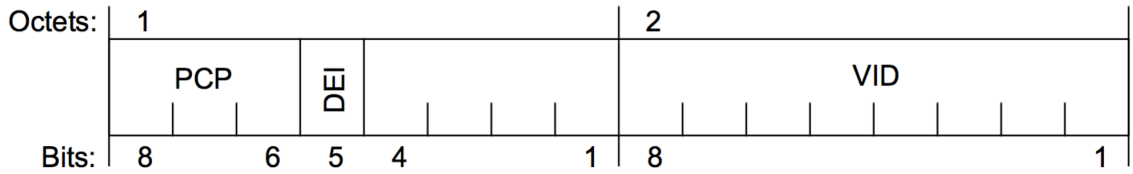
1. Classes of Targets may be identified based on the PCP, if the adversary is aware of the PCP mappings. Some mappings are de-facto or actual standards. Identification of voice and video traffic are well known and can aid in the identification of classes of Targets.

[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.

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 a VLAN Identifier (VID) used to classify the frame. A VID is often used to separate different types of traffic, such as traffic from different organizations or individuals with different roles in the organization. A VID can be included in a Customer VLAN Tag, Service VLAN Tag, Backbone VLAN Tag, Backbone Service Instance Tag

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.

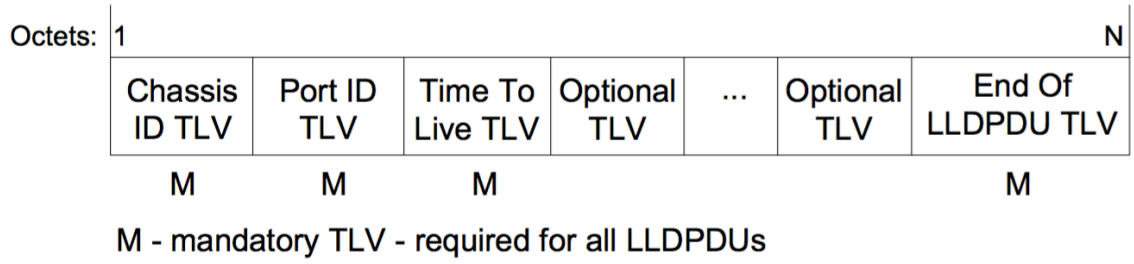
Threats:

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] messages. The EAP protocol allows a user or network device to authenticate itself to the network and be admitted . EAP 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).

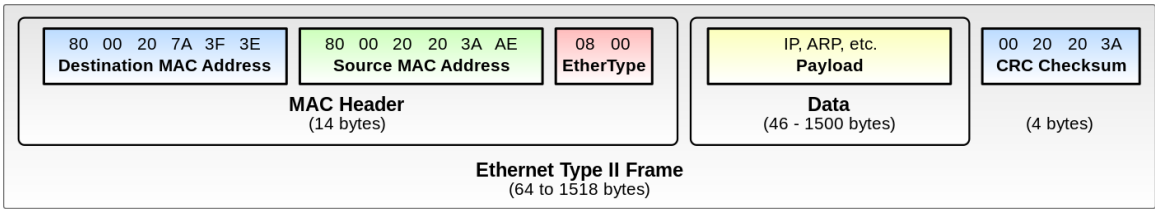
Threats:

1. A passive adversary between the target and EAP authenticator can observe any information that an EAP method passes without confidentiality protection. Some EAP methods (e.g., a “tunneled EAP” method such as TEAP (RFC 7170)) protect the complete contents of the authentication process from a passive adversary.
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

TBD

5.5 IEEE 802.15

TBD

5.6 IEEE 802.21

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.

[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.

[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.
	Adversary observes and logs the Target MAC address, correlates it with other network accesses to or from this Target	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. as used in Provider Backbone Bridged Newtorks (“MAC-in-MAC”).	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.	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 correlation can allow attacker to observe the frames of a single Talker stream and identify the type of traffic.
	Adversary observers StreamID as a single unit	Same as above.
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 at the hypervisor level of a shared data center may use the VSIID to track the target. (VALIDATE)

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.	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 CFM messages (Clauses 18 & 19)	Attacker observes a MA Endpoint (MEP) associated with an end station attachment to a LAN (Clause 19.2)	The MAC address used for discovery can refer to a host or home gateway device.
		An attacker can 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.

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.
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.

Risk	Threat	Threat Analysis
	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.
		P802.1AEcg describes the use of a local address in the SCI, however the local address is still trivially trackable to establish a session, and to which Connectivity Association it belongs.

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.

Risk	Threat	Threat Analysis
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.