21. MAC Privacy protection in Systems

This clause how MAC Privacy protection is supported by the following:

a) Interface stacks in general (21.2), and end station (21.3) and bridge interfaces (21.4) in particular.
b) Link Aggregation (21.4)
c) Ethernet Data Encryption devices (EDEs, Clause 15) and related systems (21.5)
d) Shared media (21.6)
e) Multi-access LANs (21.7)
f) MACsec and privacy protection in separate systems (21.8)

Interoperability between systems requires not only interoperability between Privacy-protecting Entity (PrY) implementations and use of the same LAN MAC technology, but also that use of the same, or compatible, functions in the same relative position within interface stacks (21.1), as specified in this clause.

NOTE 1—An understanding of architectural concepts common to this and other IEEE 802.1 standards is essential to understanding this standard's specification of MAC Privacy protection. The reader is encouraged to review Clause 7 of IEEE Std 802.1AC-2016 and Clause 11 of this standard. Clause 17 provides an overview of MAC Privacy protection, and Clause 20 specifies the internal operation of PrYs. Some, but not all, of the provisions of those clause are repeated to reduce the burden on the reader of frequent cross-referencing.

NOTE 2—The list of systems described in this clause is not intended to be exhaustive. Privacy protection can be provided wherever MACsec is used.

21.1 Privacy-protecting interface stacks

Each PrY uses a MAC Internal Sublayer Service (ISS, IEEE Std 802.1AC) access point and provides the ISS at its secure Private Port. This allows use of MAC Privacy protection with other media-independent functions. Privacy protection depends not only on the operation of the MAC Privacy-protecting Entities (PrYs) that generate and validate the MPPDUs that convey user data frames, but also on the MACsec confidentiality-protection of those MPPDUs, so each PrY should be directly supported by a MAC Security Entity (SecY), as in shown in Figure 21-1. A PrY and its supporting SecY can also be located in adjacent systems () to support deployment of privacy-protection in networks where MACsec is already deployed, or MACsec protection is separately administered.

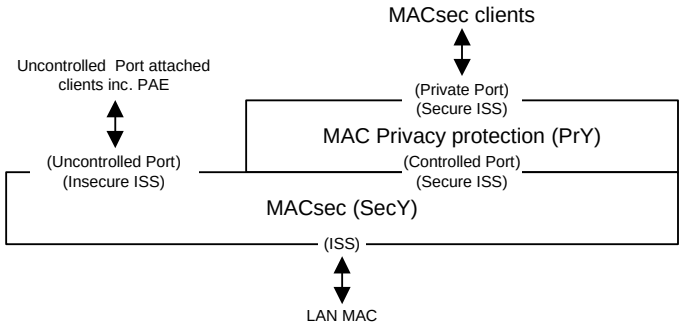


Figure 21-1—A Privacy-protecting interface stack

Where the PrY is directly supported by a SecY (as shown in Figure 21-1), all MAC Clients that would otherwise be attached to the SecY's Controlled Port should be attached to the PrY's Private Port. The overhead of privacy-protection is acceptable for most protocols (see 17.3 for discussion of the Quality of Service impact and mitigation) and a receiving peer PrY will deliver the original user data frame to its client.

NOTE 1—The transmission order of frames is determined by the PrY's client. The PrY does not buffer user data frames, except as required to fill the next MPPDU to be transmitted, with the possibility of a fragment that does not fit being held over to a subsequent MPPDU (<20.x>). However if the PrY's client requests transmission of an express frame before the

PrY has completed transmission of the fragments of a standard frame, the express frame can be encoded in an MPPDU that is transmitted prior to the MPPDU used to encode those fragments. This handling of express frames supports use of the pre-emption as provided by the IEEE Std 802.3 MAC or equivalent capabilities.

A transmitting PrY can selectively protect protocols (17.2, <>) without the need to coordinate the selection of those protocols with a peer PrY: a PrY that receives a user data frame that has been validated by its SecY but is not identified as an MPPDU to be processed by that PrY will be simply passed to its client. Once a received MPPDU addressed to a PrY has been validated by its SecY, that PrY's processing of each user data frame component (an entire frame or a fragment) conveyed by the MPPDU is independent of the processing of other components in that MPPDU (with the exception of fragment reassembly) and independent of the addressing and priority parameters of the MPPDU. This independence allows a transmitting PrY to use a range of privacy-protection and encapsulation strategies, again without the need to coordinate their selection with a peer PrY. This standard specifies management controls based on the user priority of each data frame, as the user priority is commonly used to distinguish between broad application classes (see IEEE Std 802.1Q) such a network critical frames or frames associated with flows requiring bandwidth allocation. A PrY may support additional management controls, including the use of flow classification (8.6.5 of IEEE Std 802.1Qcr-2020) to selectively or differentially protect user data frames of different protocols. Protection parameters can be associated with a stream_handle sub-parameter of the ISS connection_identifier parameter (see Clause 6 of IEEE_Std_802.1CB-2017). The PICS should include Additional Information (A.3.2) for any additional management controls provided by a PrY implementation.

NOTE 2—The use of selective protection, or of varying MPPDU parameters (priority and size), can compromise privacy by revealing the characteristics of, and changes in, protected traffic. Maintaining a constant frequency, size, and bandwidth for observably traffic types can have a greater impact on quality of service than treating those types as an undifferentiated whole. This standard accordingly specifies the use of at most two privacy channels to control transmission timing and fragmentation of user data frames.

The use of MAC Privacy-protection does not change the use or selection of MAC Clients attached to the SecY's Uncontrolled Port.

21.1.1 PrY Addressing

System interoperability also depends on the suitable selection of the destination address of the MAC Privacy-protection Data Units (MPPDUs) that each PrY uses to encapsulate user data frames. The operation of networks depends on access by the intermediate systems that make up that network (bridges, routers, and switches) to the destination and source addresses of frames to be forwarded. Forwarding systems can require access to the user data conveyed to associate frames with data flows and bandwidth reservations, and to participate in control protocols. The intermediate systems' use of MACsec to validate frames, confining frames that have been corrupted or introduced by an attacker to individual LANs and protecting control protocol operation, also means that those systems have access to user data and addresses. Privacy protection depends not only on the operation of the MAC Privacy-protecting Entities (PrYs) that generate and validate the MPPDUs that convey user data frames, but also on the MACsec confidentiality-protection of those MPPDUs. The extent of each privacy-protected region of a network is thus aligned with the MACsec protection of that region, which is typically an individual LAN but can be an equivalent LAN service supported by a provider network. To maintain this alignment without depending on additional configuration, the destination MAC address of each MPPDU should be the PAE Group Address configured for MKA support of that SecY, except as specified for non-colocated SecY and PrY ().

MAC Privacy-protection does not constrain the source MAC address of MPPDUs. The source address used by the PrY can be any address specified by IEEE 802 standards for use in conjunction with the media access control method used by the associated SecY. This includes locally assigned addresses, permamnently or temporarily assigned. The source address of MPPDUs is not checked by a receiving PrY: data origin

authenticity is verified by MACsec (confirming that the transmitting PrY possessed the SAK used to protect the MPPDU), not by inspection of the MPPDU source address.

NOTE—If the source MAC address used by a PrY is changed, the timing of any change needs to be uncorrelated with properties of the protected traffic.

21.2 Privacy protection for end station interfaces

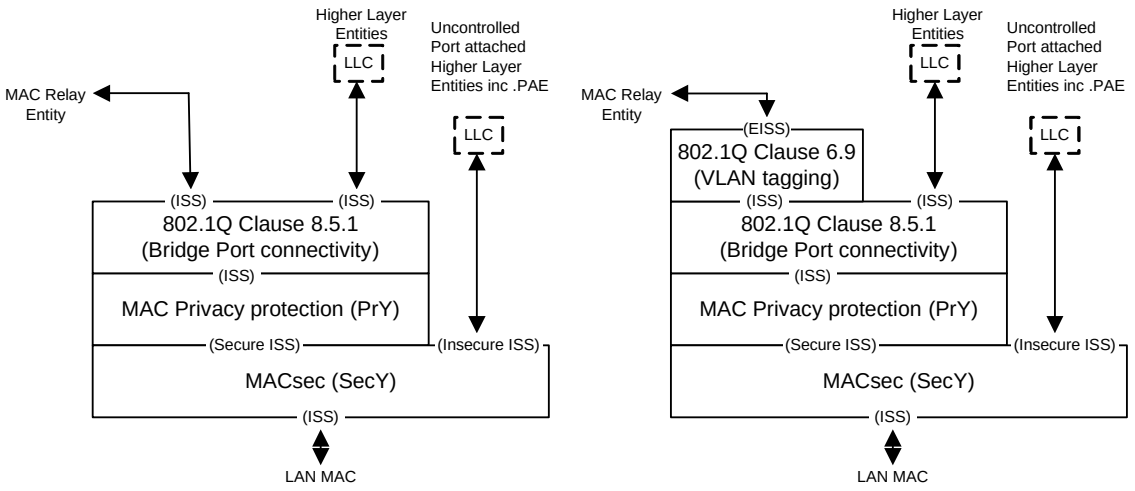
An end station can use the interface stack illustrated by Figure 21-1. If the end station transmits frames that are VLAN-tagged, tagging (for transmission) and detagging (on reception) is carried out by the MACsec Client, just as if privacy-protection was not being provided.

In network scenarios where the end station identity is not strongly correlated with location, and all frames are privacy protected, the use of a locally assigned MPPDU source MAC address can help to maintain privacy. The encapsulated user data frame's source address can continue to be used (as is common practice) by a systems that incorporates the receiving PrY to index end station related information.

NOTE—A media access control method can use control frames, or have other operational properties that are correlatable with station identity. See IEEE Std P802E-2020.

21.3 Privacy protection for bridge interfaces

MAC Bridges are specified in IEEE Std 802.1Q. The MAC Relay Entity forwards frames between the interface stacks supported by each of the Bridge Ports. Figure 21-2 shows privacy-protecting interface stacks for a VLAN-unaware Bridge (on the left) and a VLAN-aware Bridge (on the right), compare with Figure 11-5 and Figure 11-7.



Numeric references in this figure are to 8.5.1 and 6.9 of IEEE Std 802.1Q-2018.

Figure 21-2—Privacy-protected Bridge Ports

NOTE—If the MAC Bridge aggregates multiple LANs to support a single Bridge Port, each individual LAN supports its own PrY and SecY, which together provide a secure privacy-protected MAC Service to the Link Aggregation sublayer, as specified in 21.4. Each aggregated port then provides that service to the Bridge Port transmit and receive functions.

Figure 17-2 shows the MPPDU frame format supported by these interface stacks, including the relative placement of the PrY MAC Addresses, MPP EtherType, SecTAG, and user data frame (including the VLAN tag, if present). The use of MACsec and privacy protection is not necessarily enabled for, or supported by, all ports of any given bridge. The scope of privacy protection is, as for MACsec, from a bridge port to its nearest peer neighbour, e.g., from Customer Bridge to Customer Bridge, from Customer Bridge to an end system, or from Provider Bridge to Provider Bridge.

21.4 Privacy protection for Link Aggregation

Link Aggregation is specified in IEEE Std 802.1AX[B4]. The service provided by two separate point-to-point LANs is combined to provide a single service interface. To provide MAC Security for such a system, two independent SecYs operate below the link aggregation sublayer (see 11.5). Privacy protection is provided for each SecY by a PrY that is a user of the secure MAC Service (ISS) provided by that SecY, and in turn supports the link aggregation sublayer (Figure 21-3, compare with Figure 11-4). Privacy channel(s) for each PrY can be configured to schedule MPPDU transmission, eliminating or reducing the potential correlation between MPPDU transmission and changes in the traffic flows that link aggregation assigns to one individual link or another.

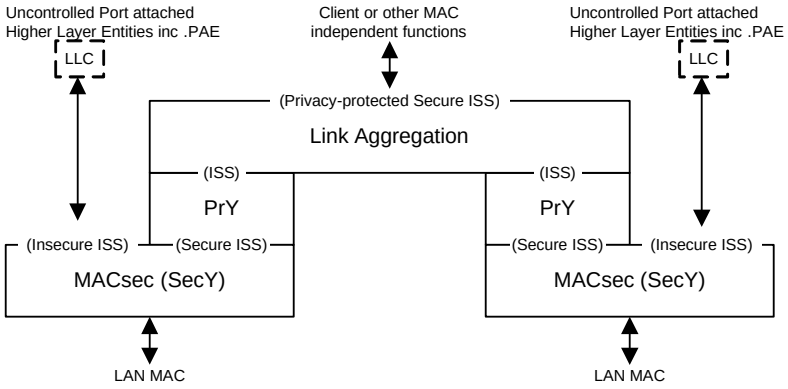


Figure 21-3—Privacy protection and Link Aggregation

If a given PrY fragments a user data frame, all the fragments of that are conveyed in MPPDUs protected by the SecY that supports that PrY. This facilitates the simple reassembly function (20.x) mandated for fragmentation support, assuming that MPPDUs transmitted with a given access priority (and thus all MPPDUs for a given privacy channel) and protected by a given SecY are received in order.

NOTE—MPPDU fragment encoding (<19.8>) can support reassembly of out of order fragments, but this is not required PrY reception capability (<20.x>).

21.5 Privacy-protecting EDEs

An EDE can provide privacy-protection for traffic transiting a Provider Bridged Network (PBN) by incorporating a PrY in the each interface stack with a SecY, as illustrated in Figure 21-4 for an EDE-CC (compare with Figure 15-9).

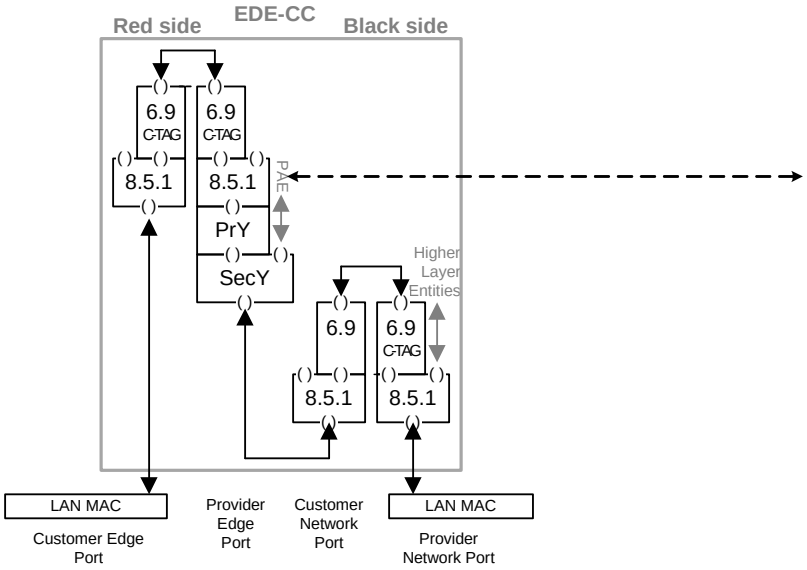


Figure 21-4—EDE-CC with privacy-protection

Figure 21-4 provides a sectional view of the interface stacks, showing a single Provider Edge Port (PEP. An EDE-CC can include multiple PEPs so the PBN can use each frame's C-TAG to select the destination interface. In Figure 21-5, the member set for each VID includes at most one PEP so the edge C-VLAN Bridge component (shown on the left of EDE-CC1, connecting the CEP and PEPs) can forward a frame received from bridge B1 to just one of the PEP (8.6.4 of IEEE Std 802.1Q-2018). That PEP can then protect the user data frame, encapsulating it within an MPPDU that is integrity and confidentiality protected by MACsec before it is forwarded to one of the Customer Network Ports (CNP) of the network C-VLAN Bridge component (shown on the right of EDE-CC1, connecting the CNPs and the Provider Network Port).

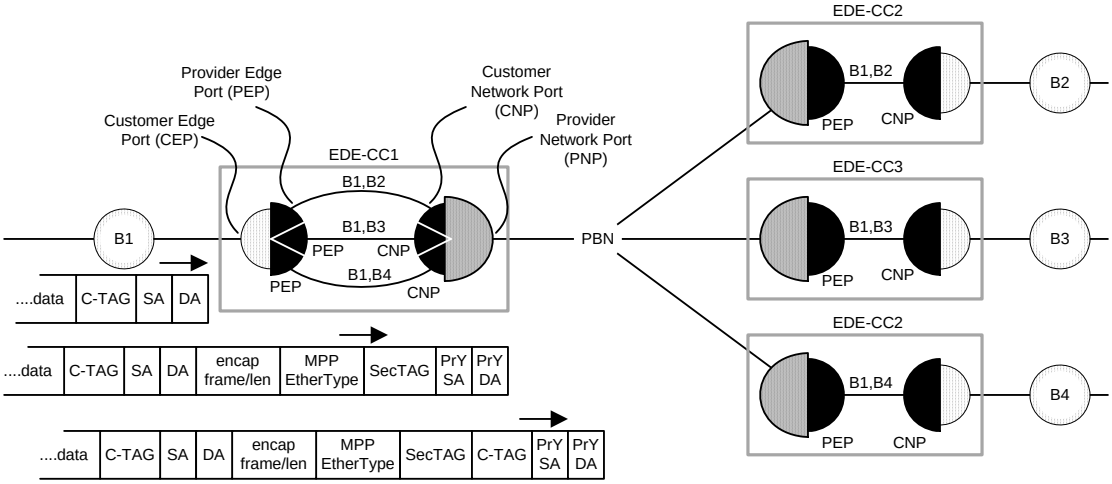


Figure 21-5—EDE-CCs communicating over a PBN

The initial octets of the protected MPPDU compose the SecTAG added by the PEP, so the CNP will assign it to the C-VLAN identified by the Port VLAN Identifier (PVID, 6.9 of IEEE Std 802.1Q-2018) for that Bridge Port. The frame is then transmitted, C-tagged with that PVID, through the Provider Network Port (PNP). The PBN can then use that outer C-TAG to identify the destination PBN interface, modifying that tag if necessary. The original user data frame C-TAG will be delivered, privacy-protected within the MPPDU, to the distant customer equipment.

NOTE 1—IEEE Std 802.1AEcg-2017 and IEEE Std 802.1AE-2018 required an EDE-CC and EDE-SS to tag frames transmitted by the PNP with the same VID as received by the CEP [5.8 e) and 5.9 e) of IEEE Std 802.1AE-2018]. This configuration constraint simplified management, and avoided potential network forwarding changes as a result of enabling or disabling MACsec protection. EDEs implementing this constraint remain conformant to IEEE Std 802.1AEdk-2021, but user data frames for different customer VLANs but destined for the same remote PBN interface can also be forwarded through the same PEP by a conformant EDE. Those user data frames so can then be encapsulated in a commemon set of MPDUs, and use the same SC and outer VID in the interests of privacy.

When an EDE-CC's PNP receives a frame, its network C-VLAN component uses the member set for the VID in the outer C-TAG to select a PNP. The frame is transmitted untagged by that PNP, allowing the SecY for the attached PEP to recognize the frame as MACsec protected and to validate the frame. An associated PrY, above the SecY in the PEP interface stack can then decapsulate the original user data frames (including their original VLAN tags, if present) and pass them up the interface stack to the edge component's MAC Relay Entity.

Privacy protection can be enabled or disabled on a PEP by PEP basis: the customer equipment associated with a remote PBN interface accessible through a given EDE is not all necessarily capable of privacy protection, and can have MACsec disabled.

NOTE 2—The use of two bridge components to model the EDE behavior follows the approach used in IEEE to model Provider Edge Bridges. In the simplest cases this is elaborate, but has the advantage that a system whose behavior can always be explained in terms of the valid interconnection of existing network components does not introduce new interoperability challenges. In other words, bundling any part of a valid network of components into a distinct physical system always yields a valid (if not necessarily desirable) system. The model has the further advantage of explaining the how further functionality, standardized separately for individual bridge components, can be added to an EDE or EDE-like syste, and what the resulting externally observable behavior of the system should be. Connectivity Fault Management, as specified by IEEE Std 802.1Q, is one example of such functionality. The internal implementation of an EDE is not over-constrained by the two component model, conformance to this standard and to the provisions of IEEE Std 802.1Q is only to the externally observable behavior implied by the model.

NOTE 3—This standard's specification of EDEs is not intended to encompass all the possible functionality of a two bridge component device. Restricting the edge component's member set for each C-VLAN to include at most one PEP means that the edge component need not learn from customer MAC Addresses (8.7.2 of IEEE Std 802.1Q-2018) and that the outer VID is determined by the inner VID. More general functionality could include learning the association of MAC Addresses with a particular PEP, with the possibility of dynamic determination of the PEP and thus of the outer VID in the VLAN TAG added prior to transmission by the PNP.

21.6 Privacy protection with shared media

Privacy protection can be used with shared media and group CAs. The use of virtual shared media with a single VLAN and explicitly configured PrY addresses to optimize delivery of MPPDUs is not recommended, as enabling or disabling privacy protection would then result in a change in the underlying connectivity, possibly introducing or revealing configuration problems and making their diagnosis more difficult. If the simple use of VLANs to partition the connectivity provided by the shared media is not sufficient to meet scaling goals, the use of Provider Bridging or Provider Backbone Bridging as specified by IEEE Std 802.1Q is indicated, with privacy protection provided by the Provider Edge Port (PEP) interface stacks.

21.7 Privacy protection and multi-access LANs

Privacy protection can be used in conjunction with MACsec to support multi-access LANs (see 11.8). The MAC Address used by each PrY as the source MAC address of transmitted MPDUs is that used by protocols

(EAPOL and MKA as specified by IEEE Std 802.1X) using the Uncontrolled Port to establish secure connectivity.

NOTE—As with end station interfaces in general (21.2) MAC Privacy protection does not prevent an observer from determing which MPPDUs are destined for which station, but does allow the end station user and a service provider to continue to use of a permanent address associated with the station to identify information (e.g. access rights) for the station, without exposing that address to an unauthorized observer.

21.8 Separate privacy protection devices

MPPDUs are identified by a distinct MPP EtherType and can be transmitted and received without MACsec confidentiality protection, so that protection and validation can be performed by separate devices or systems, possibly already deployed in a network or separately administered. Figure 21-6 illustrates the encapsulation of a user data frame, shown for simplicity as the initial component of an MPPDU, by a pair of such separate systems each on the red-side of a pair of interconnected EDEs. These systems can be modelled in the same way as a two bridge-component EDE, with the substitution (rather than the addition) of a PrY for the SecY in each PEP interface stack. The use of these separate privacy protecting systems is predicated on a desire to maintain separate MACsec protecting and validating systems for communication between all the connected PBN interfaces: if the associated EDE retains its default configuration it will add a copy of the outer C-TAG after the SecTAG prepended to each MPPDU transmitted across the PBN (compare Figure 21-6 with Figure 21-5), and will not interoperate with an EDE that has both PrY and SecY in the PEP interface stack. An MPPDU destined to the group MAC Address used by the MACsec SecY would be filtered by the receiving PEP, so a PrY in a privacy protecting system can be configured to use the individual MAC Address of its peer as the destination PrY MAC Address. Since an existing EDE or system on the path between the receiving EDE and the destination decapsulating device can be presumed not to recognize MPPDUs, the EDE and that device are best placed adjacent to one another, without intervening devices.

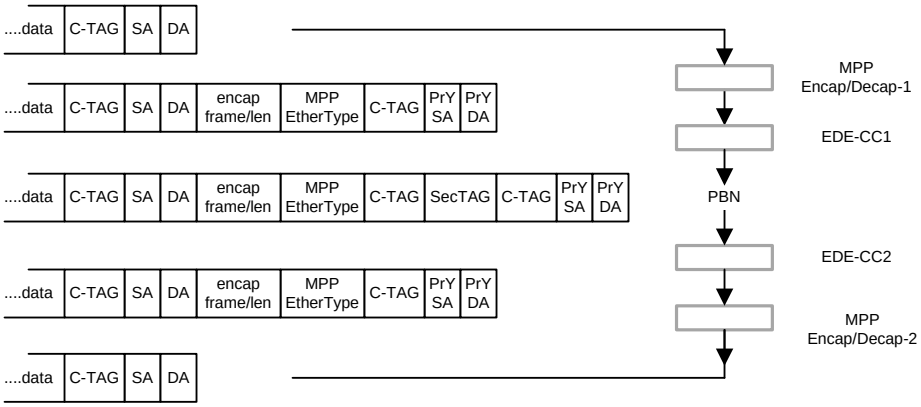


Figure 21-6—Privacy-protection using existing EDEs

The addressing and MPPDU format constraints described in this clause (21.7) for the deployment of privacy-protection and MACsec confidentiality protection in separate systems do not apply when the functionality is provided in a single system comprising multiple components. The information that a receiving SecY needs to pass to its associated PrY is all present as parameters of an ISS indication, and each receive indication from the PrY to its client comprises the parameters expected with receipt of a user data frame. Individual MPDDU components (19.2) are self decribing and can be extracted and processed separately by the PrY, with the exception of frame fragments received from a group CA. In that case the PrY needs to use the MPPDU's PrY source MAC Address to reassemble user data frame fragments received from different members of the CA.