Insert the following text (Clause 17) after Clause 16:

17. MAC Privacy protection

This clause provides an overview of MAC Privacy protection. It provides the context necessary to understand the detailed operation of the MAC Privacy-protection protocol (Clause 18) and individual MAC Privacy-protecting Entities (PrYs, Clause 20), and describes the following:

a) The need for MAC Privacy protection (17.1).

b) How individual user data frames are protected (17.2).

c) The potential impact of privacy protection on Quality of Service parameters, and the management controls provided to balance the protection provide with the effect on those parameters.

d) Privacy protection deployment, interoperability with existing systems, network configuration, and use case scenarios.

17.1 The need for MAC Privacy protection

Privacy protection is associated with the rights of individual persons to control the disclosure of information associated with themselves and their activities (personally identifiable information, PII). PII that directly describes individuals can be carried in the user data fields of IEEE 802 MAC data frames, and can be protected from adversaries (persons or organization attempting to gain unauthorized access to personal information) by the confidentiality protection provided by MACsec or higher layer protocols (e.g. IPsec). However adversaries can also acquire personal information by correlating multiple items of information (personal correlatable information, PCI) in order to construct a ‘fingerprint’ of that person or to correlate their activities with previously computed fingerprints of known activities.

A potential adversary can still observe the MAC source and destination addresses of a data frame that has been confidentiality protected by MACsec, and so might (for example) be able to associate the source MAC address of a particular device (a personal device) with an individual and subsequently track that individual and his or her interactions with other individuals or network based services. The sizes of data frames and their transmission timing can also be correlated with particular network applications or the details of those applications (e.g. the size of financial transactions). An adversary might gain important information simply from the amount of information being sent.

NOTE—IEEE Recommended Practice 802E further describes privacy considerations and the use of the terms PII, PCI, adversary, correlation, fingerprint, personal device, and shared service device in the context of IEEE 802 networks.

The need to assure privacy is not limited to individuals. Organizations can be under an obligation not to disclose certain information and need to be aware of the extent to which adversaries can draw conclusions by combining multiple observations, each of which might convey little information when considered separately. Organization that transmit data on behalf of individuals or other organizations can also be under an obligation to keep that data private.

While privacy protection is desired, the operation of networks depends on access by the devices that make up that network (bridges, routers, and switches) to the destination and source MAC addresses of frames to be forwarded. Forwarding systems can also need to access to information carried in the frames’ user data to associate (for example) certain frames with individual data flows and their bandwidth reservations. Annex I describes privacy considerations related to the use, design, and deployment of bridged networks in more detail. The requirement that intermediate forwarding systems be able to access frame addresses and user data fields means that all user PCI cannot be simply cryptographically confidentiality protected from its original source to its original destination. Just as is the case for the use of MACsec without additional privacy protection, addresses and data are protected hop-by-hop, although a single hop can extend over a service provider connection, as is the case with Ethernet Data Encryption devices (EDEs, see Clause 15).

The authenticated and authorized devices or areas of the network that protect user data frames with MACsec for transmission over potentially exposed network connections can also provide MAC Privacy protection as described in this clause. The MAC addresses of the privacy protecting devices are exposed to external observation, but these devices can be shared service devices or at least (if they are personal devices) at fixed locations so that (when privacy protection is applied) there is little or no observable correlation between the flow of protected frames and PII.

17.2 Protecting user data frames

MACsec secures communication while minimizing its impact on the MAC Service's Quality of Service (QoS) parameters (6.10). Individual frames are cryptographically protected and transmitted with minimal delay, with the addition of only those octets required to support cryptographic integrity and confidentiality protection. Each frame's source and destination MAC Addresses remain unmodified. This deliberately limited impact on the transmission and reception of frames can allow a potentially adversarial observer to correlate those addresses and the pattern of frame sizes, transmission timing, and transmission frequency with the identities of communicating users, the reason they are communicating, and even (in some cases) the content of confidentiality protected communication.

When protecting privacy is paramount, QoS and simplicity of network configuration can be less important. MAC Privacy-protecting Entities (PrYs) enhance privacy as follows:

a) User data frames, and their source and destination MAC addresses, are encapsulated within MAC Privacy-protecting Data Units (MPPDUs).

b) MPPDUs can be padded to fixed sizes before being protected by MACsec.

c) The timing of MPPDU transmissions can be controlled.

The MAC Source Address of each MPPDU identifies its encapsulating PrY. Its MAC Destination Address is a unicast or multicast address associated with its decapsulating PrY(s). When MPPDUs are confidentiality and integrity protected by MACsec, the source and destination addresses and sizes of the encapsulated user data frames are hidden from an observer who lacks the protecting secret key. Figure 17-1 shows the addition of PrYs to the interface stacks of two bridges protecting the frames they exchange with MACsec.

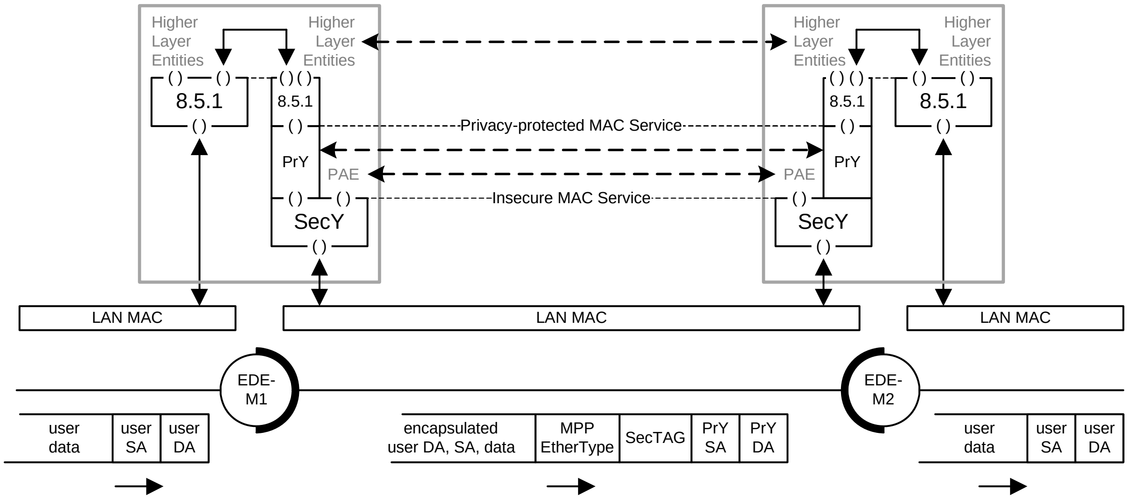


Figure 17-1—Privacy-protected communication between bridges

NOTE 1—This standard uses the formal term MPPDU to avoid any confusion with terminology defined elsewhere, and for consistency with similar terms in this and other standards. MPPDUs are also identified as individual *Privacy Frames* or as *Privacy Channel Frames* (17.3).

Figure 17-2 shows an encapsulated user data frame (DA, SA, and user data) followed by padding, in an MPPDU that is protected by MACsec.

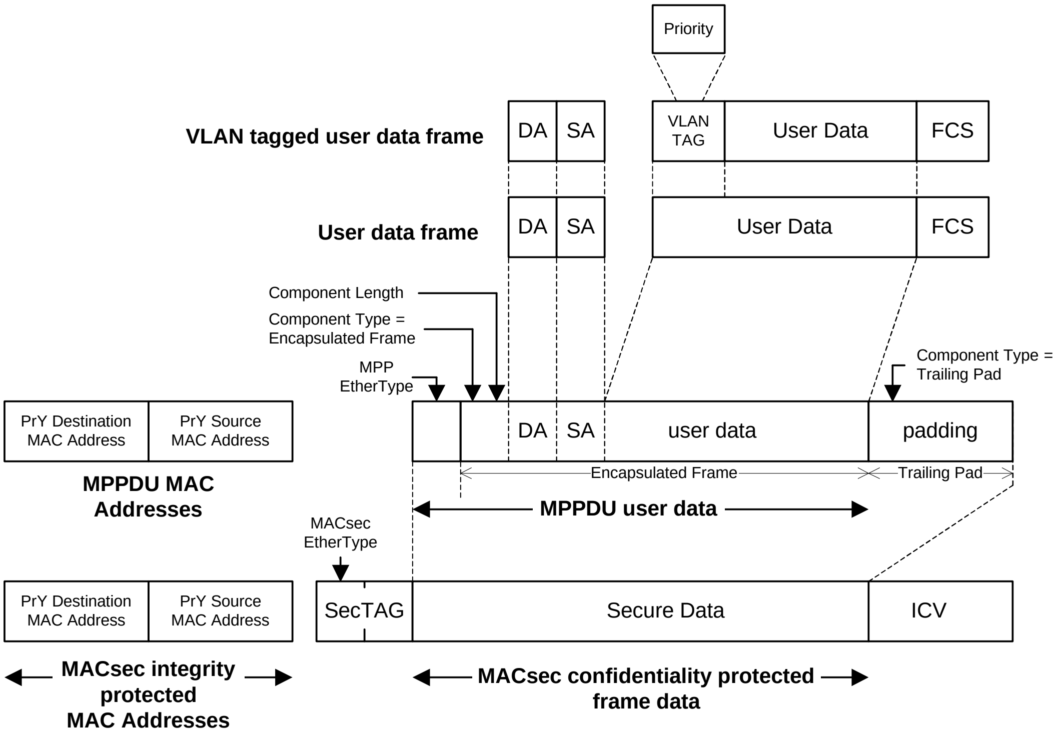


Figure 17-2—A privacy-protected frame

NOTE 2—Figure 17-2 separates source and destination addresses from the accompanying data, as they are separate ISS service request parameters. The supporting service encodes these parameters into a frame and can add octets (e.g. a SecTAG when encoding an MPPDU in an MPDU) between those addresses and the data . Strictly this standard specifies parameters of service primitives, not frames. However, it is often convenient to talk of these parameters as a frame.

If the original user data frame included a VLAN TAG, the user priority information in that tag is carried in the frame's MAC Service user data and will be unchanged when the receiving PrY decapsulates the user data frame. It do not depend on the access priority used to transmit the confidentiality protected MPPDU.

The length of the encapsulated data frame component is carried explicitly, so padding can be added preventing observation of the original data frame size once the MPPDU has been protected by MACsec. This removes or reduces the contribution that observation of MPPDU frame sizes can make to inferences about the communication. An MPPDU can also be sent without any user data, including only padding, to guard against observation of the level of user activity.

The media-dependent FCS of the user data frame is not carried within the MPPDU. The MACsec Integrity Check Value (ICV) provides superior protection against deliberate or inadvertent modification of data.

Hiding an original frame's MAC destination and source addresses is not necessarily a requirement in some network configurations. They might identify shared service devices, such as routers, and be the same for all the original user data frames transiting a given link. However MPPDUs do not provide a way to share the encoding of these addresses between encapsulated frames. Encapsulated data frames are independent of one another and, once received, of any other user frame or other information carried in the same MPPDU (as described in 7.2 below).

Clause 19 specifies MPPDU encoding details. Figure 19-2 provides examples, including mitigating the impact that privacy protection can have on quality of service (described further in 17.3 below) by encoding more than one user data frame in an MPDDU. A user data frame can be fragmented and carried in successive MPPDUs, utilizing the remaining octets of an MPPDU that would otherwise be padded.

Clause 20 specifies the operation of individual PrYs, with standard controls for MPPDU sizes and transmission timing. The self-describing format of MPPDUs permits a range of PrY transmission strategies compatible with mandatory PrY reception behavior. However fine tuning of MPPDU size and transmission timing parameters can itself reveal information about the intended mix of user protocols, as can any temporary adjustments to those parameters to better accommodate those protocols.

MAC privacy protection tends to be most effective and efficient when all the user data frames passing between two PrYs are protected. A network administrator can decide that MACsec integrity and confidentiality protection is sufficient for some user protocols, and that privacy protection is not to be applied to those protocols. Such protocols might already use frames of fixed sizes and MAC addresses that provide an external observer with little information (e.g. use of the Nearest Customer Bridge group address as the MAC destination address). A receiving PrY will accept such frames without modification.

17.3 Quality of Service impact and mitigation

Privacy protection can impact quality of service by:

a) Increasing the number of octets required to encode individual user data frames within MPPDUs.

b) Adding padding to MPPDUs.

c) Transmitting MPPDUs at intervals that are fixed, or at least uncorrelated with the user data frame sizes or transmission queue occupancy.

d) Requesting MACsec protected MPPDU transmission using a different priority (the access priority) than the priority (the user priority) associated with encoded in the VLAN TAG or locally determined for an encapsulated data frame.

Additional encoding and padding octets [a) and b) above] can be viewed either as delaying the completion of transmission or as delaying the completion of reception. On reception a privacy-protected user data frame cannot be passed to the receiving service user before the MACsec ICV protecting the entire MPPDU has been validated. The additional transmission delay is not necessarily of significant concern on network connections that are most exposed to unauthorized observers and have a high bandwidth delay product, e.g. across a Provider Bridge Network (PBN), where the effect of the delay can be equivalent to a modest increase in the distance between privacy-protecting systems.

Additional octets also reduce the total bandwidth available, potentially delaying subsequent frames. Multiple user data frames can be encapsulated in a single MPPDU, using space that might otherwise be occupied by padding octets. Encapsulating multiple data frames in this way can improve bandwidth efficiency as the media-dependent overhead of sending separate frames, as well as the number of octets required for MACsec protection, is amortized over several user data frames.

NOTE 1—MACsec and MAC Privacy protection provide media-independent integrity, confidentiality, and privacy. In a common case the medium transports 802.3 frames with an overhead of 24 octets (preamble, start of frame delimiter, and inter-packet gap) and a MACsec overhead of 32 octets (SecTAG, ICV). As compared to only providing confidentiality and integrity, privacy protecting a 1518-octet user data frame and a 64-octet user data frame in separate MPPDUs increases the required bandwidth by ~2% (using the encoding specified in Clause 19). Encoding both those user data frames in a single MPPDU (with 1590 octets of MPPDU user data, including a 4 octet trailing pad) decreases the bandwidth requirement by ~2%. The continuous transmission of privacy-protected 64-octet user data frames increases the bandwidth required by ~13% if they are encoded in separate unpadded MPPDUs, and decreases it by ~43% if encoded in a single MPPDU (using 1590 octets of MPPDU user data, with a 4 octet trailing pad). See Annex TBS for additional bandwidth and delay calculations and recommendations on the selection of fixed MPPDU sizes.

The transmission of MPPDUs can be delayed [c) above] to allow their transmission at regular intervals, but is not otherwise delayed (e.g. in the expectation of further data frames becoming available for transmission in the same MPPDU). Explicit pads (i.e. pads whose length is specified) can be encoded in an MPPDU so that user data frames that become available for transmission after part of an MPPDU has been transmitted can be encoded in that MPPDU, reducing the delay experienced by user data frames associated with time sensitive streams. If the PrY is part of an interface stack supporting the transmission of user data frames subject to the operation of a stream gate control list, MPPDU transmissions can be scheduled to allow the encoding of those user data frames towards the end of the MPPDU. Similarly eligibility times for user data frame transmission can reflect the fact that those frames will be received after the MPPDU has been completely received, validated, and decoded.

NOTE 2—8.6 of IEEE Std 802.1Q-2018 as amended by IEEE Std 802.1Qcr-2020 specifies stream gate control lists in support of Per-Stream Filtering and Policing (PSFP) and the calculation of eligibility times for Asynchronous Traffic Scheduling (ATS).

The access priority (i.e. the priority used to request transmission) of the MPPDU encapsulating a user data frame can be the same as that of the frame’s user priority. However, configuring a PrY to transmit fixed sized MPPDUs of several different access priorities on a fixed schedule for several access priorities could degrade the effectiveness of user priority: transmission of a scheduled low priority MPPDU might postpone the transmission of a high priority user data frame; if the next user data frame to be transmitted is to be encapsulated in an MPPDU with a different access priority, the opportunity to encapsulate an additional user data frame in the MPPDU (instead of adding padding) would be lost; and the number of MPPDUs transmitted without conveying a user data frame (i.e. containing only padding) is likely to increase.

NOTE 3—A PrY does not dictate the transmission order of user data frames or buffer those frames to improve MPPDU packing. In a bridge, the next frame to transmit through an interface is determined by the transmission selection algorithm (see 8.6.8 of IEEE Std 802.1Q-2018) when an opportunity to transmit arises.

A transmission schedule is associated with a *privacy channel*. A configurable Channel Table has an entry for each of the eight possible user priority values (0 through 7). Each entry indicates whether user data frames of that priority are transmitted by a privacy channel and (if they are) whether they are *express frames*. A data frame not associated with a privacy channel is encapsulated in an MPPDU (an individual *Privacy Frame*) with an access priority equal to the frame’s user priority. The use of individual Privacy Frames reflects a decision on the part of the network administrator that any leakage of PCI resulting from the use, or changes in use, of their priorities and frame transmission timing is unimportant (e.g. they might encapsulate network routing traffic, rather than packets sent by network applications).

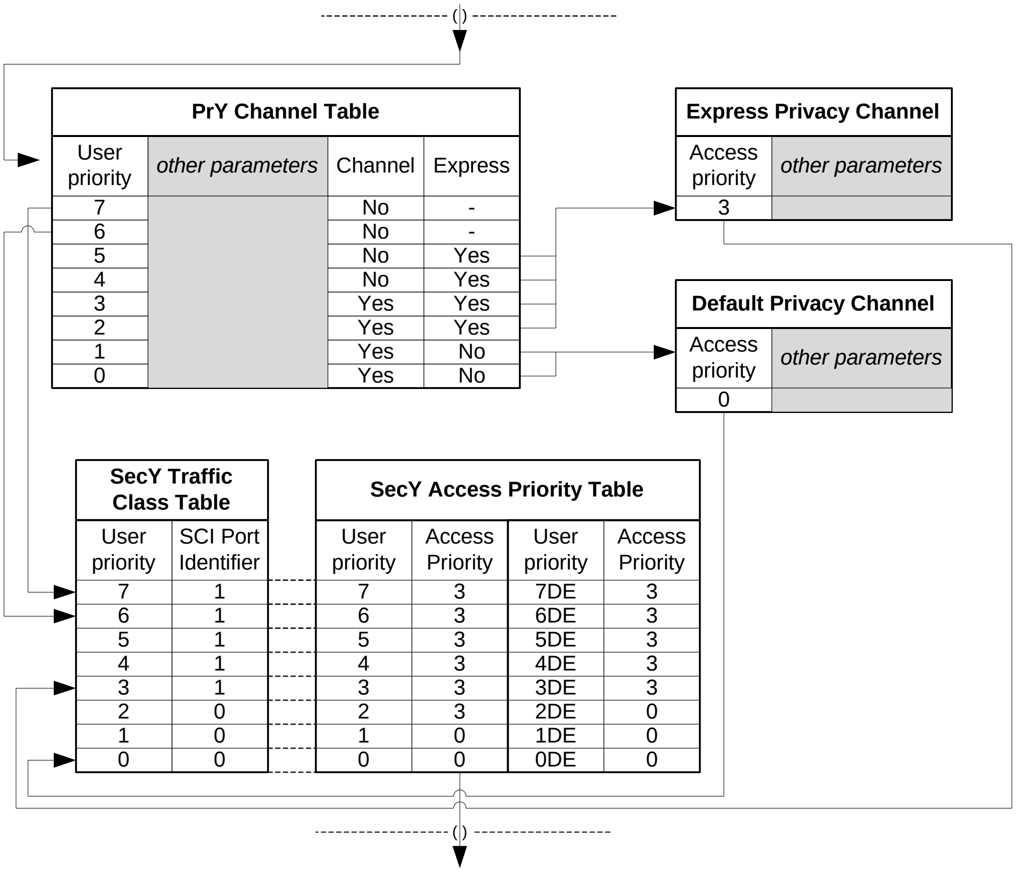
A PrY supports a *Default Privacy Channel*, and can be configured to support an additional *Express Privacy Channel*. If both privacy channels are configured, user data frames that the Channel Table has associated with a privacy channel and identified as express frames are encoded in MPPDUs (*Express Channel Privacy Frames*) associated with Express Privacy Channel parameters, and other channel associated user data frames are encoded in MPPDUs (*Default Channel Privacy Frames*) using Default Privacy Channel parameters.

A privacy channel’s parameters include the specification of the access priority used to transmit that channel’s MPPDUs. A network connection is expected to preserve the transmission order of frames of that priority. If the interface stack (or the interface stacks of frame forwarding devices on the path between peer PrYs) supports IEEE 802.3 frame preemption or other class of service differentiated forwarding capabilities, the access priority of an Express Privacy Channel can be configured to take advantage of those capabilities.

Figure 17-3 illustrates the use of a PrY’s Channel Table and Express and Default Privacy Channel parameters in conjunction with the Traffic Class and Access Priority Tables specified for a SecY (10.7.17). The user priority accompanying a user data frame transmission request to the PrY (from, for example the Bridge Port Transmit and Receive function as illustrated in Figure 17-1 and specified in 8.5.1 of IEEE Std 802.1Q-2018) is shown at the top of the figure. Frames with a user priority of 0 or 1 are assigned to the Default Privacy Channel, which uses access priority 0 to request transmission of Default Privacy Channel Frames by the supporting SecY. The PrY is the user of the service provided by the SecY, so that communicated access priority value is the SecY's user priority, and is used (by the SecY's Traffic Class Table) to assign those Default Privacy Channel Frames to the SecY's transmit Secure Channel (SC) 0. The access priority requested from the underlying medium, when the MACsec protected frames are transmitted, is 0 as specified by the SecY's Access Priority Table.

Similarly, the PrY assigns frames with user priorities of 2 through 5 to the Express Privacy Channel, and Express Privacy Channel Frames are assigned to the SecY's SC 1 and transmitted with access priority 3. The PrY does not assign user data frames with priorities of 6 or 7 to a privacy channel, but encapsulates them in individual Privacy Frames, that are then assigned by the SecY to SC 1 are transmitted with access priority 3.

NOTE 4—If the PrY and SecY form part of the Provider Edge Port of an EDE-CS or EDE-CC (see Figures 15-6, 15-7, 15-8, and Figure 17-n) the SecY's transmitted access priority is encoded by the black-side bridge component in the outer VLAN tag added to the protected frames transmitted by the Provider Network Port.



PrY Channel Table

User priority	*other parameters*	Channel	Express
7		No	-
6		No	-
5		No	Yes
4		No	Yes
3		Yes	Yes
2		Yes	Yes
1		Yes	No
0		Yes	No

Express Privacy Channel

Access priority	*other parameters*
3	

Default Privacy Channel

Access priority	*other parameters*
0	

SecY Traffic Class Table

User priority	SCI Port Identifier
7	1
6	1
5	1
4	1
3	1
2	0
1	0
0	0

SecY Access Priority Table

User priority	Access Priority	User priority	Access Priority
7	3	7DE	3
6	3	6DE	3
5	3	5DE	3
4	3	4DE	3
3	3	3DE	3
2	3	2DE	0
1	0	1DE	0
0	0	0DE	0

Figure 17-3—Priority handling and channel assignment

In Figure 17-3 user data frames with a user priority of 6 or 7 are not assigned to a privacy channel, so their transmission is not constrained by a channel schedule and can occur at any time, even though (with the configuration shown) they are assigned to the same SC. Their transmission can delay a privacy channel' s scheduled transmission, but this timing conflict and delay does not expose privacy channel PCI, unless the original source(s) of those frames correlated their transmission with frames carried by the privacy channel.

NOTE 5—A bridge that supports per-stream filtering and policing (PSFP, 8.6 of IEEE Std 802.1Q-2018) can use a number of criteria including priority to gate the transmission of frames of individual streams by bridge ports, and thus remove or reduce the impact of potential PrY scheduling conflicts on time sensitive streams.

NOTE 6—Figure 17-3 illustrates PrY and SecY priority handling, but does not specify a recommended or default configuration.

Individual Privacy Frames and Privacy Channel Frames can both encapsulate more than one user data frame with those frames having different values of the drop eligible parameter (see Clause 11 of IEEE Std 802.1AC-2018) associated with their user priority. The value of the drop eligible parameter does not influence the choice of privacy channel or individual privacy frame, and the value of the drop eligible parameter associated with the access priority of privacy channel frames is always False. The PrY Channel Table does not provide a way to set the drop eligible parameter of individual Privacy Frames, and that value should be False. If an encapsulated user data frame contains a VLAN tag, the priority and drop eligible information will be conveyed to the receiving PrY's service user.

NOTE 7—Frames can be subject to traffic shaping, e.g. by the Forwarding Process of a bridge component (see 8.6 of IEEE Std 802.1Q-2018). Traffic shaping can also be performed after user data frame are encapsulated in MPPDUs, e.g. by the network side component of an EDE-CS or EDE-CC (see 17.n).

Frames associated with a privacy channel can be fragmented, using space in fixed sized MPPDUs that would otherwise be padding. If an Express Privacy Channel has been configured, express frame fragments are encoded in the MPPDUs (Express Channel Privacy Frames) used by that channel, otherwise those express fragments are conveyed by the Default Privacy Channel. Frames that are not express frames can also be fragmented when carried by the Default Privacy Channel. A fragmented frame is transmitted as a number of fragments, each with a sequence number incrementing by one, with the first marked as the initial fragment and the last as the final fragment. One set of sequence numbers is used for express fragments, and another for other fragments. The use of the two sets of sequence numbers allows transmission of a fragmented express frame to interrupt a fragmented non-express frame. Unfragmented frames are not sequence numbered.

A receiving PrY processes all MPPDUs alike: the use of any given MPPDU to support a privacy channel or an individual privacy frame is not encoded in an MPPDU. Each of the components (entire encapsulated frames, express frame fragments, and other fragments) carried in an MPPDU is self describing, and can be separately extracted from the received stream of MPPDUs before each user data frame (reassembled from fragments if necessary) is passed to the PrYs user. Each user data frame can included priority information encoded in a VLAN TAG, allowing its recover by, for example, the Bridge Port Transmit and Receive process of a VLAN Bridge (see 8.5 of 802.1Q-2018). The access priority used to transmit an MPPDU is not used on receipt and could have been modified as the MPPDU is forwarded by a network connection.

This standard describes the PrY's Channel Table, and PrY transmission behavior in general (see Clause 20), to specify conformant base-line functionality, configurable using standardized management (<reference PrY YANG>). A PrY may also be configured to use other MPPDU encapsulation and scheduling algorithms subject to encoding rules specified in Clause 17 and the requirement that all express fragments be encoded in MPPDUs transmitted with a single access priority and all other fragments are also encoded in MPPDUs transmitted with a single, but not necessarily the same, access priority. This constraint on fragment encoding allows an interoperable receiving PrY to be capable of reassembling at most two user data frames from any given peer at any given time—one Express frame and one other frame. No additional burden is imposed on a receiving PrY by a transmitting PrY's use (well chosen or not) of multiple MPPDU priorities.

NOTE 2—MPPDU encoding does support reassembly of frame fragments received out of order, where necessary. When used in conjunction with link aggregation, a PrY (like a SecY, see 11.5, 17.n) is positioned below the Link Aggregation Collection and Distribution functions.

If the user data frame accompanying a transmit request made by a PrY's user is assigned to the same privacy channel as an MPPDU whose transmission is about to begin or is currently in progress, that encapsulated data frame (or a fragment of that user data frame) can also be encoded in the same MPPDU. Similarly a encapsulated user data frame can be added to an individual Privacy Frame. All PrY implementations are capable of encoding multiple successive user data frames in the same MPPDU (subject to MPPDU size constraints), if those user data frames are available for transmission before transmission of the MPPDU begins. A PrY may also encapsulate user data frames that become available for transmission after MPPDU transmission has started, and can add padding at the beginning of the MPPDU's data field (if scheduled transmission has begun before a user data frame is available) or between encapsulated data frames.

NOTE 8—When the transmission of individual data frames are scheduled by the PrY's user (e.g. by a bridge's Forwarding Process using a gate control list) the addition of a variable amount of padding between encapsulated user data frames in the same MPPDU can be used to match the transmission start of each of a set of variable length user data frames to the desired schedule.

The late addition of a user data frame to an in-progress MPPDU transmission reduces the transmit delay that would otherwise be experienced by that user data frame. A series of pads can be added between encapsulated frames to allow for the earliest addition of unscheduled frames. To limit the implementation-dependent workload imposed on a receiving PrY that has to scan through multiple pads, any two back to back pads should have a combined length of greater than 64 octets (see Clause 17).

<This is as far as I have got. I think it is probably covers QoS impact and mitigation, but network configuration, interoperability, system configuration (including LAG and explicitly showing an EDE with an added PrY, and addressing still need work. Everything below here is old.>

17.4 Interoperability and deployment

<<Privacy protection supports point-to-point, multipoint, and point-to-multipoint transmission between peer PrYs.>>

<<Encapsulation can be turned off. Decapsulation can still operate, can receive both MPPDU and other frames (subject to management control). Walk through the trivial deployment steps. PrY cannot encapsulate for some destinations, and not for others (separation functionality rapidly approaches that of a bridge, forward reference to multi-component model).>>

<<Introduce the important use case over provider networks, keeping it simple to begin with (one port).>>

<<Extend that use case to the EDE model. PrY in the same component as the SecY.>>

<<PrY can be in a separate system from the SecY, deployment when EDEs are already in place, EDEs can be separately administered.>>

<<Encapsulation for some destinations and not for others revisited, how do local control protocols work? Do we need a separate 'Uncontrolled Port' as for the SecY, or is the one for the SecY enough. How does this work when the PrY is in a separate system from the SecY - may well need Controlled and Uncontrolled there.>>

17.5 Network configuration

<<Relationship between PrYs constitutes a CA, as in 7.1. How do PrYs find each other, what (if anything) do they need to know about the other PrYs in the CA. MKA can carry information when PrYs are collocated with SecYs, specify necessary additional elements for this. Use manual configuration for other cases.>