# EDE deployment, configuration, and monitoring

**Mick Seaman**

This note (still an early draft!) describes the deployment, configuration, and monitoring of a (hypothetical) EDE-CC with MAC Privacy protection capability, as an exercise in explaining and checking the capabilities of the draft standard. To stimulate thought it is presented as guide for a hypothetical EDE user. At least one addition to the currently standardized EDE-CC description is suggested, en passant.

## 1. About your EDE-CC

You may be using a service provider's VLAN service to connect multiple network sites. The service provider uses the C-VLAN (Customer VLAN) tag header that you have added to each frame to deliver the frame to the appropriate site.

Your EDEs cryptographically protect each frame, so the received data remains confidential, is the data you transmitted, and has unchanged C-VLAN header. An additional, outer C-VLAN tag is created, allowing the the service provider to use that to deliver the frame, changing it if necessary (e.g., to remap VLANs within its network, or to change a frame's priority or drop eligible parameters).

Simple figure with customer network sites and attached EDEs

**Figure 1-1—EDEs protecting frames**

Your EDEs can also enhance privacy by allowing you to reduce the ability of others to make guesses about the network application you are using, sites visited and communication patterns in general, and the level of business activity as reflected in network use, by observing the sizes and timing of the transmitted frames.

## 2. Deployment overview

You may be already using an unprotected VLAN service to connect your network sites. In any case a step-wise approach to deployment helps identify any configuration issues.

1) Verify that the service is providing the expected connectivity before enabling security.

   It is essential that you have a firm understanding (a baseline) of how your network is currently configured and used before deploying MACsec and privacy protection. The initial deployment steps help to verify that this baseline is accurate.

2) Enable MACsec to protect communication between each pair of network sites,[1] verifying the operation of the authentication and key agreement processes and confidentially protected data communication.

3) Enable (and tune if necessary) privacy protection parameters.

As initially configured your EDE can be added between your existing network site equipment and the sevice provider interface without changing the frames that are transmitted to and received from that interface. The EDE has two external ports. The Customer Edge Port (CEP, red-side) is connected to your equipment, and its Provider Network Port (PNP, black-side) is connected to the service provider. All the traffic to and from the service provider passes through those two ports and through an internal interface known as a Provider Edge Port (PEP).[2]

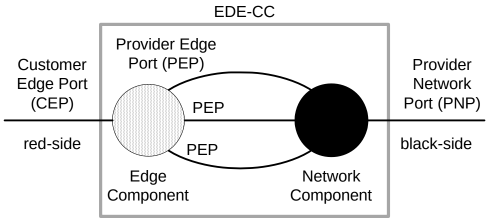

**Figure 1-2—EDE Ports**

[1] See later for a discussion of group communication between sites.

A PEP can be configured to protect traffic that flows to and from a PEP in one of the other EDEs attached to the service provider. Confidentiality and integrity protection is provided by MACsec, and privacy can be further enhanced by configuring MAC Privacy protection. Initially all traffic is assigned to a single PEP (named *pep-0*). This PEP does not use MACsec, and frames pass through the EDE unmodified.

## 3. Baseline

Your EDE is pre-configured with 8 additional PEPs, named *pep-1* through *pep-8*. Each of these interfaces is also pre-configured with MACsec and MAC Privacy protection, but MACsec is disabled. Before assigning traffic to pep-1, check this by verifying that the following 802.1X YANG nodes:[3]

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1x:pae:
        logon-process:logon        = False
        mka:enable                 = False
        macsecDesired              = False
        macsecProtect              = False
        macsecValidateFrames       = Null[4]
```

*pep-1* can be renamed, if you wish, to reflect the name of the remote site associated with the PEP, by updating the YANG node:

```
ietf-interfaces:interfaces:pep-1:name
```

Because MACsec is currently disabled, frames for each C-VLAN assigned to this PEP will pass through the EDE unchanged.[5] This allows traffic for those VLANs to continue to flow while matching assignments are made for the corresponding PEP on the EDE at the remote site.

Each assigned C-VLAN is added to the list for the PEP:

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1ae:ede:
        c-vids*
```

This addition will remove it from the C-VLAN list for any of the other PEPs.[6]

Once matching C-VLAN to PEP assignments have been made for the remote EDE, check that frames are following the anticipated path by comparing receive and transmit statistics. Changes in :

```
ietf-interfaces:interfaces:pep-1:out-octets
```

should match changes in in-octets at the remote PEP.

## 4. MACsec Deployment

Check that a non-standard deployment of MACsec is not already being used to protect frames passing through the EDEs by configuring both:

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1ae:secy:
        validateFrames             = Check
ietf-interfaces:interfaces:pep-1:ieee802-dot1x:pae:
        macsecValidateFrames       = Check.
```

There should be no increase to any SecY’s validation counts[7] other than:

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1ae:secy:
        InPktsUntagged
```

One of the C-VLANs assigned to this PEP has to be selected to be used by the outer C-VLAN tag that will be added once MACsec has been enabled. By default this will be the first C-VLAN assigned to the PEP, unless that C-VLAN assignment has been removed. It can be explicitly selected by configuring the value of:

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1ae:ede:
        black-vid [8]
```

NOTE—IEEE Std 802.1AEcg-2018 assigned each C-VLAN to a separate PEP and required the outer (black-side) C-VLAN tag to match the inner (red-side) tag. This constraint has been removed for MACsec Privacy protection, to reduce an adversary’s ability to distinguish between network flows for different VLANs that take the same path across the provider network, and to reduce the overhead that might otherwise be required to maintain each of those flows (rather their total) at a constant level.

[2] In Figure 1-2 the EDE is shown as two bridge components. All the management operations described in this guide are carried out on the Edge Component and Edge Component PEPs - in the few cases where the standard model of the EDE would require configuration of internal Network Component Ports additional PEP YANG nodes provide this functionality. The Network Component simply multiplexes/demultiplexes frames passing between the PEPs and the Provider Network Port. UNI (User Network Interface) configuration is supporeted by the Network Component PNP.

[3] Annex A (tbs) lists the initial configuration settings of other management variables for this EDE. If the EDE has been repurposed from elsewhere in the network all these values should be checked or reset.

[4] There is an error in the 1X-2020 UML and consequently in the MIB and the YANG, where macsecValidate [ieee8021XKayMacSecValidate in the MIB] are shown as boolean and read only. The correct (useful and sensible) behavior is specified by the CP state machine , where validateFrames (the signal to the secY which overrides the SecY’s 802.1AE enum validateFrames {Null, Disabled, Check, Strict} [secyIfValidateFrames] with read/write MIB access) is set equal to Check in the AUTHENTICATED and equal to macsecValidate in the INIT state.Note also: (1) UML in 1AE-2018 Figure 10-5 does not show read/read-write status of variables, and that could be usefully added.; (2) some of the MIB descriptive text refers to secyIfValidateFrames as secyValidateFrames or secyIfvalidateFrames (3) ‘macsecValidate’ appears twice in the KaY group in 1AE-2018 Figure 12-3. Changes need to be a 1X maintenance item.

[5] All frames destined for remote sites are assumed to be C-VLAN tagged. When the EDE has been fully configured to protect these frames, a single C-VLAN can still be assigned to PEP-0 with its frames untagged to allow (subject to constraints detailed later) UNI protocol to pass through the EDE unchanged, rather than being supported by the EDE’s PNP.

[6] The use of the PEP C-VLAN list is a simplification of the management functionality specified by IEEE Std 802.1Q-2018 and IEEE Std 802.1Qcp. In general frames for a given C-VLAN can be forwarded through more than two bridge ports. An EDE’s edge bridge component restricts that forwarding to the Customer Edge Port (red-side) and at most one PEP. One consequence is that an EDE does not need to learn from the source addresses of frames, or filter using their unicast destination addresses. This EDE’s Edge Component does support all the nodes specified in the 802.1Q YANG model for C-VLAN Bridges, and changes to the C-VLAN list for a PEP are reflected in the egress-ports list maintained for each C-VLAN in that model.

[7] List these or provide a reference to a list. If MACsec was being successfully used in a non-standard configuration the expectation would be that InPktsNoSA would be incrementing.

[8] In the standard model this command has the effect of configuring the PVID on the internal Network Component port connected to the PEP.

Before enabling MACsec, check that the paired PEPs (local and remote) can authenticate each other. If EAP is to be used then configure:

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1x:pae:
        useEAP                  = True[9]
        unAuthAllowed           = True
        unsecureAllowed         = True
```

true, and make the same change for the remote PEP. The variable useEAP can be cleared (False) if pre-shared or cached CAKs are to be used and have already been configured.

Initiate authentication by setting:

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1x:pae:
        logon
```

true, and make the same change for the remote PEP.[10]

Successful EAP operation can be confirmed by checking that either (or both) of the following parameters are True:

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1x:pae:
        sup:authenticated
        auth:authenticated
```

Enable the MACsec Key Agreement (MKA) protocol by setting:

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1x:pae:
        mka:enable
```

Check that MKA is operating correctly and is communicating with the remote site associated with this PEP by checking the list of live peers:

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1x:pae:kay:
        participant:peers.*live
```

There should be one entry on this list, and within that entry the first 6 octets of :

```
        ieee8021XKayMkaPeerListSCI
```

should be the MAC Address of the remote EDE.

Enable MACsec operation by setting

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1x:pae:
        mka:macsecDesired       = True[11]
        mka:macsecProtect       = True
```

for the corresponding PEP at the remote site. The local PEP's counter:

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1ae:secy:
        InPktsOK [12]
```

should now be incrementing to reflect traffic from that site. If any of the following counters are still incrementing :

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1ae:secy:
        InPktsUntagged
        InPktsBadTag
        InPktsNoSA
        InPktsLate
        InPktsInvalid
```

then there has been configuration error. It is most likely that the VLAN connectivity provided by the service provider has not been correctly configured, so frames from other remote sites are being unexpectedly received at the PEP. Your network users may be relying on these frames, so it is wise to track down their source (use of a network analyzer looking for unprotected frames or frames with an unexpected SCI is advised). There is of course the possibility that an adversary has been gaining access to your network. Once the source of the error has been located (and removed if under your control), then set:

```
ietf-interfaces:interfaces:pep-1:ieee802-dot1x:pae:
        macsecValidateFrames      = Strict
```

This will screen out unwanted traffic on reception. Repeat the process of setting macsecDesired and macsecProtect, checking counters, and then setting macsecValidate at the remote PEP.

Similarly configure PEPs for communication with your other remote sites. The interface statistics for each PEP reflect the traffic between the local network and the remote site for that PEP.

## 5. Enabling MAC Privacy protection

[9] This control is in the NID group. NID support, in general is optional. Do we have a problem here, and a need to clarify that is for the 'default' or 'anonymous' NID if NIDS in general are not being used.

[10] This command enables EAP Supplicant operation. This EDE always enables the EAP Authenticator.

[11] The 1X-2020 CP state machine and elsewhere would seem to suggest that macsecProtect is settable by management, but the 1X Figure 12-3 UML has it has read only. The latter is consistent with using macsecDesired as the sole control, but reduces diagnostic capabilities, particularly for a group. Needs a maintenance item, along with the maintenance to macsecValidate footnoted earlier.

[12] This is actually the counter for the (single) receive SC, so the object identifer here needs to be updated to reflect that.