IEEE 802.1AE

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/IEEE_802.1AE#mw-head)[Jump to search](https://en.wikipedia.org/wiki/IEEE_802.1AE#searchInput)

*Not to be confused with*[*IEEE 802.11ac*](https://en.wikipedia.org/wiki/IEEE_802.11ac)*or*[*IEEE 802.11ad*](https://en.wikipedia.org/wiki/IEEE_802.11ad)*.*

|  |  |
| --- | --- |
|  | This article **relies too much on**[**references**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability)**to**[**primary sources**](https://en.wikipedia.org/wiki/Wikipedia:No_original_research#Primary,_secondary_and_tertiary_sources). Please improve this by adding [secondary or tertiary sources](https://en.wikipedia.org/wiki/Wikipedia:No_original_research#Primary,_secondary_and_tertiary_sources). *(June 2016) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

**802.1AE** is the [IEEE](https://en.wikipedia.org/wiki/IEEE) [MAC](https://en.wikipedia.org/wiki/Media_Access_Control) Security standard (also known as **MACsec**) which defines connectionless data confidentiality and integrity for media access independent protocols. It is standardized by the [IEEE 802.1](https://en.wikipedia.org/wiki/IEEE_802.1) working group.[[1]](https://en.wikipedia.org/wiki/IEEE_802.1AE#cite_note-1)



**Contents**

* [1Details](https://en.wikipedia.org/wiki/IEEE_802.1AE#Details)
* [2See also](https://en.wikipedia.org/wiki/IEEE_802.1AE#See_also)
* [3References](https://en.wikipedia.org/wiki/IEEE_802.1AE#References)
* [4External links](https://en.wikipedia.org/wiki/IEEE_802.1AE#External_links)

Details[[edit](https://en.wikipedia.org/w/index.php?title=IEEE_802.1AE&action=edit&section=1)]

Key management and the establishment of secure associations is outside the scope of 802.1AE, but is specified by [802.1X-2010](https://en.wikipedia.org/wiki/802.1X-2010).

The 802.1AE standard specifies the implementation of a *MAC Security Entities* (SecY) that can be thought of as part of the stations attached to the same LAN, providing secure MAC service to the client. The standard defines

* **MACsec frame format**, which is similar to the [Ethernet](https://en.wikipedia.org/wiki/Ethernet) frame, but includes additional fields:
  + *Security Tag*, which is an extension of the [EtherType](https://en.wikipedia.org/wiki/EtherType)
  + [Message authentication code](https://en.wikipedia.org/wiki/Message_authentication_code) (*ICV*)
* Secure *Connectivity Associations* that represent groups of stations connected via unidirectional *Secure Channels*
* *Security Associations* within each secure channel. Each association uses its own key (SAK). More than one association is permitted within the channel for the purpose of key change without traffic interruption (standard requires devices to support at least two)
* A default [cipher](https://en.wikipedia.org/wiki/Cipher) suite of [GCM-AES-128](https://en.wikipedia.org/wiki/Galois/Counter_Mode) (Galois/Counter Mode of [Advanced Encryption Standard](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) cipher with 128-bit key)
  + [GCM-AES-256](https://en.wikipedia.org/wiki/Galois/Counter_Mode) using a 256 bit key was added to the standard 5 years later.

Security tag inside each frame in addition to [EtherType](https://en.wikipedia.org/wiki/EtherType) includes:

* association number within the channel
* packet number to provide unique [initialization vector](https://en.wikipedia.org/wiki/Initialization_vector) for encryption and authentication algorithms as well as protection against [replay attack](https://en.wikipedia.org/wiki/Replay_attack)
* optional LAN-wide secure channel identifier (not required on point-to-point links).

The IEEE 802.1AE (MACsec) standard specifies a set of protocols to meet the security requirements for protecting data traversing Ethernet LANs.

MACsec allows unauthorised LAN connections to be identified and excluded from communication within the network. In common with [IPsec](https://en.wikipedia.org/wiki/IPsec) and [TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security), MACsec defines a security infrastructure to provide data confidentiality, [data integrity](https://en.wikipedia.org/wiki/Data_integrity) and [data origin authentication](https://en.wikipedia.org/wiki/Data_origin_authentication).

By assuring that a frame comes from the station that claimed to send it, MACSec can mitigate attacks on Layer 2 protocols.

Publishing history:

* 2006 – Original publication (802.1AE-2006)[[2]](https://en.wikipedia.org/wiki/IEEE_802.1AE#cite_note-ieee_status-2)
* 2011 – 802.1AEbn amendment adds the option to use 256 bit keys to the standard. (802.1AEbn-2011)[[2]](https://en.wikipedia.org/wiki/IEEE_802.1AE#cite_note-ieee_status-2)
* 2013 – 802.1AEbw amendment defines GCM-AES-XPN-128 and GCM-AES-XPN-256 cipher suites in order to extend the packet number to 64 bits. (802.1AEbw-2013)[[3]](https://en.wikipedia.org/wiki/IEEE_802.1AE#cite_note-3)
* 2017 – 802.1AEcg amendment specifies Ethernet Data Encryption devices. (802.1AEcg-2017)[[4]](https://en.wikipedia.org/wiki/IEEE_802.1AE#cite_note-4)
* 2018 – 802.1AE-2018[[5]](https://en.wikipedia.org/wiki/IEEE_802.1AE#cite_note-5)

See also[[edit](https://en.wikipedia.org/w/index.php?title=IEEE_802.1AE&action=edit&section=2)]

* [Kerberos](https://en.wikipedia.org/wiki/Kerberos_(protocol)) – using tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner
* [OSI model § Layer 2: Data Link Layer](https://en.wikipedia.org/wiki/OSI_model#Layer_2:_Data_Link_Layer)
* [Virtual LAN](https://en.wikipedia.org/wiki/Virtual_LAN) (VLAN) – any broadcast domain that is partitioned and isolated in a computer network at the data link layer
* [IEEE 802.11i-2004](https://en.wikipedia.org/wiki/IEEE_802.11i-2004) (WPA2)
* [Wi-Fi Protected Access](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) (WPA)
* [Wired Equivalent Privacy](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) (WEP)

References[[edit](https://en.wikipedia.org/w/index.php?title=IEEE_802.1AE&action=edit&section=3)]

* 1. [**^**](https://en.wikipedia.org/wiki/IEEE_802.1AE#cite_ref-1) [*"802.1AE - Media Access Control (MAC) Security"*](http://www.ieee802.org/1/pages/802.1ae.html)*.*[*IEEE 802.1*](https://en.wikipedia.org/wiki/IEEE_802.1)*working group. 2015-09-25.*
  2. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/IEEE_802.1AE#cite_ref-ieee_status_2-0) [***b***](https://en.wikipedia.org/wiki/IEEE_802.1AE#cite_ref-ieee_status_2-1) [*"IEEE Standards Status Report: 802.1AE"*](https://standards.ieee.org/cgi-bin/status?Designation:%20802.1AE)*.*[*IEEE*](https://en.wikipedia.org/wiki/IEEE)*. Retrieved 2016-04-25.*
  3. [**^**](https://en.wikipedia.org/wiki/IEEE_802.1AE#cite_ref-3) [*"802.1AEbw - MAC Security Amendment: Extended Packet Numbering"*](http://www.ieee802.org/1/pages/802.1aebw.html)*. IEEE 802.1 working group. 2014-07-18.*
  4. [**^**](https://en.wikipedia.org/wiki/IEEE_802.1AE#cite_ref-4) *"IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security - Amendment 3:Ethernet Data Encryption devices". IEEE STD 802.1AEcg-2017 (Amendment to IEEE STD 802.1AE-2006 as Amended by IEEE STD 802.1AEbn-2011 and IEEE STD 802.1AEbw-2013): 1–143. May 2017.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1109/ieeestd.2017.7932238*](https://doi.org/10.1109%2Fieeestd.2017.7932238)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-1-5044-3725-7*](https://en.wikipedia.org/wiki/Special:BookSources/978-1-5044-3725-7)*.*
  5. [**^**](https://en.wikipedia.org/wiki/IEEE_802.1AE#cite_ref-5) *IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security. IEEE. December 2018.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1109/IEEESTD.2018.8585421*](https://doi.org/10.1109%2FIEEESTD.2018.8585421)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-1-5044-5215-1*](https://en.wikipedia.org/wiki/Special:BookSources/978-1-5044-5215-1)*.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=IEEE_802.1AE&action=edit&section=4)]

* [IEEE 802.1AE-2006 free download](http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=11085)
* [IEEE 802.1AEbn-2011 free download](http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6047534)
* [IEEE 802.1AEbw-2013 free download](http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6461374)
* [MACsec Toolkit, a source code toolkit implementation of IEEE 802.1X-2010 (MACsec control plane) and IEEE802.1AE (MACsec data plane)](http://www.insidesecure.com/Products-Technologies/Protocol-Security-Toolkits/MACsec-Toolkit)