WIKIPEDIA
The Free Encyclopedia

IEEE 802.1AE

IEEE 802.1AE (also known as **MACsec**) is a network security standard that operates at the medium access control layer and defines connectionless data confidentiality and integrity for media access independent protocols. It is standardized by the IEEE 802.1 working group.[1]

Details

Key management and the establishment of secure associations is outside the scope of 802.1AE, but is specified by 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 frame, but includes additional fields:
  - *Security Tag*, which is an extension of the EtherType
  - 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 suite of GCM-AES-128 (Galois/Counter Mode of Advanced Encryption Standard cipher with 128-bit key)
  - GCM-AES-256 using a 256 bit key was added to the standard 5 years later.

Security tag inside each frame in addition to EtherType includes:

- association number within the channel
- packet number to provide unique initialization vector for encryption and authentication algorithms as well as protection against 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 unauthorized LAN connections to be identified and excluded from communication within the network. In common with IPsec and TLS, MACsec defines a security infrastructure to provide data confidentiality, data integrity and data origin authentication.

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

Publishing history:

- 2006 – Original publication (802.1AE-2006)[2]

- 2011 – 802.1AEbn amendment adds the option to use 256 bit keys to the standard. (802.1AEbn-2011)[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]
- 2017 – 802.1AEcg amendment specifies Ethernet Data Encryption devices. (802.1AEcg-2017)[4]
- 2018 – 802.1AE-2018[5]

See also

- Kerberos – 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
- Virtual LAN (VLAN) – any broadcast domain that is partitioned and isolated in a computer network at the data link layer
- IEEE 802.11i-2004 (WPA2)
- Wi-Fi Protected Access (WPA)
- Wired Equivalent Privacy (WEP)

References

1. "802.1AE - Media Access Control (MAC) Security" (http://www.ieee802.org/1/pages/802.1ae.html). IEEE 802.1 working group. 2015-09-25.
2. "IEEE Standards Status Report: 802.1AE" (https://standards.ieee.org/cgi-bin/status?Designation:%20802.1AE). IEEE. Retrieved 2016-04-25.
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. "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:10.1109/ieeestd.2017.7932238 (https://doi.org/10.1109%2Fieeestd.2017.7932238). ISBN 978-1-5044-3725-7.
5. *IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security*. IEEE. December 2018. doi:10.1109/IEEESTD.2018.8585421 (https://doi.org/10.1109%2FIEEESTD.2018.8585421). ISBN 978-1-5044-5215-1.

External links

- 802.1AE-2018 (https://ieeexplore.ieee.org/document/8585421) (registration required)
- MACsec Toolkit (https://www.rambus.com/security/software-protocols/secure-communication-toolkits/macsec-tk/) - A source code toolkit implementation of IEEE 802.1X-2010 (MACsec control plane) and IEEE802.1AE (MACsec data plane)

Retrieved from "https://en.wikipedia.org/w/index.php?title=IEEE_802.1AE&oldid=1182005427"