(https://1.ieee802.org/)

Search

Search

Menu

- IEEE-SA (http://standards.ieee.org/)
- IEEE 802 (http://www.ieee802.org/)
- WG Policies and Procedures (https://1.ieee802.org/rules/)
    - 802.1 Email Lists (https://1.ieee802.org/email-lists/)
    - 802.1 WG Voting Membership (https://1.ieee802.org/rules/wg-membership/)
    - Confidentiality Statements and Copyright Notices (https://1.ieee802.org/confidentiality-statements-and-copyright-notices-on-communications/)
- Future Meetings (https://1.ieee802.org/meetings/)
- Documents (https://1.ieee802.org/documents/)
    - Public Documents (http://www.ieee802.org/1/files/public/)
    - Committee Documents (http://www.ieee802.org/1/files/private/)
    - Active Ballots (https://1.ieee802.org/active-ballots/)
- Time-Sensitive Networking (TSN) Task Group (https://1.ieee802.org/tsn/)
    - 802.1CS – Link-local Registration Protocol (https://1.ieee802.org/tsn/802-1cs/)
    - 802.1AX-Rev – Link Aggregation Revision (https://1.ieee802.org/tsn/802-1ax-rev/)
    - 802.1AS-Rev – Timing and Synchronization for Time-Sensitive Applications (https://1.ieee802.org/tsn/802-1as-rev/)
    - 802.1Qcc – Stream Reservation Protocol (SRP) Enhancements and Performance Improvements (https://1.ieee802.org/tsn/802-1qcc/)

  - 802.1Qcj – Automatic Attachment to Provider Backbone Bridging (PBB) services (https://1.ieee802.org/tsn/802-1qcj/)
  - 802.1CM – Time-Sensitive Networking for Fronthaul (https://1.ieee802.org/tsn/802-1cm/)
  - 802.1Qcp – Bridges and Bridged Networks Amendment: YANG Data Model (https://1.ieee802.org/tsn/802-1qcp/)
  - 802.1Qcr – Bridges and Bridged Networks Amendment: Asynchronous Traffic Shaping (https://1.ieee802.org/tsn/802-1qcr/)
  - 802.1ABcu – LLDP YANG Data Model (https://1.ieee802.org/tsn/802-1abcu/)
  - 802.1Qcw – YANG Data Models for Scheduled Traffic, Frame Preemption, and Per-Stream Filtering and Policing (https://1.ieee802.org/tsn/802-1qcw/)
  - 802.1Qcx – YANG Data Model for Connectivity Fault Management (https://1.ieee802.org/tsn/802-1qcx/)
- OmniRAN Task Group (https://1.ieee802.org/omniran/)
  - 802.1CF Network Reference Model and Functional Description of IEEE 802 Access Network (https://1.ieee802.org/omniran/802-1cf/)
- Addressing and Data Center Bridging (DCB) (https://1.ieee802.org/dcb/)
  - 802.1Qcy – VDP Extension to Support NVO3 (https://1.ieee802.org/dcb/802-1qcy/)
- Security Task Group (https://1.ieee802.org/security/)
  - P802.1AR-Rev: Secure Device Identity (Revision) (https://1.ieee802.org/security/802-1ar-rev/)
  - P802.1Xck: Port-Based Network Access Control—Amendment 2: YANG Data Model (https://1.ieee802.org/security/802-1xck/)
  - P802E: Recommended Practice for Privacy Considerations for IEEE 802 Technologies (https://1.ieee802.org/security/802e/)
- Maintenance (https://1.ieee802.org/maintenance/)
  - 802.1Q-Rev Bridges and Bridged Networks – Revision (https://1.ieee802.org/maintenance/802-1q-rev/)
  - 802.1AC-2016/Cor-1 LLC Encapsulation EtherType (https://1.ieee802.org/maintenance/802-1ac-2016-cor-1/)
- “802 Network Enhancement For the Next Decade” Industry Connections Activity (NENDica) (https://1.ieee802.org/802-nendica/)
- Object Identifiers (https://1.ieee802.org/object-identifiers/)
- YANGsters (https://1.ieee802.org/yangsters/)
  - YANGsters Call Information (https://1.ieee802.org/yangsters/yangsters-call-information/)
- Archived Activities (https://1.ieee802.org/archives/)
  - Local Address Study Group (https://1.ieee802.org/archives/lasg/)

Groups

Agenda (https://1.ieee802.org/category/agenda/)

Meetings (https://1.ieee802.org/category/meetings/)

Minutes (https://1.ieee802.org/category/minutes/)

Uncategorized (https://1.ieee802.org/category/uncategorized/)

802.1AE: MAC Security (MACsec)

Full title: IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security

IEEE 802 Local Area Networks (LANs) are deployed in networks that support mission-critical applications and a wide variety of devices, implemented and administered by different organizations, and serving customers with different economic interests. The protocols that configure, manage, and regulate access to these networks typically run over the networks themselves. Preventing disruption and data loss arising from transmission and reception by unauthorized devices is a required network capability, as it is usually not practical to secure an entire network against physical access.

This standard (MACsec) specifies provision of connectionless user data confidentiality, data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC Clients.

The MACsec Key Agreement Protocol (MKA) specified in IEEE Std 802.1X discovers mutually authenticated MACsec peers, and elects one as a Key Server that distributes the symmetric Secure Association Keys (SAKs) used by MACsec to protect frames. The 802.1AEcg amendment allows a MACsec participant to transmit using multiple secure channels (SCs), each using its own packet number (PN) sequence, to support strict replay protection when frames of different priorities can be disordered (e.g. by a Provider Bridged Network (PBN) or IEEE Std 802.3 frame preemption). 802.1AEcg Annex E describes how MKA supports the multiple transmit SCs.

Current Status

Standard	Available free from the IEEE Get Program. (http://ieeexplore.ieee.org/document/1678345/)
Status	Approved June 8th 2006, Published 18th August 2006. Revision 802.1AE-Rev in progress (http://1.ieee802.org/security/802-1ae-rev/)
Amendments	802.1AEbn–2011: GCM–AES–256 Cipher Suite (http://1.ieee802.org/security/802-1aebn/) 802.1AEbw–2013: Extended Packet Numbering (http://1.ieee802.org/security/802-1aebw/) 802.1AEcg–2017: Ethernet Data Encryption devices (http://1.ieee802.org/security/802-1aecg/)
Editors	Allyn Romanow, Mick Seaman