P802.1AEcg

Submitter Email: gparsons@ieee.org
Type of Project: Amendment to IEEE Standard 802.1AE-2006
PAR Request Date: 12-Jun-2014
PAR Approval Date:
PAR Expiration Date:
Status: Unapproved PAR, PAR for an Amendment to an existing IEEE Standard

---

1.1 Project Number: P802.1AEcg
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Title: Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security
Amendment: Ethernet Data Encryption devices

3.1 Working Group: Higher Layer LAN Protocols Working Group (C/LM/WG802.1)
Contact Information for Working Group Chair
Name: Glenn Parsons
Email Address: gparsons@ieee.org
Phone: 613-963-8141
Contact Information for Working Group Vice-Chair
Name: John Messenger
Email Address: jmessenger@advaoptical.com
Phone: +441904699309

3.2 Sponsoring Society and Committee: IEEE Computer Society/LAN/MAN Standards Committee (C/LM)
Contact Information for Sponsor Chair
Name: Paul Nikolich
Email Address: p.nikolich@ieee.org
Phone: 857.205.0050
Contact Information for Standards Representative
Name: James Gilb
Email Address: gilb@ieee.org
Phone: 858-229-4822

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE-SA for Initial Sponsor Ballot: 07/2015
4.3 Projected Completion Date for Submittal to RevCom: 03/2016

5.1 Approximate number of people expected to be actively involved in the development of this project: 12
5.2.a. Scope of the complete standard: The scope of this standard is to specify provision of connectionless user data confidentiality, frame data integrity, and data origin authenticity by

media access independent protocols and entities that operate transparently to MAC Clients.

5.2.b. Scope of the project: This amendment specifies the use of Media Access Control (MAC) security in two port bridges that provide transparent secure connectivity for customer bridges or provider bridges while allowing provider network service selection and provider backbone network selection to occur as already specified in 802.1Q.

5.3 Is the completion of this standard dependent upon the completion of another standard: No

5.4 Purpose: This standard will facilitate secure communication over publicly accessible LAN/MAN media for which security has not already been defined, and allow the use of IEEE Std 802.1X, already widespread and supported by multiple vendors, in additional applications.

5.5 Need for the Project: IEEE Std 802.1AE already specifies the use of MAC security in various interworking scenarios involving various types of bridging systems (e.g. Customer Bridges, Provider Bridges, and Provider Edge Bridges). However it is also desirable to secure connectivity by adding separate bridging systems known as Ethernet Data Encryption devices (EDEs) dedicated to that purpose and having minimal additional functionality. The desired secure connectivity can be achieved without removing existing network functionality (such as VID-based service selection) by using existing architectural components (as specified in IEEE Std 802.1AE, IEEE Std 802.1X, and IEEE Std 802.1Q). Such use needs to be documented in IEEE Std 802.1AE (specifically within Clause 11 MAC Security in Systems). To facilitate interoperability additional Group Addresses need to be assigned to allow each EDE's IEEE Std 802.1X PAE (Port Access Entity) to communicate with its peer(s). These addresses do not have to be Reserved Addresses (as specified in IEEE Std 802.1Q Clause 8).

5.6 Stakeholders for the Standard: Developers and users of secure networking equipment.

Intellectual Property

6.1.a. Is the Sponsor aware of any copyright permissions needed for this project?: No

6.1.b. Is the Sponsor aware of possible registration activity related to this project?: No

---

7.1 Are there other standards or projects with a similar scope?: No

7.2 Joint Development

Is it the intent to develop this document jointly with another organization?: No

---

8.1 Additional Explanatory Notes (Item Number and Explanation): The base standard IEEE Std 802.1AE-2006 has already been adopted by ISO/IEC JTC1 SC6 under the PSDO agreements and it is anticipated that this amendment will amend that adopted standard in due course.