P802.1AEbw

Submitter Email: tony@jeffree.co.uk
Type of Project: Amendment to IEEE Standard 802.1AE-2006
PAR Request Date: 17-Mar-2012
PAR Approval Date: 15-May-2012
PAR Expiration Date: 31-Dec-2016
Status: PAR for an Amendment to an existing IEEE Standard
Root Project: 802.1AE-2006

1.1 Project Number: P802.1AEbw
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: Extended Packet Numbering

3.1 Working Group: Higher Layer LAN Protocols Working Group (C/LM/WG802.1)
Contact Information for Working Group Chair
Name: Anthony Jeffree
Email Address: tony@jeffree.co.uk
Phone: +44-161-973-4278
Contact Information for Working Group Vice-Chair
Name: Glenn Parsons
Email Address: gparsons@ieee.org
Phone: 613-763-7582

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
None

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE-SA for Initial Sponsor Ballot: 11/2012
4.3 Projected Completion Date for Submittal to RevCom: 08/2013

5.1 Approximate number of people expected to be actively involved in the development of this project: 10

5.2.a. Scope of the complete standard: This amendment specifies the optional use of AES-128 (Advanced Encryption Standard-128) and AES-256 GCM (Galois Counter Mode) Cipher Suites that make use of a 64-bit PN (packet number) as part of their IV (Initialization Vector) parameter while retaining the existing MACsec (Media Access Control security) frame format by continuing to communicate only the least significant 32 bits of the PN in the SecTAG (security tag).

Changes in scope: ~~The~~This ~~scope~~amendment specifies the optional use of ~~this~~AES-128 ~~standard~~(Advanced ~~is~~Encryption ~~to~~Standard-128) ~~specify~~and ~~provision~~AES-256 GCM (Galois Counter Mode) Cipher Suites that make use of ~~connectionless~~a ~~user~~64-bit ~~data~~PN ~~confidentiality,~~(packet ~~frame~~number) ~~data~~as ~~integrity,~~part ~~and~~of ~~data~~their ~~origin~~IV ~~authenticity~~(Initialization ~~by~~Vector) ~~media~~parameter ~~access~~while ~~independent~~retaining ~~protocols~~the ~~and~~existing ~~entities~~MACsec ~~that~~(Media ~~operate~~Access ~~transparently~~Control security) frame format by continuing to ~~MAC~~communicate ~~Clients~~only the least significant 32 bits of the PN in the SecTAG (security tag).

5.2.b. Scope of the project:
5.3 Is the completion of this standard dependent upon the completion of another standard: No
5.4 Purpose: This standard specifies the optional use of Cipher Suites that make use of a 64-bit PN to allow more than 2**32 packets to be sent with a single Secure Association Key.

Changes in purpose: This standard ~~will~~specifies ~~facilitate~~the ~~secure~~optional ~~communication~~use ~~over~~of ~~publicly~~Cipher ~~accessible~~Suites ~~LAN/MAN~~that ~~media~~make ~~for~~use of ~~which~~a ~~security~~64-bit ~~has~~PN ~~not~~to ~~already been defined, and~~ allow ~~the~~more ~~use~~than ~~of~~2**32 ~~IEEE~~packets ~~Std~~to ~~802.1X,~~be ~~already~~sent ~~widespread~~with ~~and~~a ~~supported~~single Secure ~~by~~Association ~~multiple vendors, in additional applications~~Key.

5.5 Need for the Project: At very high speeds (100 Gb/s and above) the existing MACsec Cipher Suites can exhaust an SAK (Security Association Key), thus demanding rekeying, at a rate (~9 seconds for full utilization with

minimum Ethernet frame sizes at 400 Gb/s) that over-constrains implementation technology and does not allow adequate time for in-service software upgrades that
temporarily suspend key agreement protocol operation. There is
significant broad interest in the use of MACsec at these speeds and a
desire to address these issues while retaining a high degree of
compatibility with existing implementations and deployment.

5.6 Stakeholders for the Standard: Developers and users of 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):