Five Criteria for 802.1AEbw - Media Access Control (MAC) Security Amendment: Extended Packet Numbering

1. Broad Market Potential

a. Broad sets of applicability

This amendment is applicable to all networks that are currently using or planning to use MACsec. The addition of these Cipher Suites will continue the appeal and applicability of IEEE 802.1AE for customers deploying or planning use of the fastest LAN technologies.

b. Multiple vendors and numerous users

A number of major equipment providers have indicated support for this amendment.

c. Balanced costs (LAN versus attached stations)

There is no imbalance of cost created by this amendment.

2. Compatibility

This amendment fits within the framework of IEEE 802.1AE-2006 without changes to the frame formats. Implementations that conform to the existing standard will remain conformant. A definition of managed objects is already included in the base standard and will be retained with little (if any) extension, as it already provides for the addition of new Cipher Suites without changes to the MIB.

3. Distinct Identity

a. Substantially different from other IEEE 802 standards

IEEE 802.1AE is already a recognized and established standard.

b. One unique solution per problem (not two solutions to a problem)

This project enhances IEEE 802.1AE to meet emerging and additional needs, it does not duplicate existing capabilities.

c. Easy for the document reader to select the relevant specification

IEEE Std 802.1AE is already an established reference for MAC Security.

4. Technical Feasibility

a. Demonstrated system feasibility

The characteristics of the GCM-AES family of cipher suites is already well known. IEEE 802.1AE was one of the first vehicles for this technology. Extended packet numbering techniques similar to that proposed for this amendment have already been deployed for IP security.

b. Proven technology, reasonable testing

Technology for testing cryptographic modes of operations is well advanced.

c. Confidence in reliability

GCM-AES has been adopted by NIST. Extended packet numbering techniques have been used for other purposes. This project is expected to pose no new reliability challenges.

d. Coexistence of 802 wireless standards specifying devices for unlicensed operation

Not applicable.

5. Economic Feasibility

a. Known cost factors, reliable data

The economic factors for adoption of this technology outweigh the estimated costs of implementing the solution.

b. Reasonable cost for performance

The economic factors for adoption of this technology outweigh the estimated costs of implementing the solution.

c. Consideration of installation costs

The economic factors for adoption of this technology outweigh the estimated costs of implementing the solution.