Project : P802.1AE

Title : MAC Security

Acronym/Short Name : MACsec

Five Criteria :

1. Broad Market Potential

A standards project authorized by IEEE 802 shall have a broad market potential. Specifically, it shall have the potential for:

a) Broad sets of applicability.
b) Multiple vendors and numerous users
c) Balanced costs (LAN versus attached stations)

1. Public networks for residential and business applications represent a new and very broad application space for IEEE802 wireline technologies. LAN/MAN security is a key requirement for the deployment of 802.3, EFM, RPR and other 802 technologies in subscriber and metro access networks.
2. The proposed standard will allow vulnerable parts of networks to be transparently secured without incurring modifications or costs for attached stations or burdening network applications. This is expected to facilitate rapid deployment of solutions based on this standard.
3. At the Call for Interest on November 2002, 32 individuals from 18 companies representing both vendors and users expressed their support for the project. 50-70 individuals from more than 30 companies have attended the study group sessions.

2. Compatability

IEEE 802 defines a family of standards. All standards shall be in conformance with the IEEE 802.1 Architecture, Management and Interworking documents as follows: 802. Overview and Architecture, 802.1D, 802.1Q and parts of 802.1f. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with 802.

Each standard in the IEEE 802 family of standards shall include a definition of managed objects which are compatible with systems management standards.

1. The proposed project will be developed in conformance with the 802 Overview and Architecture.
2. The proposed project will be developed in conformance with 802.1D, 802.1Q, 802.1f.
3. Managed objects will be defined consistent with existing policies and practices for 802.1 standards.

3. Distinct Identity

Each IEEE 802 standard shall have a distinct identity. To achieve this, each authorized project shall be:

a) Substantially different from other IEEE 802 standards.
b) One unique solution per problem (not two solutions to a problem).
c) Easy for the document reader to select the relevant specification.

1. Existing standards that are applicable to all MACs specify end to end security. There is no general specification that allows individual LANs or parts of a Bridged Local Area Network to be secured.
2. The existing standards that protect individual LANs or segments are MAC specific, and do not apply to the bulk of the application space (802.3)

3. Higher layer security protocols, e.g. IPSEC, do not protect against intrusion at the MAC layer and thus do not adequately separate users of publicly accessible networks based on 802 LAN/MAN technology.
4. There is user traffic that is unlikely to be subject to IPSEC or other higher layer security mechanisms that will be protected by this standard.

4. Technical Feasibility

For a project to be authorized, it shall be able to show its technical feasibility. At a minimum, the proposed project shall show:

a) Demonstrated system feasibility.
b) Proven technology, reasonable testing.
c) Confidence in reliability.

1. Commercially available implementations of encryption/decryption products currently provide data integrity and confidentiality at Gigabit speeds, demonstrating feasibility.
2. There are widely deployed key management and secure association technologies that demonstrate that technical support will be available for this standard.

5. Economic Feasibility

For a project to be authorized, it shall be able to show economic feasibility (so far as can reasonably be estimated), for its intended applications. At a minimum, the proposed project shall show:

a) Known cost factors, reliable data.
b) Reasonable cost for performance.
c) Consideration of installation costs.

1. Similar technologies have been implemented in 802.11 and IPsec and both have been proven to be cost effective solutions.
2. Link security mechanisms have been incorporated in other link mechanisms at a reasonable cost increment. Initial studies show that encryption at the Gbps rate is also possible with a small relative network cost increment.
3. The security mechanism will add modest cost relative to the installation cost of public access network technology.