
Proposed Ethernet Security PAR and 5 Criteria

IEEE 802.3ah, Security Session,
New Orleans, Sept 30 - Oct 3 2002

Title

Standard for - Information technology -
Telecommunications and information exchange between
systems - Local and metropolitan area networks -
Specific requirements - Part 3: Carrier sense multiple
access with collision detection (CSMA/CD) access
method and physical layer specifications – **Link security
for Ethernet point-to-multipoint (P2MP) subscriber
access networks**

Scope

Extend 802.3 definition with a link security mechanism in order to overcome the security threats specific to an Ethernet optical point-to-multipoint (P2MP) subscriber access network and equate the security level to the security level needed in a point-to-point (P2P) subscriber access network within the scope of the current IEEE Std 802.3 and approved new projects.

Purpose

To expand the Ethernet definition with a link security mechanism in order to meet the link security requirements to operate in a subscriber access network.

Broad Market Potential

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

- 1.** Residential and business access networks represent a new and very broad application space for Ethernet. This project complements EFM project by addressing the security issues of the Ethernet transition from enterprise to subscriber access networks.
 - 2.** At the special security session, XXX individuals from YY companies representing both vendors and users expressed their support for the project.
 - 3.** Ethernet vendors and users are able to achieve an optimal cost balance between the network infrastructure components and the attached stations.
-

Compatibility

- a) Conformance with 802 Overview and Architecture**
 - b) Conformance with 802.1D, 802.1Q, 802.1f**
 - c) Compatible managed object definitions**
-

1. As a supplement to IEEE Std 802.3, the proposed project will remain in conformance with the 802 Overview and Architecture.
2. As a supplement to IEEE Std 802.3, the proposed project will remain in conformance with 802.1D, 802.1Q, 802.1f.
3. As a supplement to IEEE Std 802.3, the proposed project will follow the existing format and structure of 802.3 MIB definitions.
4. As a supplement to IEEE Std 802.3, the proposed project will remain in conformance with 802.1x, though extensions to these standards may be proposed as additional work items.
5. As a supplement to IEEE Std 802.3, the proposed project will remain in conformance with point-to-multipoint specification defined by 802.3ah TF.

Distinct Identity

- 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.** There is no existing link security specification for Ethernet access protocol.
- 2.** The proposed project will leverage as much as possible from existing 802 link security mechanisms that are defined in 802.10, 802.11, 802.15, 802.16.
- 3.** The proposed project will be formatted as IEEE Std 802.3, making it easy for the document reader to identify the security specification and its applicability to the relevant topologies.

Technical Feasibility

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

1. Like level encryption is cost effectively integrated HFC and wireless networks today, which are inherently easier to access than fiber. This project will be based on work done in these and other organizations.
2. Ethernet P2MP operates at Gbps rate. Initial studies show that encryption implemented in hardware is feasible and cost effective at these rates.
3. The proposed project will, to the extent possible, re-use specifications developed by other standards bodies and develop new specifications in accordance with the rigorous standards of proof applied to 802.3 projects.
4. Since security is a new area for Ethernet, the review process and standards proof policies need to be defined. The proposed project will collaborate with other WGs or TAGs in the 802 chartered with security activities in defining these policies in order to leverage expertise and experience from all other 802 groups and other standard organizations.

Economic Feasibility

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

1. The goal of this project is to offer a link security mechanism that balances the level of data security with the cost and performance of the access technology.
2. Link security mechanisms are incorporated to other link mechanisms at a reasonable cost increment. Initial studies show that encryption at the Gbps rate is also possible with a similar relative cost increment.
3. The security mechanism does not require additional infrastructure. So installation costs are reduced to the configuration of the system. In order to reduce these costs, this project may incorporate remote and automatic configuration mechanisms with authentication and code verification to guarantee a secure manipulation process.