July 18, 2003

T1M1

Internetwork Operations, Administration,
Maintenance, and Provisioning

A Technical Subcommittee of
Standards Committee T1
Telecommunications
www.t1.org

Accredited by the American National
Standards Institute

Michael J. Fargano
Chairman

Ronald Roman
Vice Chairman

A Sponsored Committee of

Alliance for Telecommunications
Industry Solutions

Michael J. Fargano
Qwest Communications
26th Floor
1801 California St.
Denver, CO 80202-1984

303 896 3618 (T)

email: Michael.Fargano@qwest.com

Howard Frazier, Chair
IEEE 802.3ah Task Force
millardo@dominetsystems.com

Subject: T1M1 Response to IEEE 802.3ah Task Force Liaison (T1M1/2003-078) – EFM OAM&P Review - IEEE P802.3ah/Draft 1.732

Dear Howard,

Thank you for your liaison regarding EFM OAM&P review - dated May 15, 2003. The T1M1.5 Working Group reviewed the OAM&P aspects of EMF that were provided in your liaison to T1M1 (document IEEE P802.3ah/Draft 1.732). Based on this, T1M1 offers the following comments for your consideration:

a) Rename section 57.2.8 from *OAM remote loopback* to *Intrusive OAM remote loopback*

b) Add section 57.2.9 *Non-intrusive OAM remote loopback*

   Requirement is to have an op-code that provides a per-packet echo reply to a query for aliveness checking. The requirement is to have the ability to have a non-intrusive loopback mechanism that would enable service providers to query and receive response back from end devices for aliveness checking. The format should support fields for location IDs; both source and destination. A loopback indicator is required as it provides a mechanism for detecting a physical versus logical loop.

c) Add Informative Annex – *Transport Layer Fault Management Escalation*

   A link segment functioning with OAM requires physical layer defects (loss of signal, alarm indications, loss of frame) to be detected and signaled to the network's OAM layer. It is understood that the network's OAM layer generates and transmits an OAMPDU containing indications of this physical layer defect via the Flags field of any OAMPDU, or via an Event Notification OAMPDU, or both. Due to separation of functions as defined in the separate clauses of P802.3ah D1.732, however, the entire picture of OAM operation is somewhat unclear. Please consider adding an informative annex that describes an example OAM operation from the physical layer upwards, including an example of mapping an EFM-compliant physical layer defect to OAMPDU flags and events, and their mapping to managed objects represented in Clause 30.

d) Comment regarding GDMO in Clause 30

   Section 30 defines the management information using GDMO and ASN.1. Has the management interface protocol been specified in another document? While T1M1 and ITU SG 4 and 15 have developed a number of specifications using CMIP as defined by X.711 Recommendation, we would like to bring to your attention the following:

- The management information specified using GDMO/ASN.1 contains the relevant information needed even though the protocol used may *not* be CMIP.

- In order to reuse the extensive library of information models already available as ITU Recommendations with other paradigms framework, services and translation methodology have been defined in ITU. In the case where CORBA is to be used, we would like you to follow the two framework documents Q.816, Q.816.1 on services and X.780 and X.780.1 for models. The two documents in each set refers to a fine grained and coarse-grained (facade) modeling approaches. Examples of these translations can be seen in Q.821.1 for fault and Q.822.1 for Performance management functions.

- Recently there has also been a lot of interest in using XML. Examples can be seen in a recently approved Draft American National Standard for Trial Use where we defined XML messages for Trouble Administration Model originally defined in GDMO in T1.227. For review purposes, see document **T1M1.5/2002-117R4** for the latest pre-publication draft that is publicly available at **ftp://ftp.t1.org/T1M1/M1.5/2002/2m151174.doc**.

e) Comments regarding State Model in Clause 30

In several sections of clause 30 attributes of the type "admin state" are used. See sections 30.3.5.1.1, 30.3.5.2.1, 30.11.1.1.2, and 30.11.1.2.1. These use the words admin state, operational state, and the values enable and disable to describe these states. The concepts provided in these attributes seem to be similar to, but slightly different than the ITU state model that has been used extensively in ITU and other bodies for state modeling. Using the same words to describe different functions may cause confusion. It may be less confusing to adopt the ITU model.

For your information the ITU state model has defined separate attributes for administrative state and operational state. Administrative reflects permission to use or prohibition against using a resource imposed by a management system. Administrative state is single valued, allows read-write access, and has possible values of *locked*, *shutting down*, and *unlocked*. Operational state reflects the physical ability of the resource to provide service to its users. It allows read access only and has possible values of *enabled* and *disabled*. See ITU documents X.731 for definitions of the ITU state model and X.721 for the GDMO for the state model.

f) Comments regarding attributes in Clause 30

We note that you have defined attributes such as vendor ID, version etc. in 30.11.1.1.x. It may be appropriate to reuse the existing definitions from ITU Recommendations. The two major sources for these generic attributes are M.3100, Generic Network Information Model and the addenda, and X.721.

We understand that the *IEEE Link Security Study Group* has been initiated to support the work needed in the area of EFM security. We would like to bring to your attention, and to the attention of the IEEE Link Security Study Group, that ***T1.276-2003*** (Committee T1 American National Standard - *Baseline Security Requirements for the Management Plane*) has just been completed. Please consider this as a reference for baseline EFM management plane security requirements for current and future EFM management plane security – as appropriate. In addition there is current work in progress in T1S1 regarding Control Plane Security requirements. Should you or any interested parties be interested in participating in the T1M1SEC and/or T1S1SEC work, please contact me for further details. [Note, T1.276-2003 is a newly created American National Standard that offers the industry increased baseline management security effectiveness and efficiency. For review purposes, see document **T1M1.5/2003-007R5** for the latest pre-publication draft of T1.276-2003 that is publicly available. The links are as follows: “New File” (pre-archived) at **ftp://ftp.t1.org/T1M1/NEW-T1M1.5/3m150075.pdf;** or, moved to archive at: **ftp://ftp.t1.org/T1M1/M1.5/2003/3m150075.pdf**].

T1M1 is willing to work with you (as needed) on the subsequent details regarding these comments (e.g., state machine details), should other interested parties that are close to the work not make those subsequent detailed contributions. Please advise us on plans, status, procedural matters, and schedule regarding the work needed on subsequent details regarding these comments.

Thank you for coordinating and collaborating with T1M1 on this important industry topic. We look forward to future coordination and collaboration opportunities. Please contact me as these opportunities arise and if there are any comments, questions, or concerns regarding this EFM OAM&P review.

Best regards,

Mike Fargano
T1M1 Chairman

CC:
IEEE IEEE802.3ah Task Force CC: Hugh Barrass; Grow, Bob; David Law (E-mail); p.nikolich@ieee.org; scarlson@hspdesign.com; Kevin.Daines@worldwidepackets.com; mattsquire@acm.org
IEEE Link Security Study Group CC: Dolors Sala (dolors@ieee.org), Chair; allyn@cisco.com
T1E1 CC: Rick Townsend, T1E1 Chair; Ed Eckert, T1E1 Vice Chair
T1S1 CC: Bon Hall, T1S1 Chair; Greg Ratta, T1S1 Vice Chair
Committee T1 Security Program Coordinator: Stephen Hayes (stephen.hayes@ericsson.com)
T1M1 CC: Ron Roman, T1M1 Vice Chair; Lakshmi Raman, T1M1.5 Chair; T1M1.5 Email List ; T1M1.5 EFM review participants.