Network Working Group
Internet-Draft
Updates: 5066 (if approved)
Intended status: Standards Track
Expires: June 13, 2014

E. Beili
Actelis Networks

December 10, 2013

Ethernet in the First Mile Copper (EFMCu) Interfaces MIB
draft-ietf-opsawg-rfc5066bis-07.txt

Abstract

This document updates RFC 5066. It amends that specification by informing the internet community about the transition of the EFM-CU-MIB module from the concluded IETF Ethernet Interfaces and Hub MIB Working Group to the Institute of Electrical and Electronics Engineers (IEEE) 802.3 working group.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 13, 2014.

Copyright Notice

Table of Contents

1. Introduction

RFC 5066 [RFC5066] defines two MIB modules:

EFM-CU-MIB, with a set of objects for managing 10PASS-TS and 2BASE-TL Ethernet in the First Mile Copper (EFMCu) interfaces;

IF-CAP-STACK-MIB, with a set of objects describing cross-connect capability of a managed device with multi-layer (stacked) interfaces, extending the stack management objects in the Interfaces Group MIB and the Inverted Stack Table MIB modules.

With the conclusion of the [HUBMIB] working group, the responsibility for the maintenance and further development of a MIB module for managing 2BASE-TL and 10PASS-TS interfaces, has been transfered to the Institute of Electrical and Electronics Engineers (IEEE) 802.3 [IEEE802.3] working group. In 2011, the IEEE developed IEEE8023-EFM-CU-MIB module, based on the original EFM-CU-MIB module [RFC5066]. The current revision of IEEE8023-EFM-CU-MIB is defined in IEEE Std 802.3.1-2013 [IEEE802.3.1].

The IEEE8023-EFM-CU-MIB and EFM-CU-MIB MIB modules can coexist. Existing deployments of the EFM-CU-MIB need not be upgraded, but operators using the MIB should expect that new equipment will use the IEEE8023-EFM-CU-MIB.

Please note that IF-CAP-STACK-MIB module was not transfered to IEEE and remains as defined in RFC 5066. This memo provides an updated security considerations section for that module, since the original RFC did not list any security consideration for IF-CAP-STACK-MIB.

2. The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of RFC 3410 [RFC3410].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Mapping between EFM-CU-MIB and IEEE8023-EFM-CU-MIB

The current version of IEEE8023-EFM-CU-MIB, defined in IEEE Std 802.3.1-2013, has MODULE-IDENTITY of ieee8023efmCuMIB with an object identifier allocated under the { org ieee standards-association-numbers-series-standards lan-man-stds ieee802dot3 ieee802dot3dot1mibs

} sub-tree.

The EFM-CU-MIB has MODULE-IDENTITY of efmCuMIB with an object identifier allocated under the mib-2 sub-tree.

The names of the objects in the first version of the IEEE8023-EFM-CU-MIB are identical to those in the EFM-CU-MIB. However, since both MIB modules have different OID values, they can coexist, allowing the management of the newer IEEE MIB-based devices, alongside the legacy IETF MIB-based devices.

4. Updating the MIB Modules

With the transfer of the responsibility for maintenance and further development of the EFM-CU-MIB module to the IEEE 802.3 working group, the EFM-CU-MIB defined in RFC 5066 becomes the last version of that MIB module.

All further development of the EFM Copper Interfaces MIB will be done by the IEEE 802.3 working group in the IEEE8023-EFM-CU-MIB module. Requests and comments pertaining to EFM Copper Interfaces MIB should be sent to the IEEE 802.3.1 task force, currently chartered with MIB development, via its mailing list [LIST802.3.1].

The IF-CAP-STACK-MIB remains under IETF control and is currently maintained by the [OPSAWG] working group.

5. Security Considerations

There are no managed objects defined in IF-CAP-STACK-MIB module with a MAX-ACCESS clause of read-write and/or read-create.

Some of the readable objects in this MIB module (i.e., those with MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments since they can reveal some configuration aspects of the network interfaces.

In particular, ifCapStackStatus and ifInvCapStackStatus can identify cross-connect capability of multi-layer (stacked) network interfaces, potentially revealing the underlying hardware architecture of the managed device.

It is thus important to control even GET access to these objects and possibly even encrypt the values of these objects when sending them over the network via SNMP.

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPSec),

there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

Implementations MUST provide the security features described by the SNMPv3 framework (see [RFC3410]), including full support for authentication and privacy via the User-based Security Model (USM) [RFC3414] with the AES cipher algorithm [RFC3826]. Implementations MAY also provide support for the Transport Security Model (TSM) [RFC5591] in combination with a secure transport such as SSH [RFC5592] or TLS/DTLS [RFC6353].

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

6. IANA Considerations

No action is required from IANA.

7. Acknowledgments

This document was produced by the OPSAWG working group, whose efforts were advanced by the contributions of the following people (in alphabetical order):

Dan Romascanu

David Harrington

Michael MacFaden

Tom Petch

This document updates RFC 5066, authored by Edward Beili of Actelis Networks, and produced by the, now concluded, HUBMIB working group.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.

[RFC3826] Blumenthal, U., Maino, F., and K. McCloghrie, "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model", RFC 3826, June 2004.

[RFC5066] Beili, E., "Ethernet in the First Mile Copper (EFMCu) Interfaces MIB", RFC 5066, November 2007.

8.2. Informative References

[HUBMIB] IETF, "Ethernet Interfaces and Hub MIB (hubmib) Charter", <http://datatracker.ietf.org/wg/hubmib/charter/>.

[IEEE802.3] IEEE, "802.3 Ethernet Working Group", <http://www.ieee802.org/3>.

[IEEE802.3.1] IEEE, "IEEE Standard for Management Information Base (MIB) Definitions for Ethernet", IEEE Std 802.3.1-2013, June 2013.

[LIST802.3.1] IEEE, "802.3 MIB Email Reflector", <http://www.ieee802.org/3/be/reflector.html>.

[OPSAWG] IETF, "Operations and Management Area Working Group (opsawg) Charter", <http://datatracker.ietf.org/wg/opsawg/charter/>.

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.

[RFC5591] Harrington, D. and W. Hardaker, "Transport Security Model for the Simple Network Management Protocol (SNMP)", RFC 5591, June 2009.

[RFC5592] Harrington, D., Salowey, J., and W. Hardaker, "Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)", RFC 5592, June 2009.

[RFC6353] Hardaker, W., "Transport Layer Security (TLS) Transport Model for the Simple Network Management

Protocol (SNMP)", RFC 6353, July 2011.

Author's Address

Edward Beili
Actelis Networks
Bazel 25
Petach-Tikva
Israel

Phone: +972-73-237-6852
EMail: edward.beili@actelis.com