Abstract

This memo defines a portion of the Management Information Base (MIB) used by Simple Network Management Protocol (SNMP) for GMPLS based networks.

In particular in the context Wavelength Switching Optical Network (WSON) two sets of information were defined: a general constrains set (reusable by other technologies) and a WSON specific set. This document defines a MIB module for supporting GMPLS WSON specific information.
Copyright (c) 2012 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents
1. Introduction ................................................. 3
2. The Internet-Standard Management Framework .................. 3
3. Conventions ................................................. 3
4. Overview .................................................. 4
5. Structure of the MIB Module .................................. 4
   5.1. tedWsonNodeTable ..................................... 4
   5.1.1. tedWsonResourceBlockInformation .................... 4
   5.1.2. tedWsonResourcePoolAccessibility .................... 4
   5.1.3. tedWsonResourceBlockWavelengthConstraints .......... 4
   5.1.4. tedWsonResourcePoolState ......................... 4
   5.1.5. tedWsonBlockSharedAccessWavelengthAvailability .... 4
6. Relationship to Other MIB Modules ............................ 4
   6.1. Relationship to the [TEMPLATE TODO] MIB .............. 4
6.2. MIB modules required for IMPORTS .......................... 4
7. Definitions ............................................... 4
8. Security Considerations .................................... 4
9. IANA Considerations ....................................... 5
10. Contributors ............................................. 6
11. References .............................................. 6
   11.1. Normative References ................................ 6
   11.2. Informative References ............................... 7
Appendix A. Change Log ........................................ 7
Appendix B. Open Issues ....................................... 8
Authors’ Addresses ........................................... 8
1. Introduction

This memo defines a portion of the Management Information Base (MIB) used by Simple Network Management Protocol (SNMP) in GMPLS networks.

Extentions to current GMPLS to support Wavelength Switched Optical Networks (WSON) [RFC6163] include new objects with specific protocol extentions. Some information where selected as a generic constrains since they could be easily apply to other technologies than WSON. As such this [I-D.ietf-ccamp-gmpls-general-constraints-ospf-te] OSPF-TE was proposed and those information will be managed through a separated MIB [ref required].

In case of WSON some technology specific information are required and defined through [I-D.ietf-ccamp-rwa-info] and [I-D.ietf-ccamp-wson-signal-compatibility-ospf]. This MIB module will defines objects related to WSON specific informaton.

[EDITOR NOTE] Very early draft to start MIB activity on GMPSL-WSON related extentions and collect feedback from working group.

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].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580 [RFC2580].

3. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119] In the description of OIDs the convention: Set (S) Get (G) and Trap (T) conventions will describe the action allowed by the parameter.
4. Overview

This MIB module should be used in conjunction with [I-D.ietf-ccamp-gmpls-ted-mib] since it only defines additional parameters to GMPLS TED MIB.

5. Structure of the MIB Module

5.1. tedWsonNodeTable

5.1.1. tedWsonResourceBlockInformation

5.1.2. tedWsonResourcePoolAccessibility

5.1.3. tedWsonResourceBlockWavelengthConstraints

5.1.4. tedWsonResourcePoolState

5.1.5. tedWsonBlockSharedAccessWavelengthAvailability

6. Relationship to Other MIB Modules

6.1. Relationship to the [TEMPLATE TODO] MIB

6.2. MIB modules required for IMPORTS

7. Definitions

[TEMPLATE TODO]: put your valid MIB module here.
A list of tools that can help automate the process of checking MIB definitions can be found at http://www.ops.ietf.org/mib-review-tools.html

8. Security Considerations

There are a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. These are the tables and objects and their sensitivity/vulnerability:
Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to 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), even then, 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.

It is RECOMMENDED that implementers consider the security features as provided by the SNMPv3 framework (see [RFC3410], section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

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.

9. IANA Considerations

Option #1:

The MIB module in this document uses the following IANA-assigned OBJECT IDENTIFIER values recorded in the SMI Numbers registry:

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>OBJECT IDENTIFIER value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sampleMIB</td>
<td>{ mib-2 XXX }</td>
</tr>
</tbody>
</table>

Option #2:

Editor’s Note (to be removed prior to publication): the IANA is requested to assign a value for "XXX" under the ‘mib-2’ subtree and to record the assignment in the SMI Numbers registry. When the assignment has been made, the RFC Editor is asked to replace "XXX" with the assigned value.
(here and in the MIB module) with the assigned value and to remove this note.

Note well: prior to official assignment by the IANA, an internet
draft MUST use placeholders (such as "XXX" above) rather than actual
numbers. See RFC4181 Section 4.5 for an example of how this is done
in an internet draft MIB module.

Option #3:

This memo includes no request to IANA.

10. Contributors
to be added.

11. References

11.1. Normative References


[I-D.ietf-ccamp-wson-signal-compatibility-ospf]

[I-D.ietf-ccamp-gmpls-ted-mib]

11.2. Informative References


[I-D.ietf-ccamp-rwa-info]

Appendix A. Change Log

This optional section should be removed before the internet draft is submitted to the IESG for publication as an RFC.

Note to RFC Editor: please remove this appendix before publication as an RFC.
Appendix B. Open Issues

Note to RFC Editor: please remove this appendix before publication as an RFC.

Authors’ Addresses

Gabriele M. Galimberti (editor)
Cisco
Via Philips,12
20900 - Monza
Italy

Phone: +390392091462
Email: ggalimbe@cisco.com

Giovanni Martinelli (editor)
Cisco
Via Philips,12
20900 - Monza
Italy

Email: giomart@cisco.com

Dharini Hiremagalur
Juniper
1194 N Mathilda Avenue
Sunnyvale - 94089 CA
USA

Email: dharinih@juniper.net

Gert Grammel
Juniper
1194 N Mathilda Avenue
Sunnyvale - 94089 CA
USA

Email: ggrammel@juniper.net