Definitions of Managed Objects for MAP-E
draft-ietf-softwire-map-mib-05

Abstract

This memo defines a portion of the Management Information Base (MIB) for using with network management protocols in the Internet community. In particular, it defines managed objects for MAP encapsulation (MAP-E) mode.

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 19, 2016.

Copyright Notice

Copyright (c) 2015 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.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction .................................................. 2
2. The Internet-Standard Management Framework .................. 3
3. Terminology .................................................... 3
4. Structure of the MIB Module .................................. 3
   4.1. The mapMIBObjects ........................................ 3
      4.1.1. The mapRule Subtree .................................. 3
      4.1.2. The mapSecurityCheck Subtree ......................... 3
   4.2. The mapMIBConformance Subtree ............................. 4
5. Definitions .................................................... 4
6. IANA Considerations .......................................... 11
7. Security Considerations ....................................... 11
8. Acknowledgements ............................................. 11
9. References ..................................................... 11
   9.1. Normative References .................................... 12
   9.2. Informative References .................................. 12
Authors’ Addresses .............................................. 13

1. Introduction

MAP [RFC7597] is a stateless mechanism for running IPv4 over IPv6-only infrastructure. In particular, it includes two mode, translation mode or encapsulation mode. For the encapsulation mode, it provides an automatic tunnelling mechanism for providing IPv4 connectivity service to end users over a service provider’s IPv6 network

This document defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet
community. This MIB module would be used for monitoring the devices in the MAP scenario, especially, for the encapsulation mode.

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 [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 [RFC2578], [RFC2579] and [RFC2580].

3. Terminology

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 [RFC2119].

4. Structure of the MIB Module

The MAP-E MIB provides a way to configure and monitor the MAP Border Relay (BR) devices in MAP encapsulation mode through SNMP.

MAP-E MIB is configurable on a per-interface basis. It depends on several parts of the IF-MIB [RFC2863].

4.1. The mapMIBObjects

4.1.1. The mapRule Subtree

The mapRule subtree describes managed objects used for managing the multiple mapping rules in the MAP encapsulation mode.

According to the MAP specification [RFC7597], the mapping rules are divided into two categories, which are Basic Mapping Rule (BMR), and Forwarding Mapping Rule (FMR).

4.1.2. The mapSecurityCheck Subtree

The mapSecurityCheck subtree is to statistic the number of invalid packets that have been identified. There are two kind of invalid packets which are defined in the MAP specification as below.
- The BR MUST perform a validation of the consistency of the source IPv6 address and source port number for the packet using BMR.

- The CE SHOULD check that MAP received packets’ transport-layer destination port number is in the range configured by MAP for the CE.

4.2. The mapMIBConformance Subtree

The mapMIBConformance subtree provides conformance information of MIB objects.

5. Definitions

MAP-E-MIB DEFINITIONS ::= BEGIN

IMPORTS
  MODULE-IDENTITY, OBJECT-TYPE, mib-2,
  Integer32, Unsigned32, Counter64
  FROM SNMPv2-SMI
  ifIndex
  FROM IF-MIB
  InetAddressType, InetAddress,
  InetAddressPrefixLength
  FROM INET-ADDRESS-MIB
  OBJECT-GROUP, MODULE-COMPLIANCE
  FROM SNMPv2-CONF;

mapMIB MODULE-IDENTITY
LAST-UPDATED "201512180000Z"
ORGANIZATION
  "IETF Softwire Working Group"
CONTACT-INFO
  *Yu Fu
  CNNIC
  No.4 South 4th Street, Zhongguancun
  Beijing, P.R. China 100190
  EMail: fuyu@cnnic.cn

  Sheng Jiang
  Huawei Technologies Co., Ltd
  Huawei Building, 156 Beiqing Rd., Hai-Dian District
  Beijing, P.R. China 100095
  EMail: jiangsheng@huawei.com

  Bing Liu
  Huawei Technologies Co., Ltd
  Huawei Building, 156 Beiqing Rd., Hai-Dian District
  Beijing, P.R. China 100095

EMail: leo.liubing@huawei.com

Jiang Dong
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing 100084
P.R. China
Email: knight.dongjiang@gmail.com

Yuchi Chen
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing 100084
P.R. China
Email: chenycmx@gmail.com

DESCRIPTION
"The MIB module is defined for management of objects in the MAP-E BRs or CEs."

REVISION    "201512180000Z"

DESCRIPTION
"Initial version. Published as RFC xxxx."

--RFC Ed.: RFC-editor pls fill in xxxx

::=  { mapMIBObjects 1 }

mapRule OBJECT IDENTIFIER ::= { mapMIBObjects 1 }

mapSecurityCheck OBJECT IDENTIFIER ::= { mapMIBObjects 2 }

mapRuleTable OBJECT-TYPE
SYNTAX    SEQUENCE OF MapRuleEntry
MAX-ACCESS not-accessible
STATUS    current
DESCRIPTION
"The (conceptual) table containing rule information of specific mapping rule. It can also be used for row creation."
::=  { mapRule 1 }

mapRuleEntry OBJECT-TYPE
SYNTAX    MapRuleEntry
MAX-ACCESS not-accessible
STATUS    current
DESCRIPTION
"Each entry in this table contains the information on a particular mapping rule."
INDEX   { mapRuleID }
::= { mapRuleTable 1 }

MapRuleEntry ::= SEQUENCE {
  mapRuleID                   Integer32,
  mapRuleIPv6PrefixType       InetAddressType,
  mapRuleIPv6Prefix           InetAddress,
  mapRuleIPv6PrefixLen        InetAddressPrefixLength,
  mapRuleIPv4PrefixType       InetAddressType,
  mapRuleIPv4Prefix           InetAddress,
  mapRuleIPv4PrefixLen        InetAddressPrefixLength,
  mapRulePSID                 Integer32,
  mapRulePSIDLen              Integer32,
  mapRuleOffset               Unsigned32,
  mapRuleEALen                Integer32,
  mapRuleType                 Integer32
}

mapRuleID OBJECT-TYPE
SYNTAX Integer32 (1..2147483647)
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"An identifier used to distinguish the multiple mapping rule which is unique with each CE in the same BR."
::= { mapRuleEntry 1 }

mapRuleIPv6PrefixType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"In this object, it MUST be set to the value of 2 to present IPv6 type. It complies the textule convention of IPv6 address defined in [RFC4001]."
::= { mapRuleEntry 2 }

mapRuleIPv6Prefix OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The IPv6 prefix defined in mapping rule which will be assigned to CE ."
::= { mapRuleEntry 3 }

mapRuleIPv6PrefixLen OBJECT-TYPE
SYNTAX     InetAddressPrefixLength
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
 "The length of the IPv6 prefix defined in the mapping rule. As a parameter for mapping rule, it will be also assigned to CE."
::= { mapRuleEntry 4 }

mapRuleIPv4PrefixType OBJECT-TYPE
SYNTAX     InetAddressType
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
 "In this object, it MUST be set to the value of 1 to present IPv4 type. It complies the textual convention of IPv6 address defined in [RFC4001]."
::= { mapRuleEntry 5 }

mapRuleIPv4Prefix OBJECT-TYPE
SYNTAX     InetAddress
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
 "The IPv4 prefix defined in mapping rule which will be assigned to CE."
::= { mapRuleEntry 6 }

mapRuleIPv4PrefixLen OBJECT-TYPE
SYNTAX     InetAddressPrefixLength
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
 "The length of the IPv4 prefix defined in the mapping rule. As a parameter for mapping rule, it will be also assigned to CE."
::= { mapRuleEntry 7 }

mapRulePSID  OBJECT-TYPE
SYNTAX     Integer32
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
 "The PSID value algorithmically identifies a set of ports assigned to a CE."
mapRulePSIDLen OBJECT-TYPE
SYNTAX     Integer32
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
"The bit length value of the number of significant bits in
the PSID field. When it is set to 0, the PSID
field is to be ignored."
::= { mapRuleEntry 8 }

mapRuleOffset OBJECT-TYPE
SYNTAX     Unsigned32(0..15)
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
"Bit length value of the number of significant bits in
the PSID field. When it is set to 0, the PSID
field is to be ignored."
::= { mapRuleEntry 9 }

mapRuleEALen OBJECT-TYPE
SYNTAX     Integer32
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
"The length of the Embedded-Address (EA) defined in
mapping rule which will be assigned to CE."
REFERENCE
"EA: section 3 of RFC 7597."
::= { mapRuleEntry 11 }

mapRuleType OBJECT-TYPE
SYNTAX     Integer32
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
"The type of the mapping rule. A value of 0 means it
is a BMR; a non-zero value means it is a FMR."
REFERENCE
"BMR, FMR: section 5 of RFC 7597."
::= { mapRuleEntry 12 }

mapSecurityCheckTable OBJECT-TYPE
SYNTAX     SEQUENCE OF MapSecurityCheckEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"The (conceptual) table containing information on MAP security checks. This table can be used to statistic the number of invalid packets that been identified"
::= { mapSecurityCheck 1 }

mapSecurityCheckEntry OBJECT-TYPE
SYNTAX MapSecurityCheckEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"Each entry in this table contains the information on a particular MAP SecurityCheck."
INDEX { ifIndex }
::= { mapSecurityCheckTable 1 }

MapSecurityCheckEntry ::= SEQUENCE {
  mapSecurityCheckInvalidv4       Counter64,
  mapSecurityCheckInvalidv6       Counter64
}

mapSecurityCheckInvalidv4 OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION
"The CE SHOULD check that MAP received packets' transport-layer destination port number is in the range configured by MAP for the CE. So this object indicate the number of the invalid IPv4 packets received by the MAP."
::= { mapSecurityCheckEntry 1 }

mapSecurityCheckInvalidv6 OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION
"The BR MUST perform a validation of the consistency of the source IPv6 address and source port number for the packet using BMR. So this object indicate the number of the invalid IPv6 packets received by the BR."
::= { mapSecurityCheckEntry 2 }
-- Conformance Information
mapMIBConformance OBJECT IDENTIFIER ::= {mapMIB 2}
mapMIBCompliances OBJECT IDENTIFIER ::= {mapMIBConformance 1}
mapMIBGroups OBJECT IDENTIFIER ::= {mapMIBConformance 2}

-- compliance statements
mapMIBCompliance MODULE-COMPLIANCE
  STATUS current
  DESCRIPTION
    " Describes the minimal requirements for conformance to the MAP-E MIB."
  MODULE -- this module
    MANDATORY-GROUPS {mapMIBRuleGroup, mapMIBSecurityGroup}
    ::= {mapMIBCompliances 1}

-- Units of Conformance
mapMIBRuleGroup OBJECT-GROUP
  OBJECTS {
    mapRuleIPv6PrefixType,
    mapRuleIPv6Prefix,
    mapRuleIPv6PrefixLen,
    mapRuleIPv4PrefixType,
    mapRuleIPv4Prefix,
    mapRuleIPv4PrefixLen,
    mapRulePSID,
    mapRulePSIDLen,
    mapRuleOffset,
    mapRuleEALen,
    mapRuleType
  }
  STATUS current
  DESCRIPTION
    " The collection of this objects are used to give the information of mapping rules in MAP-E."
  ::= {mapMIBGroups 1}

mapMIBSecurityGroup OBJECT-GROUP
  OBJECTS {
    mapSecurityCheckInvalidv4,
    mapSecurityCheckInvalidv6
  }
  STATUS current
  DESCRIPTION
    " The collection of this objects are used to give the information on MAP security checks."
  ::= {mapMIBGroups 2}

END
6. IANA Considerations

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>MAP-E-MIB</td>
<td>{ mib-2 XXX }</td>
</tr>
</tbody>
</table>

7. Security Considerations

The MAP-E MIB module can be used for configuration of certain
objects, and anything that can be configured can be incorrectly
configured, with potentially disastrous results. Because this MIB
module reuses the IP tunnel MIB, the security considerations for
these MIBs are also applicable to the MAP-E MIB.

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.

8. Acknowledgements

The authors would like to thank for valuable comments from David
Harrington, Mark Townsley, and Shishio Tsuchiya.

This document was produced using the xml2rfc tool [RFC2629].

9. References
9.1. Normative References


9.2. Informative References


Authors’ Addresses

Yu Fu
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing 100190
P.R. China

Email: fuyu@cnnic.cn

Sheng Jiang
Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 Beijing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: jiangsheng@huawei.com

Bing Liu
Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 Beijing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: leo.liubing@huawei.com

Jiang Dong
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing 100084
P.R. China

Email: knight.dongjiang@gmail.com