Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: November 28, 2017

Y. Fu
CNNIC
S. Jiang
B. Liu
Huawei Technologies Co., Ltd
J. Dong
Y. Chen
Tsinghua University

May 27, 2017

Definitions of Managed Objects for MAP-E
draft-ietf-softwire-map-mib-09

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 November 28, 2017.

Table of Contents

1. Introduction

Mapping of Address and Port (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 manage and monitor the MAP 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 [RFC7597]as below.

- The Border Relay (BR) will perform a validation of the consistency of the source IPv6 address and source port number for the packet using Basic Mapping Rule (BMR).

- The Customer Edge (CE) will 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

The following MIB module imports definitions from [RFC2578], [RFC2579],[RFC2580],[RFC2863], and [RFC4001].

```
MAP-E-MIB DEFINITIONS  ::=  BEGIN

IMPORTS
   MODULE-IDENTITY, OBJECT-TYPE, mib-2,
   Unsigned32, Counter64
      FROM SNMPv2-SMI                --RFC2578
   TEXTUAL-CONVENTION
      FROM SNMPv2-TC                 --RFC2579
   ifIndex
      FROM IF-MIB                    --RFC2863
   InetAddressIPv6, InetAddressIPv4,
   InetAddressPrefixLength
      FROM INET-ADDRESS-MIB          --RFC4001
   OBJECT-GROUP, MODULE-COMPLIANCE
      FROM SNMPv2-CONF;              --RFC2580

mapMIB MODULE-IDENTITY
LAST-UPDATED "201705270000Z"
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    "201705270000Z"
   DESCRIPTION
     "Initial version. Published as RFC xxxx."
   --RFC Ed.: RFC-edtitor pls fill in xxxx
    ::=  {  mib-2 xxx  }
   --xxx to be replaced withIANA-assigned value

   mapMIBObjects OBJECT IDENTIFIER ::= {mapMIB 1}

   mapRule   OBJECT IDENTIFIER
      ::=  { mapMIBObjects 1 }

   mapSecurityCheck   OBJECT IDENTIFIER
      ::=  { mapMIBObjects 2 }

   -- ================================================================
   -- Textual Conventions used in this MIB module
   -- ================================================================

   RulePSID ::= TEXTUAL-CONVENTION
      DISPLAY-HINT "0x:"
      STATUS       current
      DESCRIPTION
          "It represents the PSID represented in the hexadecimal version
           so as to display it more clearly."
      SYNTAX       OCTET STRING (SIZE (4))

   RuleType ::= TEXTUAL-CONVENTION
      STATUS       current
      DESCRIPTION
         "This enumeration provides the type of the mapping rule. There
```

```
        are two types of mapping rules: Basic Mapping Rule (BMR) and
        Forwarding Mapping Rule (FMR)."
    REFERENCE   "bmr, fmr: section 5 of RFC 7597"
    SYNTAX       INTEGER {
        bmr(1),
        fmr(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                  Unsigned32,
     mapRuleIPv6Prefix          InetAddressIPv6,
     mapRuleIPv6PrefixLen       InetAddressPrefixLength,
     mapRuleIPv4Prefix          InetAddressIPv4,
     mapRuleIPv4PrefixLen       InetAddressPrefixLength,
     mapRuleBRIPv6Address       InetAddressIPv6,
     mapRulePSID                RulePSID,
     mapRulePSIDLen             Unsigned32,
     mapRuleOffset              Unsigned32,
     mapRuleEALen               Unsigned32,
     mapRuleType                RuleType
}

mapRuleID OBJECT-TYPE
    SYNTAX Unsigned32 (1..4294967295)
    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 }

  -- The object mapRuleIPv6Prefix is IPv6 specific and hence it does
  -- not use the version agnostic InetAddress.

  mapRuleIPv6Prefix OBJECT-TYPE
       SYNTAX     InetAddressIPv6
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
          "The IPv6 prefix defined in mapping rule which will be
           assigned to CE. The address type is given by
           mapRuleIPv6PrefixType."
       ::= { mapRuleEntry 2 }

   mapRuleIPv6PrefixLen OBJECT-TYPE
       SYNTAX     InetAddressPrefixLength
       MAX-ACCESS read-only
       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 3 }

  -- The object mapRuleIPv4Prefix is IPv4 specific and hence it does
  -- not use the version agnostic InetAddress.

   mapRuleIPv4Prefix OBJECT-TYPE
       SYNTAX     InetAddressIPv4
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
          " The IPv4 prefix defined in mapping rule which will be
            assigned to CE. The address type is given by
            mapRuleIPv4PrefixType."
       ::= { mapRuleEntry 4 }

   mapRuleIPv4PrefixLen OBJECT-TYPE
       SYNTAX     InetAddressPrefixLength
       MAX-ACCESS read-only
       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 5 }

  -- The object mapRuleBRIPv6Address is IPv6 specific and hence it does
  -- not use the version agnostic InetAddress.

   mapRuleBRIPv6Address OBJECT-TYPE
       SYNTAX     InetAddressIPv6
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
          "The IPv6 address of the BR which will be
           conveyed to CE."
       ::= { mapRuleEntry 6 }

    mapRulePSID  OBJECT-TYPE
       SYNTAX     RulePSID
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
          "The PSID value algorithmically identifies a set of
           ports assigned to a CE."
       REFERENCE
            "PSID: section 5.1 of RFC 7597."
       ::= { mapRuleEntry 7 }

   mapRulePSIDLen  OBJECT-TYPE
       SYNTAX     Unsigned32(0..16)
       MAX-ACCESS read-only
       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-only
       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     Unsigned32
       MAX-ACCESS read-only
```

```
      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 10 }

   mapRuleType OBJECT-TYPE
      SYNTAX     RuleType
      MAX-ACCESS read-only
      STATUS     current
      DESCRIPTION
         "It represents the type of the mapping rule. the value of
          1 means it is a bmr; the value 2 means it is a fmr."
     REFERENCE
           "bmr, fmr: section 5 of RFC 7597"
      ::= { mapRuleEntry 11 }

   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 read-only
```

```
      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 read-only
      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 {
              mapRuleIPv6Prefix,
              mapRuleIPv6PrefixLen,
              mapRuleIPv4Prefix,
              mapRuleIPv4PrefixLen,
              mapRuleBRIPv6Address,
              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:

Descriptor	OBJECT IDENTIFIER value
MAP-E-MIB	{ mib-2 XXX }

7. Security Considerations

There are no management objects defined in this MIB module that have a MAX-ACCESS clause of read-write and/or read-create. So, if this MIB module is implemented correctly, then there is no risk that an intruder can alter or create any management objects of this MIB module via direct SNMP SET operations.

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.

The following objects are vulnerable in the sense that when an intruder sees the information in this MIB module, then it might help him/her to set up an attack on the MAP node. Objects that reveal rule information of the MAP Domain: Various objects can reveal the rule information of the map domain. A curious outsider could monitor

these to assess the number of rules and the IPv6 prefix performed in this domain. Futher, an intruder could use the information to guess the address-sharing ratios of the ISPs. These are the objects and their sensitivity/ vulnerability:

- mapRuleIPv6Prefix
- mapRuleIPv6PrefixLen
- mapRuleIPv4Prefix
- mapRuleIPv4PrefixLen
- mapRuleBRIPv6Address
- mapRulePSID
- mapRulePSIDLen
- mapRuleOffset
- mapRuleEALen
- mapRuleType

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.

Implementations SHOULD provide the security features described by the SNMPv3 framework (see [RFC3410]), and implementations claiming compliance to the SNMPv3 standard MUST include 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.

8. Acknowledgements

The authors would like to thank for valuable comments from David Harrington, Mark Townsley, Shishio Tsuchiya, Yong Cui, Suresh Krishnan, Bert Wijnen and Juergen Schoenwaelder.

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

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, DOI 10.17487/RFC2578, April 1999, <http://www.rfc-editor.org/info/rfc2578>.

[RFC2579] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Textual Conventions for SMIv2", STD 58, RFC 2579, DOI 10.17487/RFC2579, April 1999, <http://www.rfc-editor.org/info/rfc2579>.

[RFC2580] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Conformance Statements for SMIv2", STD 58, RFC 2580, DOI 10.17487/RFC2580, April 1999, <http://www.rfc-editor.org/info/rfc2580>.

[RFC2863] McCloghrie, K. and F. Kastenholz, "The Interfaces Group MIB", RFC 2863, DOI 10.17487/RFC2863, June 2000, <http://www.rfc-editor.org/info/rfc2863>.

[RFC4001] Daniele, M., Haberman, B., Routhier, S., and J. Schoenwaelder, "Textual Conventions for Internet Network Addresses", RFC 4001, DOI 10.17487/RFC4001, February 2005, <http://www.rfc-editor.org/info/rfc4001>.

[RFC7597] Troan, O., Ed., Dec, W., Li, X., Bao, C., Matsushima, S., Murakami, T., and T. Taylor, Ed., "Mapping of Address and Port with Encapsulation (MAP-E)", RFC 7597, DOI 10.17487/RFC7597, July 2015, <http://www.rfc-editor.org/info/rfc7597>.

9.2. Informative References

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, DOI 10.17487/RFC2629, June 1999, <http://www.rfc-editor.org/info/rfc2629>.

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, DOI 10.17487/RFC3410, December 2002, <http://www.rfc-editor.org/info/rfc3410>.

[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, DOI 10.17487/RFC3414, December 2002, <http://www.rfc-editor.org/info/rfc3414>.

[RFC3826] Blumenthal, U., Maino, F., and K. McCloghrie, "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model", RFC 3826, DOI 10.17487/RFC3826, June 2004, <http://www.rfc-editor.org/info/rfc3826>.

[RFC5591] Harrington, D. and W. Hardaker, "Transport Security Model for the Simple Network Management Protocol (SNMP)", STD 78, RFC 5591, DOI 10.17487/RFC5591, June 2009, <http://www.rfc-editor.org/info/rfc5591>.

[RFC5592] Harrington, D., Salowey, J., and W. Hardaker, "Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)", RFC 5592, DOI 10.17487/RFC5592, June 2009, <http://www.rfc-editor.org/info/rfc5592>.

[RFC6353] Hardaker, W., "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)", STD 78, RFC 6353, DOI 10.17487/RFC6353, July 2011, <http://www.rfc-editor.org/info/rfc6353>.

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 Beiqing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: jiangsheng@huawei.com

Bing Liu
Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 Beiqing 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

Yuchi Chen
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing 100084
P.R. China

Email: flashfoxmx@gmail.com