Internet Engineering Task Force (IETF)
Request for Comments: 8389
Category: Standards Track
ISSN: 2070-1721

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

December 2018

Definitions of Managed Objects for Mapping of Address and Port with Encapsulation (MAP-E)

Abstract

This memo defines a portion of the Management Information Base (MIB) for Mapping of Address and Port with Encapsulation (MAP-E) for use with network management protocols.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8389.

Table of Contents

1. Introduction

Mapping of Address and Port with Encapsulation (MAP-E) [RFC7597] is a stateless, automatic tunneling mechanism for providing an 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 monitoring MAP-E devices.

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. 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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

4. Structure of the MIB Module

The IF-MIB [RFC2863] defines generic managed objects for managing interfaces. Each logical interface (physical or virtual) has an ifEntry. Tunnels are handled by creating a logical interface (ifEntry) for each tunnel. Each MAP-E tunnel endpoint also acts as a virtual interface that has a corresponding entry in the IF-MIB. Those corresponding entries are indexed by ifIndex. The MAP-E MIB is configurable on a per-interface basis, so it depends on several parts (ifEntry) 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 MAP-E.

According to [RFC7597], the mapping rules are divided into two categories: Basic Mapping Rule (BMR) and Forwarding Mapping Rule (FMR). According to Section 4.1 of [RFC7598], an F-flag specifies whether the rule is to be used for forwarding (FMR). If set, this rule is used as an FMR; if not set, this rule is BMR only and MUST NOT be used for forwarding. A BMR can also be used as an FMR for forwarding if the F-flag is set. So, the RuleType definition in the MAP-E MIB (see Section 5) defines bmrAndfmr to specify this scenario.

4.1.2. The mapSecurityCheck Subtree

The mapSecurityCheck subtree provides statistics for the number of invalid packets that have been identified. [RFC7597] defines two kinds of invalid packets:

- The Border Relay (BR) will validate the received packet's source IPv6 address against the configured MAP domain rule and the destination IPv6 address against the configured BR IPv6 address.

- The MAP node (Customer Edge (CE) and BR) will check that the received packet's source IPv4 address and port are in the range derived from the matching MAP rule.

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                 --RFC 2578
   TEXTUAL-CONVENTION
      FROM SNMPv2-TC                  --RFC 2579
   ifIndex
      FROM IF-MIB                     --RFC 2863
   InetAddressIPv6, InetAddressIPv4,
   InetAddressPrefixLength
      FROM INET-ADDRESS-MIB           --RFC 4001
   OBJECT-GROUP, MODULE-COMPLIANCE
      FROM SNMPv2-CONF;               --RFC 2580

mapMIB MODULE-IDENTITY
LAST-UPDATED "201811260000Z"
ORGANIZATION
   "IETF Softwire Working Group"
CONTACT-INFO
   "Yu Fu
    CNNIC
    No. 4 South 4th Street, Zhongguancun
    Beijing 100190
    China
    Email: eleven711711@foxmail.com

    Sheng Jiang
    Huawei Technologies Co., Ltd
    Q14, Huawei Campus, No. 156 Beiqing Road
    Hai-Dian District, Beijing 100095
    China
    Email: jiangsheng@huawei.com

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

```
          Hai-Dian District, Beijing 100095
          China
          Email: leo.liubing@huawei.com

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

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

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

          Copyright (c) 2018 IETF Trust and the persons identified as
          authors of the code.  All rights reserved.

          Redistribution and use in source and binary forms, with or
          without modification, is permitted pursuant to, and subject to
          the license terms contained in, the Simplified BSD License set
          forth in Section 4.c of the IETF Trust's Legal Provisions
          Relating to IETF Documents
          (https://trustee.ietf.org/license-info)."
      REVISION    "201811260000Z"
      DESCRIPTION
        "Initial version.  Published as RFC 8389."
       ::=  {  mib-2 242  }

      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
          "Indicates that the Port Set ID (PSID) is represented as
           hexadecimal for clarity."
      SYNTAX       OCTET STRING (SIZE (2))

   RuleType ::= TEXTUAL-CONVENTION
      STATUS       current
      DESCRIPTION
         "Enumerates the type of the mapping rule.  It
          defines three types of mapping rules here:
            bmr: Basic Mapping Rule (not Forwarding Mapping Rule)
            fmr: Forwarding Mapping Rule (not Basic Mapping Rule)
            bmrAndfmr: Basic and Forwarding Mapping Rule
          The Basic Mapping Rule may also be a Forwarding Mapping
          Rule for mesh mode."
      REFERENCE   "bmr, fmr: Section 5 of RFC 7597.
                   bmrAndfmr: Section 5 of RFC 7597, Section 4.1
                   of RFC 7598."
      SYNTAX       INTEGER {
          bmr(1),
          fmr(2),
          bmrAndfmr(3)
          }

   mapRuleTable OBJECT-TYPE
      SYNTAX     SEQUENCE OF MapRuleEntry
      MAX-ACCESS  not-accessible
      STATUS     current
      DESCRIPTION
         "The (conceptual) table containing rule information for
          a 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   {  ifIndex,
                     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
        "A unique identifier used to distinguish mapping
         rules."
     ::= { mapRuleEntry 1 }

-- The object mapRuleIPv6Prefix is IPv6 specific; 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 the mapping rule that will be
         assigned to CEs."
     ::= { 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
         that will be assigned to CEs."
     ::= { mapRuleEntry 3 }

-- The object mapRuleIPv4Prefix is IPv4 specific; 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 the mapping rule that will be
            assigned to CEs."
        ::= { 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 that will be assigned to CEs."
        ::= { mapRuleEntry 5 }

   -- The object mapRuleBRIPv6Address is IPv6 specific; 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 that will be conveyed to CEs.
            If the BR IPv6 address is anycast, the relay must use
            this anycast IPv6 address as the source address in
            packets relayed to CEs."
        ::= { 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
             "The number of the mapRuleOffset is 6 by default to
              exclude the system ports (0-1023).  It is provided via
              the Rule Port Mapping Parameters in the Basic Mapping
              Rule."
          DEFVAL {6}
          ::= { mapRuleEntry 9 }

       mapRuleEALen OBJECT-TYPE
          SYNTAX     Unsigned32(0..48)
          MAX-ACCESS read-only
          STATUS     current
          DESCRIPTION
             "The length of the Embedded Address (EA) defined in
              mapping rule that will be assigned to CEs."
         REFERENCE
               "EA: Section 3 of RFC 7597."
          ::= { mapRuleEntry 10 }

      mapRuleType OBJECT-TYPE
          SYNTAX     RuleType
          MAX-ACCESS read-only
          STATUS     current
          DESCRIPTION
             "Indicates the type of mapping rule.
              '1' represents a BMR.
              '2' represents an FMR.
              '3' represents a BMR that is also an FMR for mesh mode."
           REFERENCE
               "bmr, fmr: Section 5 of RFC 7597.
                bmrAndfmr: Section 5 of RFC 7597, Section 4.1 of
                RFC 7598."
          ::= { 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 for
          statistics on the number of invalid packets that
          have been identified."
      ::=  { mapSecurityCheck 1 }

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

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

   mapSecurityCheckInvalidv4 OBJECT-TYPE
       SYNTAX     Counter64
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
          "Indicates the number of received IPv4 packets
           that do not have a payload source IPv4 address or
           port within the range defined in the matching MAP
           rule.  It corresponds to the second kind of
           invalid packet described in Section 4.1.2."
       ::= { mapSecurityCheckEntry 1 }

   mapSecurityCheckInvalidv6 OBJECT-TYPE
       SYNTAX     Counter64
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
          "Indicates the number of received IPv6 packets that
           do not have a source or destination IPv6 address
           matching a Basic Mapping Rule.  It corresponds
           to the first kind of invalid packet described
           in Section 4.1.2."
       ::= { 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 group of objects used to describe the MAP-E mapping
          rule."
      ::= { mapMIBGroups 1 }

  mapMIBSecurityGroup OBJECT-GROUP
     OBJECTS {
        mapSecurityCheckInvalidv4,
        mapSecurityCheckInvalidv6 }
    STATUS current
    DESCRIPTION
       "The group of objects used to provide information on the
        MAP-E 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-2 242 }

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 objects in this MIB module may be considered sensitive or vulnerable in some network environments. This includes INDEX objects with a MAX-ACCESS of not-accessible, and any indices from other modules exposed via AUGMENTS. 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. These are the tables and objects and their sensitivity/vulnerability:

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

Some of the MIB model's objects are vulnerable because the information that they hold may be used for targeting an attack against a MAP node (CE or BR). For example, an intruder could use the information to help deduce the customer IPv4 and IPv6 topologies and address-sharing ratios in use by the ISP.

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 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. References

8.1. 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, <https://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, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc2580>.

[RFC2863] McCloghrie, K. and F. Kastenholz, "The Interfaces Group MIB", RFC 2863, DOI 10.17487/RFC2863, June 2000, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc7597>.

[RFC7598] Mrugalski, T., Troan, O., Farrer, I., Perreault, S., Dec, W., Bao, C., Yeh, L., and X. Deng, "DHCPv6 Options for Configuration of Softwire Address and Port-Mapped Clients", RFC 7598, DOI 10.17487/RFC7598, July 2015, <https://www.rfc-editor.org/info/rfc7598>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

8.2. Informative References

[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, <https://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, <https://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, <https://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, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc6353>.

Acknowledgements

The authors would like to thank the following individuals for their valuable comments: David Harrington, Mark Townsley, Shishio Tsuchiya, Yong Cui, Suresh Krishnan, Bert Wijnen, Ian Farrer, and Juergen Schoenwaelder.

Authors' Addresses

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

Email: eleven711711@foxmail.com

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

Email: jiangsheng@huawei.com

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

Email: leo.liubing@huawei.com

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

Email: knight.dongjiang@gmail.com

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

Email: flashfoxmx@gmail.com