The Definitions of Managed Objects for Mobile IP UDP Tunneling
draft-sjostrand-mip4-udptunnel-mib-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

This document may not be modified, and derivative works of it may not be created, other than to extract section "Mobile IP UDP Tunnel MIP definitions" as-is for separate use.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on July 12, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).
Abstract

This memo defines the Management Information Base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it describes managed objects used for managing the Mobile Node, Foreign Agent and Home Agent when Mobile IP Traversal of Network Address Translation (NAT) Devices are used.

Conventions used in this document

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 RFC2119 [RFC2119].

Table of Contents

1. Introduction..........................................................................................3
2. The Internet-Standard Management Framework..................................3
3. Structure of the MIB...........................................................................3
   3.1. Structure of the Mobile IP UDP Tunneling......................................3
   3.2. MIB Groups.................................................................................4
4. Mobile IP UDP Tunnel MIB Definitions...........................................5
5. Security Considerations.................................................................10
6. IANA Considerations..........................................................................11
APPENDIX A: Todo and open issues......................................................12
   A.1. OID placement.............................................................................12
   A.2. Default values............................................................................12
7. References...........................................................................................12
   7.1. Normative References...................................................................12
   7.2. Informative References...............................................................13
Author’s Address......................................................................................13
Intellectual Property Statement..............................................................13
1. Introduction

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects used for managing the Mobile Node, Foreign Agent and Home Agent when Mobile IP Traversal of Network Address Translation (NAT) Devices are used.

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 RFC2119 [RFC2119].

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. Structure of the MIB

This memo defines a portion of the Management Information Base (MIB) for the use with network management protocols in the Internet community. In particular, it describes managed objects for the Mobile IP Traversal of Network Address Translation (NAT) Devices as defined in [RFC3519].

3.1. Structure of the Mobile IP UDP Tunneling

The Mobile IP Traversal of Network Address Translation (NAT) Devices specification [RFC3519] specifies a few managed entities. These are the behaviour to force and accept udp tunneling, and the configuration of the keep alive timers.

The Mobile IP Traversal of Network Address Translation (NAT) Devices specification [RFC3519] also specifies a new error code for
"Requested UDP tunnel encapsulation unavailable". Therefore a counter object for this error code is also included in this mib module.

Further, it’s good practice to include object to enable and disable the MIP UDP tuning completely.

Configuration of MIP UDP tunneling has been deployed in various vendor implementations for years. Field experience have shown that it’s indeed a good idea to always use UDP tunneling instead if the original Mobile IP tunneling methods. Therefore, an object is added in the HA to always force the use of UDP tunneling to all UDP tunneling capable nodes, regardless of F-flag or outcome of NAT test.

3.2. MIB Groups

Objects in this MIB are arranged into groups. Each group is related to the Mobile IP entities Mobile Node, Foreign Agent and Home Agent. The Mobile IP entities Mobile Node, Foreign Agent and Home Agent are described in [RFC3344].
4. Mobile IP UDP Tunnel MIB Definitions

MIP-UDPTUNNEL-MIB DEFINITIONS ::= BEGIN

IMPORTS
   Counter32, Unsigned32, MODULE-IDENTITY,
   OBJECT-TYPE
   FROM SNMPv2-SMI -- [RFC2578]
   TruthValue
   FROM SNMPv2-TC -- [RFC2579]
   MODULE-COMPLIANCE, OBJECT-GROUP
   FROM SNMPv2-CONF -- [RFC2580]
   mipMIB
   FROM MIP-MIB; -- [2006bis]

mipUdpTunnelMIB    MODULE-IDENTITY
   LAST-UPDATED    "200702120000Z"
   ORGANIZATION    "IETF Mobile IP Working Group"
   CONTACT-INFO
   " Hans Sjostrand
   ipUnplugged
   hans@ipunplugged.com"
   DESCRIPTION
   "The MIB module for configuring and displaying Mobile
   IP Traversal of Network Address Translation (NAT)
   Devices information.

   Copyright (C) IETF Trust (2007). This version
   of this MIB module is part of RFC yyyy; see the RFC
   itself for full legal notices."
   REVISION      "200702120000Z"
   DESCRIPTION
   "First version."
 ::= { mipMIB 4 }

mipUdpTunnelMIBObjects   OBJECT IDENTIFIER ::= { mipUdpTunnelMIB 1 }

mnUdpTunnel OBJECT IDENTIFIER ::= { mipUdpTunnelMIBObjects 1 }
haUdpTunnel OBJECT IDENTIFIER ::= { mipUdpTunnelMIBObjects 2 }
faUdpTunnel OBJECT IDENTIFIER ::= { mipUdpTunnelMIBObjects 3 }

-- =================================================================
-- mnUdpTunnel Group

mnUdpTunnelEnable OBJECT-TYPE
SYNTAX      TruthValue
MAX-ACCESS  read-write
STATUS     current
DESCRIPTION
 "This parameter enables and disables the RFC 3519 UDP
tunneling function in the MN completely."
DEFVAL      { true }
 ::= { mnUdpTunnel 1 }

mnUdpTunnelForce OBJECT-TYPE
SYNTAX      TruthValue
MAX-ACCESS  read-write
STATUS     current
DESCRIPTION
 "This parameter enables (or disables) the MN to set
the F (force) flag. It indicates that the mobile
node wants to use traversal regardless of the
outcome of NAT detection performed by the home agent."
DEFVAL      { false }
 ::= { mnUdpTunnel 2 }

mnUdpTunnelKeepaliveInterval OBJECT-TYPE
SYNTAX      Unsigned32
UNITS       "seconds"
MAX-ACCESS  read-write
STATUS     current
DESCRIPTION
 "Defines the default NAT keepalive interval that the
mobile node will use in the case that the HA does
not impose another value by setting the Keepalive
Interval in the UDP Tunnel Reply Extension."
DEFVAL      { 110 }
 ::= { mnUdpTunnel 3 }

-- ===================================================
-- haUdpTunnel Group

haUdpTunnelEnable OBJECT-TYPE
SYNTAX      TruthValue
MAX-ACCESS  read-write
STATUS     current
DESCRIPTION
 "This parameter enables and disables the RFC 3519 UDP
tunneling function in the HA completely."
DEFVAL      { true }
 ::= { haUdpTunnel 1 }
haUdpTunnelPermitMnForce OBJECT-TYPE
SYNTAX       TruthValue
MAX-ACCESS   read-write
STATUS       current
DESCRIPTION
"This parameter enables (or disables) permission for
the Mobile Node to force UDP tunneling. NAT
traversal according to RFC3519 permits the MN (or
FA) to set a flag in the UDP tunneling request
extension which indicates that it wants tunneling
to be done even if the HA does not detect a NAT
between the MN (or FA) and itself. This parameter
controls whether the HA will honor this request or
not."
DEFVAL       { true }
::= { haUdpTunnel 2 }

haUdpTunnelKeepaliveInterval OBJECT-TYPE
SYNTAX       Unsigned32
UNITS        "seconds"
MAX-ACCESS   read-write
STATUS       current
DESCRIPTION
"This parameter sets the keepalive interval override.
Normally, the MN uses the keepalive time that was
configured using UDP tunneling and sending
keepalive messages. The HA can override this
configured keepalive time by setting a new
interval value for this parameter to a value other
than zero."
DEFVAL       { 0 }
::= { haUdpTunnel 3 }

haUdpTunnelForce OBJECT-TYPE
SYNTAX       TruthValue
MAX-ACCESS   read-write
STATUS       current
DESCRIPTION
"This parameter enables and disables the HA forcing all
connections from MNs which support RFC 3519 UDP
tunneling to use tunneling whether or not the
presence of a NAT is detected."
DEFVAL       { false }
::= { haUdpTunnel 4 }

haUdpTunnelEncapUnavail OBJECT-TYPE
SYNTAX       Counter32
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION  "Total number of Registration Requests denied by the 
home agent -- Requested UDP tunnel encapsulation 
unavailable (code 142)."
 ::= { haUdpTunnel 5 }

-- =================================================================
-- faUdpTunnel Group

faUdpTunnelEnable OBJECT-TYPE
SYNTAX      TruthValue
MAX-ACCESS  read-write
STATUS      current
DESCRIPTION  "This parameter enables and disables the 
RFC 3519 UDP tunneling function in the FA completely."
DEFVAL      { true }
 ::= { faUdpTunnel 1 }

faUdpTunnelForce OBJECT-TYPE
SYNTAX      TruthValue
MAX-ACCESS  read-write
STATUS      current
DESCRIPTION  "This parameter enables (or disables) the FA to set 
the F (force) flag. It indicates that the foreign 
agent wants to use traversal regardless of the 
outcome of NAT detection performed by the home agent."
DEFVAL      { false }
 ::= { faUdpTunnel 2 }

faUdpTunnelKeepaliveInterval OBJECT-TYPE
SYNTAX      Unsigned32
UNITS       "seconds"
MAX-ACCESS  read-write
STATUS      current
DESCRIPTION  "Defines the default NAT keepalive interval that the 
foreign agent will use in the case that the HA does 
not impose another value by setting the Keepalive 
Interval in the UDP Tunnel Reply Extension."
DEFVAL      { 110 }
 ::= { faUdpTunnel 3 }

-- =================================================================
-- MIP Conformance Statements

mipUdpTunnelConformance
   OBJECT IDENTIFIER ::= { mipUdpTunnelMIB 2 }

mipUdpTunnelGroups
   OBJECT IDENTIFIER ::= { mipUdpTunnelConformance 1 }
mipUdpTunnelCompliances
   OBJECT IDENTIFIER ::= { mipUdpTunnelConformance 2 }

--
-- compliance statements
--

mipUdpTunnelCompliance    MODULE-COMPLIANCE
   STATUS    current
   DESCRIPTION
      "The compliance statement for SNMPv2 entities which
       implement the Mobile IP UDP Tunnel MIB."
   MODULE
       GROUP     mnUdpTunnelGroup
      DESCRIPTION
         "This group is mandatory for a mobile node."
       GROUP     haUdpTunnelGroup
      DESCRIPTION
         "This group is mandatory for a home agent."
       GROUP     faUdpTunnelGroup
      DESCRIPTION
         "This group is mandatory for a foreign agent."

   ::= { mipUdpTunnelCompliances 1 }

--
-- Units of conformance
--

mnUdpTunnelGroup    OBJECT-GROUP
   OBJECTS   { mnUdpTunnelEnable, mnUdpTunnelForce, mnUdpTunnelKeepaliveInterval }
   STATUS      current
   DESCRIPTION
      "A collection of objects providing management
5. Security Considerations

Assuming that secure network management (such as SNMP v3) is implemented, the objects represented in this MIB do not pose a threat to the security of the network.

There are a number of management objects defined in this MIB that have a MAX-ACCESS clause of read-write. 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.

Not all versions of SNMP provide features for such a secure environment. SNMPv1 by itself is not a secure environment. 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.
It is recommended that the implementers consider the security features as provided by the SNMPv3 framework. Specifically, the use of the User-based Security Model RFC 2574 [RFC2574] and the View-based Access Control Model RFC 2575 [RFC2575] is recommended.

It is then a customer/user responsibility to ensure that the SNMP entity giving access to an instance of this MIB, 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

This section is to be done. It’s still unclear whether there should be a new OID assigned from mib-2 space, or an OID under the mipMIB OID should be used.
APPENDIX A: Todo and open issues

A.1. OID placement

Since this is the first mib extending the Mobile IP mib it’s a bit unclear how this mib should be placed in the OID structure. Most probably there will be an OID assigned under mipMIB after IANA has taken control over that OID space. Alternatively there could be a new OID assigned by IANA under mib-2. For the sake of simplicity the first approach is used in this version of the mib.

A.2. Default values

In this first version of the mib default values have been defined for all objects. This is good practice, however it’s still an open issue which values these default values should have. Except in the case with keepalive timers, these values are not mandated from RFC3519, but are just some assumption of a useful configuration of the Mobile IP UDP tunnelling function.

However, it differs from the default values used in both the proprietary Cisco and ipUnplugged implementations so it would be useful with some input on the applicability.

7. References

7.1. Normative References


[2006bis] The Definitions of Managed Objects for IP Mobility Support using SMIv2, revised, Work in progress

7.2. Informative References


Author’s Address

Hans Sjostrand
ipUnplugged
Arenavagen 21
121 29 Stockholm
Sweden
Phone: +46 8 725 5900
Email: hans@ipunplugged.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an
attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgment

Funding for the RFC Editor function is currently provided by the IETF Administrative Support Activity (IASA).