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 defines objects for managing SAVI (Source Address Validation Improvements) protocol instance.

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 https://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 July 19, 2018.

Copyright Notice

Copyright (c) 2018 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 (https://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
1. Introduction

The Source Address Validation Improvement protocol was developed to complement ingress filtering with finer-grained, standardized IP source address validation (refer to [RFC7039]). A SAVI protocol instance is located on the path of hosts’ packets, enforcing the hosts’ use of legitimate IP source addresses.

SAVI protocol determines whether the IP address obtaining process is legitimate according to IP address assignment method. For links with Stateless Address Auto Configuration (SLAAC), Dynamic Host Configuration Protocol (DHCP), and Secure Neighbor Discovery (SEND), the process is defined in separate documents of SAVI Working Group (refer to [RFC6620], [RFC7513], [RFC7219].)
This document defines a MIB module that can be used to manage the SAVI protocol instance. It covers both configuration and status monitoring aspects of SAVI implementations.

This document uses terminology from the SAVI Protocol specification.

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].

4. Overview

The SAVI Protocol MIB module (SAVI-MIB) is conformant to SAVI protocol, and is designed to:

- Support centralized management and monitoring of SAVI protocol instance by standard SNMP protocol.
- Support configuration and querying of SAVI protocol parameters.
- Support configuration and querying of binding entries. Operators may insert and delete manual binding entries.
- Support querying of filtering entries.
- Support querying of the count of packets dropped because of validation failure for each interface.

Based on SAVI protocol, attributes and objects of a SAVI protocol instance can be classified into five categories:
o System attributes. These attributes are corresponding to a SAVI protocol instance, such as IP Address Assignment Methods and some constants.

o Anchor attributes. These attributes are corresponding to a SAVI anchor. Anchor is defined in [RFC7039].

o Binding Status Table. This table contains the state of binding between source address and binding anchor (refer to [RFC6620], [RFC7513], [RFC7219]).

o Filtering Table. This table contains the bindings between binding anchor and address, which is used to filter packets (refer to [RFC6620], [RFC7513], [RFC7219]).

o Counting Table. This table contains the count of fail packets for each interface.

A table is designed for each category of objects.

5. Structure of the MIB Module

This section presents the structure of the SAVI-MIB module. The MIB objects are derived from the SAVI protocol specification.

This MIB is composed of a series of tables meant to form the base for managing SAVI entities. The following subsections describe all tables in the SAVI MIB module.

5.1. The SAVI System Table

The SAVI System Table (saviObjectsSystemTable) contains the objects which are corresponding to SAVI system-wide parameters. It supports the configuration and collection of SAVI system-wide parameters.

There is an entry for each IP stack, IPv4 and IPv6. The table is indexed by:

o saviObjectsSystemIPVersion - The IP Version. A textual convention InetVersion defined in RFC4001 is used to represent the different version of IP protocol.

It contains the following objects:

o saviObjectsSystemSlaacEnable - If SAVI for SlAAC is enabled.

o saviObjectsSystemDhcpEnable - If SAVI for DHCP is enabled.
o  saviObjectsSystemSendEnable - If SAVI for SEND is enabled.

o  saviObjectsSystemManualEnable - If SAVI for MANUAL is enabled.

The MAX-ACCESS of these objects is READ-WRITE. Network Operators may do configuration by setting these objects.

5.2. The SAVI Preference Table

The SAVI System Table (saviObjectsPreferenceTable) contains savi preference parameters.

There is an entry for each IP stack, IPv4 and IPv6. The table is indexed by:

o  saviObjectsSystemIPVersion - The IP Version. A textual convention InetVersion defined in RFC4001 is used to represent the different version of IP protocol.

It contains the following objects:

o  saviObjectsPreferenceSlaac - The preference of SAVI-SlAAC.

o  saviObjectsPreferenceDhcp - The preference of SAVI-DHCP.

o  saviObjectsPreferenceSend - The preference of SAVI-SEND.

o  saviObjectsPreferenceManual - The preference of SAVI-MANUAL.

The MAX-ACCESS of these objects is READ-WRITE. Network Operators may do configuration by setting these objects.

5.3. The SAVI Port Table

The SAVI Port Table (saviObjectsPortTable) contains the objects which are corresponding to SAVI running parameters of each anchor. It supports the configuration and collection of SAVI parameters of each anchor.

There is an entry for each IP stack, IPv4 and IPv6. The table is indexed by:

o  saviObjectsPortIPVersion - The IP Version.

o  saviObjectsPortIfIndex - The index value that uniquely identifies the interface to which this entry is applicable.

It contains the following objects:
saviObjectsPortValidatingAttr - An attribute defined in SAVI protocol (refer to [RFC7513]).

saviObjectsPortDhcpTrustAttr - An attribute defined in SAVI protocol (refer to [RFC7513]).

saviObjectsPortTrustAttr - An attribute defined in SAVI protocol (refer to [RFC7513]).

saviObjectsPortDhcpSnoopingAttr - An attribute defined in SAVI protocol (refer to [RFC7513]).

saviObjectsPortDataSnoopingAttr - An attribute defined in SAVI protocol (refer to [RFC7513]).

saviObjectsPortFilteringNum - The max filtering number of the Port.

The MAX-ACCESS of these objects is READ-WRITE. Network Operators may configure by setting these objects.

5.4. The SAVI Binding Table

The SAVI Binding Table (saviObjectsBindingTable) contains the objects which are corresponding to Binding State Table (BST) defined in SAVI protocol. It contains the binding parameters and state of each binding entry. It supports the collection of binding entries. And an entry can be inserted or deleted if it is a manual binding entry.

The table is indexed by:

- saviObjectsBindingIpAddressType - IP address type. A textual convention InetAddressType defined in RFC4001 is used to represent the different kind of IP address.

- saviObjectsBindingMethod - which IP address assignment method is used to create the binding entry - manual(1), slaac(2), dhcp(3), send(4).

- saviObjectsBindingIfIndex - The index value that uniquely identifies the interface to which this entry is applicable.

- saviObjectsBindingIpAddress - The binding source IP address. A textual convention InetAddress defined in RFC4001 is used to define this object.

The SAVI Binding Table contains the following objects:
5.5. The SAVI Filtering Table

The SAVI Filtering Table (saviObjectsFilteringTable) contains the objects which are corresponding to Filtering Table (FT) defined in SAVI protocol. It supports the collection of filtering entries.

The table is indexed by:

- saviObjectsFilteringIpAddressType - IP address type.
- saviObjectsFilteringIfIndex - The index value that uniquely identifies the interface to which this entry is applicable.

It contains the following objects:

- saviObjectsFilteringIpAddress - The source IP address.

The MAX-ACCESS of the object is READ-ONLY.

5.6. The SAVI Counting Table

The SAVI Counting Table (saviObjectsCountTable) contains the objects counting packets dropped because of validation failure for each interface.

The table is indexed by:

- saviObjectsCountIPVersion - IP Version.
o `saviObjectsCountIfIndex` - The index value that uniquely identifies the interface to which this entry is applicable.

It contains the following objects:

o `saviObjectsCountFilterPkts` - The count of packets dropped because of validation failure.

o `saviObjectsCountFilterOctets` - The count of octets dropped because of validation failure.

The MAX-ACCESS of the object is READ-ONLY.

6. Textual Conventions

The textual conventions used in the SAVI-MIB are as follows.

The `MODULE-COMPLIANCE`, `OBJECT-GROUP` textual convention is imported from SNMPv2-CONF [RFC2580]. The `MODULE-IDENTITY`, `OBJECT-IDENTITY`, `OBJECT-TYPE`, `Unsigned32` textual convention is imported from SNMPv2-SMI [RFC2578].

The `MacAddress`, `TimeInterval`, `RowStatus` textual convention is imported from SNMPv2-TC [RFC2579].

The `InetVersion`, `InetAddressType`, `InetAddress` textual convention is imported from INET-ADDRESS-MIB [RFC4001].

The `InterfaceIndex` textual convention is imported from IF-MIB [RFC2863].

The `ip` textual convention is imported from IP-MIB [RFC4293].

7. Relationship to Other MIB Modules

7.1. Relationship to the INET-ADDRESS-MIB

To support extensibility, IETF defined new textual conventions to represent different IP protocol and different IP address in a unified formation in RFC4001. To support different IP version, a textual convention `InetVersion` is defined to represent the different version of IP protocol. To support different IP address, a generic Internet address is defined. It consists of two objects: The first one has the syntax `InetAddressType`, and the second object have the syntax `InetAddress`. The value of the first object determines how the value of the second is encoded.
Since SAVI running mode and parameter is independent of IPv4 and IPv6, so different OID instances should be defined for each protocol. In SAVI-MIB definition, when IP address is used as a part of binding table, it is defined using textual conventions described in INET-ADDRESS-MIB.

7.2. Relationship to the IF-MIB

The Interfaces MIB [RFC2863] defines generic managed objects for managing interfaces. This document contains the interface-specific extensions for managing SAVI anchors that are modeled as interfaces.

The IF-MIB module is required to be supported on the SAVI device. The interface MUST be modeled as an ifEntry, and ifEntry objects such as ifIndex are to be used as per [RFC2863].

An ifIndex [RFC2863] is used as a common index for interfaces in the SAVI-MIB modules.

7.3. MIB modules required for IMPORTS

The SAVI MIB module IMPORTS objects from SNMPv2-SMI [RFC2578], SNMPv2-TC [RFC2579], SNMPv2-CONF [RFC2580], IF-MIB [RFC2863] and INET-ADDRESS-MIB [RFC4001].

8. Definitions

SAVI-MIB DEFINITIONS ::= BEGIN

IMPORTS

MODULE-COMPLIANCE, OBJECT-GROUP
 FROM SNMPv2-CONF --RFC2580
MODULE-IDENTITY, OBJECT-IDENTITY, OBJECT-TYPE, Unsigned32
 FROM SNMPv2-SMI --RFC2578
TEXTUAL-CONVENTION, MacAddress, TimeInterval, RowStatus
 FROM SNMPv2-TC --RFC2579
InterfaceIndex
 FROM IF-MIB --RFC2863
InetAddressType, InetAddress
 FROM IF-MIB --RFC4001

ip
 FROM IP-MIB --RFC4293

saviMIB MODULE-IDENTITY
 LAST-UPDATED "201710170000Z"
 ORGANIZATION
 "IETF SAVI Working Group"
CONTACT-INFO

"WG charter:
http://datatracker.ietf.org/wg/savi/charter/

Editor:
Changqing An
CERNET
Postal:  Institute for Network Sciences and Cyberspace, Tsinghua University
       Beijing 100084
       China
       Email: acq@tsinghua.edu.cn
"

DESCRIPTION
"This MIB Module is designed to support configuration
and monitoring of SAVI protocol.
"

REVISION    "201710170000Z"
DESCRIPTION
"Initial version"
 ::= {ip xxx}

saviObjects OBJECT IDENTIFIER ::= { saviMIB 1 }

-- System parameters for SAVI protocol

saviObjectsSystemTable OBJECT-TYPE
SYNTAX     SEQUENCE OF SaviObjectsSystemEntry
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION
"The table containing savi system-wide parameters."
 ::= { saviObjects 1 }

saviObjectsSystemEntry OBJECT-TYPE
SYNTAX     SaviObjectsSystemEntry
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION
"An entry containing savi system-wide parameters for a
particular IP version."

INDEX { saviObjectsSystemIPVersion }
 ::= { saviObjectsSystemTable 1 }

SaviObjectsSystemEntry ::= 
SEQUENCE {
          saviObjectsSystemIPVersion InetVersion,
saviObjectsSystemSlaacEnable OBJECT-TYPE
SYNTAX INTEGER {
    enable(1),
    disable(2)
}
MAX-ACCESS read-write
STATUS current
DESCRIPTION "If SAVI for SlAAC is enabled."
::= { saviObjectsSystemEntry 2 }

saviObjectsSystemDhcpEnable OBJECT-TYPE
SYNTAX INTEGER {
    enable(1),
    disable(2)
}
MAX-ACCESS read-write
STATUS current
DESCRIPTION "If SAVI for DHCP is enabled."
::= { saviObjectsSystemEntry 3 }

saviObjectsSystemSendEnable OBJECT-TYPE
SYNTAX INTEGER {
    enable(1),
    disable(2)
}
MAX-ACCESS read-write
STATUS current
DESCRIPTION "If SAVI for SEND is enabled."
::= { saviObjectsSystemEntry 4 }
saviObjectsSystemManualEnable OBJECT-TYPE
SYNTAX    INTEGER {
    enable(1),
    disable(2)
}
MAX-ACCESS read-write
STATUS    current
DESCRIPTION
    "If SAVI for MANUAL is enabled."
::= { saviObjectsSystemEntry 5 }

-- Preference parameters for SAVI protocol

saviObjectsPreferenceTable OBJECT-TYPE
SYNTAX    SEQUENCE OF SaviObjectsPreferenceEntry
MAX-ACCESS not-accessible
STATUS    current
DESCRIPTION
    "The table containing savi preference parameters."
::= { saviObjects 2 }

saviObjectsPreferenceEntry OBJECT-TYPE
SYNTAX    SaviObjectsPreferenceEntry
MAX-ACCESS not-accessible
STATUS    current
DESCRIPTION
    "An entry containing savi system-wide parameters for a particular IP version."
INDEX { saviObjectsPreferenceIPVersion }::= { saviObjectsPreferenceTable 1 }

SaviObjectsPreferenceEntry ::= SEQUENCE {
    saviObjectsPreferenceIPVersion        InetVersion,
    saviObjectsPreferenceSlAAC            INTEGER,
    saviObjectsPreferenceDHCP             INTEGER,
    saviObjectsPreferenceSend             INTEGER,
    saviObjectsPreferenceManual           INTEGER
}

saviObjectsPreferenceIPVersion OBJECT-TYPE
SYNTAX    InetVersion
MAX-ACCESS not-accessible
STATUS    current
DESCRIPTION
"The IP version "
::= { saviObjectsPreferenceEntry 1 }

saviObjectsPreferenceSlaac OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-write
STATUS current
DESCRIPTION "Preference of SAVI-SLAAC."
::= { saviObjectsPreferenceEntry 2 }

saviObjectsPreferenceDhcp OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-write
STATUS current
DESCRIPTION "Preference of SAVI-DHCP."
::= { saviObjectsPreferenceEntry 3 }

saviObjectsPreferenceSend OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-write
STATUS current
DESCRIPTION "Preference of SAVI-SEND."
::= { saviObjectsPreferenceEntry 4 }

saviObjectsPreferenceManual OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-write
STATUS current
DESCRIPTION "Preference of SAVI-MANUAL."
::= { saviObjectsPreferenceEntry 5 }

-- Port parameters for SAVI protocol

saviObjectsPortTable OBJECT-TYPE
SYNTAX SEQUENCE OF SaviObjectsPortEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "The table containing SAVI parameters of each anchor."
saviObjectsPortEntry OBJECT-TYPE
SYNTAX   SaviObjectsPortEntry
MAX-ACCESS not-accessible
STATUS   current
DESCRIPTION
"An entry containing SAVI running parameters of an anchor."
INDEX {
   saviObjectsPortIPVersion,
   saviObjectsPortIfIndex
}
::= { saviObjectsPortTable 1 }

SaviObjectsPortEntry ::= SEQUENCE {
   saviObjectsPortIPVersion          InetVersion,
   saviObjectsPortIfIndex            InterfaceIndex,
   saviObjectsPortValidatingAttr     INTEGER,
   saviObjectsPortDhcpTrustAttr      INTEGER,
   saviObjectsPortTrustAttr          INTEGER,
   saviObjectsPortDhcpSnoopingAttr   INTEGER,
   saviObjectsPortDataSnoopingAttr   INTEGER,
   saviObjectsPortFilteringNum       Unsigned32
}

saviObjectsPortIPVersion  OBJECT-TYPE
SYNTAX     InetVersion
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION
"The IP version "
 ::= { saviObjectsPortEntry 1 }

saviObjectsPortIfIndex      OBJECT-TYPE
SYNTAX     InterfaceIndex
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION
"The index value that uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of the IF-MIB’s ifIndex."
 ::= { saviObjectsPortEntry 2 }
saviObjectsPortValidatingAttr OBJECT-TYPE
SYNTAX INTEGER {
   enable(1),
   disable(2)
 }
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"An attribute defined in SAVI protocol. enable(1), the attribute is set.
disable(2), the attribute is not set."
::= { saviObjectsPortEntry 3 }

saviObjectsPortDhcpTrustAttr OBJECT-TYPE
SYNTAX INTEGER {
   enable(1),
   disable(2)
 }
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"An attribute defined in SAVI protocol. enable(1), the attribute is set.
disable(2), the attribute is not set."
::= { saviObjectsPortEntry 4 }

saviObjectsPortTrustAttr OBJECT-TYPE
SYNTAX INTEGER {
   enable(1),
   disable(2)
 }
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"An attribute defined in SAVI protocol. enable(1), the attribute is set.
disable(2), the attribute is not set."
::= { saviObjectsPortEntry 5 }

saviObjectsPortDhcpSnoopingAttr OBJECT-TYPE
SYNTAX INTEGER {
   enable(1),
   disable(2)
 }
MAX-ACCESS read-write
saviObjectsPortDataSnoopingAttr OBJECT-TYPE
SYNTAX     INTEGER  {
   enable(1),
   disable(2)
}
MAX-ACCESS read-write
STATUS     current
DESCRIPTION
   "An attribute defined in SAVI protocol.
   enable(1), the attribute is set.
   disable(2), the attribute is not set."
 ::= { saviObjectsPortEntry 6 }

saviObjectsPortFilteringNum OBJECT-TYPE
SYNTAX     Unsigned32
MAX-ACCESS read-write
STATUS     current
DESCRIPTION
   "The max filtering number of the Port."
 ::= { saviObjectsPortEntry 7 }

-- Binding Status Table for SAVI protocol

saviObjectsBindingTable OBJECT-TYPE
SYNTAX     SEQUENCE OF SaviObjectsBindingEntry
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION
   "The table containing the state of binding
    between source address and anchor."
 ::= { saviObjects 4 }

saviObjectsBindingEntry OBJECT-TYPE
SYNTAX     SaviObjectsBindingEntry
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION
"An entry containing the state of binding between source address and anchor. Entries are keyed on the source IP address type, binding type, anchor, and source IP address.

INDEX {
  saviObjectsBindingIpAddressType,
  saviObjectsBindingMethod,
  saviObjectsBindingIfIndex,
  saviObjectsBindingIpAddress
}
::= { saviObjectsBindingTable 1 }

SaviObjectsBindingEntry ::= SEQUENCE {
  saviObjectsBindingIpAddressType  InetAddressType,
  saviObjectsBindingMethod         INTEGER,
  saviObjectsBindingIfIndex        InterfaceIndex,
  saviObjectsBindingIpAddress      InetAddress,
  saviObjectsBindingMacAddr        MacAddress,
  saviObjectsBindingLifetime       TimeInterval,
  saviObjectsBindingCreationtime   DateAndTime,
  saviObjectsBindingRowStatus      RowStatus
}

saviObjectsBindingIpAddressType OBJECT-TYPE
SYNTAX    InetAddressType
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION 
  "IP address type of the binding source IP."
::= { saviObjectsBindingEntry 1 }

saviObjectsBindingMethod OBJECT-TYPE
SYNTAX    INTEGER {
  manual(1),
  slaac(2),
  dhcp(3),
  send(4)
}
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION 
  "IP address assignment methods."
::= { saviObjectsBindingEntry 2 }

saviObjectsBindingIfIndex OBJECT-TYPE
SYNTAX    InterfaceIndex
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"The index value that uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of the IF-MIB’s ifIndex."

::= { saviObjectsBindingEntry 3 }
saviObjectsBindingIpAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"The binding source IP address"
::= { saviObjectsBindingEntry 4 }
saviObjectsBindingMacAddr OBJECT-TYPE
SYNTAX MacAddress
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The binding source mac address."
::= { saviObjectsBindingEntry 5 }
saviObjectsBindingLifetime OBJECT-TYPE
SYNTAX TimeInterval
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The remaining lifetime of the entry. TimeInterval is defined in RFC 2579, it’s a period of time, measured in units of 0.01 seconds, and the value is (0..2147483647).
If saviObjectsBindingMethod=manual, a value of 2147483647 represents infinity."

::= { saviObjectsBindingEntry 6 }
saviObjectsBindingCreationtime OBJECT-TYPE
SYNTAX DateAndTime
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The value of the local clock when the entry was firstly created."

::= { saviObjectsBindingEntry 7 }

saviObjectsBindingRowStatus OBJECT-TYPE
SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION "The status of this row, by which new entries may be
created, or old entries deleted from this table.
An Entry can be created or deleted only when
saviObjectsBindingMethod=manual."
 ::= { saviObjectsBindingEntry 8 }

-- Filtering Table for SAVI protocol

saviObjectsFilteringTable OBJECT-TYPE
SYNTAX SEQUENCE OF SaviObjectsFilteringEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "The table containing the filtering entries."
 ::= { saviObjects 5 }

saviObjectsFilteringEntry OBJECT-TYPE
SYNTAX SaviObjectsFilteringEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "An entry containing the filtering parameters. Entries are keyed on the source IP address type, anchor, and source IP address."
INDEX { saviObjectsFilteringIpAddressType,
         saviObjectsFilteringIfIndex,
         saviObjectsFilteringIpAddress }
 ::= { saviObjectsFilteringTable 1 }

SaviObjectsFilteringEntry ::= Sequences { saviObjectsFilteringIpAddressType InetAddressType,
                                          saviObjectsFilteringIfIndex InterfaceIndex,
                                          saviObjectsFilteringIpAddress InetAddress,
                                          saviObjectsFilteringMacAddr MacAddress }

saviObjectsFilteringIpAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"IP address type of the filtering source IP"
::= { saviObjectsFilteringEntry 1 }

saviObjectsFilteringIfIndex OBJECT-TYPE
SYNTAX InterfaceIndex
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"The index value that uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of the IF-MIB’s ifIndex."
::= { saviObjectsFilteringEntry 2 }

saviObjectsFilteringIpAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"The filtering source IP address."
::= { saviObjectsFilteringEntry 3 }

saviObjectsFilteringMacAddr OBJECT-TYPE
SYNTAX MacAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The filtering source mac address."
::= { saviObjectsFilteringEntry 4 }

--Count of packets dropped because of validation failure for each interface.

saviObjectsCountTable OBJECT-TYPE
SYNTAX SEQUENCE OF saviObjectsCountEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"The table containing count of packets dropped because of validation failure."
::= { saviObjects 6 }

saviObjectsCountEntry OBJECT-TYPE
SYNTAX saviObjectsCountEntry
MAX-ACCESS not-accessible
An entry containing count of packets dropped because of validation failure for each interface.

\[
\text{saviObjectsCountEntry ::= SEQUENCE { }
  \text{saviObjectsCountIPVersion InetVersion,}
  \text{saviObjectsCountIfIndex InterfaceIndex,}
  \text{saviObjectsCountFilterPkts Counter64,}
  \text{saviObjectsCountFilterOctets Counter64}
\]

\text{saviObjectsCountIPVersion OBJECT-TYPE}
\text{SYNTAX InetVersion}
\text{MAX-ACCESS not-accessible}
\text{DESCRIPTION "The IP version"}
::= { saviObjectsCountEntry 1 }

\text{saviObjectsCountIfIndex OBJECT-TYPE}
\text{SYNTAX InterfaceIndex}
\text{MAX-ACCESS not-accessible}
\text{STATUS current}
\text{DESCRIPTION "The Interface."}
::= { saviObjectsCountEntry 2 }

\text{saviObjectsCountFilterPkts OBJECT-TYPE}
\text{SYNTAX Counter64}
\text{MAX-ACCESS read-only}
\text{STATUS current}
\text{DESCRIPTION "The count of Pkts dropped."}
::= { saviObjectsCountEntry 3 }

\text{saviObjectsCountFilterOctets OBJECT-TYPE}
\text{SYNTAX Counter64}
\text{MAX-ACCESS read-only}
\text{STATUS current}
DESCRIPTION
"The count of Octets dropped."
 ::= { saviObjectsCountEntry 4 }

-- Conformance information
saviConformance OBJECT IDENTIFIER ::= { saviMIB 2 }
saviCompliances OBJECT IDENTIFIER ::= { saviConformance 1 }

-- Compliance statements
saviCompliance MODULE-COMPLIANCE
  STATUS current
  DESCRIPTION
"The compliance statement for entities which implement SAVI protocol."

MODULE
MANDATORY-GROUPS {
  systemGroup,
  portGroup,
  bindingGroup,
  filteringGroup
}
 ::= { saviCompliances 1}

saviGroups OBJECT IDENTIFIER ::= { saviConformance 2 }

-- Units of conformance

systemGroup OBJECT-GROUP
  OBJECTS {
    saviObjectsSystemSlaacEnable,
    saviObjectsSystemDhcpEnable,
    saviObjectsSystemSendEnable,
    saviObjectsSystemManualEnable
  }
  STATUS current
  DESCRIPTION
"The system group contains objects corresponding to savi system parameters."

 ::= {saviGroups 1}

portGroup OBJECT-GROUP
  OBJECTS {
    saviObjectsPortValidatingAttr,
    saviObjectsPortDhcpTrustAttr,
    saviObjectsPortTrustAttr,
    saviObjectsPortDhcpSnoopingAttr,
saviObjectsPortDataSnoopingAttr,
saviObjectsPortFilteringNum
}
STATUS current
DESCRIPTION
"The if group contains objects corresponding to the savi running
parameters of each anchor."
::= {saviGroups 2}

bindingGroup OBJECT-GROUP
OBJECTS {
  saviObjectsBindingMacAddr,
  saviObjectsBindingLifetime,
  saviObjectsBindingCreationtime,
  saviObjectsBindingRowStatus
}
STATUS current
DESCRIPTION
"The binding group contains the binding
information of anchor and soure ip address."
::= {saviGroups 3}

filteringGroup OBJECT-GROUP
OBJECTS {
  saviObjectsFilteringMacAddr
}
STATUS current
DESCRIPTION
"The filtering group contains the filtering
information of anchor and soure ip address."
::= {saviGroups 4}

END

9. 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:
o saviObjectsSystemTable - Unauthorized changes to the writable objects under saviObjectsSystemTable MAY disrupt allocation of resources in the network. For example, a device’s SAVI system mode be changed by set operation to SAVI-DISABLE will give chance to IP source address spoofing.

o saviObjectsPortTable - Unauthorized changes to the writable objects under saviObjectsPortTable MAY disrupt allocation of resources in the network. For example, an anchor’s ValidatingAttr be changed by set operation to DISABLE will give chance to IP source address spoofing.

o saviObjectsBindingTable - Unauthorized changes to the writable objects under this table MAY disrupt allocation of resources in the network. For example, a manual binding entry is inserted to the BST will give chance to IP source address spoofing.

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. These are the tables and objects and their sensitivity/vulnerability:

o saviObjectsBindingTable, saviObjectsFilteringTable - The IP address and binding anchor information will be helpful to some attacks.

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.

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.
10.  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>SAVI-MIB</td>
<td>{ ip XXX }</td>
</tr>
</tbody>
</table>

11.  Contributors

12.  References

12.1.  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,

RFC 2131, DOI 10.17487/RFC2131, March 1997,

Schoenwaelder, Ed., "Structure of Management Information
Version 2 (SMIv2)", STD 58, RFC 2578,
DOI 10.17487/RFC2578, April 1999,

Schoenwaelder, Ed., "Textual Conventions for SMIv2",
STD 58, RFC 2579, DOI 10.17487/RFC2579, April 1999,

Schoenwaelder, Ed., "Conformance Statements for SMIv2",
STD 58, RFC 2580, DOI 10.17487/RFC2580, April 1999,

C., and M. Carney, "Dynamic Host Configuration Protocol
for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July

12.2. Informative References


12.3. URL References

[idguidelines]  IETF Internet Drafts editor,  
                "http://www.ietf.org/ietf/1id-guidelines.txt".

[idnits]        IETF Internet Drafts editor,  
                "http://www.ietf.org/ID-Checklist.html".


[ops]           the IETF OPS Area,  "http://www.ops.ietf.org".

[xml2rfc]       XML2RFC tools and documentation,  
                "http://xml.resource.org".
Appendix A. Change Log

From draft 00 to draft 01

- Change the value range of object saviObjectsSystemMode and add a new value savi-send(6).

From draft 01 to draft 02

- Change saviObjectsTrustStatus into two booleans, one is saviObjectsDhcpTrustStatus, another is saviObjectsRaTrustStatus.
- Change the character string saviObjectsIf to saviObjectsPort globally.
- Change saviObjectsBindingState according to the latest version of solution drafts.

From draft 02 to draft 03

- Add a new object saviObjectsPortBindRecoveryAttr, and change the object saviObjectsPortRaTrustStatus to saviObjectsPortTrustAttr according to the latest version of solution drafts and RFC.
- Change the value range and meaning of saviObjectsBindingState according to the latest version of solution drafts and RFC.
- Change the value range of object saviObjectsBindingType, add a new value send(4), and change the value static(1) to manual(1).

From draft 03 to draft 04

- Add three new objects according to the latest version of solution drafts and RFC, i.e. saviObjectsSystemTentLT, saviObjectsSystemDefaultLT, saviObjectsSystemTWAIT.

From draft 04 to draft 05

- Add two new objects according to the latest version of solution drafts and RFC, i.e. saviObjectsBindingCreationtime, saviObjectsBindingTID.

From draft 05 to draft 06

- Add three new objects, saviObjectsSystemDadTimeout, saviObjectsPortDhcpSnoopingAttr and saviObjectsPortDataSnoopingAttr.
o Replace object saviObjectsSystemBindRecoveryInterval with saviObjectsSystemDataSnoopingInterval.

o Replace object saviObjectsPortSAVISAVIAtrr with saviObjectsPortTrustAttr.

o Delete object saviObjectsPortBindRecoveryAttr.

From draft 06 to draft 07

o Replace object saviObjectsSystemDadTimeout with saviObjectsSystemDetectionTimeout.

From draft 07 to draft 08

o Add a new table to count the fail packets of each interface.

From draft 08 to draft 09

o Change the value range and meaning of saviObjectsBindingState according to the latest version of solution RFC.

From draft 09 to draft 10

o Replace object saviObjectsSystemMode with saviObjectsSystemSlaacEnable, saviObjectsSystemDhcpEnable, saviObjectsSystemSendEnable, saviObjectsManualEnable.

From draft 10 to draft 11

o Add a new table SaviObjectsPreferenceTable to reflect the preference of each savi method.

From draft 11 to draft 12

o Replace object saviObjectsBindingType with saviObjectsBindingMethod.

From draft 12 to draft 13

o Add a new object saviObjectsCountFilterOctets to count the octets dropped by SAVI protocol.

Appendix B. Open Issues

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

Changqing An
Tsinghua University
Institute for Network Sciences and Cyberspace, Tsinghua University
Beijing  100084
China
Phone: +86 10 62603113
EMail: acq@cernet.edu.cn

Jiahai Yang
Tsinghua University
Institute for Network Sciences and Cyberspace, Tsinghua University
Beijing  100084
China
Phone: +86 10 62783492
EMail: yang@cernet.edu.cn

Jianping Wu
Tsinghua University
Institute for Network Sciences and Cyberspace, Tsinghua University
Beijing  100084
China
EMail: jianping@cernet.edu.cn

Jun Bi
Tsinghua University
Institute for Network Sciences and Cyberspace, Tsinghua University
Beijing  100084
China
EMail: junbi@cernet.edu.cn