PANA Working Group
Internet-Draft
Expires: August 13, 2004

Y. El Mghazli
Alcatel
Y. Ohba
Toshiba
J. Bournelle
GET/INT

February 13, 2004

SNMP usage for PAA-2-EP interface
<draft-yacine-pana-snmp-01.txt>

Status of this Memo

Copyright Notice

Abstract

The PANA Authentication Agent (PAA) does not necessarily act as an Enforcement Point (EP) to prevent unauthorized access or usage of the network. When a PANA Client (PaC) successfully authenticates itself to the PAA, EP(s) (e.g., access routers) will need to be suitably notified. The PANA working group mandates the use of Simple Network Management Protocol (SNMP) to deliver the authorization information to one or more EPs when the PAA is separated from EPs.

The present document provides the necessary information and

extensions needed to use SNMP as the PAA-2-EP protocol.

Table of Contents

1. Glossary

PANA: Protocol for Carrying Authentication for Network Access.

PaC (PANA Client): The client side of the protocol that resides in the host device, which is responsible for providing the credentials to prove its identity for network access authorization.

DI (Device Identifier): The identifier used by the network as a handle to control and police the network access of a client. Depending on the access technology, this identifier might contain any of IP address, link- layer address, switch port number, etc. of a connected device.

PAA (PANA Authentication Agent): The access network side entity of the protocol whose responsibility is to verify the credentials provided by a PANA client and grant network access service to the device associated with the client and identified by a DI.

EP (Enforcement Point): A node on the access network where per-packet enforcement policies (i.e., filters) are applied on the inbound and outbound traffic of client devices. Information such as DI and (optionally) cryptographic keys are provided by PAA per client for constructing filters on the EP.

2. Introduction

Client access authentication should be followed by access control to make sure only authenticated and authorized clients can send and receive IP packets via access network. Access control can involve setting access control lists on the enforcement points. Identification of clients, which are authorized to access the network, is done by the PANA protocol exchange.

PANA does not assume that the PAA is always co-located with the EP(s). Network access enforcement can be provided by one or more nodes on the same IP subnet as the client (e.g., multiple routers). When the PAA and the EP(s) are separated, there needs to be another transport for client provisioning. This PAA-2-EP transport is needed to create access control lists to allow authenticated and authorized clients' traffic through the EPs.

The present document provides the necessary information and extensions needed to use SNMP as the PAA-2-EP protocol.

2.1 scope

The next section 3 gives references for the SNMP framework.

Then section 4 provides a general statement with regards to the applicability of SNMP as the PAA-2-EP protocol.

IPSec MIB modules were found to have general applicability and

varying levels of re-usability for PANA EP configuration using SNMP. Section 5 details the applicability of this MIB set to the EP configuration.

Section 6 provides usage examples of these MIB modules in the context of PANA.

Section 7 defines some additional PANA-specific objects that extend the IPSec-SPD-MIB module in order to entirely satisfy the PAA-2-EP interface requirements.

Finally, section 8 addresses the security considerations.

3. 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].

4. SNMP Applicability with the PANA framework

This section provides a general statement with regards to the applicability of SNMP as the PAA-2-EP protocol. This analysis of SNMP is specific to SNMPv3, which provides the security required for PANA usage. SNMPv1 and SNMPv2c would be inappropriate for PANA since they have been declared Historic, and because their messages have only trivial security.

4.1 SNMPv3 General applicability

The primary advantages of SNMPv3 are that it is a mature, well understood protocol, currently deployed in various scenarios, with mature toolsets available for SNMP managers and agents.

Application intelligence is captured in MIB modules, rather than in the messaging protocol. MIB modules define a data model of the information that can be collected and configured for a managed functionality. The SNMP messaging protocol transports the data in a standardized format without needing to understand the semantics of the data being transferred. The endpoints of the communication understand the semantics of the data.

Partly due to the lack of security in SNMPv1 and SNMPv2c, and partly due to variations in configuration requirements across vendors, few MIB modules have been developed that enable standardized configuration of managed devices across vendors. Since monitoring can be done using only a least-common-denominator subset of information across vendors, many MIB modules have been developed to provide standardized monitoring of managed devices. As a result, SNMP has been used primarily for monitoring rather than for configuring network nodes.

SNMPv3 builds upon the design of widely-deployed SNMPv1 and SNMPv2c versions. Specifically, SNMPv3 shares the separation of data modeling (MIBs) from the protocol to transfer data, so all existing MIBs can be used with SNMPv3. SNMPv3 also uses the SMIv2 standard, and it shares operations and transport with SNMPv2c. The major difference between SNMPv3 and earlier versions is the addition of strong message security and controlled access to data.

SNMPv3 uses the architecture detailed in [RFC3411], where all SNMP entities are capable of performing certain functions, such as the generation of requests, response to requests, the generation of asynchronous notifications, the receipt of notifications, and the proxy-forwarding of SNMP messages. SNMP is used to read and manipulate virtual databases of managed-application-specific operational parameters and statistics, which are defined in MIB

modules.

4.2 Compliancy of SNMP against the PAA-EP requirements

[I-D.yacine-pana-paa2ep-prot-eval] gives further details about the choice of SNMP as the PAA-2-EP protocol.

The following section illustrate how all the PAA-2-EP protocol requirements are fully supported by SNMP:

4.2.1 Authorization Consideration

This section discusses PAA-EP communication in terms of authorization aspects.

Filter Rule Installation: Filtering rules to be installed on EP generally include a device- identifier of PaC, and also cryptographic keying material (such as keys, key pairs, and initialization values) when needed. The keying material is needed when attackers can eavesdrop and spoof on the device identifiers easily. Each keying material is uniquely identified with a keying material name and has a lifetime for key management purpose. The keying material is used with link-layer or network-layer ciphering to provide additional protection. In addition to the device identifier and keying material, other filter rules, such as the IP filter rules specified in NAS-Filter-Rule AVPs carried in Diameter EAP application [I-D.ietf-aaa-eap] may be installed on EP.

Using SNMP to configure the EPs, one can re-use existing MIBs, this is detailed in section 5. Additional PANA-specific objects may be needed and are defined in section 7.

Authorization Based on Maximum Amount of Units : In addition to filter rules, there is another type of authorization parameter in which the maximum amount of units is specified as an authorization parameter. The type of units can be time (e.g., authorization lifetime), volume (e.g., the number of incoming and/or outgoing packets and/or bytes), service specific or money depending on the type of service event [I-D.ietf-aaa-diameter-cc].

There are two possible methods to support this type of authorization model: polling and notification. In the polling model, the PAA (most probably) periodically sends its EP(s) queries on the current amount of units used by each PaC. In the notification model, the PAA sends the maximum amount units to EP(s) when a PaC is successfully authenticated and authorized, and waits notification events from EP(s). The notification events are sent by EP(s) when each PaC has spent the maximum amount of units.

With the use of SNMPv3 as the PAA- EP protocol, the polling and notification models are supported by SNMP get and trap operations, respectively. In general, the polling model is less scalable than the notification model as the number of PaCs and/or EPs increases.

On the other hand, the notification model based on SNMP trap is unreliable since SNMP Trap message is not responded. However, SNMP applications can be designed to add reliability to the trap operation, by sending SNMP query to the sender of the Trap message from PAA when a Trap message is received. Thus, the notification model should be used for supporting this type of authorization. This type of authorization might also require that the communicating pair of PAA and EP to detect a dead or rebooted peer in order to avoid possible inaccurate accounting. This aspect is discussed in section 4.2.6.

4.2.2 One-to-many PAA-EP relation

This means that there might be multiple EPs per PAA. The SNMP framework [RFC3410] clearly states that an SNMP manager (PAA) can communicate simultaneously with several agents (EPs).

4.2.3 Secure Communication

SNMPv3 includes the User-based Security Model [RFC3414], which defines three standardized methods for providing authentication, confidentiality, and integrity. Additionally, USM has specific built-in mechanisms for preventing replay attacks including unique protocol engine IDs, timers and counters per engine and time windows for the validity of messages.

See section 8.

4.2.4 Notification of PaC presence

PaC may also choose to start sending packets before getting authenticated. In that case, the network should detect this and the PAA must send an unsolicited PANA-Start-Request message to PaC. EP is the node that can detect such activity. In case they are separate, there needs to be an explicit message to prompt PAA.

The PAA-2-EP protocol may allow the EP to notify a new PaC to the PAA. When SNMPv3 is used as the PAA-EP protocol, such a presence notification is done by using the SNMP trap operation. See section 5.3 for details on how new and existing SNMP objects provide this feature.

4.2.5 Accounting Consideration

Since authentication and authorization are closely related to accounting in many cases, accounting aspects need to be considered in the PAA-EP protocol. There are logically two models with regard to where the accounting client is located.

In the first model, the accounting client is co-located with PAA. The PAA device acts as an accounting client of a AAA protocol. The PAA collects accounting information from the EP(s) it controls, and sends the gathered data to the accounting server by using the AAA protocol. In the case where accounting is performed in usage basis, i.e., the number of transmitted/received octets/packets, the PAA-EP protocol also needs to carry these usage data.

In the second model, the accounting client is co-located with EP. In this model, the EP device acts as an accounting client of a AAA protocol. The EP obtains the authentication/authorization session identifier for each PaC from the PAA, where the authentication/ authorization session identifier is assigned by a AAA protocol running on the PAA, and sends the accounting information directly to the accounting server by using the AAA protocol, without sending the accounting information to the PAA.

The authentication/authorization session identifier of a AAA protocol is used by the accounting server to associate accounting information with a particular authentication/authorization session to calculate bills. The authentication/authorization session identifier may or may not be the same as the PANA session identifier.

Both models might need for the communicating pair of PAA and EP to detect a dead or rebooted peer to avoid possible inaccurate accounting. This aspect is discussed in section 4.2.6.

4.2.6 Peer Liveness Test and Rebooted Peer Detection

PAA-EP protocol implementations need to be stateful when considering the authorization and accounting aspects as described in the previous sections. The stateful nature provides the functionality to detect a dead or rebooted peer in a timely fashion. On the other hand, this does not mean that the PAA-EP protocol itself needs to be stateful. For example, an SNMP entity (i.e., an SNMP engine plus SNMP applications) can generate SNMP queries on a particular MIB at an

interval shorter enough to perform peer liveness test and rebooted peer detection.

Also, the peer liveness test and rebooted peer detection need to be performed securely.

When SNMPv3 is used as the PAA-EP protocol, the SNMP management framework supports snmpEngineBoots MIB [RFC3411]. By periodically sending SNMP query to the peer to check the current value of this MIB with the use of SNMP Security Subsystem, it is possible for an SNMP entity to securely perform peer liveness test and rebooted peer detection between PAA and EP.

When a PAA finds a dead or rebooted EP, the PAA should immediately terminate PANA sessions for PaCs that are authorized for access through the EP.

5. Applicability of IPSec configuration MIBs

This section details the applicability of existing IPSec configuration MIB modules to the EP configuration. These were found to have general applicability and a fair level of re-usability for PANA EP configuration:

IPSec Security Policy Database (SPD) MIB [I-D.ietf-ipsp-ipsec-conf-mib]:

This document defines a MIB module for configuration of an IPsec SPD. No IPsec or IKE specific actions are defined within this document.

IPSec IKE Action MIB [I-D.ietf-ipsp-ikeaction-mib]:

This document defines a MIB module for configuration of an IKE action within the IPsec security policy database (SPD).

The IPSec Configuration MIBs set does not define MIB modules for monitoring the state of an IPsec device. Neither it does define MIB modules for configuring other policy related actions. The purpose of these MIBs is to allow administrators to be able to configure policy with respect to the IPsec [RFC2401]/IKE [RFC2409] protocols.

5.1 General Access Control

The PAA must provision its EPs with DI-based filters in order to control and police the network access of a PaC. According to the definition of the Device Identifier in [I-D.ietf-pana-requirements],

such filters - depending on the access technology - might contain any of IP address or link-layer address of a connected device. See section 4.2.1 for further considerations.

Do note also that keying material might be provisioned for the particular case where access control is performed using IPSec [I-D.ietf-pana-ipsec]. This particular case is detailed in next section 5.2.

The IPSec SPD MIB module is designed to configure an IPsec security policy database in a policy and rule oriented fashion. This module is divided into 3 portions (Rules, Filters, Actions). Specifically, the SPD MIB provides a generic mechanism for performing packet processing based on a rule set.

The policy-based packet filtering and the corresponding execution of actions is of a more general nature than for IPsec configuration only, such as for configuration of a firewall. Rules within the IPSec Configuration MIB are generic and simply bind a filter to an action.

Filters provided within the IPSec MIB itself are numerous and fairly complete for most common packet filtering usage but externally defined filters are supported.

-- Ipv4/v6 address-based filter

For Ipv4/v6 address-based filters provisioning, the IPSec SPD MIB module (SPD-MIB) provides means to filter the traffic based on the IP header information. SPD-MIB "spdIpHeaderFilter" table provides such facilities: one can define the various tests that are used when evaluating a given IP packet. The various tests definable in this table are as follows:

Source Address Match

Destination Address Match

Source Port Range Match

Destination Port Range Match

Protocol Match

IPv6 Flow Label Match (Ipv6 only)

The results of each test are ANDed together to produce the result of the entire filter.

-- L2 address-based filter

For Layer 2 address-based classification, additional filters might be designed if needed. Section 7 defines a IEEE 802-based filter, which may be useful in appropriate access networks. The various tests definable in this table are as follows:

Source Address (802) Match

Destination Address (802) Match

VlanId Match

VlanTag Test

IEEE 802 EtherType Match

802.1 UserPriority Match

-- Static Actions

The actions encapsulated within this module are basic drop/accept actions. These are sufficient to perform EP general access control at the EP.

5.2 IPSec Access Control

The PANA protocol authenticates the client and also establishes a PANA security association between the PANA client and PANA authentication agent at the end of successful authentication. The PANA authentication agent (PAA) indicates the results of the

authentication using the PANA-Bind-Request message wherein it can indicate the access control method enforced by the access network and the IP address of the corresponding EP.

When IPSec is used to perform access control, the PANA protocol [I-D.ietf-pana-pana] does not discuss any details of IPsec [RFC2401] SA establishment. Indeed, [I-D.ietf-pana-ipsec] discusses the details for establishing an IPsec security association between the PaC and the EP. When the IPsec SA is successfully established, it can be used to enforce access control and specifically used to prevent the service theft mentioned in [I-D.ietf-pana-threats-eval].

In this particular context, one assumes that the following have already happened before the IPSec SA is established:

- PANA client (PaC) and PAA mutually authenticate each other using EAP methods that derive Master Session Key (MSK).

- PaC learns the IP address of the Enforcement point (EP) during the PANA exchange.

- PaC learns that the network uses IPsec [RFC2401] for securing the link between PaC and EP during the PANA exchange.

- PaC configures an IP address address before the PANA protocol begins.

The IPSec IKE Action MIB module (IKEACTION-MIB) works within the framework of the IPsec Security Policy Database Configuration MIB (SPD-MIB). It can be referenced as an action by the SPD-MIB and is used to configure IKE negotiations between network devices. Hence, together with the SPD-MIB, the IKEACTION-MIB module enables the PAA to configure IPSEC-based access control at the EP.

The PAA is then responsible to communicate to EP the following before IKE phase 1 exchange begins:

the IKE pre-shared key:

- To this end, the PAA must set a row in the IKE Credential Filter table of the IKEACTION-MIB. This table defines filters, which can be used to match credentials of IKE peers, where the credentials

in question have been obtained from an IKE phase 1 exchange. They may be X.509 certificates, Kerberos tickets, or Pre-shared keys, etc.

the IP address of the PaC

An IP Header Filter of the SPD-MIB is used for configuring the SPD accordingly. See the previous section 5.1 for further details.

the PANA session ID (optionally)

[I-D.ietf-pana-ipsec] states that aggressive mode must be supported. Pac and EP should use the PANA session ID (see [I-D.ietf-pana-pana]) as the payload of the ID_KEY_ID in aggressive mode for establishing the phase 1 SA. To this end, the PAA must use the IKE Peer Identity Filter table of the IKEACTION-MIB.

5.3 Notification of PaC presence

The SPD-MIB provides a means to notify to the SNMP manager (PAA) information on packets matching/not matching the filters of given rule. Such notification mechanisms and objects can be re-used for notifying the PAA that unauthorized packets are trying to pass through the EP.

Section 7 defines a new SNMP notification, which aims at satisfying this requirement. It re-uses existing notification variable objects pre-defined in the SPD MIB.

This "New PaC" notification (panaNewPacNotification) is triggered when the the EP detects traffic coming from an unauthorized source. The objects sent must include ipspIPSourceType, ipspIPSourceAddress, ipspIPDestinationType, and ipspIPDestinationAddress objects to indicate the packet source and destination of the packet that triggered the action. Additionally, the ipspIPInterfaceType, ipspIPInterfaceAddress, and ipspPacketDirection objects are included to indicate which interface the action was executed in association with and if the packet was inbound or outbound through the endpoint.

See [I-D.ietf-ipsp-ipsec-conf-mib] for further details.

6. EP Configuration Example

6.1 General Access Control

TBD.

6.2 IPSec-based Access Control

TBD.

7. PANA extension to the IPSec SPD MIB

Many existing IPSec MIB objects defined in the IPSec Configuration MIB modules can be efficiently re-used for the PANA-specific needs. This is detailed in section 5.

The following sections define additional PANA-specific objects that extend the IPSec MIB module in order to entirely satisfy the PAA-2-EP interface requirements.

7.1 PANA MIB Overview

. 802 filters

. "New PaC" notification

7.2 PANA-specific objects definition

```
PANA-MIB DEFINITIONS ::= BEGIN

IMPORTS

MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, Integer32
                        FROM SNMPv2-SMI

RowStatus, PhysAddress,  StorageType, TimeStamp
                        FROM SNMPv2-TC

MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
                        FROM SNMPv2-CONF

SnmpAdminString
                        FROM SNMP-FRAMEWORK-MIB


spdMIB, spdActionExecuted, spdIPInterfaceType, spdIPInterfaceAddress,
spdIPSourceType, spdIPSourceAddress, spdIPDestinationType,
```

```
spdIPDestinationAddress, spdPacketDirection
                                FROM IPSEC-SPD-MIB;

  -- Module identity
--

panaMIB MODULE-IDENTITY
  LAST-UPDATED
     "200402050000Z"            -- 05 February 2004
```



```
  ORGANIZATION
     "IETF PANA Working Group"
  CONTACT-INFO
    "Yacine El Mghazli
     Alcatel
     91460 Marcoussis, France
     Phone: +33 1 69 63 41 87
     Email: yacine.el_mghazli@alcatel.fr"
  DESCRIPTION
     "The MIB module for defining additional PANA-specific objects to
      the IPSec SPD MIB. Copyright (C) The Internet Society (2003).
      This version of this MIB module is part of RFC XXXX, see the
      RFC itself for full legal notices."

-- Revision History
  REVISION
     "200402050000Z"            -- 05 February 2004
  DESCRIPTION
     "Version 01, draft-yacine-pana-paa2ep-snmp-01.txt"
  REVISION
     "200310310000Z"            -- 31 October 2003
  DESCRIPTION
     "Initial version, draft-yacine-pana-paa2ep-snmp-00.txt"
::= { spdMIB XXX } -- XXX to be assigned by IANA

--
-- groups of related objects
--

panaConfigObjects         OBJECT IDENTIFIER
     ::= { panaMIB 1 }
panaNotificationObjects   OBJECT IDENTIFIER
```

```
     ::= { panaMIB 2}
panaConformanceObjects    OBJECT IDENTIFIER
     ::= { panaMIB 3 }

--
-- Textual Conventions
--

-- TBD.

--
-- PANA Additional Filters Objects
--


--
```



```
-- The IEEE 802 Filter Table
--


pana802FilterTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF Pana802FilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
      " IEEE 802-based filter definitions. A class that contains
        attributes of IEEE 802 (e.g., 802.3) traffic that form
        filters that are used to perform traffic classification."
    ::= { panaConfigObjects 1 }

pana802FilterEntry OBJECT-TYPE
    SYNTAX      Pana802FilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
      " IEEE 802-based filter definitions.  An entry specifies
        (potentially) several distinct matching components. Each
        component is tested against the data in a frame
        individually. An overall match occurs when all of the
        individual components match the data they are compared
        against in the frame being processed. A failure of any
```

```
            one test causes the overall match to fail.
            Wildcards may be specified for those fields that are not
            relevant."
        INDEX       { pana802FilterName }
        ::= { pana802FilterTable 1 }

    Pana802FilterEntry ::= SEQUENCE {
            pana802FilterName            SnmpAdminString,
            pana802FilterType              BITS,
            pana802FilterDstAddr         PhysAddress,
            pana802FilterSrcAddr         PhysAddress,
            pana802FilterVlanId          Integer32,
            pana802FilterVlanTagRequired INTEGER,
            pana802FilterEtherType       Integer32,
            pana802FilterUserPriority    BITS,
            pana802FiltLastChanged       TimeStamp,
            pana802FiltStorageType       StorageType,
            pana802FiltRowStatus         RowStatus

    }

    pana802FilterName OBJECT-TYPE
        SYNTAX         SnmpAdminString (SIZE(1..32))
```



```
        MAX-ACCESS     not-accessible
        STATUS         current
        DESCRIPTION
            "The administrative name for this filter. "
        ::= { pana802FilterEntry 1 }

    pana802FilterType OBJECT-TYPE
        SYNTAX      BITS { srcAddress(0),
                           dstAddress(1),
                           vlanId(4),
                           etherType(5),
                           userPriority(6) }
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
            "This defines the various tests that are used when evaluating
             a given filter.  The results of each test are ANDed together
             to produce the result of the entire filter.  When processing
```

```
                this filter, it is recommended for efficiency reasons that
                the filter halt processing the instant any of the specified
                tests fail.
                Once a row is 'active', this object's value may not be
                changed unless all the appropriate columns needed by the new
                value to be imposed on this object have been appropriately
                configured. . "
            ::= { pana802FilterEntry 2 }

        pana802FilterDstAddr OBJECT-TYPE
            SYNTAX          PhysAddress
            MAX-ACCESS      read-create
            STATUS          current
            DESCRIPTION
                "The 802 address against which the 802 DA of incoming
                traffic streams will be compared. Frames whose 802 DA
                matches the physical address specified by this object,
                taking into account address wildcarding as specified by the
                pana802FilterDstAddrMask object, are potentially subject to
                the processing guidelines that are associated with this
                entry through the related action class."
            ::= { pana802FilterEntry 3 }

        pana802FilterSrcAddr OBJECT-TYPE
            SYNTAX          PhysAddress
            MAX-ACCESS      read-create
            STATUS          current
            DESCRIPTION
               "The 802 MAC address against which the 802 MAC SA of
                incoming traffic streams will be compared. Frames whose 802
```



```
                MAC SA matches the physical address specified by this
                object, taking into account address wildcarding as specified
                by the pana802FilterSrcAddrMask object, are potentially
                subject to the processing guidelines that are associated
                with this entry through the related action class."
            ::= { pana802FilterEntry 4 }

        pana802FilterVlanId OBJECT-TYPE
            SYNTAX          Integer32 (-1 | 1..4094)
            MAX-ACCESS      read-create
            STATUS          current
```

```
        DESCRIPTION
            "The VLAN ID (VID) that uniquely identifies a VLAN
            within the device. This VLAN may be known or unknown
            (i.e., traffic associated with this VID has not yet
            been seen by the device) at the time this entry
            is instantiated.
            Setting the pana802FilterVlanId object to -1 indicates that
            VLAN data should not be considered during traffic
            classification."
        ::= { pana802FilterEntry 5 }

    pana802FilterVlanTagRequired OBJECT-TYPE
        SYNTAX          INTEGER {
                           taggedOnly(1),
                           priorityTaggedPlus(2),
                           untaggedOnly(3),
                           ignoreTag(4)
                        }
        MAX-ACCESS      read-create
        STATUS          current
        DESCRIPTION
            "This object indicates whether the presence of an
            IEEE 802.1Q VLAN tag in data link layer frames must
            be considered when determining if a given frame
            matches this 802 filter entry.
            A value of 'taggedOnly(1)' means that only frames
            containing a VLAN tag with a non-Null VID (i.e., a
            VID in the range 1..4094) will be considered a match.
            A value of 'priorityTaggedPlus(2)' means that only
            frames containing a VLAN tag, regardless of the value
            of the VID, will be considered a match.
            A value of 'untaggedOnly(3)' indicates that only
            untagged frames will match this filter component.
            The presence of a VLAN tag is not taken into
            consideration in terms of a match if the value is
            'ignoreTag(4)'."
        ::= { pana802FilterEntry 6 }
```



```
    pana802FilterEtherType OBJECT-TYPE
        SYNTAX          Integer32 (-1 | 0..'ffff'h)
        MAX-ACCESS      read-create
        STATUS          current
```

```
        DESCRIPTION
            "This object specifies the value that will be compared
            against the value contained in the EtherType field of an
            IEEE 802 frame. Example settings would include 'IP'
            (0x0800), 'ARP' (0x0806) and 'IPX' (0x8137).
             Setting the pana802FilterEtherTypeMin object to -1 indicates
            that EtherType data should not be considered during traffic
            classification.
            Note that the position of the EtherType field depends on
            the underlying frame format. For Ethernet-II encapsulation,
            the EtherType field follows the 802 MAC source address. For
            802.2 LLC/SNAP encapsulation, the EtherType value follows
            the Organization Code field in the 802.2 SNAP header. The
            value that is tested with regard to this filter component
            therefore depends on the data link layer frame format being
            used. If this 802 filter component is active when there is
            no EtherType field in a frame (e.g., 802.2 LLC), a match is
            implied."
        ::= { pana802FilterEntry 7 }

    pana802FilterUserPriority OBJECT-TYPE
        SYNTAX         BITS {
                            matchPriority0(0),
                            matchPriority1(1),
                            matchPriority2(2),
                            matchPriority3(3),
                            matchPriority4(4),
                            matchPriority5(5),
                            matchPriority6(6),
                            matchPriority7(7)
                       }
        MAX-ACCESS     read-create
        STATUS         current
        DESCRIPTION
            "The set of values, representing the potential range
            of user priority values, against which the value contained
            in the user priority field of a tagged 802.1 frame is
            compared. A test for equality is performed when determining
            if a match exists between the data in a data link layer
            frame and the value of this 802 filter component. Multiple
            values may be set at one time such that potentially several
            different user priority values may match this 802 filter
            component.
            Setting all of the bits that are associated with this
```

```
            object causes all user priority values to match this
            attribute. This essentially makes any comparisons
            with regard to user priority values unnecessary. Untagged
            frames are treated as an implicit match."
        ::= { pana802FilterEntry 8 }

    pana802FiltLastChanged OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
          "The value of sysUpTime when this row was last modified or
           created either through SNMP SETs or by some other external
           means."
        ::= { pana802FilterEntry 9 }

    pana802FiltStorageType OBJECT-TYPE
        SYNTAX      StorageType
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
          "The storage type for this row.  Rows in this table which were
           created through an external process may have a storage type
           of readOnly or permanent."
       DEFVAL { nonVolatile }
        ::= { pana802FilterEntry 10 }

    pana802FiltRowStatus OBJECT-TYPE
        SYNTAX      RowStatus
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
          "This object indicates the conceptual status of this row.
           This object may not be set to active if the requirements of
           the pana802FilterType object are not met.  In other words,
           if the associated value columns needed by a particular test
           have not been set, then attempting to change this row to an
           active state will result in an inconsistentValue error.  See
           the pana802FilterType object description for further
           details."
        ::= { pana802FilterEntry 11 }


    --
    --
    -- Notification objects information
```

```
--
```



```
--

panaNotifications OBJECT IDENTIFIER ::=
   { panaNotificationObjects 0 }

panaNewPacNotification NOTIFICATION-TYPE
  OBJECTS { spdActionExecuted, spdIPInterfaceType,
            spdIPInterfaceAddress,
            spdIPSourceType, spdIPSourceAddress,
            spdIPDestinationType,
            spdIPDestinationAddress,
            spdPacketDirection }
  STATUS  current
  DESCRIPTION
      "Notification that AP detected traffic coming from an
unauthorized source. The objects sent must include the
ipspActionExecuted which will indicate which action was executed
within the scope of the rule.  Additionally, the ipspIPSourceType,
ipspIPSourceAddress, ipspIPDestinationType, and
ipspIPDestinationAddress, objects must be included to indicate the
packet source and destination of the packet that triggered the
action.  The ipspIPInterfaceType, ipspIPInterfaceAddress, and
ipspPacketDirection objects are included to indicate which endpoint
the packet was associated with."
  ::= { panaNotifications 1 }


--
--
-- Conformance information
--
--

-- TBD.

END
```

8. Security Considerations

-- if you have any read-write and/or read-create objects, please -- describe their specific sensitivity or vulnerability. -- RFC 2669 has a very good example.

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:

< list the tables and objects and state why they are sensitive >

-- else if there are no read-write objects in your MIB module

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.

-- for all MIB modules you must evaluate whether any readable objects -- are sensitive or vulnerable (for instance, if they might reveal -- customer information or violate personal privacy laws such as -- those of the European Union if exposed to unathorized parties)

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:

<list the tables and objects and state why they are sensitive>

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPSec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

It is RECOMMENDED that implementers consider the security features as provided by the SNMPv3 framework (see [RFC3410], section 8), including full support for the SNMPv3 cryptographic mechanisms (for

authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

9. Acknowledgements

This document leverages on similar works done in the MIDCOM working group. Thanks to the authors of those IDs.

The author would like to thank Thomas Moore for his grateful help during the edition of this document.

Normative References

[I-D.ietf-pana-pana]
Forsberg, D., "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-03 (work in progress), February 2004.

[I-D.ietf-pana-requirements]
Yegin, A. and Y. Ohba, "Protocol for Carrying Authentication for Network Access (PANA)Requirements", draft-ietf-pana-requirements-07 (work in progress), June 2003.

[I-D.ietf-pana-ipsec]
Parthasarathy, M., "PANA enabling IPsec based Access Control", draft-ietf-pana-ipsec-01 (work in progress), January 2004.

[I-D.ietf-pana-threats-eval]
Parthasarathy, M., "PANA Threat Analysis and security requirements", draft-ietf-pana-threats-eval-04 (work in progress), May 2003.

[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, December 2002.

[I-D.ietf-ipsp-ipsec-conf-mib]
Baer, M., "IPsec Policy Configuration MIB", draft-ietf-ipsp-ipsec-conf-mib-03 (work in progress), June 2002.

[I-D.ietf-ipsp-ikeaction-mib]
Hardaker, W., "IPsec Security Policy IKE Action MIB", draft-ietf-ipsp-ikeaction-mib-00 (work in progress), January 2004.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC3410] Case, J., Mundy, R., Partain, D. and B. Stewart, "Introduction and Applicability Statements for

Internet-Standard Management Framework", RFC 3410, December 2002.

[RFC3411] Harrington, D., Presuhn, R. and B. Wijnen, "An Architecture for Describing Simple Network Management

Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2578] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

[RFC2579] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

[RFC2580] McCloghrie, K., Perkins, D. and J. Schoenwaelder, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999.

Informative References

[I-D.yacine-pana-paa2ep-prot-eval]
Mghazli, Y., "PANA PAA-EP protocol considerations", draft-yacine-pana-paa2ep-prot-eval-00 (work in progress), October 2003.

[I-D.yacine-pana-paa-ep-reqs]
Mghazli, Y., "PANA PAA-EP Protocol Requirements", draft-yacine-pana-paa-ep-reqs-00 (work in progress), October 2003.

[I-D.ietf-aaa-diameter-cc]
Hakala, H., "Diameter Credit-control Application", draft-ietf-aaa-diameter-cc-02 (work in progress), December 2003.

[I-D.ietf-aaa-eap]
Eronen, P., Hiller, T. and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-03 (work in progress), October 2003.

Authors' Addresses

Yacine El Mghazli (Editor)
Alcatel
Route de Nozay
Marcoussis 91460
France

EMail: yacine.el_mghazli@alcatel.fr

Yoshihiro Ohba
Toshiba America Information Systems, Inc.
9740 Irvine Blvd.
Irvine, CA 92619-1697
USA

EMail: yohba@tari.toshiba.com

Julien Bournelle
GET/INT
9 rue Charles Fourier
Evry 91011
France

EMail: julien.bournelle@int-evry.fr

Intellectual Property Statement

Full Copyright Statement

Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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 Internet Society.