PANA Working Group
Internet-Draft
Expires: April 22, 2005

Y. El Mghazli
Alcatel
Y. Ohba
Toshiba
J. Bournelle
GET/INT
October 22, 2004

SNMP usage for PAA-EP interface
draft-ietf-pana-snmp-02

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 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 Version 3 (SNMPv3) 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 SNMPv3 as the PAA-EP protocol.

Table of Contents

1. Terminology and Definitions

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. A PaC is responsible for requesting network access and engaging in authentication process using the PANA protocol.

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 (server) side entity of the PANA protocol. A PAA is in charge of interfacing with the PaCs for authenticating and authorizing them for the network access service. To this end, the PAA verifies the credentials provided by a PANA client and grants network access service to the device associated with the client and identified by a DI.
The PAA is also responsible for updating the access control state (i.e., filters) depending on the creation and deletion of the authorization state. The PAA communicates the updated state to the enforcement points in the network. When the PAA and the EP are separated, a protocol is required to carry the authorized client attributes from the PAA to the EP. SNMP is mandated for this task.

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. The EP uses non-cryptographic or cryptographic filters to selectively allow and discard data packets. These filters may be applied at the link-layer or the IP-layer. An EP learns the attributes of the authorized clients (DI and (optionally) cryptographic keys) from the PAA.

2. Introduction

2.1 PAA/EP separation context

PANA enables access control by identifying legitimate clients and generating filtering information for access control mechanisms. [I-D.ietf-pana-framework] defines a general AAA and access control framework. The PANA protocol itself provides client authentication and authorization functionality for securing network access. The other component of a complete solution is the access control which ensures that only authenticated and authorized clients can gain access to the network.

Access control can be achieved by placing EPs (Enforcement Points) in the network for policing the traffic flow. EPs should prevent data traffic from and to any unauthorized client unless it's either PANA or one of the other allowed traffic types (e.g., ARP, IPv6 neighbor discovery, DHCP, etc.).

Figure 1 below illustrates the functional entities and the interfaces (protocols, APIs) among them.

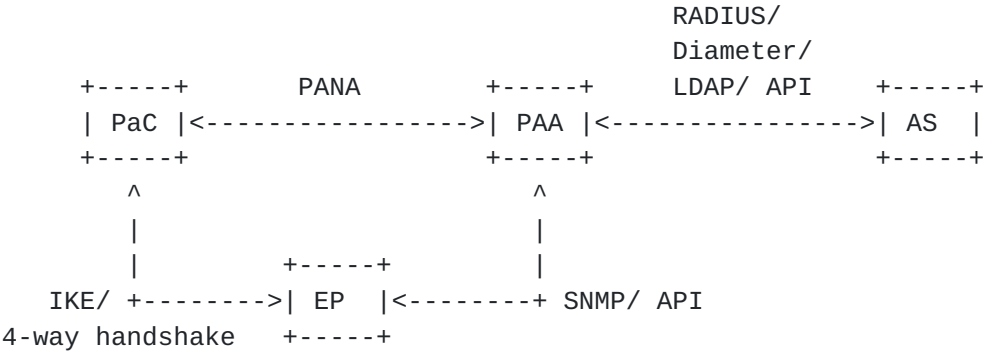

Figure 1: PANA Functional Model

Some of the entities may be co-located depending on the deployment scenario.

The EP on the access network allows general data traffic from any authorized PaC, whereas it allows only limited type of traffic (e.g., PANA, DHCP, router discovery) for the unauthorized PaCs. This ensures that the newly attached clients have the minimum access service to engage in PANA and get authorized for the unlimited service.

If the PaC is authorized to gain the access to the network, the PAA also sends the PaC-specific attributes (e.g., IP address, cryptographic keys, etc.) to the EP by using SNMP. The EP uses this

information to enforce policy rules allowing data traffic from and to the PaC to pass through.

In case a cryptographic access control needs to be enabled after the PANA authentication, a secure association protocol runs between the PaC and the EP. The PaC should already have the input parameters to this process as a result of the successful PANA exchange. Similarly, the EP should have obtained them from the PAA via SNMP. Secure association exchange produces the required security associations between the PaC and the EP to enable per-packet protection.

Finally data traffic can start flowing from and to the newly authorized PaC.

2.2 Scope

Section 3 gives references for the SNMP framework.

Section 4 provides a general statement with regards to the applicability of SNMP as the PAA-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 [I-D.ietf-ipsp-spd-mib] in order to entirely satisfy the PAA-EP interface requirements.

Finally, Section 9 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 [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 [RFC2578], STD 58 [RFC2579] and STD 58 [RFC2580].

4. SNMP Applicability with the PANA framework

This section provides a general statement with regards to the applicability of SNMP as the PAA-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 PANA requirements

The following sections detail how the PAA-EP protocol requirements are fully supported by SNMP:

4.2.1 Authorization Consideration

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

Binary Authorization:

Filtering rules to be installed on EP generally include a device identifier of PaC, and also a cryptographic keying material (e.g., IKE [RFC2409] pre-shared key) when cryptographic data traffic protection is needed. Each keying material is uniquely identified with a keying material name (e.g., ID_KEY_ID in IKE) and has a lifetime for key management, accounting, access control and security reasons in general.

PANA management can be modeled in a way that is consistent with existing standard MIB modules, this is detailed in Section 5. Additional PANA-specific objects may be needed and are defined in Section 7.

Profile-based authorization:

In addition to the device identifier and keying material, the PAA may provide the EP with additional authorization information. For instance, a user may be authorized to access the network within a given class of service or for a maximum amount of units. 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 models to support this type of authorization:

* In the polling model, the PAA (most probably) periodically sends queries to its EP(s) 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 a 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 notification operations, respectively.

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.

In any case, even if it is very likely to occur between the PAA and EP, this kind of profile-based authorization is beyond the scope of the PANA working group. Hence, the specification of the MIB modules (existing or not) necessary to provide such policy information is outside the scope of the present document, which deals only with the so-called binary authorization.

4.2.2 PAA-EP relation

A number of deployment options are envisaged within the PANA framework. See [I-D.ietf-pana-framework] for further details.

The SNMP framework [RFC3410] supports one-to-many, many-to-one, and many-to-many relationships between the SNMP managers (PAAs) and agents (EPs).

4.2.3 Secure Communication

SNMPv3 includes the User-based Security Model (USM, [RFC3414]), which provides 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 [RFC3410] for the security features provided by the SNMPv3 framework.

4.2.4 Notification of PaC presence

The 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 the PaC. The EP is the node that can detect such activity. In case they are separate, there needs to be an explicit message to prompt the PAA.

Such a presence notification is done by using the SNMP notification 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 the 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 the PAA and the 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 short 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 the PANA EP configuration:

IPSec Security Policy Database (SPD) MIB:
[I-D.ietf-ipsp-spd-mib] defines a MIB module for configuration of an IPSec Security Policy Database (SPD). No IPSec or IKE specific actions are defined within this document.

IPSec IKE Action MIB:
[I-D.ietf-ipsp-ikeaction-mib] defines a MIB module for configuration of an IKE action within the IPSec 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 EP enforces binary authorization by filtering data traffic on the basis of the Device Identifier (DI) of the PaC. 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 be either a IPv4/6 address or a link-layer address of a connected device. Do note also that a keying material might be provisioned. The particular case where access control is performed using IPSec is specified in [I-D.ietf-pana-ipsec]. The configuration aspects are detailed in Section 5.2.

The IPSec SPD MIB module (SPD-MIB) 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, 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 SPD-MIB are generic and simply bind a filter to an action. Filters provided within the SPD-MIB itself are numerous and fairly complete for most common packet filtering usage but externally

defined filters are supported.

Below are basic DI-based filters and static actions that are used -- together with the other SPD tables -- to enforce binary packet authorization at the EP:

-- Ipv4/v6 address-based filter:

For Ipv4/v6 address-based filters provisioning, the IPSec 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:

[I-D.ietf-pana-pana] says the Device-Id AVP (code 1025) is of Address Type [RFC3588]. The content for link-layer addresses is expected to be specified in specific documents that describe how IP operates over different link-layers. For instance, [RFC2464]. To this end, additional filters are designed in the present document. Section 7 defines a link-layer filter table, which test the L2 address (e.g. MAC address, port, DSL line) of a given packet.
Do note that the definition of this table does not assume the usage of any particular Link layer.

-- Static Actions:

The actions encapsulated within the SPD-MIB module are basic drop/accept actions. These are sufficient to perform EP general binary authorization enforcement at the EP.
When profile-based authorization information is provided to the EP, more advanced actions like classifiers, meters and schedulers might be configured by the PAA. This is out of the scope of the present document.

5.2 Network Layer Secure Access Control (IPSec)

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 PAA indicates the results of the authentication using the PANA-Bind-Request (PBR) 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:

1. PANA client (PaC) and PAA mutually authenticate each other using EAP methods that derive the AAA-Key [I-D.ietf-eap-keying].
2. PaC learns the IP address of the Enforcement point (EP) during the PANA exchange.
3. PaC learns that the network uses IPSec [RFC2401] for securing the link between PaC and EP during the PANA exchange (PBR message).
4. PaC configures an IP address address before the PANA protocol begins (the pre-PANA Address (PRPA), see [I-D.ietf-pana-pana]).

The IPSec IKE Action MIB module (IKEACTION-MIB) works within the framework of the IPSec 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 information before IKE phase 1 exchange begins between PaC and EP:

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 PRPA of the PaC:
An IP Header Filter of the SPD-MIB is used for configuring the SPD in a similar manner than what is described in Section 5.1.

The Key-Id and PANA session ID:
[I-D.ietf-pana-ipsec] states that Pac and EP should use the PANA session ID concatenated with the AAA-key as the value of the ID_KEY_ID in aggressive mode for establishing the phase 1 SA. Section 6 details usage examples that illustrate the way the IKEACTION-MIB is used for this purpose.

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 new notifications, which aims at satisfying this requirement. It re-uses existing notification variable objects pre-defined in the SPD-MIB.

These "New PaC" notifications (panaNewPacIPNotification and panaNewPaCL2Notification) are triggered when the the EP detects traffic coming from an unauthorized source.

If the traffic detected is an IP flow, the objects sent must include spdIPSourceType, spdIPSourceAddress, spdIPDestinationType, and spdIPDestinationAddress objects to indicate the packet source and destination of the packet that triggered the action. Additionally, the spdIPInterfaceType and spdIPInterfaceAddress 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-spd-mib] for further details.

If the traffic detected is Link-layer traffic, the objects sent must include the index of the interface which detected such traffic and potentially the L2 address source of the traffic. See Section 7 for further details.

6. EP Configuration Example

Below are usage examples of the IPSec modules in the PANA context.

6.1 General IP-based Access Control

Below is a usage example of the IPSec modules. In this example, we need to configure the SPD so that EP accepts IP packets coming from/going to the PaC.

The "EndPoint to Group" table is used to map policy (groupings) onto an endpoint (EP-ADDR is the IP address) where traffic is to pass by. Any policy group assigned to an endpoint is then used to control access to the traffic passing by it.

So far, we define below two policy groups at the EP interface ("EP-SPD-IN" and "EP-SPD-OUT").

```
spdEndpointToGroupTable.1 =
   spdEndGroupDirection = incoming;
   spdEndGroupIdentType = IPv4;
   spdEndGroupAddress   = EP-ADDR;
   spdEndGroupName      = "EP-SPD-IN";

spdEndpointToGroupTable.2 =
   spdEndGroupDirection = outgoing;
   spdEndGroupIdentType = IPv4;
   spdEndGroupAddress   = EP-ADDR;
   spdEndGroupName      = "EP-SPD-OUT";
```

Within each of the policy group defined above, we define a rule dedicated to the treatment of packets coming from/going to "PaC1" and the EP we are provisioning.

```
spdGroupContentsTable.2 =
   spdGroupContName          = "EP-SPD-IN";
   spdGroupContPriority      = 1;
   spdGroupContFilter        = spdIpHeaderFilterTable.1;
   spdGroupContComponentType = rule;
   spdGroupContComponentName = "EP-PaC1-IN";

spdGroupContentsTable.2 =
   spdGroupContName          = "EP-SPD-OUT";
   spdGroupContPriority      = 1;
   spdGroupContFilter        = spdIpHeaderFilterTable.2;
   spdGroupContComponentType = rule;
   spdGroupContComponentName = "EP-PaC1-OUT";
```

We define two filters in the "IP Header filter" table: one match IP packets coming from the PaC, the other match IP packets going to the PaC.

```
spdIpHeaderFilterTable.1 =
   spdIpHeadFiltName            = "PaC1-IP@ Filter SOURCE";
   spdIpHeadFiltType            = { sourceAddress ON };
   spdIpHeadFiltIPVersion       = v4;
   spdIpHeadFiltSrcAddressBegin = PaC1-IP@;
   spdIpHeadFiltSrcAddressEnd   = PaC1-IP@;

spdIpHeaderFilterTable.2 =
   spdIpHeadFiltName            = "PaC1-IP@ Filter DEST";
   spdIpHeadFiltType            = { destAddress ON };
   spdIpHeadFiltIPVersion       = v4;
   spdIpHeadFiltSrcAddressBegin = PaC1-IP@;
   spdIpHeadFiltSrcAddressEnd   = PaC1-IP@;
```

The "Rule Defininition" table links a rule with a given action in the SPD action MIB. E.g. the following entries links the two filters defined above with the "accept" action statically defined in the SPD MIB (spdStaticActions.3).

```
spdRuleDefinitionTable.1 =
   spdRuleDefName          = "PaC1-ACCEPT-IN";
   spdRuleDefDescription   = "Allow Incoming IP packets from PaC1";
   spdRuleDefFilter        = spdIpHeaderFilterTable.1;
   spdRuleDefFilterNegated = false (default);
   spdRuleDefAction        = spdStaticActions.3;

spdRuleDefinitionTable.2 =
   spdRuleDefName          = "PaC1-ACCEPT-OUT";
   spdRuleDefDescription   = "Allow Outgoing IP packets to PaC1";
   spdRuleDefFilter        = spdIpHeaderFilterTable.2;
   spdRuleDefFilterNegated = false (default);
   spdRuleDefAction        = spdStaticActions.3;
```

This means that any packet coming from/going to the PaC is now allowed to go through the EP (via EP-ADDR endpoint).

6.2 IPSec-based Access Control

In this section we consider the case when IPSec is used to control access at the IP level. In order to avoid many redundancies, the previous configuration set is still valid. See below a usage example of IKEACTION-MIB.

```
-- IKE Phase 1 configuration (agressive mode):
```

We define a rule in policy group "EP-SPD-IN" of the SPD MIB, using the "Group contents" table. This rule is dedicated to all IKE phase 1 traffic coming to the EP on this interface:

```
spdGroupContentsTable.1 =
   spdGroupContName          = "EP-SPD-IN";
   spdGroupContPriority      = 1;
   spdGroupContFilter        = ipiaStaticFilters.1;
   spdGroupContComponentType = sub-group;
   spdGroupContComponentName = "EP-IKE-Phase1-IN";
```

And within this IKE-specific policy sub-group we now specify the rule to apply for the IKE traffic coming from PaC1.

```
spdGroupContentsTable.2 =
   spdGroupContName          = "EP-IKE-Phase1-IN";
   spdGroupContPriority      = 1;
   spdGroupContFilter        = spdIpHeaderFilterTable.1;
   spdGroupContComponentType = rule;
   spdGroupContComponentName = "PaC1-IKE-RULE";
```

The spdIpHeaderFilterTable.1 entry has been defined in the previous seciton.

The "Rule Defininition" table links a rule with a given action in the IKE action MIB. This action will be triggereed upon reception at the EP of an IKE packet coming from PaC1.

```
spdRuleDefinitionTable.3 =
   spdRuleDefName          = "PaC1-IKE-RULE";
   spdRuleDefDescription   = "IPSec Access Control for PaC1";
   spdRuleDefFilter        = spdIpHeaderFilterTable.1;
   spdRuleDefFilterNegated = false (default);
   spdRuleDefAction        = spdIkeActionTable.1;
```

The "IKE action" entry below specifies the main parameters for the IKE exchanges.

```
ipiaIkeActionTable.1 =
   ipiaIkeActName                = "PaC1-IKE";
   ipiaIkeActParametersName      = "SA-PaC1";
   ipiaIkeActThresholdDerivedKeys = 100 (default);
   ipiaIkeActExchangeMode        = aggressive;
   ipiaIkeActAgressiveModeGroupId = xxx [Diffie-Hellman values];
   ipiaIkeActIdentityType        = id_Key_Id;
   ipiaIkeActIdentityContext     = "PANA";
   ipiaIkeActPeerName            = "PaC1";
```

```
   ipiaSaNegotiationParametersTable.1 =
      ipiaSaNegParamName              = "SA-PaC1";
      ipiaSaNegParamMinLifetimeSecs   = xxx;
      ipiaSaNegParamMinLifetimeKB     = xxx;
      ipiaSaNegParamRefreshThreshSecs = xxx;
      ipiaSaNegParamRefreshThresholdKB = xxx;
      ipiaSaNegParamIdleDurationSecs  = xxx;
```

The "Peer Identity" table specifically informs the EP on the value of the idKeyId to use in IKE messages with PaC1:

```
   ipiaPeerIdentityFilterTable.1 =
      ipiaPeerIdFiltName          = "PaC1";
      ipiaPeerIdFiltIdentityType  = id_key_id;
      ipiaPeerIdFiltIdentityValue = "PANA-Session-Id|PANA-Key-Id";
```

The following entry links a given identity (PaC1) with an entry in the "Credentials" table.

```
   ipiaIkeIdentityTable.1 =
      spdEndGroupIdentType      = IPv4;
      spdEndGroupAddress        = EP-ADDR;
      ipiaIkeActIdentityType    = id_key_id;
      ipiaIkeActIdentityContext = PANA;
      ipiaIkeIdCredentialName   = "PaC1-PSK";
```

Finally the pre-shared key derivated at the PAA is set here:

```
   ipiaCredentialFilterTable.1 =
      ipiaCredFiltName            = "PaC1-PSK";
      ipiaCredFiltCredentialType  = sharedSecret;
      ipiaCredFiltMatchFieldName  = none;
      ipiaCredFiltMatchFieldValue = "PSK-from-PAA";
```

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-EP interface requirements.

7.1 PANA MIB Overview

- Link-Layer filter table
- New PaC notification

7.2 PANA-specific objects definition

```
        PANA-EP-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

            InterfaceIndex
            FROM IF-MIB

            spdMIB, spdActionExecuted, spdIPInterfaceType,
spdIPInterfaceAddress,
            spdIPSourceType, spdIPSourceAddress, spdIPDestinationType,
            spdIPDestinationAddress, spdPacketDirection
            FROM IPSEC-SPD-MIB;

            -- Module identity
            --

            panaMIB MODULE-IDENTITY
            LAST-UPDATED
            "200410220000Z"           -- 22 October 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
            "200410220000Z"            -- 22 October 2004
            DESCRIPTION
            "Version 02, draft-ietf-pana-snmp-02.txt"
            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  99999999 } -- 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 Link-layer Filter Table
--


panaL2FilterTable OBJECT-TYPE
SYNTAX      SEQUENCE OF PanaL2FilterEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
"Link-layer filter definitions."
::= { panaConfigObjects 1 }

panaL2FilterEntry OBJECT-TYPE
SYNTAX      PanaL2FilterEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
"An entry in the Link-layer filter table."
INDEX       { panaL2FiltEpIfIndex }
::= { panaL2FilterTable 1 }

PanaL2FilterEntry ::= SEQUENCE {
    panaL2FiltEpIfIndex             InterfaceIndex,
panaL2FiltAddr              PhysAddress,
panaL2FiltLastChanged       TimeStamp,
panaL2FiltStorageType       StorageType,
panaL2FiltRowStatus         RowStatus
}

panaL2FiltEpIfIndex OBJECT-TYPE
SYNTAX         InterfaceIndex
MAX-ACCESS     read-create
STATUS         current
DESCRIPTION
"The index identifying the EP interface where the filter
    policy must be enforced on."
::= { panaL2FilterEntry 1 }

panaL2FiltAddr OBJECT-TYPE
SYNTAX         PhysAddress
MAX-ACCESS     read-create
STATUS         current
DESCRIPTION
"The authorized device Link-layer address (DI). For
```

```
            example, for a 802.x interface, this object normally
            contains a MAC address. For interfaces which do not have such
                an address (e.g., a serial line), this object should contain
                an octet string of zero length."
            ::= { panaL2FilterEntry 2 }

            panaL2FiltLastChanged 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."
            ::= { panaL2FilterEntry 3 }

            panaL2FiltStorageType 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 }
            ::= { panaL2FilterEntry 4 }

            panaL2FiltRowStatus OBJECT-TYPE
            SYNTAX      RowStatus
            MAX-ACCESS  read-create
            STATUS      current
            DESCRIPTION
            "This object indicates the conceptual status of this row."
            ::= { panaL2FilterEntry 5 }


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

            panaNotificationVariables OBJECT IDENTIFIER ::=
            { panaNotificationObjects 1 }

            panaNotifications OBJECT IDENTIFIER ::=
            { panaNotificationObjects 0 }
```

```
panaEpIfIndex OBJECT-TYPE
SYNTAX      InterfaceIndex
MAX-ACCESS  accessible-for-notify
STATUS      current
DESCRIPTION
"Contains the interface index on which the packet triggered
the notification in question."
::= { panaNotificationVariables 1 }

panaL2SourceAddress OBJECT-TYPE
SYNTAX      PhysAddress
MAX-ACCESS  accessible-for-notify
STATUS      current
DESCRIPTION
"Contains the source Link layer address of the packet which
triggered the notification in question. For
example, for a 802.x frame, this object normally
contains a MAC address. For interfaces which do not have such
an address (e.g., a serial line), this object should contain
an octet string of zero length. "
::= { panaNotificationVariables 2 }


panaNewPacIPNotification NOTIFICATION-TYPE
OBJECTS {
  spdActionExecuted,
  spdIPInterfaceType,
  spdIPInterfaceAddress,
  spdIPSourceType,
  spdIPSourceAddress,
  spdIPDestinationType,
  spdIPDestinationAddress}
STATUS  current
DESCRIPTION
"Notification that EP detected IP traffic coming from an
unauthorized source."
::= { panaNotifications 1 }


panaNewPacL2Notification NOTIFICATION-TYPE
OBJECTS {
  spdActionExecuted,
  panaEpIfIndex,
  panaL2SourceAddress
}
STATUS  current
DESCRIPTION
"Notification that EP detected L2 traffic coming from an
```

```
            unauthorized source. "
            ::= { panaNotifications 2 }

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

            panaGroups OBJECT IDENTIFIER
            ::= { panaConformanceObjects 1 }
            panaCompliances OBJECT IDENTIFIER
            ::= { panaConformanceObjects 2 }


            --
            -- Compliance Groups Definitions
            --

            panaL2FilterGroup OBJECT-GROUP
            OBJECTS {
              panaL2FiltAddr,
              panaL2FiltLastChanged,
              panaL2FiltStorageType,
              panaL2FiltRowStatus }
            STATUS current
            DESCRIPTION
            "The Link-layer Filter Group."
            ::= { panaGroups 1 }

            panaNewPacL2NotificationObjectsGroup OBJECT-GROUP
            OBJECTS {
              panaEpIfIndex,
              panaL2SourceAddress}
            STATUS current
            DESCRIPTION
            "PaC Presence Notification Objects Group."
            ::= { panaGroups 2 }

            panaNewPacNotificationGroup NOTIFICATION-GROUP
            NOTIFICATIONS {
              panaNewPacIPNotification,
              panaNewPacL2Notification}
            STATUS current
            DESCRIPTION
            "PaC Presence Notification Group."
            ::= { panaGroups 3 }
```

```
        --
        -- Compliance statements
        --

        panaFilterCompliance MODULE-COMPLIANCE
        STATUS      current
        DESCRIPTION
        "The compliance statement for SNMP entities that support
        PANA DI-based filtering."

        MODULE -- This Module

        MANDATORY-GROUPS { panaL2FilterGroup }

        OBJECT      panaL2FiltRowStatus
        SYNTAX      RowStatus { active(1), createAndGo(4), destroy(6) }
        DESCRIPTION
        "Support of the values notInService(2), notReady(3),
        and createAndWait(5) is not required."

        OBJECT      panaL2FiltLastChanged
        MIN-ACCESS  not-accessible
        DESCRIPTION
        "This object not required for compliance."


        MODULE IPSEC-SPD-MIB

        MANDATORY-GROUPS {
          spdEndpointGroup,
          spdGroupContentsGroup,
          spdRuleDefinitionGroup,
          spdIPHeaderFilterGroup,
          spdStaticFilterGroup,
          spdStaticActionGroup }

        GROUP spdIpsecSystemPolicyNameGroup
        DESCRIPTION
        "This group is mandatory for IPsec Policy
        implementations which support a system policy group
        name."

        GROUP spdCompoundFilterGroup
        DESCRIPTION
        "This group is mandatory for IPsec Policy
        implementations which support compound filters."

        GROUP  spdCompoundActionGroup
```

```
            DESCRIPTION
            "This group is mandatory for IPsec Policy
            implementations which support compound actions."

            OBJECT      spdEndGroupRowStatus
            SYNTAX      RowStatus { active(1), createAndGo(4), destroy(6) }
            DESCRIPTION
            "Support of the values notInService(2), notReady(3),
            and createAndWait(5) is not required."

            OBJECT      spdEndGroupLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
            "This object not required for compliance."

            OBJECT      spdGroupContComponentType
            SYNTAX      INTEGER { rule(2) }
            DESCRIPTION
            "Support of the value group(1) is only required for
            implementations which support Policy Groups within
            Policy Groups."

            OBJECT      spdGroupContRowStatus
            SYNTAX      RowStatus { active(1), createAndGo(4), destroy(6) }
            DESCRIPTION
            "Support of the values notInService(2), notReady(3),
            and createAndWait(5) is not required."

            OBJECT      spdGroupContLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
            "This object not required for compliance."

            OBJECT      spdRuleDefRowStatus
            SYNTAX      RowStatus { active(1), createAndGo(4), destroy(6) }
            DESCRIPTION
            "Support of the values notInService(2), notReady(3),
            and createAndWait(5) is not required."

            OBJECT      spdRuleDefLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
            "This object not required for compliance."

            OBJECT      spdCompFiltRowStatus
            SYNTAX      RowStatus { active(1), createAndGo(4), destroy(6) }
            DESCRIPTION
            "Support of the values notInService(2), notReady(3),
```

```
            and createAndWait(5) is not required."

            OBJECT      spdCompFiltLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
            "This object not required for compliance."

            OBJECT      spdSubFiltRowStatus
            SYNTAX      RowStatus { active(1), createAndGo(4), destroy(6) }
            DESCRIPTION
            "Support of the values notInService(2), notReady(3),
            and createAndWait(5) is not required."

            OBJECT      spdSubFiltLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
            "This object not required for compliance."

            OBJECT      spdIpHeadFiltIPVersion
            SYNTAX      InetAddressType { ipv4(1), ipv6(2) }
            DESCRIPTION
            "Only the ipv4 and ipv6 values make sense for this
            object."

            OBJECT      spdIpHeadFiltRowStatus
            SYNTAX      RowStatus { active(1), createAndGo(4), destroy(6) }
            DESCRIPTION
            "Support of the values notInService(2), notReady(3),
            and createAndWait(5) is not required."

            OBJECT      spdIpHeadFiltLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
            "This object not required for compliance."

            OBJECT      spdCompActRowStatus
            SYNTAX      RowStatus { active(1), createAndGo(4), destroy(6) }
            DESCRIPTION
            "Support of the values notInService(2), notReady(3),
            and createAndWait(5) is not required."

            OBJECT      spdCompActLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
            "This object not required for compliance."

            OBJECT      spdSubActRowStatus
            SYNTAX      RowStatus { active(1), createAndGo(4), destroy(6) }
```

```
            DESCRIPTION
            "Support of the values notInService(2), notReady(3),
            and createAndWait(5) is not required."

            OBJECT      spdSubActLastChanged
            MIN-ACCESS  not-accessible
            DESCRIPTION
            "This object not required for compliance."

            ::= { panaCompliances 1 }

            panaNewPacNotificationCompliance MODULE-COMPLIANCE
            STATUS      current
            DESCRIPTION
            "The compliance statement for SNMP entities that support
            new PaC presence Notification."

            MODULE -- This Module

            MANDATORY-GROUPS {
              panaNewPacL2NotificationObjectsGroup,
              panaNewPacNotificationGroup
            }

            MODULE IPSEC-SPD-MIB

            MANDATORY-GROUPS { spdActionLoggingObjectGroup }

            ::= { panaCompliances 2 }

            END
```

8. Open Issues

8.1 Security Issue on PaC presence notification

It has been reported that the PANA-specific notification of PaC presence could be used to overwhelm an SNMP application, thus creating a DoS attack on the management of the network. A attacker could detect that such notifications are sent by multiple devices, and the attacker could deliberately send lots of traffic through the devices.

8.2 MIB usage example

The MIB usage example (Section 6) needs to be further developped with the support of the IPSP working group.

8.3 Link-layer protection support

[I-D.ietf-pana-framework] envisages the case, where enabling link-layer ciphering (e.g. [802.11i]) or network-layer ciphering might rely on PANA authentication. The user and network then have to make sure an appropriate EAP method that can generate required keying materials is used. Once the keying material is available, it needs to be provided to the EP(s) for use with ciphering.

Network-layer ciphering configuration, i.e., IPsec, including IKE configuration is fully supported in the present document.

However link-layer ciphers control is not supported yet. The PANA working group must define the L2 techniques supported (e.g.[802.11i]) for realizing this feature and the present document should take it into account.

9. Security Considerations

The MIB defined in the present document relates to a system which will provide network access. As such, improper manipulation of the objects represented by this MIB may result in denial of service to a large number of end-users. In addition, manipulation of the panaL2FilterTable and spdIpHeaderFilterTable may allow an end-user to gain network access, spoof their IP addresses, change the authorized device identifiers, or affect other end-users in either a positive or negative manner.

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:

- The use of panaIPL2FilterTable to specify which Link-layer addresses are authorized to access the network is considered to be only limited protection and does not protect against attacks which spoof the management station's IP address. The use of SNMPv3 security is mandated. Specifically, SNMPv3 VACM and USM MUST be used with any v3 agent which implements this MIB.

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.

10. Acknowledgements

This document originaly 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 and Olivier Marce for their grateful help during the edition of this document.

11. References

11.1 Normative References

[I-D.ietf-pana-pana]
Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H. and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-06 (work in progress), October 2004.

[I-D.ietf-pana-requirements]
Yegin, A. and Y. Ohba, "Protocol for Carrying Authentication for Network Access (PANA)Requirements", draft-ietf-pana-requirements-09 (work in progress), August 2004.

[I-D.ietf-pana-ipsec]
Parthasarathy, M., "PANA enabling IPsec based Access Control", draft-ietf-pana-ipsec-04 (work in progress), September 2004.

[I-D.ietf-pana-threats-eval]
Parthasarathy, M., "Protocol for Carrying Authentication and Network Access Threat Analysis and Security Requirements", draft-ietf-pana-threats-eval-07 (work in progress), August 2004.

[I-D.ietf-pana-framework]
Jayaraman, P., "PANA Framework", draft-ietf-pana-framework-02 (work in progress), September 2004.

[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-spd-mib]
Hardaker, W., "IPsec Security Policy Database Configuration MIB", draft-ietf-ipsp-spd-mib-01 (work in progress), October 2004.

[I-D.ietf-ipsp-ikeaction-mib]
Hardaker, W., "IPsec Security Policy IKE Action MIB", draft-ietf-ipsp-ikeaction-mib-01 (work in progress), October 2004.

[I-D.ietf-aaa-diameter-cc]
Mattila, L., Koskinen, J., Stura, M., Loughney, J. and H.

Hakala, "Diameter Credit-control Application", draft-ietf-aaa-diameter-cc-06 (work in progress), August 2004.

[I-D.ietf-aaa-eap] Eronen, P., Hiller, T. and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-09 (work in progress), August 2004.

[I-D.ietf-eap-keying] Aboba, B., "Extensible Authentication Protocol (EAP) Key Management Framework", draft-ietf-eap-keying-03 (work in progress), July 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.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[802.11i] IEEE P802, "Wireless MAC and PHY specifications, MAC security enhancements", IEEE 802.11i, July 2004.

11.2 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.

Authors' Addresses

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

EMail: yacine.el_mghazli@alcatel.fr

Yoshihiro Ohba
Toshiba America Research, Inc.
1, Telcordia Drive
Piscataway, NJ 08854
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

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.