PANA WG
Internet Draft
Category: Informational
Document:
draft-yacine-pana-paa2ep-prot-eval-00.txt
Expires: April 2004

Yacine El Mghazli
Alcatel

October 2003

PANA
PAA-EP protocol considerations

Status of this Memo

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 will identify a (preferably existing) protocol solution that allows the PAA to deliver the authorization information to one or more EPs when the PAA is separated from EPs.

The present document aims at discussing the various protocol solutions available and identifying one, which better fits the whole PANA picture.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

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), or on another subnet in the access domain (e.g., gateway to the Internet, depending on the network architecture). When the PAA and the EP(s) are separated, there needs to be another transport for client provisioning. This transport is needed to create access

control lists to allow authenticated and authorized clients' traffic through the EPs. PANA Working Group will preferably identify an existing protocol solution that allows the PAA to deliver the authorization information to one or more EPs when the PAA is separated from EPs.

2.1. Document History

This document is based on an individual submission [PAA-EP-REQ], which was used as a work basis for discussions around the PAA-EP interface issues within the PANA working group.

2.2. Scope

First, section 3 details the requirements that the PAA-EP protocol must satisfy in order to meet the needs of PANA when the PAA is separated from EP(s). These are specified in [PANAREQ].

The following section 4 presents some functions the PAA-EP protocol should offer, which have already been discussed on the mailing list. These are not mandatory at all, but one can consider them as "nice-to-have".

Then, section 5 discusses the PANA framework assumptions that are being made within the PANA working group. It deals with crucial issues around the authentication process, when the PAA is separated from EP(s).

Finally, the last section 6 introduces and compares the various protocol solutions available against the identified requirements for the PAA-EP interface.

A compliancy summary of each of the proposed solutions is provided.

3. PAA-EP Protocol Requirements

3.1. Push model

PAA must be able to "push" the provisioning information down to EPs, without any of the EPs "pulling" it. Since PANA exchange takes place between PaC and PAA, EPs are unlikely to be aware of it.

EP provisioning takes place once the PaC is authenticated and authorized, hence the event triggering the EP configuration takes place at the PAA. Then it's straightforward to initiate the exchange at the PAA.

3.2. One-to-many PAA-EP relation

One PAA have to communicate with several EPs once a PaC is authenticated. The PAA-EP protocol must be able to handle this 1:n communication.

3.3. Provisioned Data

The protocol must carry DI-based filters and cryptographic keys.

3.4. Re-use of an existing protocol

This work hopefully will not involve any new protocol design, it may involve definition of new AVPs for existing protocols. The PANA working group should try to re-use one of the many protocols around to do this.

3.5. General Security Requirements

The PAA-EP protocol must provide for message authentication, confidentiality, and integrity.

The PAA-EP protocol must define mechanisms to mitigate attacks on the control messages.

4. Nice-to-have functions

4.1. Pull model

The PUSH model (PAA-initiated configuration) should be used for the communication between PAA and EP.

However, the PULL model (EP-initiated configuration) might be supported for the following purposes:

1. EP Registration/Recovery:

   When a EP is newly connected to the network, it needs to register itself to the PAA.

   In a similar manner, when an EP crashes and comes up again, it needs to re-connect its PAA. In general, when a failure is detected, the EP must try to reconnect to the remote PAA or attempt to connect to PAA.

2. Traffic-driven configuration (a.k.a. new PAC notification):

   As stated in [PANA], PaC may also choose to start sending packets before getting authenticated. In that case, the network should detect this and send an unsolicited PANA_start message to PaC. EP is the node that can detect such activity. If EP and PAA are co-located, then an internal mechanism (e.g. API) between the EP module and the PAA module on the same host can prompt PAA to start PANA. In case they are separate, there needs an explicit message to prompt PAA.

   Upon detecting the need to authenticate a client, EP can send a trigger message to the PAA on behalf of the PaC. This can be one of the messages provided by the PAA-EP protocol, or, in the absence of such a facility, PAC_discovery can be used as well. This message MUST carry the device identifier of the PaC. So that, PAA can send the unsolicited PANA_start message directly to the PaC.

4.2. Inactive peer detection

The protocol used between PAA and EP should be able to detect inactive peer within an appropriate time period.

This can be achieved by having both the EP and remote PAA constantly verify their connection to each other via keep-alive messages: a heartbeat in fact.

4.3. Stateful approach

The protocol must allow to maintain some states in the PAA in order for an EP that went down and came back up, or an EP that is being introduced in the network to (re-)synchronize with the PAA.

In general terms, the PAA-EP protocol needs to support the stateful model between the PAA and the EP(s) and some other mechanism for the EP to learn the policies currently in effect on that access network.

4.4. Accounting/Feedback from the EPs

The PAA must have an efficient way to to get the accounting information of PaC from EP since the PAA may be a client of the AAA backend infrastructure.

5. PANA framework Assumptions/Issues

5.1. Multiple PAAs

Multiple PAAs may be used for redundancy, load sharing, distributed authentication, or other purposes:

a) Redundancy is the case where one or more PAAs are prepared to take over if an active PAA fails.

b) Load sharing is the case where two or more PAAs are concurrently active and any PaC that can be authenticated by one of the PAAs can also be authenticated by any of the other PAA.

For both redundancy and load sharing, the PAAs involved are equivalently capable. The only difference between these two cases a) and b) is in terms of how many active PAAs there are.

c) Distributed authentication is the case where two or more PAAs are concurrently active but certain PANA requests using PANA can only be serviced by certain PAAs. The logical separation can be based on:

. Topology: One given PAA is in charge of authenticating a pool of PaCs belonging to the same topological area.

. The ISP: One given PAA is in charge of authenticating the PaCs clients to a given ISP. Then it forwards the PANA requests based on the NAI or other identifier.

. Etc.

Clearly stating the motivation for having multiples PAAs authenticating PaCs and provisioning EPs in an access network has direct consequences on both PAA-PaC and PAA-EP relations.

5.1.1. PAA-PaC relation assumption

According to [PANA] (section "Discovery and Initial Handshake Phase"), "There can be multiple PAAs on the link. The result does not depend on which PAA PaC chooses. By default PaC chooses the PAA that sent the first response."
Then, it is straightforward that the assumption that is being made here is that two or more PAAs are concurrently active and any PaC that can be authenticated by one of the PAAs can also be authenticated by any of the other PAAs. We are clearly in the case where the PaCs load is shared between the multiple PAAs (b).

Do note that discovery issues are raised with allowing muliples PAAs to authenticate the various PaCs. [PANA] solves the problem simply stating that the chosen PAA corresponds to the first response. It is consistent with case b).

From the PaC perspective, multiple PAAs are concurrently active and any PaC that can be authenticated by one of the PAAs can also be authenticated by any of the other PAA.

5.1.2. PAA-EP relation issue

In a similar manner, it is crucial for identifying the various PAA-EP protocol requirements to clearly identify the context for having multiples PAAs with respect to the EPs provisioning.

One PAA have to communicate with several EPs once a PaC is authenticated is a requirement for the PAA-EP protocol (see section 3.2). In the case where there is a single PAA, the assumption being made is that the PAA will provision all the EPs. However, it remains an issue in case we have multiple PAAs.

When multiple PAAs authenticates the PaCs, a given PAA can either:

a) Redundancy:
provision all the EPs of the underlying access network and each EP has a single active PAA. A back-up PAA is ready to take over if the first one fails.

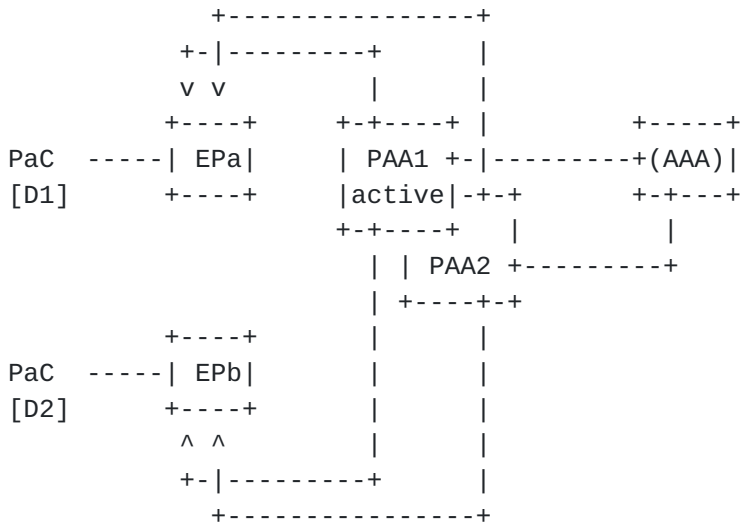

Figure 1. One single active PAA provisioning all the EPs

b) Load sharing:
provision all the EPs of the underlying access network and each EP can be controlled by another active PAA.

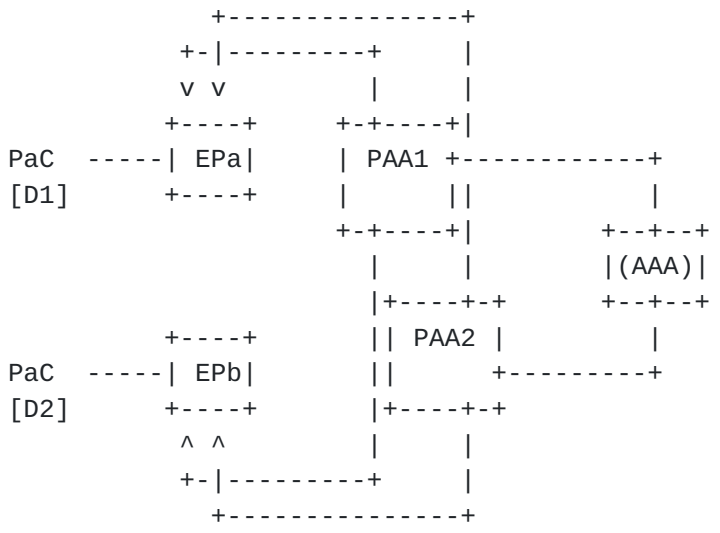

Figure 2. Multiple active PAAs provisioning all the EPs

Such a deployment option can prove to be very well adapted to situations where there are multiple PAAs belonging to multiple ISPs. A given PAA belonging to a certain ISP can configure all the EPs of the Access Network.

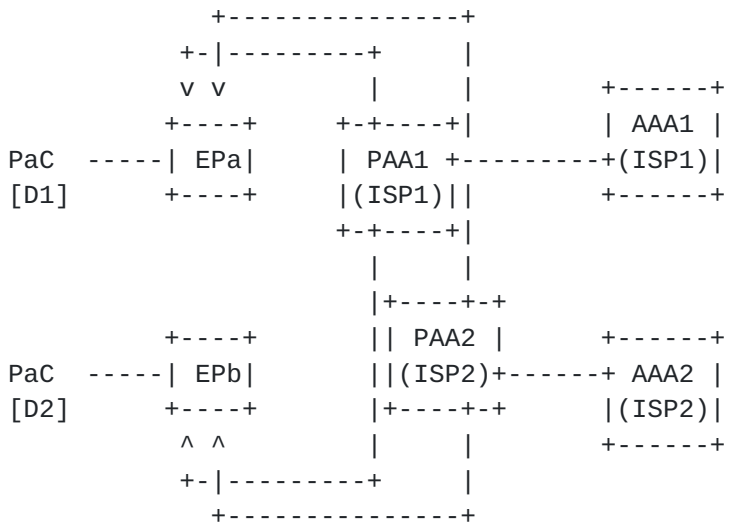

Figure 3. Multiple PAAs belonging to multiple ISPs

c) Distributed control:
provision a pool of EPs within a given area. The pool can be identified based on topological criteria for instance.

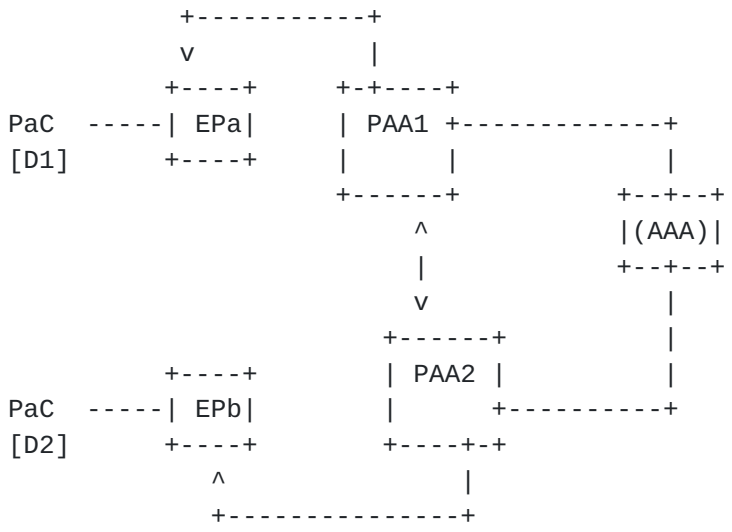

Figure 4. Distributed control of the EPs

Such a deployment option can prove to be very well adapted to Access Network with a large number of EP nodes. In such a situation, a single PAA cannot deal with so many EPs, then the NAP can use a given PAA for a given pool of EPs. Do note that this certainly imply inter-PAA communication for synchronization purposes (see next section).

Another reason for using this deployment scheme would be to configure only the EPs concerned by the traffic of the authenticated PaC. But this brings up other issues (e.g. mobility case) and it's out of the scope of the present document.

The choice between these various deployment options is motivated by PANA-specific considerations. Typically, these can be:

. Scalability: How many EPs are managed by the PAA(s)?

. Symmetry: Does all the EPs need to be configured with the same rules?

. Dynamicity: How often does the EP configuration has to be refreshed?

5.2. Inter-PAAs communication

When multiple PAAs are employed, their internal organization is considered an implementation issue that is beyond the scope of PANA. PAAs are wholly responsible for coordinating amongst themselves to provide consistency and synchronization. However, PANA does not define the implementation or protocols used between PAAs, nor does it define how to distribute functionality among PAAs. Nevertheless, PANA will support mechanisms for PAA redundancy or fail over, and it is expected that vendors will provide redundancy or fail over solutions within the PANA framework.

6. PAA-EP Protocol Evaluation

The previous sections described the functions required or simply wished for the PAA-to-EP communication. Do note that the so-called requirements are general enough to allow a large amount of possible solutions for this interface, namely: SNMP, COPS-PR, Diameter, Radius, ForCES, NetConf, directory-based solutions, etc.

However, the PANA working group does not wish to choose a disruptive solution for this PAA-EP management interface. In a similar manner, the PANA working group does not wish to bet on premature solutions, whose design is on-going. Hence, the working group will consider the classical configuration protocols available and consequently, only the following protocols were mentioned for final consideration:

. SNMP [SNMP]
. COPS-PR [COPS-PR]

The following sections provide an overview of each of these protocols and its applicability to the PAA-EP interface.

6.1. SNMP

This section provides a general statement with regards to the applicability of SNMP as the PAA-EP protocol. This evaluation 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.

6.1.1. SNMP 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 RFC2571, 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.

6.1.2. Compliancy of SNMP against the PAA-EP reqs

All the requirements as described in section 3 are fully supported by SNMP:

a) The protocol must carry DI and keys
   Already defined MIBs (for filters, IPSec policy, etc.) can be re-used. if not sufficient, PANA-specific MIBs can be designed.

b) There might be multiple EPs per PAA.
   An SNMP manager (PAA) can communicate simultaneously with several agents (EPs).

c) The protocol must be secured
   SNMPv3 includes the User-based Security Model (USM, [RFC2574]), 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.

d) The protocol may allow the EP to notify a new PaC

Using SMI notifications

6.1.3.
Compliancy of SNMP against the PANA framework

When multiple PAAs, since SNMP allow multiple managers (PAAs) per agent (EP), it fits better deployments where the multiple PAAs are configuring all the access network EPs (section 5.1.2, option b, load sharing). SNMP is the very usual Internet Management protocol.

SNMP does not provide heartbeat mechanisms, nor a stateful model (see section 2), but this is not required by PANA.

6.2. COPS-PR

The Common Open Policy Service (COPS) [RFC2748] protocol has been extended to provision configuration information on devices (COPS-PR) [RFC3084]. Work is underway to define data definitions for specific services such as Differentiated Services (DiffServ).

6.2.1.
COPS General Applicability

IETF has defined the COPS protocol [COPS] as a scalable protocol that allows policy servers (PDPs) to communicate policy decisions to network devices (PEPs). COPS was designed to support multiple types of policy clients.

The main characteristics of the COPS base protocol include the following:

1. The protocol employs a client/server model. The PEP sends requests, updates, and deletions to the remote PDP and the PDP returns decisions back to the PEP.

2. The protocol uses TCP as its transport protocol for reliable exchange of messages between policy clients and a server.

3. The protocol is extensible in that it is designed to leverage self-identifying objects and can support diverse client specific information without requiring modification of the COPS protocol.

4. The protocol was created for the general administration, configuration, and enforcement of policies.

5. COPS provides message level security for authentication, replay protection, and message integrity. COPS can make use of

existing protocols for security such as IPSEC or TLS to authenticate and secure the channel between the PEP and the PDP.

6. The protocol is stateful in two main aspects:
   a. Request/Decision state is shared and kept synchronized in a transactional manner between client and server. Requests from the client PEP are installed or remembered by the remote PDP until they are explicitly deleted by the PEP. At the same time, Decisions from the remote PDP can be generated asynchronously at any time for a currently installed request state.
   b. State from various events (Request/Decision pairs) may be inter-associated. The server may respond to new queries differently because of previously installed, related Request/Decision state(s).

7. The protocol is also stateful in that it allows the server to push configuration information to the client, and then allows the server to remove such state from the client when it is no longer applicable.

6.2.2. COPS extension for provisioning (COPS-PR)

In COPS-PR, the PDP may proactively provision the PEP reacting to external events, such as successful client authentication. This model is also known as the push/configuration model. Provisioning may be performed in bulk (e.g., entire EP configuration) or in portions (e.g., updating a filter).

The COPS-PR specification [COPS-PR] is independent of the type of policy being provisioned (QoS, Security, etc.). Rather, it focuses on the mechanisms and conventions used to communicate provisioned information between the PDP and its PEPs. The data model assumed in [COPS-PR] is based on the concept of Policy Information Bases (PIBs) that define the policy data. There may be one or more PIBs for given area of policy and different areas of policy may have different sets of PIBs.

COPS-PR has been designed within a framework that is optimized for efficiently provisioning policies across devices:

. First, COPS-PR allows for efficient transport of attributes, large atomic transactions of data, and efficient and flexible error reporting.

. Second, as it has a single connection between the policy client

and server per area of policy control identified by a COPS

Client-Type, it guarantees only one server updates a particular policy configuration at any given time. Such a policy configuration is effectively locked, even from local console configuration, while the PEP is connected to a PDP via COPS. COPS uses reliable TCP transport and, thus, uses a state sharing/synchronization mechanism and exchanges differential updates only. If either the server or client are rebooted (or restarted) the other would know about it quickly.

. Last, it is defined as a real-time event-driven communications mechanism, never requiring polling between the PEP and PDP.

6.2.3. Compliancy of COPS-PR against the PAA-EP reqs

All the requirements as described in section 3 are fully supported by COPS-PR:

a) The protocol must carry DI-based filters and keys:
Already defined PIBs (for filters, IPSec policy, etc.) can be re-used. if not sufficient, PANA-specific PIBs can be designed.

b) There might be multiple EPs per PAA:
COPS-PR PDPs (PAAs) are designed to communicate with several PEPs (EPs).

c) The protocol must be secured:
COPS-PR has built-in message level security for authentication, replay protection, and message integrity. COPS-PR can also use TLS or IPSec, thus reusing existing security mechanisms that have interoperated in the markets.

d) The protocol may allow the EP to notify a new PaC:
COPS-PR outsourcing allowed (3GPP-like)

6.2.4. Compliancy of COPS-PR against the PANA framework

When multiple PAAs, since the COPS-PR framework allow only a single PDP (PAA) to configure a given PEP (EP), it fits better deployments where the multiple PAAs are configuring pools of EPs (section 5.1.2, option c, distributed control).

COPS-PR naturally provides heartbeat mechanisms, a stateful model, accounting facilities and nicely supports dynamic configuration (see section 2), but this is not required by PANA.

A little more detailed information can be found in [COPS-PANA].

6.3. IAB notice on COPS-PR and PIBs

On the one hand, purely technically speaking, when compared to both the whished (section 4) and required (section 3) functions, COPS-PR seems to offer a slightly better solution for the EP configuration.

On the other hand, [RFC3535] provides an overview of a workshop held recently by the IAB on Network Management. In the recommendations section, one can read the following:

"2. The workshop had rough consensus from the protocol developers that the IETF should not spend resources on COPS-PR development. So far, the operators have only very limited experience with COPS-PR. In general, however, they felt that further development of COPS-PR might be a waste of resources as they assume that COPS-PR does not really address their requirements.

3. The workshop had rough consensus from the protocol developers that the IETF should not spend resources on SPPI PIB definitions. The operators had rough consensus that they do not care about SPPI PIBs."

7. Conclusion

The main output of this evaluation paper is that the PANA requirements for the PAA-EP interface are soft enough to allow almost any of the protocol solutions available. Nevertheless, the PANA working group restrict its choice to the 'classical' and available device configuration protocols, namely SNMP and COPS-PR.

Moreover and according the operators will (via the IAB recommendations), today COPS-PR is not promised to a nice future. It could prove to be hazardous to bet on this protocol, however efficient it is. In addition, COPS-PR is maybe too heavy for small configuration sets like those needed in PANA.

Hence, since the PAA-EP requirements are well validated by SNMP, it seems better for the PANA working group to mandate this latest solution and take advantage of its widely deployed framework.

Security Considerations

See section 3.5

Acknowledgements

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

References

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

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

[PANAREQ] R. Penno, et al., "Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology" (draft-ietf-pana-requirements-07.txt).

[RADIUS] C. Rigney et. al, "Remote Authentication Dial In User Service", RFC2865, June 2000.

[COPS-PR] K. Chan, D. Durham, S. Gai, S. Herzog, K. McCloghrie, F. Reichmeyer, J. Seligson, A. Smith, R. Yavatkar, "COPS Usage for Policy Provisioning,", RFC 3084, March 2001

[COPS] Boyle, J., Cohen, R., Durham, D., Herzog, S., Rajan, R., and A. Sastry, "The COPS (Common Open Policy Service) Protocol" RFC 2748, January 2000.

[PANA] D. Forsberg, Y. Ohba, B. Pati, H. Tschofenig, A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)"(draft-ietf-pana-pana-01.txt).

[DIAMETER] P. Calhoun, J. Arkko, E. Guttman, G. Zorn, J. Loughney, "Diameter Base Protocol" (draft-ietf-aaa-diameter-15.txt).

[PAA-EP-REQ] Y. El Mghazli , "PANA PAA-EP Protocol Requirements" (draft-yacine-pana-paa-ep-reqs-00.txt).

[COPS-PANA] Y. El Mghazli, " Enforcement Point(s) Provisioning and Accounting using COPS-PR" (draft-yacine-pana-cops-ep-00.txt).

Author's Addresses

Yacine El Mghazli
Alcatel
Route de Nozay
91460 Marcoussis cedex
Phone: +33 (0)1 69 63 41 87
Email: yacine.el_mghazli@alcatel.fr

Full Copyright Statement