PANA Working Group
INTERNET-DRAFT
Date: October 2002
Expires: April 2003

Reinaldo Penno, Editor
Alper E. Yegin
Yoshihiro Ohba
George Tsirtsis
Cliff Wang

Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology

<draft-ietf-pana-requirements-04.txt>

Status of this Memo

Abstract

It is expected that future IP devices will have a variety of access technologies to gain network connectivity. Currently there are access-specific mechanisms for providing client information to the network for authentication and authorization purposes. In addition to being limited to specific access media (e.g., 802.1x for IEEE 802 links), some of these protocols are limited to specific network topologies (e.g., PPP for point-to-point links). The goal of the PANA is to provide a layer two agnostic and IPv4/IPv6 compatible client-server protocol that allows a host to be authenticated for network access. The protocol will run between a client's device and an agent device in the network where the agent might be a client of the AAA infrastructure. This document defines the common terminology and identifies the requirements for PANA.

Table of Contents

1. Introduction

Network access technologies for wired and wireless media are evolving rapidly. With the rapid growth in the number and type of devices and terminals that support IP stacks and can access the Internet, users can potentially use a single device having the capability of attaching via different multiple access media and technologies to interface to the network.

If a client can have more than one type of interface, using access-specific authentication mechanisms leads to running a collection of protocols on the client for the same purpose.

For example, the authentication mechanisms in PPP are being used for many wired access scenarios as well as some wireless access, which requires using PPP encapsulation for the data packets. Using

PPP just for client authentication is viewed as a sub-optimal solution as it causes extra round-trips, overhead of encapsulation and processing,

and forces the network topology into a point-to-point model. A point in case is PPPoE which is used over multi-access networks primarily for the purpose of exploiting the authentication scheme provided by PPP. Also, IEEE 802 relies on 802.1X which provides EAP authentication that is limited to IEEE 802 link layers.

It is clearly advantageous to use a general protocol to authenticate the client for network access on any type of technology. There is currently no general protocol to be used by a client for gaining network access, and the PANA Working Group will attempt to fill that hole.

The protocol design will be limited to defining a client-server messaging protocol (i.e., a carrier) that will allow authentication payload to be carried between the host/client (PaC) and an agent/server (PAA) in the access network for authentication and authorization purposes regardless of the AAA infrastructure that may (or may not) reside on the network. As a network-layer protocol, it will be independent of the underlying access technologies. It will also be applicable to any network topology.

The Working Group will not invent new security protocols and mechanisms but instead will use the existing mechanisms. In particular, the Working Group will not define authentication protocols, key distribution or key agreement protocols, or key derivation. The desired protocol can be viewed as the front-end of the AAA protocol or any other protocol/mechanisms the network is running at the background to authenticate its clients. It will act as a carrier for an already defined security protocol or mechanism.

As an example, Mobile IP Working Group has already defined such a carrier for Mobile IPv4 [MIPV4]. Mobile IPv4 registration request message is used as the carrier for authentication extensions (MN-FA [MIPV4], or MN-AAA [MNAAA]) to receive forwarding service from the foreign agents. In that sense, designing the equivalent of Mobile IPv4 registration request messages for general network access is the goal of this work, but not defining the equivalent of MN-FA or MN-AAA extensions.

This document defines the common terminology and identifies the requirements of a protocol for PANA. These terminology and requirements will be used to define and limit the scope of the work to be done in this group.

2. Key Words

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 [KEYWORDS].

3. Terminology

Device Identifier (DI)

> The identifier used by the network as a handle to control and police the network access of a client. Depending on the access technology, identifier might contain any of IP address, link-layer address, switch port number, etc. of a device. PANA authentication agent keeps a table for binding device identifiers to the PANA clients. At most one PANA client should be associated with a DI on a PANA authentication agent.

PANA Client (PaC)

> The entity wishing to obtain network access from a PANA authentication agent within a network. A PANA client is associated with a network device and a set of credentials to prove its identity within the scope of PANA.

PANA Authentication Agent (PAA)

> The entity whose responsibility is to authenticate the credentials provided by a PANA client and grant network access service to the device associated with the client and identified by a DI.

4. Requirements

4.1. Authentication

4.1.1. Authentication of Client

PANA MUST authenticate a PaC for network access. A PaC can be identified by the credentials (identifier, authenticator) supplied by one of the users of the device or the device itself. PANA MUST only grant network access service to the device identified by the DI, rather than granting separate access to multiple simultaneous users of the device. Once the network access is granted to the device, the methods used by the device on arbitrating which one of its users can access the network is outside the scope of PANA.

PANA MUST NOT define new security protocols or mechanisms. Instead it must be defined as a "carrier" for such protocols. PANA MUST identify which specific security protocol(s) or mechanism(s) it can carry (the "payload"). The current thinking is that a sufficient solution would be for PANA to carry EAP. If PANA WG decides that extensions to EAP are needed, it will define requirements for an EAP WG instead of defining these extensions.

Authentication and encryption of data traffic except between the Pac and PAA is outside the scope of PANA. Providing a complete secure network access solution by also securing router discovery [RDISC], neighbor discovery [NDISC], and address resolution protocols [ARP] is outside the scope as well.

Both the PaC and the PAA MUST be able to authenticate each other for network access. Providing capability of only PAA authenticating the PaC is not sufficient.

PANA MUST be capable of carrying out both periodic and on-demand re-authentication. Both the PaC and the PAA MUST be able to initiate both the initial authentication and the re-authentication process.

When the DI is carried explicitly as part of the PANA payload, the authentication computation MUST also include this field to provide integrity protection for the DI. When the DI is carried implicitly as the source of the PANA message, the protocol has to make sure that the DI's integrity is protected by some other means (e.g., physical verification of incoming port number of the PANA message in the case of switch port number as a DI and PAA co-located with the link-layer access device). Protecting PaCs against DI theft is outside the scope of PANA.

4.1.2. Authorization, Accounting and Access Control

In addition to carrying authentication information, PANA MUST also provides only a binary authorization to indicate whether the PaC is allowed to access full IP services on the network. Providing finer granularity authorization, such as negotiating QoS parameters, authorizing individual services (http vs. ssh), individual users sharing the same device, etc. is outside the scope of PANA.

Providing access control functionality in the network is outside the scope of PANA. 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.

Carrying accounting data is outside the scope of PANA.

4.1.3. Authentication Backend

PANA protocol MUST NOT make any assumptions on the backend authentication protocol or mechanisms. PAA may interact with backend AAA infrastructures such as RADIUS or Diameter, but it is not a requirement. When the access network doesn't rely on a IETF-defined AAA protocol (e.g., RADIUS, Diameter), then it can still use a proprietary backend system, or rely on the information locally stored on the authentication agents.

The interaction between the PAA and the backend authentication entities is outside the scope of PANA.

4.1.4. Identifiers

PANA SHOULD allow various types of identifiers to be used for the PaC (e.g., NAI, IP address, FQDN, etc.)

PANA SHOULD allow various types of identifiers to be used as the DI (IP address, link-layer address, port number of a switch, etc.)

PAA MUST be able to create a binding between the PaC and the associated DI upon successful PANA exchange. The DI MUST be carried either explicitly as part of the PANA payload, or implicitly as the source of the PANA message, or both. This binding is used for access control and accounting in the network as described in section 4.1.2.

4.1.5. IP Address Assignment

PANA does not perform any address assignment functions but MUST only be invoked after the client has a usable IP address (e.g., a link-local address in IPv6 or a DHCP-learned address in IPv4)

4.2. Network

4.2.1. Multi-access

Protocol MUST support PaCs with multiple interfaces, and networks with multiple routers on multi-access links.

4.2.2. Disconnect Indication

PANA MUST NOT assume connection-oriented links. Links may or may not provide disconnect indication. Such notification is desirable in order for the PAA to cleanup resources when a client moves away from the network (e.g., inform the enforcement points that the

client is no longer connected). PANA SHOULD have a mechanism to provide disconnect indication.

This mechanism must allow PAAs to detect the departure of a PaC from the network. This mechanism SHOULD also allow a PaC to detect the discontinuation of the network access service. Access discontinuation can happen due to various reasons such as network systems going down, or a change in access policy.

Several mechanisms can be used to provide disconnect indication, e.g., frequent re-authentication; but the use of a heartbeat function is not recommended.

4.2.3. Location of PAA

The PAA must be on an IP capable network element on the same IP link as the PaC. Hence it can be on the NAS or WLAN AP or first hop router (most likely scenario). The use of PANA when the PAA is not on the same link as the PaC is outside the scope of PANA.

Since a PaC may not be pre-configured with the IP address of PAA, but may have to dynamically discover instead. Therefore PANA protocol must define a dynamic discovery method. Given that the PAA is on the same link as the PaC, there are number of discovery techniques that could be used (e.g., multicast or anycast) by the PaC to find out the address of the PAA.

PANA does not assumes the PAA is co-located with the enforcement point. 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 enforcement point(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 on the enforcement points. This WG 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.

4.2.4. Secure Channel

PANA MUST not assume a secure channel between the PaC and the PAA. PANA MUST be able to provide authentication especially in networks which are not protected against eavesdropping and spoofing. PANA MUST provide protection against replay attacks on both PaCs and PAAs.

Alternatively a combination of PANA with its chosen payload (EAP) can be used to meet the requirements stated above.

4.3. Interaction with Other Protocols

Mobility management is outside the scope of PANA. Though, PANA MUST be able to co-exist and not interfere with various mobility management protocols, such as Mobile IPv4 [MIPV4], Mobile IPv6 [MIPV6], fast handover protocols [FMIPV4, FMIPV6], and other standard protocols like IPv6 stateless address auto-configuration [ADDRCONF] (including privacy extensions [PRIVACY]), and DHCP [DHCP]. It MUST NOT make any assumptions on the protocols or mechanisms used for IP address configuration of the PaC.

4.4. Performance

PANA design SHOULD give consideration to efficient handling of authentication process. This is important for gaining network access with minimum latency. As an example, a method like minimizing the protocol signaling by creating local security associations can be used for this purpose.

4.5. Reliability and Congestion Control

PANA MUST provide reliability and congestion control. It can do so by using techniques like re-transmissions, cyclic redundancy check, delayed initialization and exponential back-off.

In order to satisfy the these requirements, the PANA MAY specify that high layer protocols, such as EAP, provide these services

4.6. Miscellaneous

4.6.1. IP Version Independence

PANA MUST work for both IPv4 and IPv6.

4.6.2. Denial of Service Attacks

PANA MUST be robust against a class of DoS attacks such as blind masquerade attacks through IP spoofing that swamp the PAA in spending much resources and prevent legitimate clients attempts of network access.

4.6.3. Location Privacy

Location privacy is outside the scope of PANA.

4.7. Change Log

Version 04

* Minor Editorial corrections

* Inserted the PANA model appendix

Version 03

* In section 4.2.2 the requirement for a heartbeat mechanism to provide disconnect indication was removed. Rewording of the section was done

* In section 4.2.3 and 4.1.2 rewording was done to account for the separation of PAA and EP and the protocol between them.

* In section 4.2.4 new text was added to account for the possibility to rely on the high layer protocol (EAP) to meet the requirements stated

* In section 4.5 new text was added to allow reliability and congestion control to be provided by the payload protocol, e.g., EAP.

Acknowledgements

We would like to thank Basavaraj Patil, Subir Das, and the PANA Working Group members for their valuable contributions to the discussions and preparation of this document.

References

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

[8021X] "IEEE Standards for Local and Metropolitan Area Networks: Port Based Network Access Control", IEEE Draft 802.1X/D11, March 2001.

[PPP] W. Simpson (editor), "The Point-To-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[MIPV4] C. Perkins (editor), "IP Mobility Support", RFC 2002, October 1996.

[MIPV6] D. Johnson and C. Perkins, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-15.txt, July 2001. Work in progress.

[MNAAA] C. Perkins, P. Calhoun, "Mobile IPv4 Challenge/Response

Extensions", RFC3012, November 2000.

[NDISC] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)",RFC 2461, December 1998.

[ARP] D. Plummer, "An Ethernet Address Resolution Protocol", STD 37, RFC 826, November 1982.

[FMIPV4] K. ElMalki (editor), et. al., "Low latency Handoffs in Mobile IPv4", November 2001. Work in progress.

[FMIPV6] G. Dommety (editor), et. al., "Fast Handovers for Mobile IPv6", July 2001. Work in progress.

[DHCP] R. Droms (editor), et. al., "Dynamic Host Configuration Protocol for IPv6", December 2001. Work in progress.

[PRIVACY] T. Narten, R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

Authors' Addresses

Alper E. Yegin
DoCoMo USA Labs
181 Metro Drive, Suite 300
San Jose, CA, 95110
USA
Phone: +1 408 451 4743
Email: alper@docomolabs-usa.com

Yoshihiro Ohba
Toshiba America Research, Inc.
P.O. Box 136
Convent Station, NJ, 07961-0136
USA
Phone: +1 973 829 5174
Email: yohba@tari.toshiba.com

Reinaldo Penno
Nortel Networks
600 Technology Park
Billerica, MA, 01821
USA
Phone: +1 978 288 8011
Email: rpenno@nortelnetworks.com

George Tsirtsis
Flarion Technologies
Bedminster One
135 Route 202/206 South
Bedminster, NJ, 07921
USA

Phone : +44 20 88260073
E-mail: G.Tsirtsis@Flarion.com, gtsirt@hotmail.com

Cliff Wang
Smart Pipes
565 Metro Place South
Dublin, OH, 43017
USA
Phone: +1 614 923 6241
Email: cwang@smartpipes.com

Appendix

A. PANA Model

Following sub-sections capture the PANA usage model in different network architectures with reference to its placement of logical elements such as, PANA Client (PaC) and PANA Authentication Agent (PAA) w.r.t Enforcement Point (EP) and Access Router (AR). Four different scenarios are described in following sub-sections. Note that PAA may or may not use AAA infrastructure to verify the credentials of PaC and grants or deny the device (belongs to that particular PaC) to access the network resources.

A.1. PAA Co-located with EP but separated from AR

In this scenario (Figure 1), PAA is co-located with the enforcement point on which access control is performed. PaCs communicate with the PAA for network access on behalf of a device (D1, D2,... etc.). PANA in this case provides a means to transport the authentication parameters from the PaC to PAA securely. PAA understands how to verify the credentials. After verification, PAA sends back the success or failure to PaC. However, PANA does not play any explicit role in performing access control except that it provides a hook to access control mechanisms.

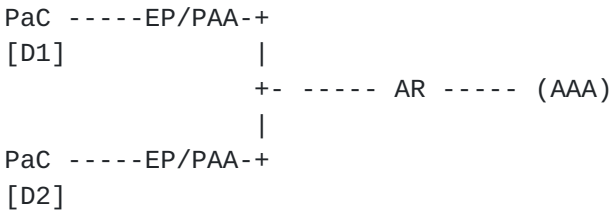

Figure 1: An example of PANA Model
[PAA co-located with EP but separated from AR]

A.2. PAA Co-located with AR but separated from EP

Figure 2 describes this model. In this scenario, PAA is not co-located with EPs but resides in the edge subnet. Although we have shown only one AR here there could be multiple ARs with PAAs co-located. PaC exchanges the same messages with PAA as discussed earlier. The difference here is when initial authentication for the PaC is successful, access control parameters are to be distributed to respective enforcement points residing in the edge subnet so that the corresponding device on which PaC is authenticated must get the access to the network. Similar to earlier case, PANA does not play any explicit role in performing access control except that it provides a hook to access control mechanisms. However, a separate protocol is needed between PAA and EP to carry access control parameters.

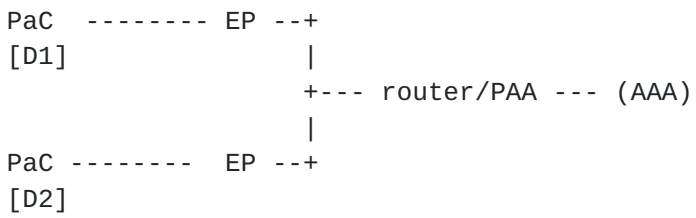

Figure 2: An example of PANA Model
[PAA co-located with AR but separated from EP]

A.3. PAA colocated with EP and router

In this scenario (Figure 3), PAA is co-located with the EP and AR on which access control and routing are performed. PaC exchanges the same messages with PAA and PAA performs similar functionalities as above. PANA in this case also does not play any explicit role in performing access control except that it provides a hook to access control mechanisms.

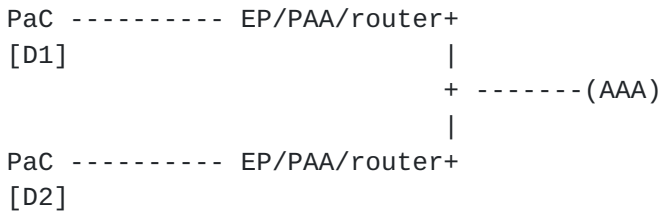

Figure 3: An example of PANA Model
[PAA co-located with EP and AR]

A.4. PAA Separated from EP and AR

Figure 4 represents this model. In this scenario, PAA is neither co-located with EPs nor ARs but resides on the edge subnet. Although we have shown only one PAA here there could be multiple PAAs in the edge subnet. PaC does similar exchanges with PAA as discussed earlier. Similar to model 5.2, after successful authentication, access control parameters will be distributed to respective enforcement points via a separate protocol and PANA does not play any explicit role to this.

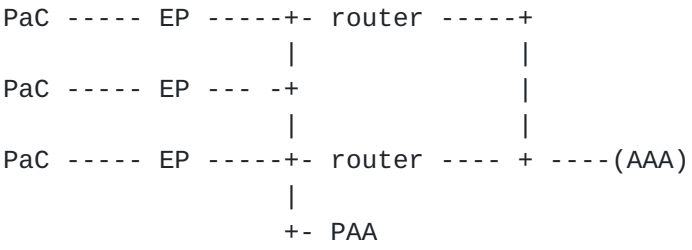

Figure 4: An example of PANA Model
[PAA separated from EP and AR]