Internet-Draft
Expires: September, 2002

Yoshihiro Ohba (Editor)
Subir Das
Basavaraj Patil
Hesham Soliman

March 1, 2002

Problem Space and Usage Scenarios for PANA

<draft-ietf-pana-usage-scenarios-01.txt>

Status of This Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents, valid for a maximum of six months, and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

Most of the commercial networks today require users (or devices on behalf of users) to provide their authentication information, such as identity, device identifier, etc., before being allowed access to network resources. Resources here include basic access to the network, specific value added services, different grade of services etc. While such networks are available in the market place, the authentication process and access control mechanisms depend upon the type of network that a user is attaching to and in most cases it is specific to an access technology. Due to the rapid proliferation of access technologies, wireless devices and next generation services offerings, a flexible authentication (which is independent of underlying access technologies) and access control mechanisms are deemed necessary. This document therefore attempts to describe several such scenarios where existing mechanisms are not sufficient

and finally argue the need for a new higher layer protocol called PANA (Protocol for carrying Authentication for Network Access). It also helps to understand the problem space clearly and facilitate the discussion for PANA requirements and framework.

Table of Contents

1 Terms

1.1. Requirements Language

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].

1.2. Acronyms

AAA: Authentication, Authorization and Accounting

AP: Access Point

AR: Access Router

DSL: Digital Subscriber Line

EAP: Extensible Authentication Protocol

GPRS: General Packet Radio Service

LSA: Local Security Association

PDP: Packet Data Protocol

PKI: Public Key Infrastructure

NAS: Network Access Server

PAA: PANA Authentication Agent

PaC: PANA Client

PPP: Point-to-Point Protocol

1.3. Terminology

Following terminologies are defined for this document. See also [PANAREQ].

Device

A network element (namely notebook computers, PDAs, etc.) that requires access to a provider's network.

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.

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 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 either locally or by using a back-end authentication infrastructure such as a AAA infrastructure and grant basic network access and specific service (if requested) to the device associated with the client and identified by a DI.

Local Network

The immediate network(s) that is available to the device for network access.

Client

An entity that resides on the device and provides authentication information to a NAS in the local network. PaC is a client.

Network Access Server (NAS)

An entity in the local network which resides at the edge and allows network access to the device after verifying the credentials provided by the client. For example, PAA is a NAS.

Access Point

A first-hop wireless L2 attachment point from the device in the local network.

Access Router

A first-hop router from the device in the local network.

Local Security Association (LSA)

A temporary security association between a client and a NAS, which is derived from credentials of the client during initial authentication.

Initial Authentication

Authentication performed when a device enters into a local network and provides the credentials to be authorized for network access without having any a priori authorization information. This will require a NAS to verify the credentials either locally or by using a back-end authentication infrastructure.

Re-authentication

Authentication that occurs when a device needs to extend the authorization lifetime, changes attributes such as, IP address and/or MAC address, etc., for the same network access after successful initial authentication. This may require a NAS to verify the credentials (used for initial authentication) either locally or by using a back-end authentication infrastructure.

Local re-authentication

A type of re-authentication that occurs locally between a client and a NAS by using the LSA established between them. In this type of re-authentication, the client does not use the same credentials as used for initial authentication.

Higher Layer

A layer that is higher than layer two.

2. **Problem Space**

Today's technologies mostly rely on access specific authentication mechanisms (i.e., L2 authentication mechanisms) for network access. For example, PPP has a built-in mechanism for peer authentication [RFC1661] and IEEE 802 networks define a port-based network access control with peer authentication in point-to-point LAN segments [802.1X]. However, it is not guaranteed that L2 authentication is always available in the local network as long as authentication for establishing L2 connectivity is not a mandatory part in the specification of an L2 protocol, and this leads to the following need:

i) Need for authentication over unauthenticated L2 links

In order to satisfy this need where authentication for network access is required, a higher layer protocol for authentication is clearly needed. While it is true that L2 can be extended to support authentication, we argue that a common higher layer protocol will provide a flexible and generic solution to all L2s.

Due to the rapid proliferation of access technologies, wireless devices are becoming very popular. On the other hand, these technologies demands different kinds of authentication, such as:

ii) Need for local re-authentication

Re-authentication is necessary at least in the following situations:

a) If the underlying access network does not have a capability to detect physical disconnection of devices, periodical re-authentication is necessary for minimizing the impact of attacks (e.g., free riding) due to IP address and/or MAC address spoofing, which would possibly occur when the device is shutdown or the user leaves the local network with the device without performing explicit log-off from the local network.

b) If there is a change in attributes (e.g., IP address and/or MAC address) of a device, re-authentication is necessary in order to make sure that the change is informed by the entity that was once authenticated successfully.

It is desired that re-authentication is performed locally between client and NAS as much as possible. However, there might be some cases where re-authentication with help of back-end authentication infrastructure is necessary in addition to local re-authentication, considering security for accounting such as non-repudiation.

While L2 authentication with some EAP mechanism [EAPSRP,RFC2284] that supports built-in local re-authentication may be used for situations in case (a), there are some scenarios where L2 authentication is not desired. For example, considering mobile and wireless environments, it is possible that a device has multiple wireless interfaces and switches from one interface to other in the same administrative domain with or without changing an IP address based on variable requirements (e.g., power saving vs. throughput). In this case, re-authentication is necessary for the new interface to be authorized for network access, and it is desired that re-authentication is performed locally between the client and NAS in order to perform interface switching quickly. The need for local re-authentication for interface switching immediately leads to a need for an access-independent authentication mechanism that supports:

- an access technology independent authentication protocol for providing a generic method for local re-authentication among different interfaces, AND

- an access independent client identifier for associating the different interfaces with the same LSA that is used for local re-authentication.

On the other hand, using an access-independent authentication mechanism is not sufficient for local re-authentication, and additional consideration for location of NAS is also necessary.

For example, if two NASes of L2 technologies A and B are physically in different boxes, it is not possible to use L2 authentication to perform local re-authentication without using another protocol such as a context transfer protocol and/or a AAA protocol (note: initial authentication does not necessarily require a AAA protocol) in order to share the LSA used for local re-authentication directly or indirectly between the two L2 NASes.

Thus, a higher layer protocol that provides not only an access-independent authentication mechanism but also flexibility in location of NAS is needed so that a client can continue to use a single NAS for performing local re-authentication in a "self-contained" manner (i.e., without requiring other protocols) when interface switching occurs.

So far we have described the problem space and the need for an additional authentication protocol at the higher layer. In the following section we present some important issues that such a higher protocol MUST satisfy and consider them as base requirements.

iii) Need for authentication independent of IP address configuration

There are two types of independence between authentication and IP address configuration as described below. Note that "IP address configuration" in this document means configuration of an IP address that needs to be authorized for network access, and thus configuring an IPv6 link local address or any temporal IP address that is used only for authentication purpose and not necessarily authorized for network access is excluded from the definition of "IP address configuration."

- Method independence. Authentication MUST be independent of any IP address configuration method for both dynamic address configuration (e.g., DHCPv4/v6, and IPv6 stateless address autoconfiguration, etc.) and static address configuration.

- Timing independence. Authentication MUST be able to occur both before and after configuring an IP address. There are a number of situations where authentication before IP address configuration would be necessary, for example:

  a) If strict access control is required or the IP address resource used for network access is scarce, authentication should occur before IP address configuration.

  b) If an AP supports multiple VLANs and it is possible to dynamically associate a device with one of the VLANs depending on the authentication and authorization result, authentication should occur before IP address configuration.

c) If a distinct IPv6 64-bit prefix can be assigned to each PDP context in GPRS[GPRS] or to each subscriber of DSL or cable internet, authentication should occur before IP address configuration.

On the other hand, authentication after IP address configuration would be useful for providing a network access service in which access to local information such as local-area map and flight information for free of charge, while access to specific external web-sites is subject to charge.

In conclusion, we anticipate that a higher layer protocol like PANA (Protocol carrying Authentication for Network Access) will satisfy all of the above needs that are emerging. We also understand that there are some functional overlap between L2 authentication and PANA. However, it is not very clear at this moment whether PANA and L2 authentication both are required for a network or they can be used exclusively for different scenarios.

In the following section, the problem domain is translated into few scenarios which we believe MUST be supported by PANA:

- Multiple access routers

- Multiple-interface device

3. Usage Scenarios

3.1. Multiple Access Routers

In multi-access environments, such as IEEE 802 networks, it is possible for multiple ARs to coexist on the same shared media. In such a scenario, it would be desirable to use multiple ARs in such a way that traffic coming from and going to a specific device always goes through a single AR for ease of access control, but traffic from different devices diverges over multiple ARs for the purpose of load balancing and redundancy. If such a routing control is possible, it would be easier to perform authentication via the same AR. On the other hand, there are some cases in which such a routing control would not be possible. This is due to e.g., ICMP Redirect or the use of "IPv6 Host to Router Load Sharing" [Hinden], and it may be better to put a PANA authentication agent separately from ARs in those cases. In other words, the types of routing control would affect the location of PAA in multi-AR environments. Given that the location of PAA is not restricted within ARs, PANA MUST have a mechanism to provide the information of the location of PAA(s) to devices.

The multi-AR scenario also addresses the issue of multiple providers on the same shared media, i.e., each AR may not be administered by the same provider. In this case, it would be necessary for PANA to have a mechanism to provide the identity of PAA(s) for a PaC so that the PaC can choose an appropriate provider to access. The important point is PANA MUST support all multi-AR scenarios.

3.2. Multiple-Interface Device

PANA MUST support a device with multiple interfaces of homogeneous or heterogeneous technologies. There are two possible scenarios: multi-homing and interface switching.

In case of multi-homing, the multiple interfaces of a device may be activated at the same time for various requirements such as increased bandwidth, load balancing and reliability. PANA MUST provide a way for the PaC of the device to perform initial authentication and local re-authentication for each interface.

In case of interface switching, PANA MUST use an access-independent authentication mechanism (as described in section 2). This access-independent authentication mechanism allows a PaC to perform local re-authentication with a PAA when interface switching occurs. Location of the PAA MUST be flexible so that the PaC can use the same PAA for each interface while it is roaming within the same domain. This will allow a device to roam seamlessly among different access technologies within an operator's domain.

4. Security Consideration

We anticipate following security issues or concerns relating to a higher layer protocol such as PANA.

- Consideration for Eavesdropping

  Since PANA protocol carries authentication information, consideration is necessary for preventing confidential part of the credentials of a PaC from being known by eavesdroppers in the local network. The eavesdroppers include users and operators in the local network.

- Consideration for Denial of Service Attacks

  Since PANA protocol is used for authentication, consideration is necessary for preventing authentication of a legitimate PaC from being denied as a result of processing PANA messages sent from attackers. Next, since both initial authentication and re-authentication would require cryptographic computation on both PaC and PAA, consideration is necessary for both PaC and PAA not to spend CPU and memory resources for processing PANA messages sent from an attacker more than that is spent by the attacker to attack. The attackers may or may not be on the same link as the PaC or PAA.

  Additionally, since during initial authentication PAA may use back-end authentication infrastructure, consideration is necessary to prevent the authentication infrastructure from being attacked via PAA while using PANA.

- Consideration for Man-In-The-Middle Attacks

Since PANA protocol needs to be able to operate over multiple router hops, consideration is necessary for preventing the communication between PaC and PAA from being spoofed by an attacker in between.

5. Acknowledgments

The authors would like to thank James Carlson, Jacques Caron, Paal Engelstad, Henry Haverinen, James Kempf, Phil Roberts, David Spence, Barani Subbiah, George Tsirtsis, Cliff Wang, Alper Yegin, and the rest of the PANA Working Group for the ideas and support they have given to this document.

6. References

[802.1X] IEEE Standard for Local and Metropolitan Area Networks, "Port-Based Network Access Control", IEEE Std 802.1X-2001.

[EAPSRP] J. Carlson, et al., "EAP SRP-SHA1 Authentication Protocol", Internet-Draft, Work in progress, July 2001.

[GPRS] R. Bates, "GPRS", McGraw-Hill TELECOM, ISBN 007138188, 2002.

[Hinden] R. Hinden, "IPv6 Host to Router Load Sharing", Internet-Draft, Work in progress, January 2002.

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

[PANAREQ] A. Yegin, et al., "Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology", Internet-Draft, Work in progress, February 2001.

[RFC1661] W. Simpson, "The Point-to-Point Protocol (PPP)", RFC 1661 (STD 51), July 1994.

[RFC2284] L. Blunk, et. al., "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

7. Authors' Information

Yoshihiro Ohba
Toshiba America Research, Inc.
P.O. Box 136
Convent Station, NJ 07961-0136
USA
Phone: +1 973 829 5174
Fax: +1 973 829 5601
Email: yohba@tari.toshiba.com

Subir Das
MCC 1D210R, Telcordia Technologies
445 South Street, Morristown, NJ 07960
Phone: +1 973 829 4959

email: subir@research.telcordia.com

Basavaraj Patil
Nokia
6000 Connection Dr.
Irving, TX. 75039
USA
Phone: +1 972-894-6709

Email: Basavaraj.Patil@nokia.com

Hesham Soliman
Ericsson Radio Systems AB
Torshamnsgatan 29,
Kista, Stockholm 16480
Sweden
Phone: +46 8 4046619
Fax: +46 8 4047020
E-mail: Hesham.Soliman@era.ericsson.se