Network Working Group A. Yegin
Internet-Draft Samsung
Intended status: Standards Track Y. Ohba
Expires: September 2, 2010 Toshiba
March 1, 2010

Protocol for Carrying Authentication for Network Access (PANA) with IPv4 Unspecified Address

draft-yegin-pana-unspecified-addr-00

Abstract

This document defines how PANA client (PaC) can perform PANA authentication prior to configuring an IP address.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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.

This Internet-Draft will expire on September 2, 2010.

Copyright Notice

Table of Contents

1. Introduction

PANA (Protocol for carrying Authentication for Network Access) [RFC5191] as a UDP-based protocol operates with the assumption that the PANA client (PaC) is already configured with an IP address. Private IPv4, globally-routable IPv4 [RFC1918] or IPv6, IPv4 or IPv6 link-local are the types of addresses that can be configured by PaCs prior to running PANA [RFC5193].

In case the PaC and the PANA Authentication Agent (PAA) are on the same IP subnet, PaC can run PANA with the PAA prior to configuring an IP address.

This document defines an extension of PANA to allow the PaC to use IPv4 unspecified address (0.0.0.0) until it gets authenticated/ authorized; and configures an IP address afterwards (possibly using DHCP). Such a feature is already available in Mobile IPv4 [RFC3344] where MN can use unspecified IPv4 address with Mobile IP protocol until it is assigned a home address, and also DHCP [RFC2131].

1.1. Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. 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].

2. Details

Figure 1 is an example call flow that illustrates use of unspecified IPv4 address with the PaC during PANA authentication. Note that there can be other ways for combining DHCP and PANA call flows.

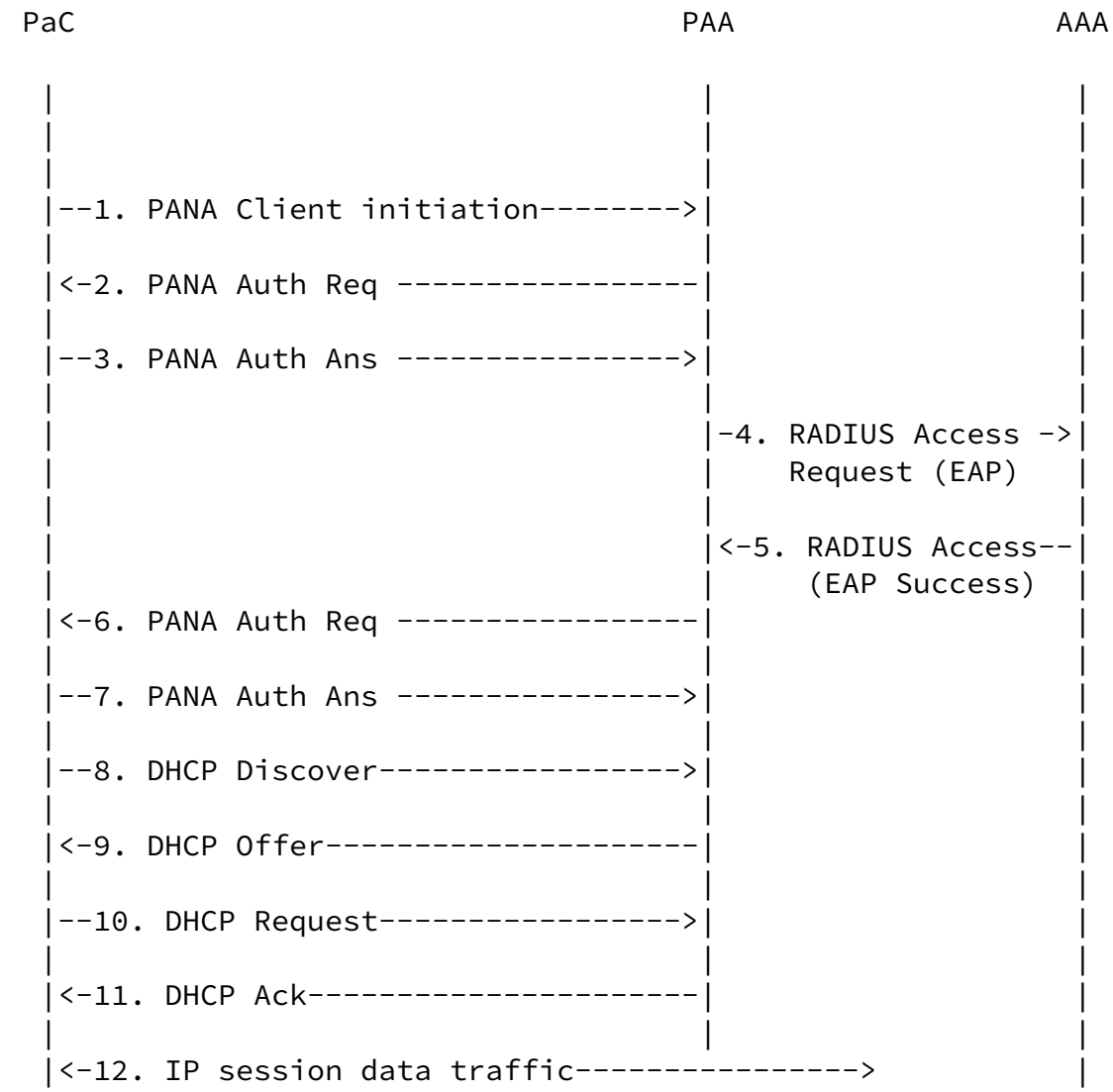
PaC
PAA
AAA
1. PANA Client initiation
2. PANA Auth Req
3. PANA Auth Ans
4. RADIUS Access Request (EAP)
5. RADIUS Access (EAP Success)
6. PANA Auth Req
7. PANA Auth Ans
8. DHCP Discover
9. DHCP Offer
10. DHCP Request
11. DHCP Ack
12. IP session data traffic

Figure 1: Example Call Flow for PANA with IPv4 Unspecified Address

Step 1: The PaC initiates PANA by sending a broadcasted PCI.

The source IPv4 address of the PCI is set to 0.0.0.0. The destination IPv4 address is set to 255.255.255.255.

Step 2: The PAA responds with a PAR message which has its source IPv4 address set to the PAA's IP address, and the destination IPv4 address is set to 255.255.255.255. If the PAA is capable of retrieving the PaC's L2 address from incoming PCI, then the PAR is L2-unicasted using that L2 address. Otherwise, the PAR message will be L2-broadcasted.

The PaC discovers the PAA's IPv4 address when it receives the PAR message.

Step 3: The PaC sends the PAN message to the PAA's newly discovered IPv4 address.

Steps 4-7: PANA and RADIUS carrying out the selected EAP method.

Steps 8-11: Now that the PaC is authenticated, it proceeds to configuring service IP address using DHCPv4. As soon as the new IPv4 address is confirmed by the DHCPACK, the PaC can stop using the unspecified address.

Step 12: The PaC can transmit and receive IP data packets using its IP address.

A PAA implementation may not be capable of retrieving the PaC's L2 address from L2 header of the incoming PANA messages, or be able to send a L2-unicast even if it could retrieve the address. In such a case, the PAA sends PANA messages as L2-broadcast. In order to prevent other PaCs from processing the messages destined for a specific PaC, each PaC is required to supply its own L2 address as a payload AVP to PCI and expect it to be echoed back by the PAA in the initial PAR. PAC-L2-ADDR AVP is defined for this purpose.

[TBD: Or, alternatively a randomly-generated token can be carried instead of the L2 address. It serves the same purpose.]

Note that any message beyond Step 2 would include the PAA-assigned and PaC-acknowledged PANA Session Id, hence use of PAC-L2-ADDR AVP is not needed for those messages.

3. PaC Behavior

A PaC shall use unspecified address as its source IP address until it configures another IP address. The PaC shall send a PCI that carries its L2 address in the PAC-L2-ADDR AVP. The PaC shall not include PAC-L2-ADDR AVP in any other message.

The PaC shall silently drop any PAR that carries a PAC-L2-ADDR AVP whose L2 address payload does not match the L2 address on the receiving interface of the PaC.

Any legacy PaC that does not implement this specification would automatically drop the incoming PAR that carries the PAC-L2-ADDR AVP as this is an unrecognized AVP. This is the standard behavior defined in [RFC5191].

4. PAA Behavior

If a PAA receives a PCI whose source IP address is unspecified but that does not carry a PAC-L2-ADDR AVP, then it shall drop the PCI. The PAA shall drop any message with PAC-L2-ADDR AVP if the message type is other than PCI. When the PAA is capable of retrieving the source L2 address of the incoming packets, if the address retrieved does not match the address in the PAC-L2-ADDR AVP payload, then the PAA shall drop the packet.

When the PAA needs to send a packet to a PaC that is using an unspecified IP address, then the PAA shall set the destination IP address to 255.255.255.255. The PAA should set the destination L2 address to the source L2 address retrieved from the incoming PaC packet, when possible; otherwise set to L2 broadcast address. If

this is the very first PAR message in PANA session, then the PAA shall include a PAC-L2-ADDR AVP with the payload set to the L2 address of the PaC. The PAA shall not include PAC-L2-ADDR AVP in any other PANA message, as an already-assigned PANA Session Id serves the need.

The PAA shall set the 'I' (IP Reconfiguration) bit of PAR messages in authentication and authorization phase so that the PaC proceeds to IP address configuration.

5. AVP Definition

This document defines one new AVP as described below.

5.1. PAC-L2-ADDR AVP

The PAC-L2-ADDR AVP (AVP Code TBD) contains a link-layer address of the PaC. The first two octets represents the AddressType, which contains an Address Family defined in [IANAADFAM]. Address families other than that are defined for link-layer MUST NOT be used for this AVP. The remaining octets encode the address value. The length of the address value is determined by the AddressType. The AddressType is used to discriminate the content and format of the remaining octets for the address value.

6. Message Size Considerations

Since IP fragmentation for IP packets using unspecified address is prohibited, link-layer MTU needs to be no less than the IP packet size carrying the largest PANA message in the case where EAP message size is the same as the minimum EAP MTU size (i.e., 1020 octets

[RFC3748]). Such a PANA message is the very first PANA-Auth-Request message in Authentication and Authorization phase carrying the following AVPs.

- An EAP-Payload AVP that carries an EAP-Request of size being equal to the minimum EAP MTU size. The size of such an AVP is 1020 + 8 = 1028 octets.

- A Nonce AVP that carries the largest nonce of size 256 octets. The size of such an AVP is 256 + 8 = 264 octets.

- An Integrity-Algorithm AVP (12 octets)

- A PRF-Algorithm AVP (12 octets)

- A PAC-L2-ADDR AVP (L2_ADDR_LEN + 10 octets) where L2_ADDR_LEN represents the length of the link-layer address in octets. For example, L2_ADDR_LEN = 6 for IEEE 802 MAC address.

In this case, the PANA message size including PANA header (16 octets), UDP header (8 octets) and IPv4 header (20 octets) is 1028 + 264 + 12 + 12 + L2_ADDR_LEN + 10 + 16 + 8 + 20 = (1370 + L2_ADDR_LEN) octets. Therefore, the link-layer MTU size for IP packets MUST be no less than (1370 + L2_ADDR_LEN) octets when unspecified IPv4 address is used for PANA. Note that Ethernet (MTU = 1500 octets) meets this requirement.

PANA as an EAP lower-layer reports the EAP MTU to the EAP layer, so that EAP methods can perform appropriate fragmentation [RFC3748]. The EAP MTU is calculated as follows:

EAP_MTU = L2_MTU - (350 + L2_ADDR_LEN)

In the above formula, the value of (350 + L2_ADDR_LEN) is the PANA overhead (IP and PANA headers, and PANA AVPs except for the EAP-Payload AVP payload).

7. Security Considerations

When the PAA is not capable of L2-unicasting PANA messages to the target PaC, other nodes on the same subnet can receive those messages. This may pose a risk if there is any confidential data exposed in the messages. Typically no such exposure exists as PANA, EAP, an EAP methods are defined in a way they can also be used in wireless networks where snooping is always a possibility.

8. IANA Considerations

As described in Section 5.1 and following the new IANA allocation policy on PANA message [I-D.arkko-pana-iana], a new AVP Code for PAC-L2-ADDR AVP needs to be assigned by IANA.

9. Acknowledgments

TBD.

10. References

10.1. Normative References

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.

[RFC5193] Jayaraman, P., Lopez, R., Ohba, Y., Parthasarathy, M., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA) Framework", RFC 5193, May 2008.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[I-D.arkko-pana-iana] Arkko, J. and A. Yegin, "IANA Rules for PANA (Protocol for Carrying Authentication for Network Access)", draft-arkko-pana-iana-02 (work in progress), February 2010.

[IANAADFAM] IANA, "Address Family Numbers", http://www.iana.org/assignments/address-family-numbers.

10.2. Informative References

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

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

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol",

RFC 2131, March 1997.

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

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

Authors' Addresses

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@yegin.org

Yoshihiro Ohba
Toshiba Corporate Research and Development Center
1 Komukai-Toshiba-cho
Saiwai-ku, Kawasaki, Kanagawa 212-8582
Japan

Phone: +81 44 549 2230
Email: yoshihiro.ohba@toshiba.co.jp