PANA Working Group
Internet-Draft
Intended status: Informational
Expires: July 29, 2010

L. Morand
France Telecom R&D
A. Yegin
Samsung
Y. Ohba
Toshiba America Research, Inc.
J. Kaippallimalil
Huawei Technologies
January 25, 2010

Application of PANA framework to DSL networks
draft-ietf-pana-panaoverdsl-01

Abstract

This document provides guidelines for PANA deployment over DSL access networks. The document specifically describes the introduction of PANA in DSL networks migrating from a traditional PPP access model to a pure IP-based access environment.

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 July 29, 2010.

Copyright Notice

Table of Contents

1. Introduction

PANA (Protocol for carrying Authentication for Network Access) design provides support for various types of deployments. DSL networks were identified as a typical example of such a deployment. This document provides guidelines for PANA deployment over DSL access networks. The document specifically describes the introduction of PANA in DSL networks migrating from a traditional PPP access model to a pure IP-based access environment. In such environment, additional authentication mechanisms are required to provide a complete secure network access solution to Network Access Providers (NAP) willing to overtake inadequate methods such as basic DSL link-layer identification or application-layer ad-hoc authentication mechanisms (e.g., HTTP redirects with web-based login).

2. Specification of Requirements

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].

3. Terminology

This document uses the PANA terminology defined in [RFC5191]. This document uses the DSL Forum terminology defined in [TR25], [TR59], [TR101] and [WT146].

4. PANA Framework Overview

PANA (Protocol for carrying Authentication for Network Access) is a link-layer agnostic transport for EAP [RFC3748] to enable network access authentication between clients and access networks.

The motivation to define such a protocol and the requirements are described in [RFC4058]. Protocol details are documented in [RFC5191]. There are components that are part of a complete secure network access solution but are outside of the PANA protocol specification. These components include PANA Authentication Agent (PAA) discovery mechanisms, based either on DHCP [RFC5192] or a simple multicast-based protocol [I-D.fajardo-pana-paa-discovery], as well as IP address configuration, authentication method choice, filter rule installation, data traffic protection, and PAA-EP protocol [RFC5193].

Figure 1 illustrates the functional entities involved in the PANA framework and the interfaces (protocols, APIs) among them. See [RFC5191] and [RFC5193] for further details.

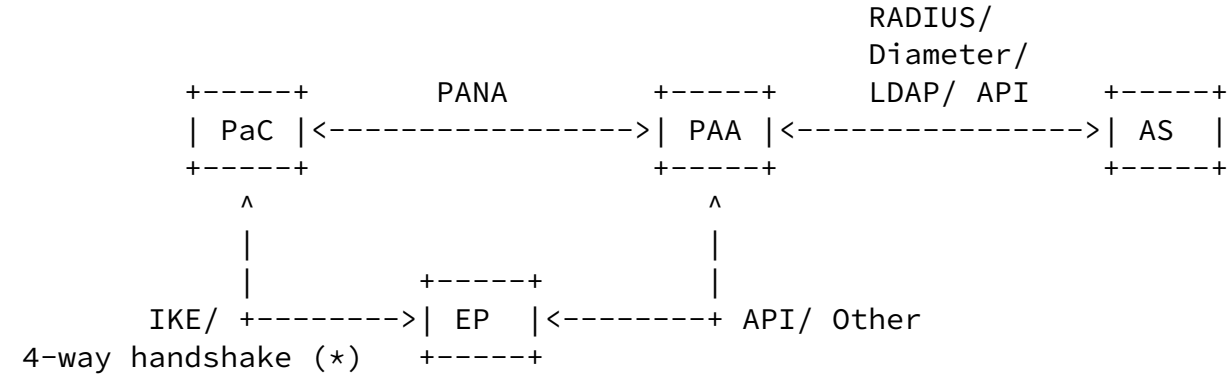


Figure 1: PANA Functional Model

PaC: PANA Client

PAA: PANA Authentication Agent

AS: Authentication Server

EP: Enforcement Point

(*) PaC-EP secure association protocol is not needed in DSL networks unless per-packet cryptographic security is needed.

The PANA design provides support for various types of deployments. DSL networks were identified as a typical example of such a

deployment (see Appendix A of [RFC4058]).

5. PANA in DSL environment

5.1. Evolution of DSL Environment

Traditional DSL deployments followed the architectural guidelines provided in [TR25] or [TR59]. Theses architectures use ATM to aggregate the access networks into a regional broadband network. The traffic aggregated from the access nodes (DSLAM) is steered to an IP node, the Broadband Remote Access Server (BRAS). In this environment, PPP sessions are set-up between the CPN (Customer Premises Network) and the BRAS, which acts as either a PPP termination point or a L2TP Access Concentrator (LAC) tunnelling multiple subscriber PPP sessions directly to an Internet/Corporate Service Provider. The CPN is usually defined as the combination of the DSL Modem or Residential Gateway (RG), acting as termination point of the physical DSL signal, and the subscriber's computers and

other devices (named hosts hereafter) connected to the DSL Modem/RG.

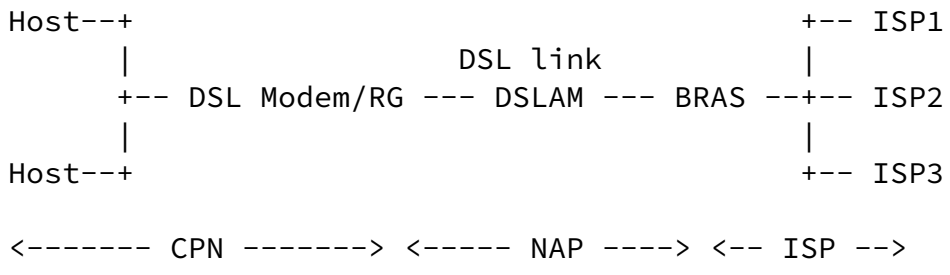


Figure 2: DSL Model

The devices at the customer premises have been shown as "hosts" in the above network.

DSL architectures are now emerging from a "low" speed best effort delivery network to an infrastructure capable of supporting higher subscriber bit rates. At the application layer, DSL service providers are looking to support enhanced services layered on top of basic Internet access, including entertainment video services (Broadcast TV and VoD), video conferencing, VoIP, gaming, and business class services (e.g. IP VPN), that have prohibitive

requirements to deploy them in a pure ATM based environment. Moving to on a Gigabit Ethernet instead of an ATM aggregation network offers an highly efficient transport technology for delivering large amounts of bandwidth to a highly distributed access node topology. Migration from ATM-based to an Ethernet based aggregation network in the context of TR-25 and TR-59 based architectures is described in [TR101].

In this evolution path towards Giga Ethernet, there is in parallel a growing interest in migrating from the traditional PPP access model to one relying on an network access control of IP sessions establishment. The "IP Sessions" model is a concept introduced in DSL Forum that covers a cycle consisting of IP session Detection and creation, application of IP session policies, and IP session termination. Details of this work are documented in [WT146]. Basically, an IP session represents subscriber IP traffic which is associated with a subscriber's IP address parameters. A subscriber may have multiple IP addresses (or sessions) in simultaneous use. An IP session may in turn be associated with multiple IP flows. The relation between subscribers and policies associated with it are described in [WT134]. The policy relationships in this document show that subscribers have services that are governed by policies. Thus, the same subscriber policies govern all IP sessions/flows belonging to the subscriber.

5.2. Advisability of Introducing PANA in DSL Environment

Among other challenges for DSL environment migrating from pure PPP based networks, one is the need for the creation of an IP session subscriber authentication model to secure network access and IP address management provided by a DHCP infrastructure. Indeed, contrary to PPP environment, an IP sessions model has no built-in mechanisms for authentication purposes in a DHCP based environment. If location-based authentication relying on access line identification is actually possible (see in [TR101] the use of the DHCP Relay Agent Information option, aka DHCP option 82 [RFC3046], inserted by the Access Node), additional mechanisms are required to provide Network Access Providers (NAP) with an explicit per-subscriber access authentication solution, in order to .

Providing a native support of EAP frames over IP, PANA is therefore a natural candidate to provide the protocol support of an IP subscriber authentication model. Moreover, PANA provides functionalities fulfilling basic and advanced security requirements within an IP session based environment (as described in [WT146]) , such as:

- IP address based session management mechanisms, using an explicit session identifier;
- Authentication mechanism independent of the physical medium type;
- Enabling per-session enforcement policies (i.e. filters) depending on the creation and deletion of the PANA session;
- Enabling session keep-alive and session monitoring functionalities to optimize the use of resources and provide an accurate picture of the state of a subscriber session (as described in [WT146]).

In this new context for DSL networks, PANA may be introduced to authenticate the credentials of a user prior to the setup of an IP session. The user selects the service provider and authenticates itself. During IP session setup, policies for the use of connection resources related to the IP session are established in the BRAS. These policies govern the subscriber's use of network resources. IP flows are accounted for and associated with the IP session and the service session that triggered it.

Based on the content of the Liaison Statement sent by the DSL Forum to the IETF, the specific subscriber authentication requirements were discussed at the PANA WG meeting at IETF70 in Vancouver (Dec 5, 2007). The result of this analysis confirmed the applicability of the PANA protocol for the DSL Forum's subscriber authentication

requirements. PANA WG Meeting analysis can be found in the 70th IETF meeting proceedings (http://www.ietf.org/proceedings/07dec/slides/pana-3/sld1.htm).

6. Applicability of PANA to IP Session based DSL Environment

6.1. Functional Architecture

6.1.1. Location of PAA and EP

In a PPP based environment, the BRAS is in charge of interfacing with CPE for authenticating and authorizing them for the network access service as well as performing policy control by acting as en enforcement point. In an IP session based environment, such functionalities may be provided at the same level by locating the PAA and EP entities in the BRAS. One advantage provided by this implementation is to preserve a improved and well-established DSL network configuration. Moreover, PAA and EP being collocated, there is no need to rely on an external interface between them to carry the authorized client attributes i.e. filters, an API being sufficient in that case.

The PANA design providing also the support for network configuration in which PAA and EP are not collocated, as described in [RFC5193], the PAA may be located in the BRAS while the EP function is the DSLAM. In that specific case, the PAA-EP interface implemented between the BRAS and the DSLAM may be based on the current DHCP triggering or on a dedicated API.

In an IP session based environment, the PAA will have to verify the credentials provided by a PaC located in the CPN and authorize network access to the host/gateway associated with the client.

6.1.2. Location of the PaC

6.1.2.1. Bridged Mode

In the Bridged mode, the DSL Modem/RG acts as a simple link-layer bridge. The DSL Modem/RG is here transparent at the IP layer. The hosts (e.g. PC) connected to the DSL Modem/RG in the CPN and the BRAS are then on the same IP link. Hosts may have a statically configured IP address or obtain an IP address from a DHCP server through the DSLAM (acting as a Layer-2 DHCP Relay agent as described in [TR101]) and the BRAS (filtering DHCP requests towards the DHCP server).

In this model, the PaC can be easily implemented in the hosts. Any

host connected to the DSL Modem/RG will be authenticated by the PAA

locating in the BRAS. It is therefore possible to perform a network access control on a per-host basis, as required by the IP session model.

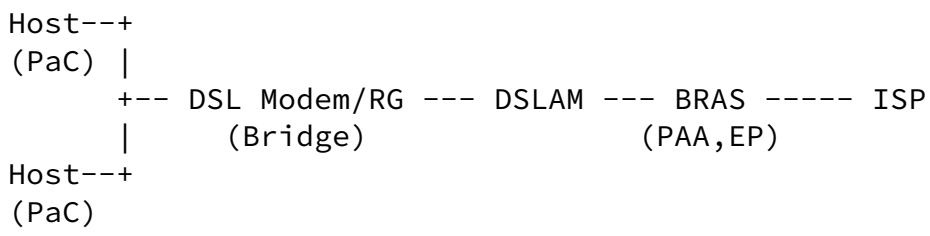


Figure 3: Bridged Mode

6.1.2.2. Routed Mode

In the Routed mode, the DSL Modem/RG acts as an IP router for the CPN. In this configuration, only the DSL Modem/RG and BRAS are on the same IP link. The DSL Modem/RG may have a statically configured IP address or obtain an IPv4 address or an IPv6 prefix from a DHCP server through the DSLAM (acting as a Layer-2 DHCP-Relay agent as described in [TR101]) and the BRAS (filtering DHCP requests towards the DHCP server). Hosts connected to the DSL Modem/RG may use either (1) either private IP addresses in an IPv4 environment with the DSL Modem/RG implemented a Network Address Port Translation (NAPT) function or (2) routable IP addresses if the modem is an IPv6 router.

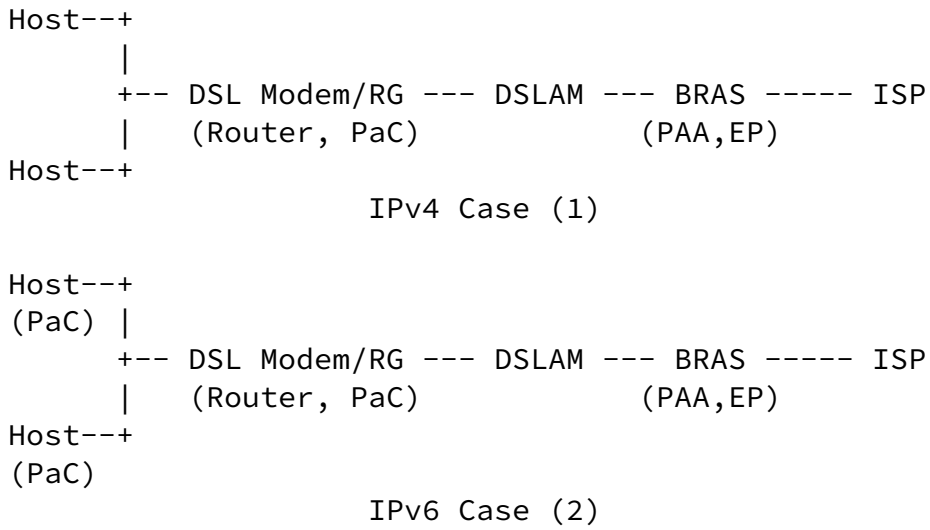


Figure 4: Routed Mode

In the IPv4 case (1), the simplest method is to implement the PaC in the DSL Modem/RG. Only the DSL Modem/RG will be authenticated/ authorized by the PAA. All hosts at the customer premises will then have access to the service provider's network using private IP

addresses obtained from the DSL Modem/RG.

(NOTE: Per-host authentication may be achieved also in the Routed mode if the EP function is performed by the DSL Modem/RG. However, it is for further studies to see how to introduce such a configuration in the global DSL Forum "IP Sessions" model.)

In the IPv6 case (2), the BRAS will detect any new IP address used by the DSL Modem/RG and the hosts connected to the DSL Modem/RG when using global scope IPv6 addresses. To allow a suitable network access rights management based on the IP address, PANA clients will have to be therefore implemented in the DSL Modem/RG and the hosts. The network access control is therefore performed on a per-host basis, in addition to the handling of the DSL Modem/RG 's own IP sessions.

6.2. IP Address Configuration

In the context of PANA deployment in DSL environment based on the IP Sessions model, the IP address configured by the PaC prior to PANA execution (so-called Pre-PANA Address or PRPA) MAY be obtained by one of the following methods:

1. Static IP Address confniguration: the PaC MAY be statically configured with an IP address. This address is therefore used as a PRPA.

2. DHCP-based IP Address Confirguration: the PaC MAY dynamically configure the PRPA using DHCPv4 [RFC2131] or DHCPv6 [RFC3315].

3. IPv6 Global Adress Stateless Address Autoconfiguration: in IPv6 environment, the PaC MAY configure global address(es) using IPv6 stateless auto-configuration [RFC2462] if router advertisements with prefixes are made available, as specified in [RFC2461].

4. Dynamic Configuration of Link-Local Address: The PaC MAY configure an IPv4 link-local address [RFC3927] and/or an IPv6 link-local address [RFC2462].

5. Unspecified IPv4 Address: PaC MAY use an unspecified IPv4 address (IPv4 address set to 0.0.0.0) as source IPv4 address.

After a successful authentication, the PaC MAY have to configure a new IP address for communication with other nodes if the PRPA is an

unspecified IPv4 address, a local-use IP address (e.g., a link-local or private IP address) or a temporarily allocated IP address. This

IP address is called a post-PANA address (POPA). An operator might choose allocating a POPA only after successful PANA authorization either to prevent waste of premium (e.g., globally routable) IP resources until the PaC is authorized (especially in the IPv4 case), or to enable PaC identity based address assignment. POPA can be configured using DHCP [RFC2131] [RFC3315] or using IPv6 stateless auto-configuration [RFC2462].

6.3. Authorized Device ID

The MAC address of the PaC can be used as a session attribute of the subscriber and used by the Enforcement Point (EP) for packet filtering once the PANA authentication successfully completed. The MAC address can also be used by the network to assign a subscriber-dependent IP address using DHCP. Therefore, the association between the subscriber ID that was used with the PANA authentication and the session attributes (MAC address and IP address) can be formed.

6.4. Cryptographic Protection

DSL networks are protected by physical means. Eavesdropping and spoofing attacks are prevented by keeping the unintended users physically away from the network media. Therefore, generally cryptographic protection of data traffic is not common. Nevertheless, if enhanced security is deemed necessary for any reason, IPsec-based access control can be enabled on DSL networks as well by using the method described in [I-D.ietf-pana-ipsec].

6.5. Implementation Options

This section provides possible implementation options of PANA in DSL deployments.

Section 6.5.1 describes the basic components of generic message flows.

Section 6.5.2 describes the specific use of IPv6 link-local address as Pre-PANA Address (PRPA).

Section 6.5.3 describes the specific use of IPv4 link-local address as PRPA.

Section 6.5.4 describes the specific use of unspecified IPv4 address as PRPA.

For each specific scenario, the features required from various network elements in DSL deployment are described.

6.5.1. Generic Message Flows

This is the description of the basic components of generic message flows.

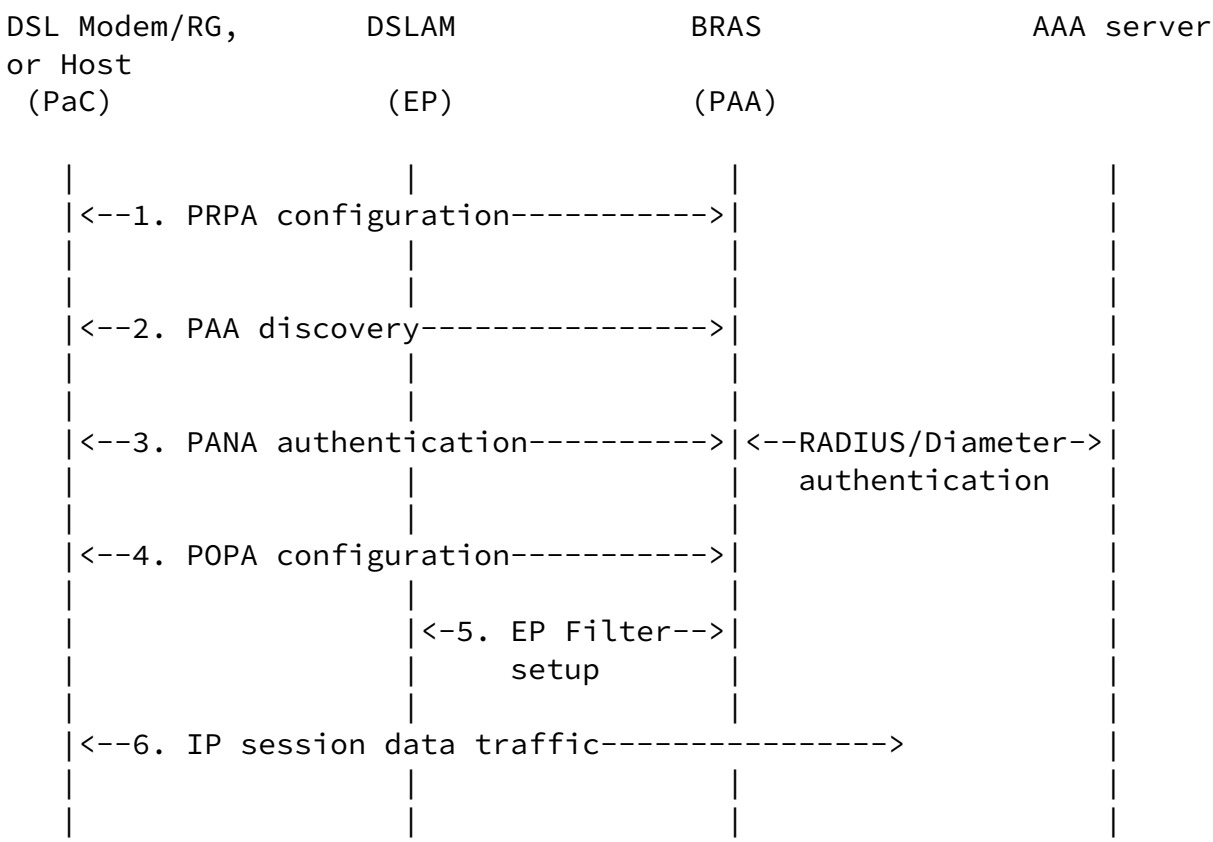


Figure 5. Generic PANA over DSL call flow

Depending on the deployment, either the DSL Modem acts as a RG and therefore only that node is authenticated; or the DSL Modem acts as a

bridge and hosts connected to that bridge gets individually authenticated.

Step 1: The DSL Modem/RG or host, acting as PaC, configures a pre-PANA IP address (PRPA).This step is skipped if the PaC is using an unspecified IPv4 address.

Step 2: PaC discovers the IP address of the PAA. PaC may use DHCP [RFC5192] or the discovery mechanism provided by PANA [I-D.fajardo-pana-paa-discovery].

Step 3: PaC and PAA performs authentication using EAP and AAA protocols (RADIUS, Diameter, etc.)

Step 4: In case the PRPA was an unspecified IPv4 address, temporary IP address or limited-use IP address, the PaC configures

a post-PANA IP address (POPA). This is the service IP address.

Step 5: PAA instructs the EP to allow authorized IP traffic of PaC. This step may be implicitly part of step 4 (e.g. DHCPACK with IP address configuration) or performed using a specific API.

Step 6: PaC can transmit and receive IP data packets.

Note that the step 4 is optional. Depending on the network configuration and the IP address resource management, it may not be needed for the PaC to configure a new IP address after the PANA authentication.

6.5.2. Use of IPv6 Link-Local Address

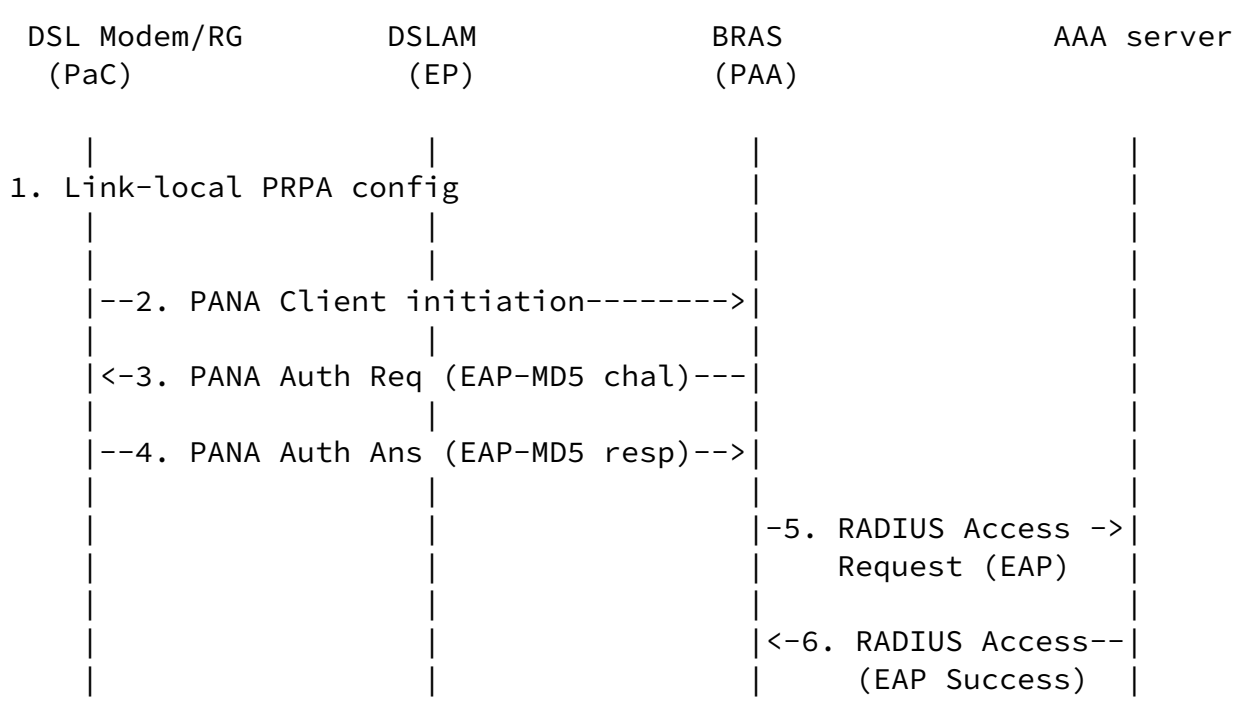
In this example, the following configuration is considered:

- The DSL modem/RG is authenticated;.
- PRPA is an IPv6 link-local address obtained by using IPv6 stateless auto-configuration [RFC2462];
- PAA discovery is based on PAA responding to the PANA Client Initiation request sent to a multicast address;

- Authentication method used is EAP-MD5;
- POPA is configured using DHCPv6 after successful authentication;
- EP is triggered by the DHCREPLY sent by the DHCP server, including the assigned IPv6 address in the option 'OPTION_IAADDR'.

6.5.2.1. Message Flows

This section describes the message flows for a DSL modem/RG using an IPv6 link-local address as PRPA.



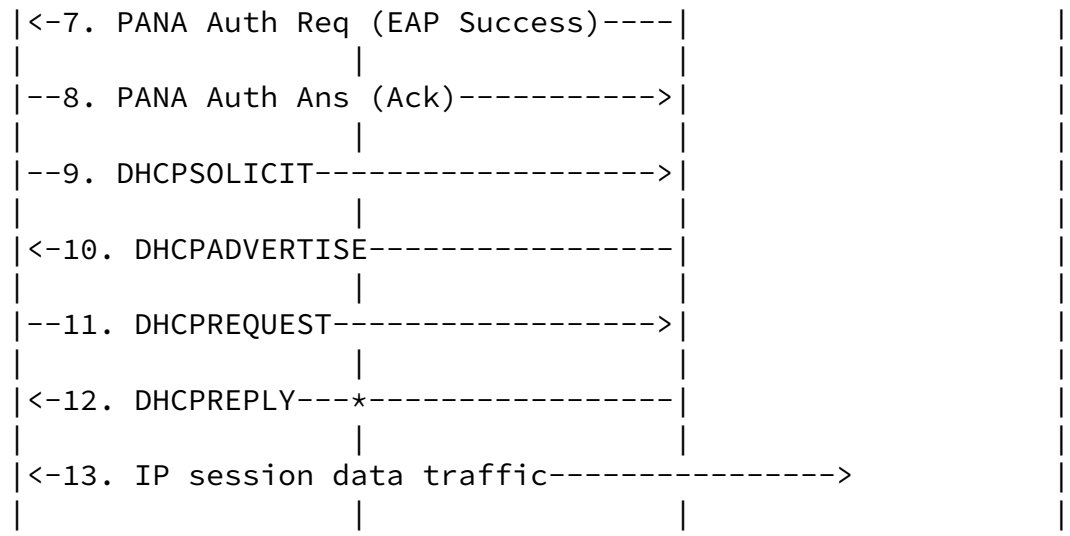


Figure 6. Specific use of IPv6 link-local address as PRPA

Depending on the deployment, either the DSL Modem acts as a RG and therefore only that node is authenticated; or the DSL Modem acts as a bridge and hosts connected to that bridge gets individually authenticated.

Step 1: The DSL Modem/RG configures an IPv6 link-local address [RFC2462]. It is assumed that, if the DSL network does not allow modems sending and receiving Neighbor Disovery messages to each other, then the network allows IP address collision among the modems and deals with it by using auxiliary information such as MAC address, VLAN, etc.

Step 2: The DSL Modem/RG initiates PANA by sending a PCI.

The source IPv6 address of the PCI is the IPv6 link-local address configured in Step 1. The destination IPv6 address is set to a reserved multicast address. This message is transparently forwarded to the BRAS.

Step 3: PAA responds with a PANA-Authentication-Request message, including its own IPv6 address as source IPv6 address.

PaC discovers the PAA's IPv6 address when it receives the PAR

message.

Step 4: PaC sends the PANA-Authentication-Answer message to the PAA's newly discovered IPv6 address.

Steps 5-8: PANA and RADIUS carrying out EAP-MD5 authentication. Note that it is possible to translate EAP-MD5/PANA to CHAP/RADIUS and eliminate the need to support EAP/RADIUS. But the details of such translation is outside the scope of this I-D.

Steps 9-12: Now that the DSL Modem/RG is authenticated, it proceeds to configuring a global (service) IPv6 address using DHCPv6. As soon as the gloabl IPv6 address is confirmed by the DHCPREPLY, the DSL Modem/RG stops using the link-local address. In Step 12, the DHCPREPLY message carrying the IPv6 address triggers the DSLAM to update its filters with the authorized IP/MAC address of the DSL Modem/RG.

Step 13: The DSL Modem/RG can transmit and receive IP data packets using the service IP address.

Note that, during steps 1-12, the DSLAM (acting as EP) allows only DHCP and PANA messages and, depending on network configuration, address resolution messages such as IPv6 Neighbor Discovery messages.

A variation of this call flow can be generated by using DHCP-based PAA discovery [RFC5192] instead of the multicasted PCI (Step 2). If DHCP Option 82 value is needed by the BRAS, it can be inserted at this stage by the DSLAM.

6.5.2.2. Required Support from DSL Environment

This section describes the features required from various network elements in DSL deployment in order to realize the described call flow. Note that not all requirements are imposed due to choice of PANA and some are already available irrespective of the

authentication protocol used (e.g., insertion of DHCP Option 82 by the DSLAM).

6.5.2.2.1. Required Support from the DSL Modem/RG

The DSL modem/RG must host the PANA client (PAC).

The DSL modem/RG must configure an IPv6 link-local address before sending PANA messages.

The PaC of the DSL modem/RG must be prepared to receive unsollicited PANA-Authentication-Request, following a first DHCP Discover.

The DHCP client of the DSL modem/RG must be triggered by a successful PANA authentication to configure a global IP address used as service IP address.

6.5.2.2.2. Required Support from the DSLAM

The DSLAM must be configured to act as an Enforcement Point and authorize only DHCP messages and PANA messages before successful PANA authentication.

The DSLAM must be configured to snoop DHCP messages and insert DHCP option 82 in DHCP messages sent by the DSL modem/RG and use the IP address found in the DHCPREPLY received from the DHCP server to update its IP filters for authorized IPaddress/MAC address.

6.5.2.2.3. Required Support from the BRAS

The BRAS should host the PANA Authentication Agent (PAA), the DHCP relay or server, and the AAA client. A given deployment can choose to host these implementations on separate nodes as long as it defines interfaces among them to pass information.

The reception of DHCP Solicit message from an unauthenticated MAC address should trigger a PAA-initiated PANA authentication procedure.

The DHCP server should allocate global IP addresses only to authenticated MAC addresses.

6.5.3. Use of IPv4 Link-Local Address

In this example, the following configuration is considered:

- DSL modem/RG is authenticated,

- PRPA is a IPv4 link-local address,
- PAA discovery is based on DHCP,
- Authentication method used is EAP-MD5,
- POPA is configured using DHCPv4 after successful authentication,
- EP is triggered by DHCPACK whose 'yiaddr' field is filled.

6.5.3.1. Message Flows

This section describes the message flows for a DSL modem/RG using a IPv4 link-local address as PRPA.

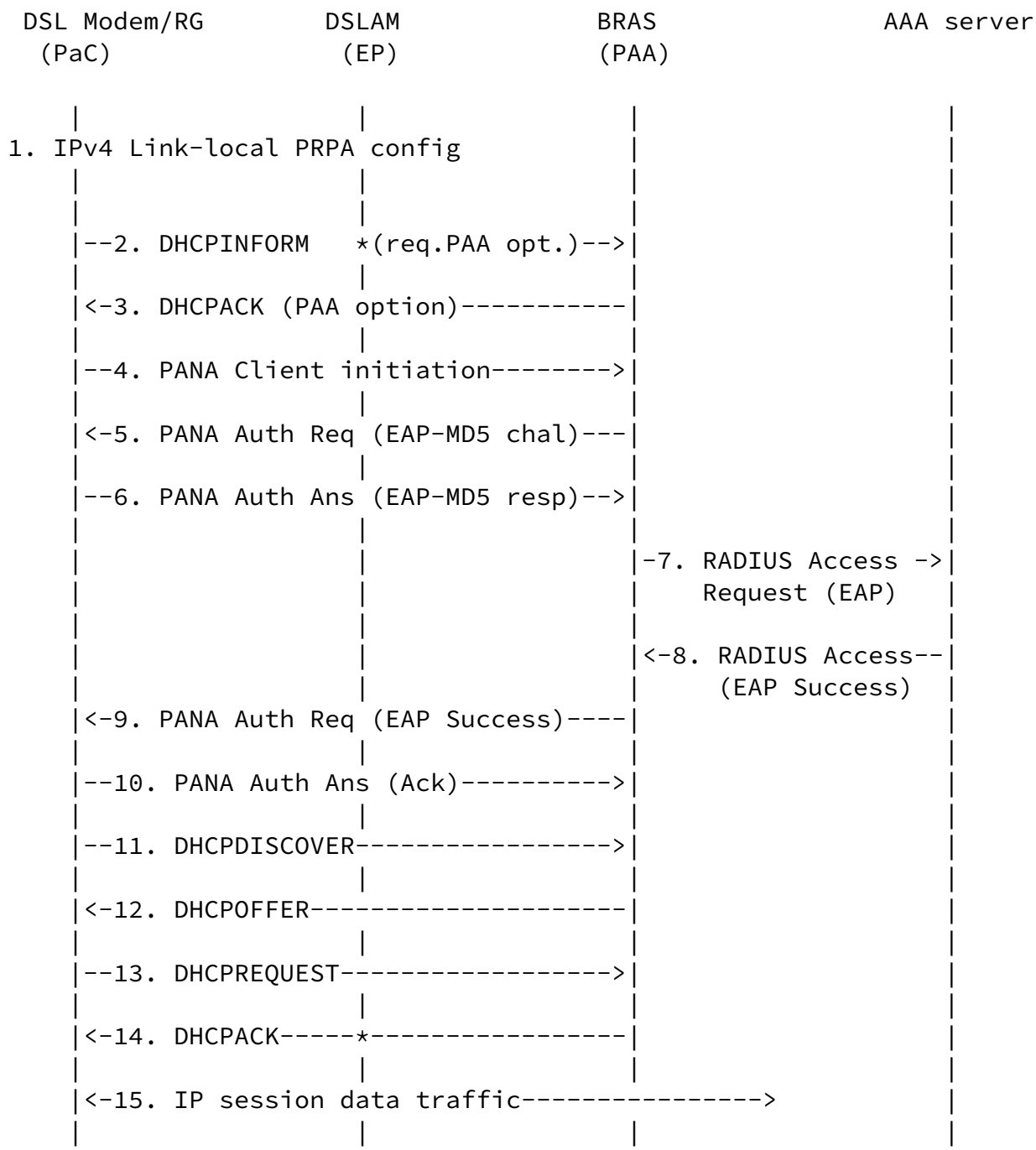


Figure 7. Specific use of IPv4 link-local address as PRPA.

Step 1: The DSL Modem/RG configures an IPv4 link-local address

[RFC3927]. It is assumed that, if the DSL network does not allow modems sending and receiving ARP requests/responses to each other, then the network allows IP address collision among the modems and deals with it by using auxiliary information such as MAC address, VLAN, etc.

Steps 2-3: the DSL Modem/RG discovers the IPv4 address of the PAA using the PANA Authentication Agent DHCPv4 Option [RFC5192]. The

DSL Modem/RG uses its IPv4 link-local address with DHCP and it does not request IP address allocation (i.e., DHCP server will not fill 'yiaddr' in DHCP ACK in response to DHCP Inform). the DHCP Option 82 is inserted into the DHCP Inform message by the DSLAM.

Step 4: The DSL Modem/RG initiates PANA with the newly-discovered PAA. Alternatively, the PAA could initiate PANA in unsolicited fashion. In that latter case, Step 4 may be skipped or run in parallel with Step 5.

Steps 5-10: PANA and RADIUS carrying out EAP-MD5 authentication. BRAS can utilize the Option 82 value discovered during Step 2.

Steps 11-14: Now that the DSL Modem/RG is authenticated, it proceeds to configuring service IP address using DHCPv4. As soon as the new IP address is confirmed by the DHCP ACK, the DSL Modem/RG can stop using the IPv4 link-local address. In Step 14, the DHCP ACK message carrying the IP address triggers the DSLAM to update its filters with the authorized IP/MAC address of the DSL Modem/RG.

Step 15: The DSL Modem/RG can transmit and receive IP data packets using the service IP address.

Note that, during steps 1-14, the DSLAM (acting as EP) allows only DHCP and PANA messages,and depending on deployment, address resolution messages such as ARP.

A variation of this call flow can be generated using PANA-based PAA discovery [I-D.fajardo-pana-paa-discovery] instead of DHCP for the Steps 2 and 3. If DHCP Option 82 value is needed by the BRAS, it can be inserted into the PANA messages as they go through the DSLAM.

6.5.3.2. Required Support from DSL Environment

This section describes the features required from various network elements in DSL deployment in order to realize the described call flow. Note that not all requirements are imposed due to choice of PANA and some are already available irrespective of the authentication protocol used (e.g., insertion of DHCP Option 82 by the DSLAM).

6.5.3.2.1. Required Support from DSL Modem/RG

The DSL modem/RG must host the PANA client (PAC).

The DSL modem/RG must configure an IPv4 link-local address as

described in [RFC3927]

The DSL modem/RG must perform two DHCP procedures: one to discover the PAA, another one to be allocated with a service/routable IP address after successful PANA authentication.

6.5.3.2.2. Required Support from DSLAM

The DSLAM must be configured to act as an Enforcement Point and authorize only DHCP messages and PANA messages before successful PANA authentication.

The DSLAM must be configured to snoop DHCP messages and insert DHCP option 82 in DHCP messages sent by the DSL modem/RG and use the IP address found in the 'yiaddr' field of the DHCP ACK received from the DHCP server to update its IP filters for authorized IPaddress/MAC address.

6.5.3.2.3. Required Support from BRAS

The BRAS should host the PANA Authentication Agent (PAA), the DHCP relay or server, and the AAA client. A given deployment can choose to host these implementations on separate nodes as long as it defines interfaces among them to pass information.

The reception of DHCP Discover message from an unauthenticated MAC

address should trigger a PAA-initiated PANA authentication procedure.

The DHCP server should allocate global IP addresses only to authenticated MAC addresses.

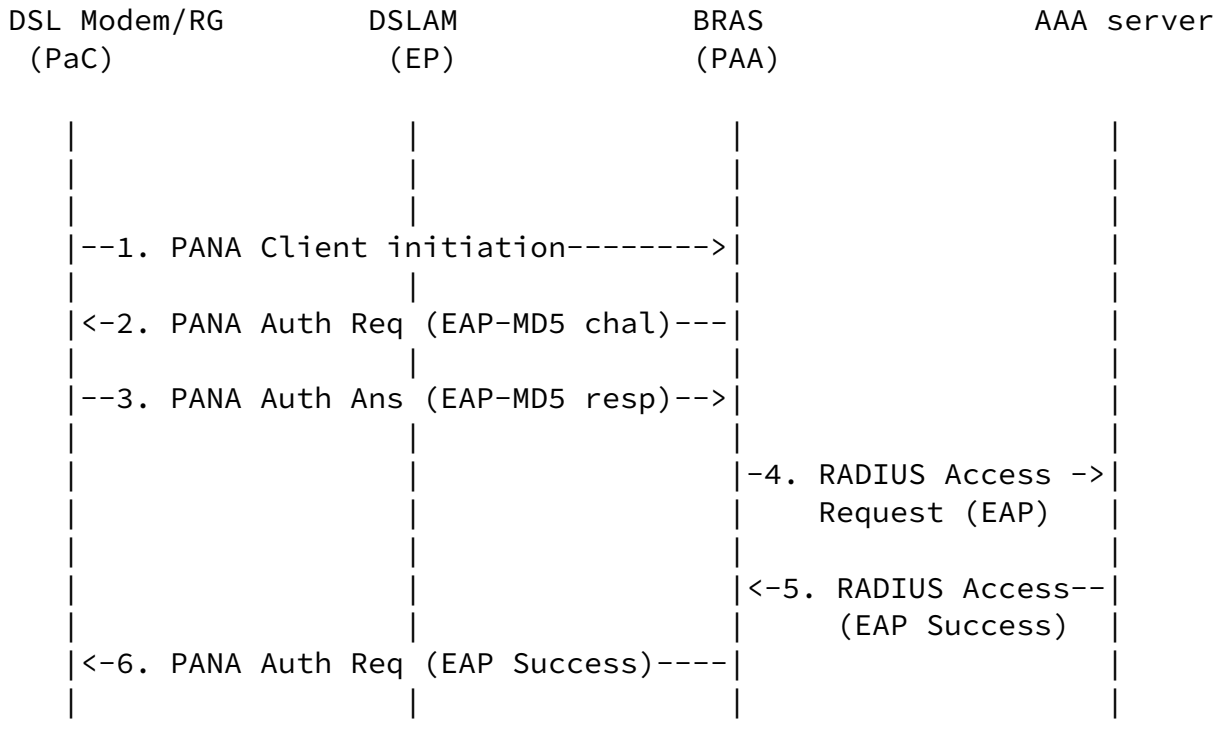
6.5.4. Use of Unspecified IPv4 Address

This is a similar example to the previous one with the exception that:

- PRPA is the unspecified IPv4 address,
- PAA discovery is based on PAA responding to broadcast PCI.

6.5.4.1. Message Flows

This section describes the message flows for a DSL modem/RG using an unspecified IPv4 address as PRPA.



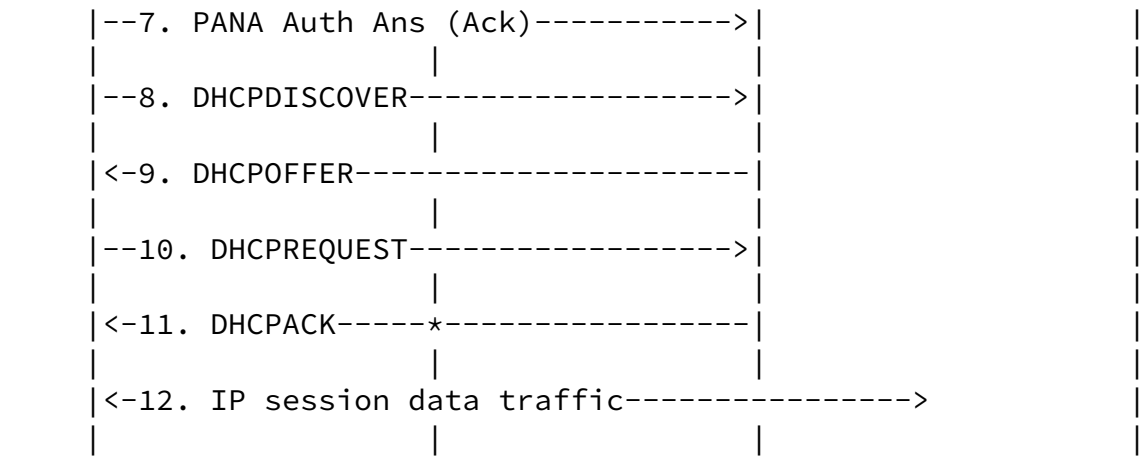


Figure 8. Specific use of unspecified IPv4 address as PRPA.

Step 1: The DSL Modem/RG 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: 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 MAC address from incoming PCI, then the PAR is L2-unicasted using that MAC address. Otherwise, the PAR message will be L2-broadcasted.

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

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

Steps 4-7: PANA and RADIUS carrying out EAP-MD5 authentication. Note that it is possible to translate EAP-MD5/PANA to CHAP/RADIUS and eliminate the need to support EAP/RADIUS. But the details of such translation is outside the scope of this I-D.

Steps 8-11: Now that the DSL Modem/RG is authenticated, it

proceeds to configuring service IP address using DHCPv4. As soon as the new IPv4 address is confirmed by the DHCP ACK, the DSL Modem/RG can stop using the unspecified address. In Step 11, the DHCP ACK message carrying the IPv4 address triggers the DSLAM to update its filters with the authorized IP/MAC address of the DSL Modem/RG.

Step 12: The DSL Modem/RG can transmit and receive IP data packets using the service IP address.

In case the deployment requires the DHCP Option 82 as a by-product of DHCP-based PAA discovery, then Steps 2-3 from previous call flow can be added to this one as well.

A PAA implementation may not be capable of retrieving the PaC's MAC 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 MAC address as a payload AVP to PCI and expect it to be echoed back by the PAA in the initial PAR (TBD: Define an AVP for that). PaCs shall drop PARs with mismatching MAC payloads. If the PAA is capable of L2-unicasting PANA messages by using the MAC address learned from the PCI payload, it can do so.

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

6.5.4.2. Required Support from DSL Environment

This section describes the features required from various network elements in DSL deployment in order to realize the described call flow. Note that not all requirements are imposed due to choice of PANA and some are already available irrespective of the

authentication protocol used (e.g., insertion of DHCP Option 82 by the DSLAM).

6.5.4.2.1. Required Support from the DSL Modem/RG

The DSL modem/RG must host the PANA client (PAC).

The DSL modem/RG must use an unspecified IPv4 address to send PANA messages.

The DHCP client of the DSL modem/RG must be triggered by a successful PANA authentication to configure a global IP address used as service IP address.

6.5.4.2.2. Required Support from the DSLAM

The DSLAM must be configured to act as an Enforcement Point and authorize only DHCP messages and PANA messages before successful PANA authentication.

The DSLAM must be configured to snoop DHCP messages and insert DHCP option 82 in DHCP messages sent by the DSL modem/RG and use the IP address found in the 'yiaddr' field of the DHCP ACK received from the DHCP server to update its IP filters for authorized IPaddress/MAC address.

6.5.4.2.3. Required Support from the BRAS

The BRAS should host the PANA Authentication Agent (PAA), the DHCP relay or server, and the AAA client. A given deployment can choose to host these implementations on separate nodes as long as it defines interfaces among them to pass information.

The PAA must be capable of L2-unicasting PANA messages by using the MAC address learned from the received DHCP Discover.

The reception of DHCP Discover from an unauthenticated MAC address should trigger a PAA-initiated PANA authentication procedure.

The DHCP server should allocate IP addresses only to authenticated MAC addresses.

7. Security Considerations

The DSL infrastructure that connects the CPE to the DSLAM/BRAS is assumed to run over a physically-secured non-shared media. For that reason, neither the use of a key-generating EAP method nor a secure

L2/L3 channel bootstrapped by PANA is required. The current DSL deployments are satisfied by using non-key-generating client-only authentication methods (e.g., CHAP and its EAP equivalent EAP-MD5). The same model can be maintained even with the PANA-based deployments. If next generation deployments prefer key-generating mutual authentication methods, they can be naturally used with PANA too.

8. IANA Considerations

This document has no actions for IANA.

9. Acknowledgements

We would like to thank to Ted Lemon, Peter Arberg, Iljitsch van Beijnum, Friedrich Armbruster, Aurelien Violet and Blandine Cauwet for their valuable comments that contribute to improve this document.

10. References

10.1. Normative References

[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.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

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

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

[RFC5192] Morand, L., Yegin, A., Kumar, S., and S. Madanapalli, "DHCP Options for Protocol for Carrying Authentication for

Network Access (PANA) Authentication Agents", RFC 5192, May 2008.

10.2. Informative References

[I-D.fajardo-pana-paa-discovery]
Fajardo, V., "Simple PANA PAA Discovery Protocol", draft-fajardo-pana-paa-discovery-00 (work in progress), January 2008.

[I-D.ietf-pana-ipsec]
Parthasarathy, M., "PANA Enabling IPsec based Access Control", draft-ietf-pana-ipsec-07 (work in progress), July 2005.

[RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, May 2005.

[RFC4058] Yegin, A., Ohba, Y., Penno, R., Tsirtsis, G., and C. Wang, "Protocol for Carrying Authentication for Network Access (PANA) Requirements", RFC 4058, May 2005.

[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.

[TR101] DSL Forum TR-101, "Migration to Ethernet Based DSL Aggregation", April 2006.

[TR25] DSL Forum TR-025, "Core Network Architecture for Access to Legacy Data Network over ADSL", September 1999.

[TR59] DSL Forum TR-059, "DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services",

September 2003.

[WT134] DSL Forum WT-134 Draft Version 1.0, "Policy Control Framework for DSL", April 2006.

[WT146] DSL Forum WT-146 Draft Version 1.0, "IP Sessions",

February 2006.

Authors' Addresses

Lionel Morand
France Telecom R&D
France

Email: lionel.morand@orange-ftgroup.com

Alper E. Yegin
Samsung
Turkey

Email: alper.yegin@yegin.org

Yoshihiro Ohba
Toshiba America Research, Inc.
USA

Email: yohba@tari.toshiba.com

John Kaippallimalil
Huawei Technologies
USA

Email: jkaippal@huawei.com