PANA Working Group
Internet-Draft
Expires: April 23, 2004

D. Forsberg
Nokia
Y. Ohba
Toshiba
B. Patil
Nokia
H. Tschofenig
Siemens
A. Yegin
DoCoMo USA Labs
October 24, 2003

Protocol for Carrying Authentication for Network Access (PANA) draft-ietf-pana-pana-02

Status of this Memo

Copyright Notice

Abstract

This document defines the Protocol for Carrying Authentication for Network Access (PANA), a link-layer agnostic transport for Extensible Authentication Protocol (EAP) to enable network access authentication between clients and access networks. PANA can carry any authentication method that can be specified as an EAP method, and can

be used on any link that can carry IP. PANA covers the client-to-network access authentication part of an overall secure network access framework, which additionally includes other protocols and mechanisms for service provisioning, access control as a result of initial authentication, and accounting.

Table of Contents

1. Introduction

Providing secure network access service requires access control based on the authentication and authorization of the clients and the access networks. Initial and subsequent client-to-network authentication provides parameters that are needed to police the traffic flow through the enforcement points. A protocol is needed to carry authentication methods between the client and the access network.

Currently there is no standard network-layer solution for authenticating clients for network access. [I-D.ietf-pana-usage-scenarios] describes the problem statement that led to the development of PANA.

Scope of this working group is identified as designing a link-layer agnostic transport for network access authentication methods. PANA Working Group has identified EAP [RFC2284] as the payload for this protocol and carrier for authentication methods. In other words, PANA will carry EAP which can carry various authentication methods. By the virtue of enabling transport of EAP above IP, any authentication method that can be carried as an EAP method is made available to PANA and hence to any link-layer technology. There is a clear division of labor between PANA, EAP and EAP methods.

Various environments and usage models for PANA are identified in the [I-D.ietf-pana-usage-scenarios] Internet-Draft. Potential security threats for network-layer access authentication protocol is discussed in [I-D.ietf-pana-threats-eval] draft. These two drafts have been essential in defining the requirements [I-D.ietf-pana-requirements] on the PANA protocol. Note that some of these requirements are imposed by the chosen payload, EAP [RFC2284].

This Internet-Draft makes an attempt for defining the PANA protocol based on the other drafts discussed above. Special care has been given to ensure the currently stated scope is observed and to keep the protocol as simple as possible. The current state of this draft is not complete, but it should be regarded as a work in progress. The authors made effort to capture the common understanding developed within the working group as much as possible. The design choices being made in this draft should not be considered as cast in stone.

2. Terminology

This section describes some terms introduced in this document:

PANA Session:

PANA session is defined as the exchange of messages between the PANA Client (PaC) and the PANA Authentication Agent (PAA) to authenticate a user (PaC) for network access. If the authentication is unsuccessful, the session is terminated. The session is considered as active until there is a disconnect indication by the PaC or the PAA terminates it.

Session Identifier:

This identifier is used to uniquely identify a PANA session on the PAA and PaC. It is included in PANA messages to bind the message to a specific PANA session.

PANA Security Association:

The representation of the trust relation between the PaC and the PAA that is created at the end of the authentication phase. This security association includes the device identifier of the peer, and a shared key when available.

The definition of the terms PANA Client (PaC), PANA Authentication Agent (PAA), Enforcement Point (EP) and Device Identifier (DI) can be found in [I-D.ietf-pana-requirements].

3. Protocol Overview

The PANA protocol involves two functional entities namely the PaC and the PAA. The EP, mentioned in the context with PANA, is a logical entity. There is, however, the option that the EP is not physically co-located with the PAA. In case that the PAA and the EP are co-located only an API is required for intercommunication instead of a separate protocol. In the case where the PAA is separated from the EP, a separate protocol will be used between the PAA and the EP for managing access control. The protocol and messaging between the PAA and EP for access authorization is outside the scope of this draft and will be dealt separately.

The PANA protocol (PaC<->PAA) resides above the transport layer and the details are explained in Section 4. Although this document describes the interaction with a number of entities and with other protocol which enable network access authentication; the PANA protocol itself is executed between the PaC and the PAA.

The placement of the entities used in PANA largely depends on a certain architecture. The PAA may optionally interact with a AAA backend to authenticate the user (PaC). And in the case where the PAA and EP are co-located, the intercommunication may not require a separate protocol. Figure 1 illustrates the interactions in a simplified manner:

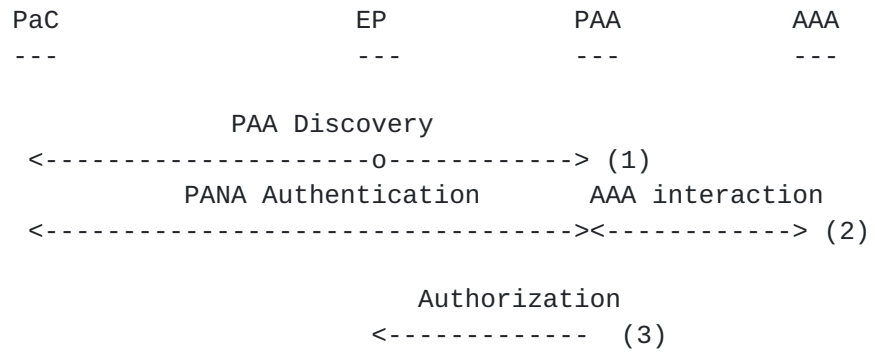


Figure 1: PANA Framework

The details of each of these aspects of the protocol are described in Section 4 of this document. PANA supports authentication of a PaC using various EAP methods. The EAP method used depends on the level of security required for the EAP messaging itself. PANA does not secure the data traffic itself. However, EAP methods that enable key exchange may allow other protocols to be bootstrapped for securing the data traffic [I-D.ietf-pana-ipsec].

From a state machine aspect, PANA protocol consists of three phases

1. Discovery and initial handshake phase

2. Authentication phase

3. Termination phase

In the first phase, an IP address of PAA is discovered and a PANA session is established between PaC and PAA. EAP messages are exchanged and a PANA SA is established in the second phase. The established PANA session as well as a PANA SA is deleted in the third phase.

4. Protocol Details

4.1 Common Processing Rules

4.1.1 Payload Encoding

The payload of any PANA message consists of zero or more AVPs (Attribute Value Pairs). A brief description of the AVPs defined in this document is listed below:

- Cookie AVP: contains a random value that is used for making initial handshake robust against blind resource consumption DoS attacks.
- Protection-Capability AVP: contains information which protection should be initiated after the PANA exchange (e.g. link-layer or network layer protection).
- Device-Id AVP: contains a device identifier of the sender of the message. A device identifier is represented as a pair of device identifier type and device identifier value. Either a layer-2 address or an IP address is used for the device identifier value.
- EAP AVP: contains an EAP PDU.
- MAC AVP: contains a Message Authentication Code that protects a PANA message PDU.
- Termination-Cause AVP: contains the reason of session termination.
- Result-Code AVP: contains information about the protocol execution results.
- Session-Id AVP: contains the session identifier value.
- Session-Lifetime AVP: contains the duration of authorized access.
- Failed-AVP: contains the offending AVP that caused a failure.
- NAP-Information AVP, ISP-Information AVP: contains the information on a NAP and an ISP, respectively.

4.1.2 Transport Layer Protocol

PANA uses UDP as its transport layer protocol. The UDP port number is TBD. All messages except for PANA-PAA-Discover are always unicast. PaC MAY use unspecified IP address for communicating with

PAA.

4.1.3 Fragmentation

PANA does not provide fragmentation of PANA messages. Instead, it relies on fragmentation provided by EAP methods and IP layer when needed.

4.1.4 Sequence Number and Retransmission

PANA uses sequence numbers to provide ordered delivery of EAP messages. The design involves use of two sequence numbers to prevent some of the DoS attacks on the sequencing scheme. Every PANA packet include one transmitted sequence number (tseq) and one received sequence number (rseq) in the PANA header. See Appendix A for detailed explanation on why two sequence numbers are needed.

The two sequence number fields have the same length of 32 bits and appear in PANA header. tseq starts from initial sequence number (ISN) and is monotonically increased by 1. The serial number arithmetic defined in [RFC1982] is used for sequence number operation. The ISNs are exchanged between PaC and PAA during the discovery and initial handshake phase (see Section 4.2). The rules that govern the sequence numbers in other phases are described as follows.

- When a message is sent, a new sequence number is placed on the tseq field of message regardless of whether it is sent as a result of retransmission or not. When a message is sent, rseq is copied from the tseq field of the last accepted message.

- When a message is received, it is considered valid in terms of sequence numbers if and only if (i) its tseq is greater than the tseq of the last accepted message and (ii) its rseq falls in the range between the tseq of the last acknowledged message + 1 and the tseq of the last transmitted message.

PANA relies on EAP-layer retransmissions, or for example NAS functionality [I-D.ietf-aaa-eap], for retransmitting EAP Requests based on timer. Other PANA layer messages that require a response from the communicating peer are retransmitted based on timer at PANA-layer until a response is received (in which case the retransmission timer is stopped) or the number of retransmission reaches the maximum value (in which case the PANA session MUST be deleted immediately). For PANA-layer retransmission, the retransmission timer SHOULD be calculated as described in [RFC2988] to provide congestion control. See Section 10 for default timer and maximum retransmission count parameters.

4.1.5 PANA Security Association

A PANA SA is created as an attribute of a PANA session when EAP authentication succeeds with a creation of a Master Session Key (MSK) [I-D.ietf-eap-rfc2284bis]. A PANA SA is not created when the PANA authentication fails or no MSK is produced by any EAP authentication method. In the case where two EAP authentications are performed in a sequence in a single PANA authentication, it is possible that two MSKs are derived. If this happens, the PANA SA MUST be bound to the MSK derived from the first EAP authentication. When a new MSK is derived as a result of EAP-based re-authentication, any key derived from the old MSK MUST be updated to a new one that is derived from the new MSK.

The created PANA SA is deleted when the corresponding PANA session is deleted. The lifetime of the PANA SA is the same as the lifetime of the PANA session for simplicity.

PANA SA attributes as well as PANA session attributes are listed below:

PANA Session attributes:

* Session-Id
* Device-Id of PaC
* Device-Id of PAA
* Initial tseq of PaC (ISN_pac)
* Initial tseq of PAA (ISN_paa)
* Last transmitted tseq value
* Last received rseq value
* Last transmitted message payload
* Retransmission interval
* Session lifetime
* Protection-Capability
* PANA SA attributes:
    + MSK

+ PANA_MAC_Key

The PANA_MAC_Key is used to integrity protect PANA messages and derived from the MSK in the following way:

```
PANA_MAC_KEY = The first N-bit of
               HMAC_SHA1(MSK, ISN_pac | ISN_paa | Session-ID)
```

where the value of N depends on the integrity protection algorithm in use, i.e., N=128 for HMAC-MD5 and N=160 for HMAC-SHA1.

The length of MSK MUST be N-bit or longer. See Section 4.1.6 for the detailed usage of the PANA_MAC_Key.

4.1.6 Message Authentication Code

A PANA message can contain a MAC (Message Authentication Code) AVP for cryptographically protecting the message.

When a MAC AVP is included in a PANA message, the value field of the MAC AVP is calculated by using the PANA_MAC_Key in the following way:

```
MAC AVP value = HMAC_SHA1(PANA_MAC_Key, PANA_PDU)
```

where PANA_PDU is the PANA message including the PANA header, with the MAC AVP value field first initialized to 0.

4.1.7 Message Validity Check

When a PANA message is received, the message is considered to be invalid at least when one of the following conditions are not met:

- Each field in the message header contains a valid value including sequence number, message length, message type, version number, flags, etc.
- When a device identifier of the communication peer is bound to the PANA session, it matches the device identifier carried in MAC and/or IP header(s).
- The message type is one of the expected types in the current state.
- The message payload contains a valid set of AVPs allowed for the message type and there is no missing AVP that needs to be included in the payload.

- Each AVP is decoded correctly.

- When a MAC AVP is included, the AVP value matches the MAC value computed against the received message.

- When a Device-Id AVP is included, the AVP is valid if the device identifier type contained in the AVP is supported (this check is for both PaC and PAA) and is the requested one (this check is for PAA only) and the device identifier value contained in the AVP matches the value extracted from the lower-layer encapsulation header corresponding to the device identifier type contained in the AVP. Note that a Device-Id AVP carries the PaC's device identifier in messages from PaC to PAA and PAA's device identifier in messages from PAA to PaC.

Invalid messages MUST be discarded in order to provide robustness against DoS attacks and an unprotected. In addition, a non-acknowledged error notification message MAY be returned to the sender. See Section 4.1.8 for details.

4.1.8 Error Handling

PANA-Error message MAY be sent by either PaC or PAA when a badly formed PANA message is received or in case of other errors. If the cause of this error message was a request message (e.g., PANA-PAA-Discover or *-Request), then the request MAY be retransmitted immediately without waiting for its retransmission timer to go off. If the cause of the error was a response message, the receiver of the PANA-Error message SHOULD NOT resend the same response until it receives the next request.

To defend against DoS attacks a timer MAY be used. One (1) error notification is sent to each different sender each N seconds. N is a configurable parameter.

When an error message is sent unprotected with MAC AVP and the lower-layer is insecure, the error message is treated as an informational message. The receiver of such an error message MUST NOT change its state unless the error persists and the PANA session is not making any progress.

4.2 Discovery and Initial Handshake Phase

When a PaC attaches to a network, and knows that it has to discover PAA for PANA, it SHOULD send a PANA-PAA-Discover message to a well-known link local multicast address (TBD) and UDP port (TBD). The source address is set to the unspecified IP address if the PaC has not configured an address yet. PANA PAA discovery assumes that PaC

and PAA are one hop away from each other. If PaC knows the IP address of the PAA (some pre-configuration), it MAY unicast the PANA discovery message to that address. PAA SHOULD answer to the PANA-PAA-Discover message with a PANA-Start-Request message.

When the PAA receives such a request, or upon receiving some lower layer indications of a new PaC, PAA SHOULD unicast a PANA-Start-Request message. The destination address may be unspecified IP address, but the L2 destination would be a unicast address (something for the implementations to deal with).

There can be multiple PAAs on the link. The authentication and authorization result does not depend on which PAA is chosen by the PaC. By default the PaC MAY choose the PAA that sent the that sent the first response.

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-Request 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 to be an explicit message to prompt PAA. Upon detecting the need to authenticate a client, EP can send a PANA-PAA-Discover message to the PAA on behalf of the PaC. This message carries a device identifier of the PaC in a Device-ID AVP. So that, the PAA can send the unsolicited PANA-Start-Request message directly to the PaC. If the link between the EP and PAA is not secure, the PANA-PAA-Discover message sent from the EP to the PAA MUST be protected by using, e.g., IPsec.

A PANA-Start-Request message contains a cookie carried in a Cookie AVP in the payload, respectively. The rseq field of the header is set to zero (0). The tseq field of the header contains the initial sequence number. The cookie is used for preventing the PAA from resource consumption DoS attacks by blind attackers. The cookie is computed in such a way that it does not require any per-session state maintenance on the PAA in order to verify the cookie returned in a PANA-Start-Answer message. The exact algorithms and syntax used for generating cookies does not affect interoperability and hence is not specified here. An example algorithm is described below.

```
Cookie =
  <secret-version> | HMAC_SHA1( <Device-Id of PaC> | <secret> )
```

where <secret> is a randomly generated secret known only to the PAA, <secret-version> is an index used for choosing the secret for generating the cookie and '|' indicates concatenation. The secret-

version should be changed frequently enough to prevent replay attacks. The secret key is locally known to the PAA only and valid for a certain time frame.

PAA MAY enable NAP-ISP authentication separation by setting the S-flag of the message header of the PANA-Start-Request. Also, the PANA-Start-Request MAY contain zero or one NAP-Information AVP and zero or more ISP-Information AVPs to advertise the information on the NAP and/or ISPs.

When a PaC receives the PANA-Start-Request message in response to the PANA-PAA-Discover message, it responds with a PANA-Start-Answer message if it wishes to enter the authentication phase. The PANA-Start-Answer message contains the initial sequence numbers in the tseq and rseq fields of the PANA header, a copy of the received Cookie (if any) as the PANA payload.

If the S-flag of the received PANA-Start-Request message is not set, PaC MUST NOT set the S-flag in the PANA-Start-Answer message sent back to the PAA. In this case, PaC can indicate its choice of ISP by including its ISP-Information AVP in the PANA-Start-Answer message. AAA routing will be based on the ISP choice if an ISP-Information AVP is specified in the PANA-Start-Answer message, otherwise it will be based on EAP identifier.

If the S-flag of the received PANA-Start-Request message is set, PaC can indicate its desire to perform separate EAP authentication for NAP and ISP by setting the S-flag in the PANA-Start-Answer message. In this case, PaC can also indicate its choice of ISP by including its ISP-Information AVP in the PANA-Start-Answer message. AAA routing for NAP authentication will be based on the NAP. AAA routing for ISP authentication will be based on the ISP choice if an ISP-Information AVP is specified in the PANA-Start-Answer message, otherwise it will be based on EAP identifier."

When the PAA receives the PANA-Start-Answer message from the PaC, it verifies the cookie. The cookie is considered as valid if the received cookie has the expected value. If the computed cookie is valid, the protocol enters the authentication phase. Otherwise, it MUST silently discard the received message.

The PANA-Start-Request/Answer exchange is needed before entering authentication phase even when the PaC is pre-configured with PAAs IP address and the PANA-PAA-Discover message is unicast.

A PANA-Start-Request message is never retransmitted. A PANA-Start-Answer message is retransmitted based on timer in the same manner as other messages retransmitted at PANA-layer.

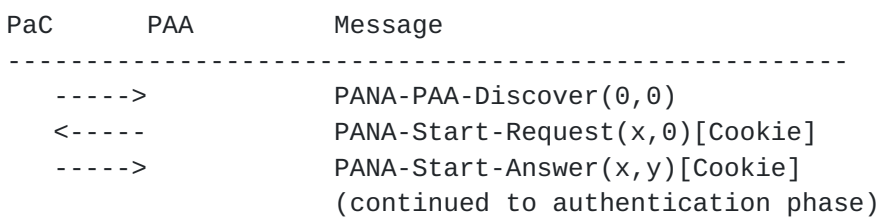


Figure 2: Example Sequence for Discovery and Initial Handshake Phase

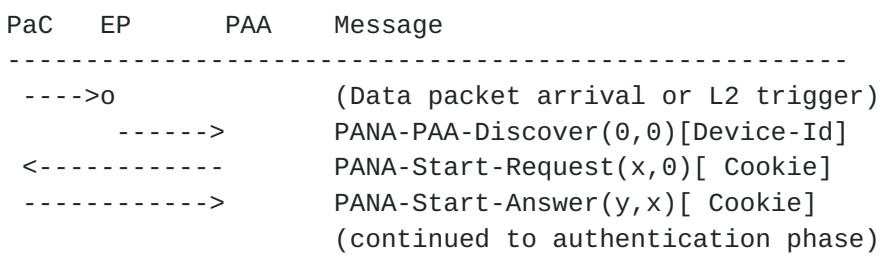


Figure 3: Example Sequence for Discovery and Initial Handshake Phase when PANA-PAA-Discover is sent by PaC

4.3 Authentication Phase when PANA-PAA-Discover is sent by EP

The main task in authentication phase is to carry EAP messages between PaC and PAA. All EAP messages except for EAP Success/Failure messages are carried in the PANA-Auth-Request/PANA-Auth-Answer messages. When an EAP Success/Failure message is sent from a PAA, the message is carried in the PANA-Bind-Request message. The PANA-Bind-Request message is acknowledged with a PANA-Bind-Answer. It is possible to carry multiple EAP sequences in a single PANA session.

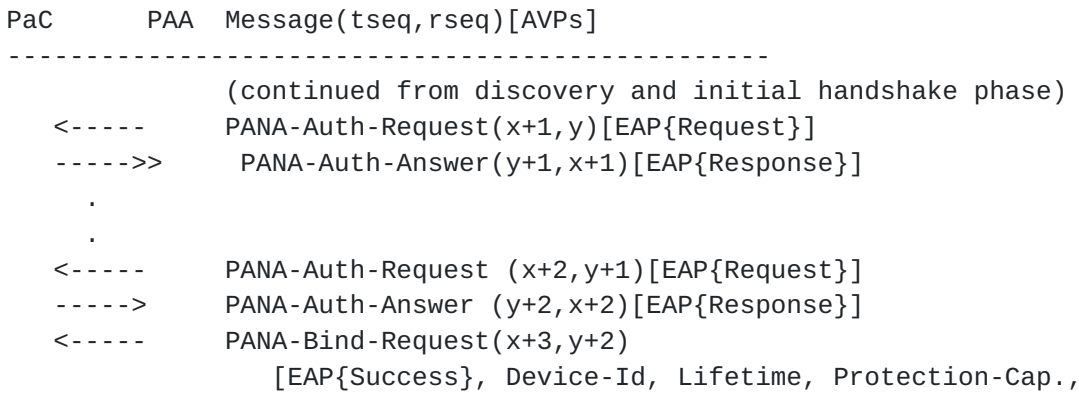
When PaC and PAA negotiated during the discovery and initial handshake phase to perform separate NAP and ISP authentications in a single PANA session, the PAA determines the execution order of NAP authentication and ISP authentication. In this case, the PAA can indicate which EAP authentication is currently occurring by including a NAP-Information or an ISP-Information AVP of the corresponding EAP authentication in the first PANA-Auth-Request message sent to the PaC. In the case where the PaC agreed to perform separate authentications but did not specify its ISP choice in PANA-Start-Answer message, the PAA MUST include its NAP-Information AVP in PANA-Auth-Request message when it performs NAP authentication and MUST NOT include any service provider information AVP when it performs ISP authentication so that the PaC can always distinguish ISP authentication from NAP authentication. The PAA SHOULD stop

including a NAP-Information or an ISP-Information AVP once it receives the first PANA-Auth-Answer message of the current EAP authentication.

Currently, use of multiple EAP methods in PANA is designed only for NAP-ISP authentication separation. It is not for arbitrary EAP method sequencing, or giving the PaC another chance when an authentication method fails. The NAP and ISP authentication are considered completely independent. Presence or success of one should not effect the other. Making an authentication decision based on the success or failure of each authentication is a network policy issue. PANA signals only the result of the immediately preceding EAP authentication method in PANA-Bind-Request messages.

When an EAP method that is capable of deriving keys is used during the authentication phase and the keys are successfully derived the PANA-Bind-Request and PANA-Bind-Answer messages and all subsequent PANA messages MUST contain a MAC AVP. The PANA-Bind-Request and the PANA-Bind-Answer message exchange is also used for binding device identifiers of the PaC and the PAA to the PANA SA. To achieve this, the PANA-Bind-Request and the PANA-Bind-Answer SHOULD contain a device identifier of the PAA and the PaC, respectively, in a Device-Id AVP. The PaC MUST use the same type of device identifier as contained in the PANA-Bind-Request message. The PANA-Bind-Request message MAY also contain a Protection-Capability AVP to indicate if link-layer or network-layer ciphering should be initiated after PANA. No link layer or network layer specific information is included in the Protection-Capability AVP. When the information is preconfigured on the PaC and the PAA this AVP can be omitted. It is assumed that at least PAA is aware of the security capabilities of the access network. The PANA protocol does not specify how the PANA SA and the Protection-Capability AVP will be used to provide per-packet protection for data traffic.

PANA-Bind-Request and PANA-Bind-Answer messages MUST be retransmitted based on the retransmission rule described in Appendix A.



MAC]

```
          ----->     PANA-Bind-Answer(y+3,x+3)
                        [Device-Id, Protection-Cap., MAC]
```

Figure 4: Example Sequence in Authentication Phase

4.4 Re-authentication

There are two types of re-authentication supported by PANA.

The first type of re-authentication is based on EAP by entering an authentication phase. In this case, some or all message exchanges for discovery and initial handshake phase MAY be omitted in the following way. When a PaC wants to initiate EAP-based re-authentication, it sends a unicast PANA-PAA-Discovery message to the PAA. This message MUST contain a Session-Id AVP which is used for identifying the PANA session on the PAA. If the PAA already has an established PANA session for the PaC with the matching identifier, it sends a PANA-Auth-Request message containing the same identifier to start an authentication phase. If the PAA can not recognize the session identifier, it proceeds with regular authentication by sending back PANA-Start-Request. When the PAA initiates EAP-based re-authentication, it sends a PANA-Auth-Request message containing the session identifier for the PaC to enter an authentication phase. PAA SHOULD initiate EAP authentication before the current session lifetime expires. In both cases, the tseq and rseq values are inherited from the previous (re-)authentication. For any EAP-based re-authentication, if there is an established PANA SA, PANA-Auth-Request and PANA-Auth-Answer messages SHOULD be protected by adding a MAC AVP to each message.

The second type of re-authentication is based on a single protected message exchange without entering the authentication phase. PANA-Reauth-Request and PANA-Reauth-Answer messages are used for this purpose. If there is an established PANA SA, both the PaC and the PAA are allowed to send a PANA-Reauth-Request message to the communicating peer whenever it needs to make sure the availability of the PANA SA on the peer and expect the peer to return a PANA-Reauth-Answer message. Both PANA-Reauth-Request/ PANA-Reauth-Answer messages MUST be protected with a MAC AVP.

Implementations MUST limit the rate of performing re-authentication for both types of re-authentication.

```
PaC      PAA     Message(tseq,rseq)[AVPs]
-----------------------------------------------------
   ----->        PANA-Reauth-Request(q,p)[MAC]
   <-----        PANA-Reauth-Answer(p+1,q)[MAC]
```

Figure 5: Example Sequence for PaC-initiated second type Re-authentication

```
PaC      PAA     Message(tseq,rseq)[AVPs]
-----------------------------------------------------
   <-----        PANA-Reauth-Request(p,q)[MAC]
   ----->        PANA-Reauth-Answer(q+1,p)[MAC]
```

Figure 6: Example Sequence for PAA-initiated second type Re-authentication

4.5 Termination Phase

A procedure for explicitly terminating a PANA session can be initiated either from PaC (i.e., disconnect indication) or from PAA (i.e., session revocation). The PANA-Termination-Request and the PANA-Termination-Answer message exchanges are used for disconnect indication and session revocation procedures.

The reason for termination is indicated in the Termination-Cause AVP. When there is an established PANA SA established between the PaC and the PAA, all messages exchanged during the termination phase MUST be protected with a MAC AVP. When the sender of the PANA-Termination-Request receives a valid acknowledgment, all states maintained for the PANA session MUST be deleted immediately.

```
PaC      PAA     Message(tseq,rseq)[AVPs]
-----------------------------------------------------
   ----->        PANA-Termination-Request(q,p)[MAC]
   <-----        PANA-Termination-Answer(p+1,q)[MAC]
```

Figure 7: Example Sequence for Session Termination

4.6 Illustration of a Complete Message Sequence

A complete PANA message sequence is illustrated in Figure 8. The example assumes the following scenario:

- PaC multicasts PANA-PAA-Discover message
- The ISNs used by the PAA and the PaC are x and y, respectively.
- A single EAP sequence is used in authentication phase.
- An EAP authentication method with a single round trip is used in the EAP sequence.
- The EAP authentication method derives keys. The PANA SA is established based on the unique and fresh session key provided by the EAP method.
- After PANA SA is established, all messages are integrity and replay protected with the MAC AVP.
- Re-authentication based on the PANA-Reauth-Request/ PANA-Reauth-Answer exchange is performed.
- The PANA session is terminated as a result of the PANA-Termination-Request indication from the PaC.

```
PaC      PAA  Message(tseq,rseq)[AVPs]
-----------------------------------------------------
// Discovery and initial handshake phase
   ----->     PANA-PAA-Discover (0,0)
   <-----     PANA-Start-Request (x,0)[Cookie]
   ----->     PANA-Start-Request-Answer (y,x)[Cookie]

// Authentication phase
   <-----     PANA-Auth-Request(x+1,y)[EAP]
   ----->     PANA-Auth-Answer(y+1,x+1)[EAP]
   <-----     PANA-Auth-Request(x+2,y+1)[EAP]
   ----->     PANA-Auth-Answer(y+2,x+2)[EAP]
   <-----     PANA-Bind-Request(x+3,y+2)
                [EAP{Success}, Device-Id, Lifetime, Protection-Cap., MAC]
   ----->     PANA-Bind-Answer(y+3,x+3)
                [Device-Id, Protection-Cap., MAC]

// Re-authentication
   <-----     PANA-Reauth-Request (x+4,y+3)[MAC]
   ----->     PANA-Reauth-Answer (y+4,x+4)[MAC]

// Termination phase
   ----->     PANA-Termination-Request(y+5,x+4)[MAC]
   <-----     PANA-Termination-Answer (x+5,y+5)[MAC]
```

Figure 8: A Complete Message Sequence

4.7 Device ID Choice

A PaC SHOULD configure an IP address before PANA if it can. It might either have a pre-configured IP address, or have to obtain one via dynamic methods such as DHCP or stateless address autoconfiguration. Dynamic methods may or may not succeed depending on the local security policy. In networks where clients have to be authorized before they are allowed to obtain an IP address, EPs will detect the associated activity and PANA protocol will be engaged before the clients can configure a valid IP address.

Either an IP address or a link-layer address SHOULD be used as device ID at any time. It is assumed that PAA knows the security mechanisms being provided or required on the access network (e.g., based on physical security, link-layer ciphers enabled before or after PANA, or IPsec). When IPsec-based mechanism [I-D.ietf-pana-ipsec] is the choice of access control, PAA SHOULD provide its IP address as device ID, and expect the PaC to provide its IP address in return. In all other cases, link-layer addresses can be provided from both sides.

When IPsec-based access control is used but the PaC is using an unspecified IP address in the authentication phase, the device ID reported by the PaC MUST be either 0.0.0.0 or 0::0. This device ID MUST be recorded as a temporary one by the PAA until the PaC obtains a valid one and informs the PAA. Eventually PaC MUST obtain an IP address, possibly by relying on the newly-created PANA session [I-D.tschofenig-pana-bootstrap-rfc3118], in order to gain full access to the network. PaC MUST update the device identifier registered on the PAA from unspecified to the valid IP address by initiating a PANA-Reauth-Request/PANA-Reauth-Answer exchange in which the IP address of the PaC is contained in the Device-Id AVP.

4.8 Session Lifetime

The authentication phase determines the PANA session lifetime when the network access authorization succeeds. The Session-Lifetime AVP MAY be optionally included in the PANA-Bind-Request message to inform PaC about the valid lifetime of the PANA session. It MUST be ignored when included in other PANA messages. When there are multiple EAP authentication taking place, this AVP SHOULD be included after the final authentication.

The lifetime is a non-negotiable parameter that can be used by PaC to manage PANA-related state. PaC does not have to perform any actions when the lifetime expires, other than optionally purging local state.

PAA SHOULD initiate EAP authentication before the current session lifetime expires.

PaC and PAA MAY optionally rely on lower-layer indications to expedite the detection of a disconnected peer. Availability and reliability of such indications depend on the specific access technologies. PANA peer can use PANA-Reauth-Request message to verify the disconnection before taking an action.

The session lifetime parameter is not related to the transmission of PANA-Reauth-Request messages. These messages can be used for asynchronously verifying the liveness of the peer and enabling mobility optimizations. The decision to send PANA-Reauth-Request message is taken locally and does not require coordination between the peers.

4.9 Mobility Handling

When a PaC wants to resume an ongoing PANA session after connecting to another link in the same access network, it MAY send the unexpired PANA session identifier in its PANA-Start-Answer message. In the absence of a Session-Id AVP in this message, PAA MUST assume this is a fresh session and continue its normal execution.

If PAA receives a session identifier in the PANA-Start-Answer message, and it is configured to enable fast re-authentication, it SHOULD retrieve the PANA session attributes from the previous PAA of the PaC. The mechanism required to determine the previous PAA of the PaC by relying on the PANA session identifier is outside the scope of PANA protocol. A possible solution is to embed the PAA identifier in the PANA session identifier. Furthermore, the mechanism required to retrieve the session attributes from the previous PAA is outside the scope of this protocol. Seamoby Context Transfer Protocol [I-D.ietf-seamoby-ctp] might be useful for this purpose.

When the PAA is not configured to enable fast re-authentication, or can not retrieve the PANA session attributes, or the PANA session has already expired (i.e., session lifetime is zero), the PAA MUST send the PANA-Auth-Request message with the new session identifier and let the PANA exchange take its usual course. This action will engage EAP authentication and create a fresh PANA session from scratch.

In case the new PAA retrieves the on-going PANA session attributes from the previous PAA, the PANA session continues with a PANA-Reauth exchange. The MAC AVP contained in the PANA-Reauth messages MUST be generated and verified by using the retrieved PANA SA attributes. This exchange MUST also include Session-Id AVP that contains the newly assigned session identifier, and Device-Id AVP. A new PANA

session is created upon successful completion of this exchange. This session inherits only the session lifetime, protection capability, and MSK attributes from the previous session. Other attributes are generated based on the PANA exchanges on the new link. While MSK stays the same, a new PANA_MAC_Key is computed using the new parameters. Subsequent MAC-AVPs are processed using this new PANA SA.

4.10 Event Notification

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-to-EP protocol, or, in the absence of such a facility, PANA-PAA_Discover can be used as well. This message MUST carry the device identifier of the PaC. So that, the PAA can send the unsolicited PANA-Start-Request message directly to the PaC. If the link between the EP and PAA is not physically secured, this message sent from EP to PAA MUST be cryptographically protected (e.g., by using IPsec).

4.11 PaC Implications

- PaC state machine. [TBD]

4.12 PAA Implications

- PAA state machine. [TBD]

5. PANA Security Association Establishment

When PANA is used over an already established secure channel, such as physically secured wires or ciphered link-layers, we can reasonably assume that man-in-the-middle attack or service theft is not possible [I-D.ietf-pana-threats-eval].

Anywhere else where there is no secure channel prior to PANA, the protocol needs to protect itself against such attacks. The device identifier that is used during the authentication needs to be verified at the end of the authentication to prevent service theft and DoS attacks. Additionally, a free loader should be prevented from spoofing data packets by using the device identifier of an already authorized legitimate client. Both of these requirements necessitate generation of a security association between the PaC and the PAA at the end of the authentication. This can only be done when the authentication method used can generate cryptographic keys. Use of secret keys can prevent attacks which would otherwise be very easy to launch by eavesdropping on and spoofing traffic over an insecure link.

PANA relies on EAP and the EAP methods to provide a session key in order to establish a PANA security association. An example of such a method is EAP-TLS [RFC2716], whereas EAP-MD5 [RFC2284] is an example of a method that cannot create such keying material. The choice of EAP method becomes important, as already discussed in the next section.

This keying material is already used within PANA during the final handshake. This handshake ensures that the device identifier that is bound to the PaC at the end of the authentication process is not coming from a man-in-the-middle, but from the legitimate PaC. Knowledge of the same keying material on both PaC and the PAA helps prove this. The other use of the keying material will be discussed in Section 7 and Section 8.

6. Authentication Method Choice

Authentication methods' capabilities and therefore applicability to various environments differ among them. Not all methods provide support for mutual authentication, key derivation or distribution, and DoS attack resiliency that are necessary for operating in insecure networks. Such networks might be susceptible to eavesdropping and spoofing, therefore a stronger authentication method needs to be used to prevent attacks on the client and the network.

The authentication method choice is a function of the underlying security of the network (e.g., physically secured, shared link, etc.). It is the responsibility of the user and the network operator to pick the right method for authentication. PANA carries EAP regardless of the EAP method used. It is outside the scope of PANA to mandate, recommend, or limit use of any authentication methods. PANA cannot increase the strength of a weak authentication method to make it suitable for an insecure environment. There are some EAP- based approaches to achieve this goal (see [I-D.josefsson-pppext-eap-tls-eap],[I-D.ietf-pppext-eap-ttls],[I-D.tschofenig-eap-ikev2]). PANA can carry these EAP encapsulating methods but it does not concern itself with how they achieve protection for the weak methods (i.e., their EAP method payloads).

7. Filter Rule Installation

PANA protocol provides client authentication and authorization functionality for securing network access. The other component of a complete solution is the access control which ensures that only authenticated and authorized clients can gain access to the network. PANA enables access control by identifying legitimate clients and generating filtering information for access control mechanisms. Getting this filtering information to the EPs (Enforcement Points) and performing filtering are outside the scope of PANA.

Access control can be achieved by placing EPs in the network for policing the traffic flow. EPs should prevent data traffic from and to any unauthorized client unless it's PANA traffic. When a client is authenticated and authorized, PAA should notify EP(s) and ask for changing filtering rules to allow traffic for a recently authorized client. There needs to be a protocol between PAA and EP(s) when these entities are not co-located. PANA Working Group will not be defining a new protocol for this interaction. Instead, it will (preferably) identify one of the existing protocols that can fit the requirements. Possible candidates include but not limited to COPS, SNMP, DIAMETER. This task is similar to what MIDCOM Working Group is trying to achieve, therefore some of the MIDCOM's output might be useful here.

EPs' location in the network topology should be appropriate for performing access control functionality. The closest IP-capable access device to the client devices is the logical choice. PAA and EPs on an access network should be aware of each other as this is necessary for access control. Generally this can be achieved by manual configuration. Dynamic discovery is another possibility, but this is clearly outside the scope of PANA.

Filtering rules generally include device identifiers for a client, and also cryptographic keying material when needed. Such keys are needed when attackers can eavesdrop and spoof on the device identifiers easily. They are used with link-layer or network-layer ciphering to provide additional protection. For issues regarding data-origin authentication see Section 8.

8. Data Traffic Protection

Protecting data traffic of authenticated and authorized clients from others is another component of providing a complete secure network access solution. Authentication, integrity and replay protection of data packets are needed to prevent spoofing when the underlying network is not physically secured. Encryption is needed when eavesdropping is a concern in the network.

When the network is physically secured, or the link-layer ciphering is already enabled prior to PANA, data traffic protection is already in place. In other cases, enabling link-layer ciphering or network-layer ciphering might rely on PANA authentication. The user and network have to make sure an appropriate EAP method that can generate required keying materials is used. Once the keying material is available, it needs to be provided to the EP(s) for use with ciphering.

Network-layer ciphering, i.e., IPsec, can be used when data traffic protection is required but link-layer ciphering capability is not available. Note that a simple shared secret generated by an EAP method is not readily usable by IPsec for authentication and encryption of IP packets. Fresh and unique session key derived from the EAP method is still insufficient to produce an IPsec SA since both traffic selectors and other IPsec SA parameters are missing. The shared secret can be used in conjunction with a key management protocol like IKE [RFC2409] to turn a simple shared secret into the required IPsec SA. The details of this mechanism is outside the scope of PANA protocol [I-D.ietf-pana-ipsec], PANA provides bootstrapping functionality for such a mechanism by carrying EAP methods that can generate initial keying material.

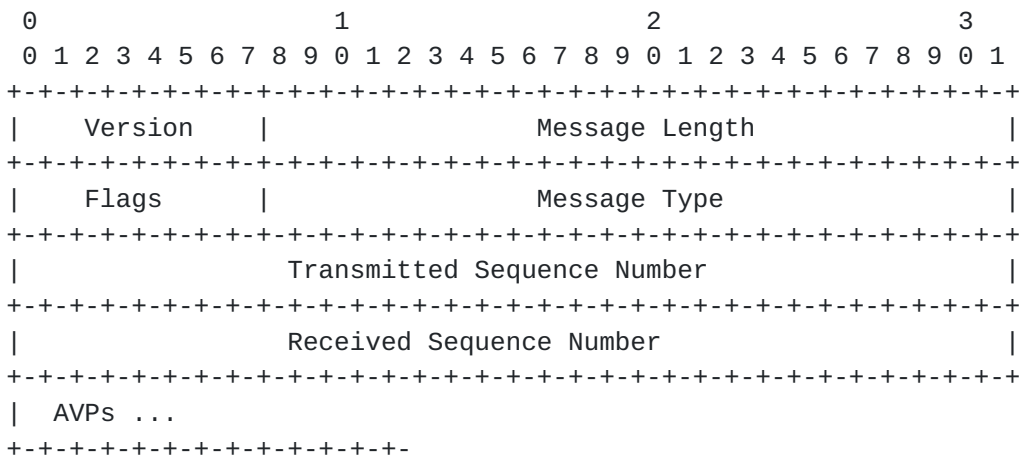
Using network-layer ciphers should be regarded as a substitute for link-layer ciphers when the latter is not available. IKE involves several message exchanges which can incur additional delay in getting basic IP connectivity for a mobile device. Such a latency is inevitable when there is no other alternative and this level of protection is required. Network-layer ciphering can also be used in addition to link-layer ciphering if the added benefits outweigh its cost to the user and the network.

9. Message Formats

This section defines message formats for PANA protocol.

9.1 PANA Header

A summary of the PANA header format is shown below. The fields are transmitted in network byte order.



Version

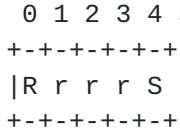
This Version field MUST be set to 1 to indicate PANA Version 1.

Message Length

The Message Length field is three octets and indicates the length of the PANA message including the header fields.

Flags

The Flags field is eight bits. The following bits are assigned:



R(equest)

If set, the message is a request. If cleared, the message is an answer.

S(eparate)

When the S-flag is set in a PANA-Start-Request message it indicates that PAA is willing to offer separate EAP authentication for NAP and ISP. When the S-flag is set in a PANA-Start-Answer message it indicates that PaC accepts on performing separate EAP authentication for NAP and ISP."

r(eserved)

these flag bits are reserved for future use, and MUST be set to zero, and ignored by the receiver.

Message Type

The Message Type field is three octets, and is used in order to communicate the message type with the message. The 24-bit address space is managed by IANA [ianaweb]. PANA uses its own address space for this field.

Transmitted Sequence Number

The Transmitted Sequence Number field contains the monotonically increasing 32 bit sequence number that the message sender increments every time a new PANA message is sent.

Received Sequence Number

The Received Sequence Number field contains the 32 bit transmitted sequence number that the message sender has last received from its peer.

AVPs

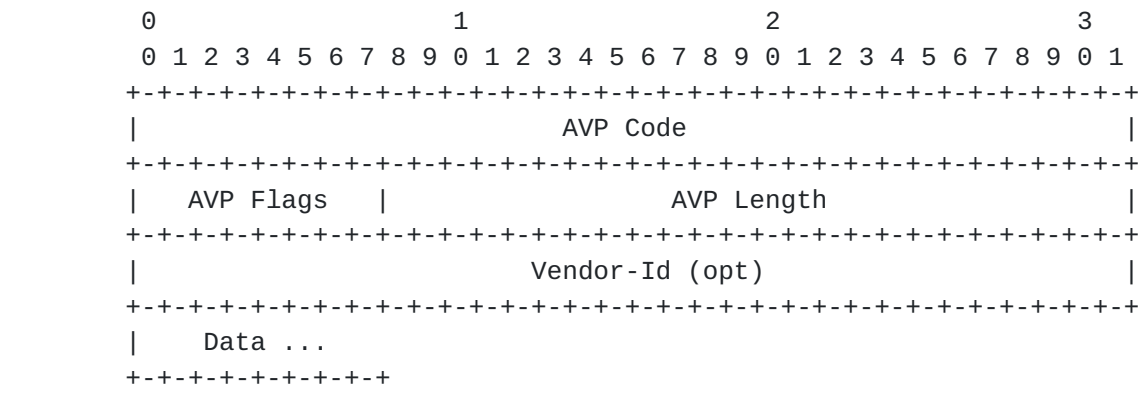
AVPs are a method of encapsulating information relevant to the PANA message. See section Section 9.2 for more information on AVPs.

9.2 AVP Header

Each AVP of type OctetString MUST be padded to align on a 32-bit boundary, while other AVP types align naturally. A number of zero-valued bytes are added to the end of the AVP Data field till a word boundary is reached. The length of the padding is not reflected in the AVP Length field [RFC3588].

The fields in the AVP header MUST be sent in network byte order. The

format of the header is:

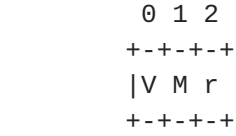


AVP Code

The AVP Code, combined with the Vendor-Id field, identifies the attribute uniquely. AVP numbers are allocated by IANA [ianaweb]. PANA uses its own address space for this field although some of the AVP formats are borrowed from Diameter protocol [RFC3588].

AVP Flags

The AVP Flags field is eight bits. The following bits are assigned:



M(andatory)

The 'M' Bit, known as the Mandatory bit, indicates whether support of the AVP is required.

V(endor)

The 'V' bit, known as the Vendor-Specific bit, indicates whether the optional Vendor-Id field is present in the AVP header.

r(eserved)

these flag bits are reserved for future use, and MUST be set to zero, and ignored by the receiver.

AVP Length

The AVP Length field is three octets, and indicates the number of octets in this AVP including the AVP Code, AVP Length, AVP Flags, and the AVP data

Vendor-Id

The Vendor-Id field is present if the 'V' bit is set in the AVP Flags field. The optional four-octet Vendor-Id field contains the uniquely assigned id value, encoded in network byte order. Any vendor wishing to implement a vendor-specific PANA AVP MUST use their own Vendor-Id along with their privately managed AVP address space, guaranteeing that they will not collide with any other vendor's vendor-specific AVP(s), nor with future IETF applications.

Data

The Data field is zero or more octets and contains information specific to the Attribute. The format and length of the Data field is determined by the AVP Code and AVP Length fields.

9.3 PANA Messages

Figure 9 lists all PANA messages defined in this document

```
Message       Direction: PaC---PAA
-----------------------------------
PANA-PAA-Discover        -------->

PANA-Start-Request       <--------
PANA-Start-Answer        -------->

PANA-Auth-Request        <--------
PANA-Auth-Answer         -------->

PANA-Bind-Request        <--------
PANA-Bind-Answer         -------->

PANA-Reauth-Request      <------->
PANA-Reauth-Answer       <------->

PANA-Termination-Request <------->
PANA-Termination-Answer  <------->

PANA-Error               <------->
```

Figure 9: PANA Message Overview

Additionally the EP can also send a PANA-PAA-Discover message to the PAA.

9.3.1 Message Specifications

Every PANA message MUST include a corresponding ABNF [RFC2234] specification found in [RFC3588]. Note that PANA messages have a different header format compared to Diameter.

Example:

```
message ::= < PANA-Header: <Message type>, [REQ] [SEP] >
                              * [ AVP ]
```

9.3.2 PANA-PAA-Discover (PDI)

The PANA-PAA-Discover (PDI) message is used to discover the address of PAA(s). Both sequence numbers in this message are set to zero (0). If the EP detects a new PaC and sends the PANA-PAA-Discover to the PAA, it MUST include the Device-Id of the PaC.

```
PANA-PAA-Discover ::= < PANA-Header: 1 >
          0*1 < Device-Id >
           *  [ AVP ]
```

9.3.3 PANA-Start-Request (PSR)

PANA-Start-Request (PSR) is sent by the PAA to the PaC. The PAA sets the transmission sequence number to an initial random value. The received sequence number is set to zero (0).

```
PANA-Start-Request ::= < PANA-Header: 2, REQ [SEP] >
              [ Cookie ]
              [ NAP-Information ]
           *  [ ISP-Information ]
           *  [ AVP ]
```

9.3.4 PANA-Start-Answer (PSA)

PANA-Start-Answer (PSA) is sent by the PaC to the PAA in response to a PANA-Start-Request message. The PANA_start message transmission sequence number field is copied to the received sequence number field. The transmission sequence number is set to initial random

value.

```
PANA-Start-Answer ::= < PANA-Header: 2 [SEP] >
                      [ Cookie ]
                      [ ISP-Information ]
                    *  [ AVP ]
```

9.3.5 PANA-Auth-Request (PAR)

PANA-Auth-Request (PAR) is sent by the PAA to the PaC.

```
PANA-Auth-Request ::= < PANA-Header: 3, REQ >
                      < Session-Id >
                      < EAP-Payload >
                    0*1 [ NAP-Information ]
                    0*1 [ ISP-Information ]
                     *  [ AVP ]
                    0*1 < MAC >
```

(Both NAP-Information and ISP-Information MUST NOT be included at the same time)"

9.3.6 PANA-Auth-Answer (PAN)

PANA-Auth-Answer (PAN) is sent by the PaC to the PAA in response to a PANA-Auth-Request message.

```
PANA-Auth-Answer ::= < PANA-Header: 3 >
                     < Session-Id >
                     < EAP-Payload >
                      *  [ AVP ]
                    0*1 < MAC >
```

9.3.7 PANA-Bind-Request (PBR)

PANA-Bind-Request (PBR) is sent by the PAA to the PaC.

```
PANA-Bind-Request ::= < PANA-Header: 4, REQ >
                      < Session-Id >
                      < Device-Id >
                      { EAP-Payload }
                      { Result-Code }
                      [ Session-Lifetime ]
                      [ Protection-Capability ]
                       *  [ AVP ]
                      0*1 < MAC >
```

9.3.8 PANA-Bind-Answer (PBA)

PANA-Bind-Answer (PBA) is sent by the PaC to the PAA in response to a PANA-Result-Request message.

```
      PANA-Bind-Answer ::= < PANA-Header: 4 >
                           < Session-Id >
                           < Device-Id >
                         *  [ AVP ]
                        0*1 < MAC >
```

9.3.9 PANA-Reauth-Request (PRAR)

PANA-Reauth-Request (PRAR) is either sent by the PaC or the PAA.

```
      PANA-Reauth-Request ::= < PANA-Header: 5, REQ >
                           < Session-Id >
                           < Device-Id >
                         *  [ AVP ]
                        0*1 < MAC >
```

9.3.10 PANA-Reauth-Answer (PRAA)

PANA-Reauth-Answer (PRAA) is sent in response to a PANA-Reauth-Request.

```
      PANA-Reauth-Answer ::= < PANA-Header: 5 >
                           < Session-Id >
                           < Device-Id >
                         *  [ AVP ]
                        0*1 < MAC >
```

9.3.11 PANA-Termination-Request (PTR)

PANA-Termination-Request (PTR) is sent either by the PaC or the PAA.

```
      PANA-Termination-Request ::= < PANA-Header: 6, REQ >
                           < Session-Id >
                           < Termination-Cause >
                         *  [ AVP ]
                        0*1 < MAC >
```

9.3.12 PANA-Termination-Answer (PTA)

PANA-Termination-Answer (PTA) is sent either by the PaC or the PAA in response to PANA-Termination-Request.

```
PANA-Termination-Answer ::= < PANA-Header: 6 >
                            < Session-Id >
                         *  [ AVP ]
                        0*1 < MAC >
```

9.3.13 PANA-Error (PER)

PANA-Error is sent either by the PaC or the PAA.

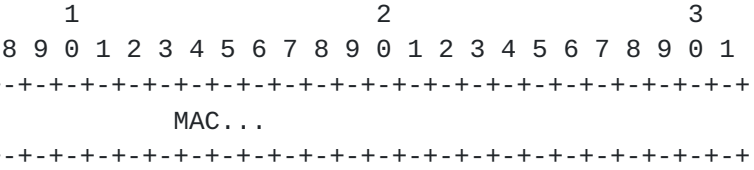
```
PANA-Error ::= < PANA-Header: 7 >
               < Session-Id >
               < Result-Code >
               { Failed-AVP }
            *  [ AVP ]
           0*1 < MAC >
```

9.4 AVPs in PANA

Some of the used AVPs are defined in this document and some of them are defined in other documents like [RFC3588]. PANA proposes to use the same name space with the Diameter spec. For temporary allocation, PANA uses AVP type numbers starting from 1024.

9.4.1 MAC AVP

The first octet (8 bits) of the MAC (Code 1024) AVP data contains the MAC algorithm type. Rest of the AVP data payload contains the MAC encoded in network byte order. The Algorithm 8 bit name space is managed by IANA [ianaweb]. The AVP length varies depending on the used algorithm.



Algorithm

```
1             HMAC-MD5 (16 bytes)
2             HMAC-SHA1 (20 bytes)
```

MAC

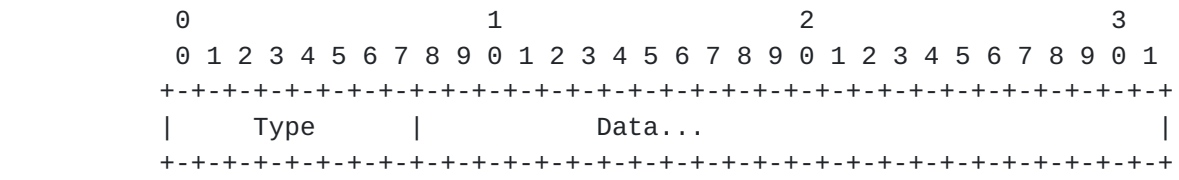
The Message Authentication Code is encoded in network byte order.

9.4.2 Device-Id AVP

The first octet (8 bits) of the Device-Id (Code 1025) AVP data contains the device type. Rest of the AVP data payload contains the device data. The content and format of data (including byte and bit ordering) for L2_ADDRESS is expected to be specified in specific documents that describe how IP operates over different link-layers. For instance, [RFC2464].

RESERVED	0
IPV4_ADDRESS	1
IPV6_ADDRESS	2
L2_ADDRESS	3

For type 1 (IPv4 address), data size is 32 bits and for type 2 (IPv6 address), data size is 128 bits.



9.4.3 Session-Id AVP

Session-Id AVP (Code 1026) has an opaque data field, which is assigned by the PAA. All messages pertaining to a specific PANA Session MUST include only one Session-Id AVP and the same value MUST be used throughout the lifetime of a session. When present, the Session-Id SHOULD appear immediately following the PANA header.

The Session-Id MUST be globally and eternally unique, as it is meant to identify a PANA Session without reference to any other information, and may be needed to correlate historical authentication information with accounting information.

The Session-Id AVP MAY use Diameter [RFC3588] message formatting. In this case the AVP code is 263.

9.4.4 Cookie AVP

The Cookie AVP (Code 1027) is of type OctetString. The data is opaque

and the exact content is outside the scope of this protocol.

9.4.5 Protection-Capability AVP

The Protection-Capability AVP (Code 1028) is of type Unsigned32. The AVP data is used as a collection of flags for different data protection capability indications. Below is a list of specified data protection capabilities:

0	UNKNOWN
1	L2_PROTECTION
2	IPSEC_PROTECTION

9.4.6 Termination-Cause AVP

The Termination-Cause AVP (Code 1029) is of type of type Enumerated, and is used to indicate the reason why a session was terminated on the access device. The AVP data is used as a collection of flags The following Termination-Cause AVP defined in [RFC3588] are used for PANA.

LOGOUT 1 (PaC -> PAA)

The client initiated a disconnect

ADMINISTRATIVE 4 (PAA -> Pac)

The client was not granted access, or was disconnected, due to administrative reasons, such as the receipt of a Abort-Session-Request message.

SESSION_TIMEOUT 8 (PAA -> PaC)

The session has timed out, and service has been terminated.

9.4.7 Result-Code AVP

The Result-Code AVP (AVP Code 1030) is of type Unsigned32 and indicates whether an EAP authentication was completed successfully or whether an error occurred. Here are Result-Code AVP values taken from [RFC3588] and adapted for PANA.

9.4.7.1 Authentication Results Codes

These result code values inform the PaC about the EAP authentication method success or failure.

PANA_SUCCESS 2001

The EAP method authentication was successful (EAP-Success).

PANA_AUTHENTICATION_REJECTED 4001

The authentication process for the client failed (EAP-Failure).

PANA_AUTHORIZATION_REJECTED 5003

A request was received for which the client could not be authorized. This error could occur if the service requested is not permitted to the client.

9.4.7.2 Protocol Error Result Codes

Protocol error result code values.

PANA_MESSAGE_UNSUPPORTED 3001

Error code from PAA to PaC or from PaC to PAA. Message type not recognized or supported.

PANA_UNABLE_TO_DELIVER 3002

Error code from PAA to PaC. PAA was unable to deliver the EAP payload to the authentication server.

PANA_INVALID_HDR_BITS 3008

Error code from PAA to PaC or from PaC to PAA. A message was received whose bits in the PANA header were either set to an invalid combination, or to a value that is inconsistent with the message type's definition.

PANA_INVALID_AVP_BITS 3009

Error code from PAA to PaC or from PaC to PAA. A message was received that included an AVP whose flag bits are set to an unrecognized value, or that is inconsistent with the AVP's definition.

PANA_AVP_UNSUPPORTED 5001

Error code from PAA to PaC or from PaC to PAA. The received message contained an AVP that is not recognized or supported and was marked with the Mandatory bit. A PANA message with this error

MUST contain one or more Failed-AVP AVP containing the AVPs that caused the failure.

PANA_UNKNOWN_SESSION_ID 5002

Error code from PAA to PaC or from PaC to PAA. The message contained an unknown Session-Id. PAA MUST NOT send this error result code value to PaC if PaC sent an unknown Session-Id in the PANA-Start-Answer message (session resumption).

PANA_INVALID_AVP_VALUE 5004

Error code from PAA to PaC or from PaC to PAA. The message contained an AVP with an invalid value in its data portion. A PANA message indicating this error MUST include the offending AVPs within a Failed-AVP AVP.

PANA_MISSING_AVP 5005

Error code from PAA to PaC or from PaC to PAA. The message did not contain an AVP that is required by the message type definition. If this value is sent in the Result-Code AVP, a Failed-AVP AVP SHOULD be included in the message. The Failed-AVP AVP MUST contain an example of the missing AVP complete with the Vendor-Id if applicable. The value field of the missing AVP should be of correct minimum length and contain zeroes.

PANA_RESOURCES_EXCEEDED 5006

Error code from PAA to PaC. A message was received that cannot be authorized because the client has already expended allowed resources. An example of this error condition is a client that is restricted to one PANA session and attempts to establish a second session.

PANA_CONTRADICTING_AVPS 5007

Error code from PAA to PaC. The PAA has detected AVPs in the message that contradicted each other, and is not willing to provide service to the client. One or more Failed-AVP AVPs MUST be present, containing the AVPs that contradicted each other.

PANA_AVP_NOT_ALLOWED 5008

Error code from PAA to PaC or from PaC to PAA. A message was received with an AVP that MUST NOT be present. The Failed-AVP AVP MUST be included and contain a copy of the offending AVP.

PANA_AVP_OCCURS_TOO_MANY_TIMES 5009

Error code from PAA to PaC or from PaC to PAA. A message was received that included an AVP that appeared more often than permitted in the message definition. The Failed-AVP AVP MUST be included and contain a copy of the first instance of the offending AVP that exceeded the maximum number of occurrences.

PANA_UNSUPPORTED_VERSION 5011

Error code from PAA to PaC or from PaC to PAA. This error is returned when a message was received, whose version number is unsupported.

PANA_INVALID_AVP_LENGTH 5014

Error code from PAA to PaC or from PaC to PAA. The message contained an AVP with an invalid length. The PANA-Error message indicating this error MUST include the offending AVPs within a Failed-AVP AVP.

PANA_INVALID_MESSAGE_LENGTH 5015

Error code from PAA to PaC or from PaC to PAA. This error is returned when a message is received with an invalid message length.

9.4.8 EAP-Payload AVP

The EAP-Payload AVP (AVP Code 1031) is of type OctetString and is used to encapsulate the actual EAP packet that is being exchanged between the EAP peer and the EAP authenticator.

9.4.9 Session-Lifetime AVP

The Session-Lifetime AVP (Code 1032) data is of type Unsigned32. It contains the number of seconds remaining before the current session is considered expired.

9.4.10 Failed-AVP AVP

The Failed-AVP AVP (AVP Code 1033) is of type Grouped and provides debugging information in cases where a request is rejected or not fully processed due to erroneous information in a specific AVP. The format of the Failed-AVP AVP is defined in [RFC3588].

9.4.11 NAP-Information AVP

The NAP-Information AVP (AVP Code: 1034) is of type Grouped, and contains zero or one Provider-Identifier AVP which carries the identifier of the NAP and one Provider-Name AVP which carries the name of the NAP. Its Data field has the following ABNF grammar:

```
NAP-Information ::= < AVP Header: 1034 >
                    0*1 { Provider-Identifier }
                        { Provider-Name }
                     *  [ AVP ]
```

9.4.12 ISP-Information AVP

The ISP-Information AVP (AVP Code: 1035) is of type Grouped, and contains zero or one Provider-Identifier AVP which carries the identifier of the ISP and one Provider-Name AVP which carries the name of the ISP. Its Data field has the following ABNF grammar:

```
ISP-Information ::= < AVP Header: 1035 >
                    0*1 { Provider-Identifier }
                        { Provider-Name }
                     *  [ AVP ]
```

9.4.13 Provider-Identifier AVP

The Provider-Identifier AVP (AVP Code: 1036) is of type Unsigned32, and contains an IANA assigned "SMI Network Management Private Enterprise Codes" [ianaweb] value, encoded in network byte order.

9.4.14 Provider-Name AVP

The Provider-Name AVP (AVP Code: 1037) is of type UTF8String, and contains the UTF8-encoded name of the provider.

9.5 AVP Occurrence Table

The following tables lists the AVPs used in this document, and specifies in which PANA messages they MAY, or MAY NOT be present.

The table uses the following symbols:

0 The AVP MUST NOT be present in the message.

0+ Zero or more instances of the AVP MAY be present in the message.

0-1 Zero or one instance of the AVP MAY be present in the message. It is considered an error if there are more than one instance of the AVP.

1 One instance of the AVP MUST be present in the message.

1+ At least one instance of the AVP MUST be present in the message.

	Message Type						
Attribute Name	PSR	PSA	PAR	PAN	PBR	PBA	PDI
Result-Code	0	0	0	0	1	0	0
Session-Id	0	0	1	1	1	1	0
Termination-Cause	0	0	0	0	0	0	0
EAP-Payload	0	0	1	1	1	0	0
MAC	0	0	0-1	0-1	0-1	0-1	0
Device-Id	0	0	0	0	1+	1+	0-1
Cookie	0-1	0-1	0	0	0	0	0
Protection-Cap.	0	0	0	0	0-1	0	0
Session-Lifetime	0	0	0	0	0-1	0	0
Failed-AVP	0	0	0	0	0	0	0
ISP-Information	0+	0-1	0-1	0	0	0	0
NAP-Information	0-1	0	0-1	0	0	0	0

	Message Type				
Attribute Name	PRAR	PRAA	PTR	PTA	PER
Result-Code	0	0	0	0	1
Session-Id	1	1	1	1	1
Termination-Cause	0	0	1	0	0
EAP-Payload	0-1	0-1	0	0	0
MAC	0-1	0-1	0-1	0-1	0-1
Device-Id	1+	1+	0	0	0
Cookie	0	0	0	0	0
Protection-Cap.	0	0	0	0	0
Session-Lifetime	0	0	0	0	0

Failed-AVP	0	0	0	0	1
ISP-Information	0	0	0	0	0
NAP-Information	0	0	0	0	0

Figure 10: AVP Occurrence Table

10. PANA Protocol Message Retransmissions

The PANA protocol provides retransmissions for all the message exchanges except PANA-Auth-Request/Answer. PANA-Auth-Request messages carry EAP requests which are retransmitted by the EAP protocol entities when needed. The messages that need PANA-level retransmissions are listed below:

PANA-PAA-Discover (PDI)
PANA-Start-Answer (PSA)
PANA-Bind-Request (PBR)
PANA-Reauth-Request (PRAR)
PANA-Termination-Request (PTR)

The PDI and PSA messages are always sent by the PaC. PBR is sent by PAA. The last two messages, PRAR and PTR are sent either by PaC or PAA.

The rule is that the sender of the request message retransmits the request if the corresponding answer is not received in time. Answer messages are sent as answers to the request messages, not based on a timer. Exception to this rule is the PSA message. Because of the stateless nature of the PAA in the beginning PaC provides retransmission also for the PSA message. PANA-Error messages MUST not be retransmitted. See Section 4.1.8 for more details of PANA error handling.

PANA retransmission timers are based on the model used in DHCPv6 [RFC3315]. Variables used here are also borrowed from this specification. PANA is a request response like protocol. The message exchange terminates when either the request sender successfully receives the appropriate answer, or when the message exchange is considered to have failed according to the retransmission mechanism described below.

The retransmission behavior is controlled and described by the following variables:

RT	Retransmission timeout
IRT	Initial retransmission time
MRC	Maximum retransmission count
MRT	Maximum retransmission time
MRD	Maximum retransmission duration

RAND Randomization factor

With each message transmission or retransmission, the sender sets RT according to the rules given below. If RT expires before the message exchange terminates, the sender recomputes RT and retransmits the message.

Each of the computations of a new RT include a randomization factor (RAND), which is a random number chosen with a uniform distribution between -0.1 and +0.1. The randomization factor is included to minimize synchronization of messages.

The algorithm for choosing a random number does not need to be cryptographically sound. The algorithm SHOULD produce a different sequence of random numbers from each invocation.

RT for the first message transmission is based on IRT:

```
RT = IRT + RAND*IRT
```

RT for each subsequent message transmission is based on the previous value of RT:

```
RT = 2*RTprev + RAND*RTprev
```

MRT specifies an upper bound on the value of RT (disregarding the randomization added by the use of RAND). If MRT has a value of 0, there is no upper limit on the value of RT. Otherwise:

```
if (RT > MRT)
   RT = MRT + RAND*MRT
```

MRC specifies an upper bound on the number of times a sender may retransmit a message. Unless MRC is zero, the message exchange fails once the sender has transmitted the message MRC times.

MRD specifies an upper bound on the length of time a sender may retransmit a message. Unless MRD is zero, the message exchange fails once MRD seconds have elapsed since the client first transmitted the message.

If both MRC and MRD are non-zero, the message exchange fails whenever either of the conditions specified in the previous two paragraphs are met.

If both MRC and MRD are zero, the client continues to transmit the message until it receives a response.

10.1 Transmission and Retransmission Parameters

This section presents a table of values used to describe the message retransmission behavior of request and PANA-Start-Answer messages marked with REQ_*. PANA-PAA-Discover message retransmission values are marked with PDI_*. The table shows default values.

Parameter	Default	Description
PDI_IRT	1 sec	Initial PDI timeout.
PDI_MRT	120 secs	Max PDI timeout value.
PDI_MRC	0	Configurable.
PDI_MRD	0	Configurable.
REQ_IRT	1 sec	Initial Request timeout.
REQ_MRT	30 secs	Max Request timeout value.
REQ_MRC	10	Max Request retry attempts.
REQ_MRD	0	Configurable.

So for example the first RT for the PBR message is calculated using REQ_IRT as the IRT:

RT = REQ_IRT + RAND*REQ_IRT

11. Security Considerations

The PANA protocol provides ordered delivery for EAP messages. If an EAP method that provides session keys is used, a PANA SA is created. The EAP Success/Failure message is one of the signaling messages which is integrity protected with this PANA SA. The PANA protocol does not provide security protection for the initial EAP message exchange. Integrity protection can only be provided after the PANA SA has been established. Thus, PANA re-authentication, revocation and disconnect notifications can be authenticated, integrity and replay protected. In certain environments (e.g. on a shared link) the EAP method selection is an important issue.

The PANA framework described in this document covers the discussion of different protocols which are of interest for a protocol between the PaC and the PAA (typically referred as the PANA protocol).

The PANA itself consists of a sequence of steps which are executed to complete the network access authentication procedure. Some of these steps are optional.

The following execution steps have been identified as being relevant for PANA. They security considerations will be discussed in detail subsequently.

a) Discovery message exchange

In general it is difficult to prevent a vulnerabilities of the discovery protocol since the initial discovery are unsecured. To prevent very basic attacks an adversary should not be able to cause state creation with discovery messages at the PAA. This is prevented by re-using a cookie concept (see [RFC2522] which allows the responder to be stateless in the first message exchange. Because of the architectural assumptions made in PANA (i.e. the PAA is the on the same link as the PaC) the return-routability concept does not provide additional protection. Hence it is difficult to prevent this threat entirely. Furthermore it is not possible to shift heavy cryptographic operations to the PaC at the first few messages since the computational effort depends on the EAP method. The usage of client-puzzles as introduced by [jb99] is under investigation.

Resistance against blind DoS attacks (i.e. attacks by off-path adversaries) is achieved with sequence numbers and cookies.

Since PAA and PaC are supposed to be one IP hop away, a simple TTL check can prevent off-link attacks. Furthermore, additional filtering can be enabled on the EPs. An EP may be able to filter unauthorized PAA advertisements when they are received on the access side of the

network where only PaCs are connected.

b) EAP over PANA message exchange

The EAP derived session key is used to create a PANA security association. Since the execution of an EAP method might require a large number of roundtrips and no other session key is available it is not possible to secure the EAP message exchange itself. Hence an adversary can both eavesdrop the EAP messages and is also able to inject arbitrary messages which might confuse both the EAP peer on PaC and the EAP authenticator or authentication server on the PAA. The threats caused by this ability heavily depend on the EAP state machine. Since especially the PAA is not allowed to discard packets and packets have to be stored or forwarded to an AAA infrastructure some risk of DoS attacks exists.

Eavesdropping EAP packets might cause problems when (a) the EAP method is weak and enables dictionary or replay attacks or even allows an adversary to learn the long-term password directly. Furthermore, if the optional EAP Identity payload is used then it allows the adversary to learn the identity of the PaC. In such a case a privacy problem is prevalent.

To prevent these threats Section 6 suggests using proper EAP methods for particular environments. Depending on the usage environment an EAP authentication has to be used for example which supports user identity confidentiality, protection against dictionary attacks and session key establishment. It is therefore the responsibility of the network operators and end users to choose the proper EAP method.

PANA does not protect the EAP method exchange, but provides ordered delivery with sequence numbers. Sequence numbers and cookies provide resistance against blind DoS attacks.

c) PANA SA establishment

Once the EAP message authentication is finished a fresh and unique session key is available to the PaC and the PAA. This assumes that the EAP method allows session key derivation and that the generated session key has a good quality. For further discussion about the importance of the session key generation refer to the next subsection (d) about compound authentication. The session key available for the PaC is established as part of the authentication and key exchange procedure of the selected EAP method. The PAA obtains the session key via the AAA infrastructure (if used). Draft [I-D.ietf-aaa-diameter-cms-sec] describes how a session key is securely carried (i.e. CMS protected) between AAA servers. Security issues raised with this session key transport are described in

[I-D.walker-aaa-key-distribution].

The establishment of a PANA SA is required in environments where no physical or link layer security is available. The PANA SA allows subsequently exchanged messages to experience cryptographic protection. For the current version of the document an integrity object (MAC AVP) is defined which supports data-origin authentication, replay protection based on sequence numbers and integrity protection based on a keyed message digest. Confidentiality protection is not provided. The session keys used for this object have to be provided by the EAP method. For this version of the document it is assumed that no negotiation of algorithms and parameters takes place. Instead HMAC-SHA1 is used by default. A different algorithm such as HMAC-MD5 might be used as an option. The used algorithm is indicated in the header of the Integrity object. To select the security association for signaling message protection the Session ID is conveyed. The keyed message digest included in the Integrity object will include all fields of the PANA signaling message including the sequence number field of the packet.

The protection of subsequent signaling messages prevents an adversary from acting as a man-in-the-middle adversary, from injecting packets, from replaying messages and from modifying the content of the exchanged packets. This prevents subsequently described threats.

If an entity (PAA or PaC) loses its state (especially the current sequence number) then the entire PANA protocol has to be restarted. No re-synchronization procedure is provided.

The lifetime of the PANA SA has to be bound to the AAA-authorized session lifetime with an additional tolerance period. Unless PANA state is updated by executing another EAP authentication, PANA SA is removed when the current session expires. The lifetime of the PANA SA has to be bound to the AAA-authorized session lifetime with an additional tolerance period. Unless PANA state is updated by executing another EAP authentication, PANA SA is removed when the current session expires.

d) Enabling weak legacy authentication methods in insecure networks

Some of the authentication methods are not strong enough to be used in insecure networks where attackers can easily eavesdrop and spoof on the link. They may not be able to produce much needed keying material either. An example would be using EAP-MD5 over wireless links. Use of such legacy methods can be enabled by carrying them over a secure channel. There are EAP methods which are specifically designed for this purpose, such as EAP-TTLS [I-D.ietf-pppext-eap-ttls],PEAP [I-D.josefsson-pppext-eap-tls-eap] or

EAP-IKEv2 [I-D.tschofenig-eap-ikev2]. PANA can carry these EAP tunneling methods which can carry the legacy methods. PANA does not do anything special for this case. The EAP tunneling method will have to produce keying material for PANA SA when needed. There are certain MitM vulnerabilities with tunneling EAP methods [mitm]. Solving these problems is outside the scope of PANA. The compound authentication problem described in [I-D.puthenkulam-eap-binding] is likely to be solved in EAP itself rather than in PANA.

e) Preventing downgrading attacks

EAP supports a number of different EAP methods for authentication and therefore it might be required to agree on a specific mechanism. An unprotected negotiation mechanism is supported in EAP and a secure negotiation procedure for the GSS-API methods. The support of the GSS-API as an EAP method is described in [I-D.aboba-pppext-eapgss]. A protected negotiation is supported by the GSS-API with RFC 2478 [RFC2478]. If desired, such a protection can also be offered by PANA by repeating the list of supported EAP methods protected with the PANA SA. This type of protection is similar to the protected negotiation described in [RFC3329].

This issue requires further investigation especially since the EAP protocol is executed between different endpoints than the PANA protocol.

f) Device Identifier exchange

As part of the authorization procedure a Device Identifier has to be installed at the EP by the PAA. The PaC provides the Device Identifier information to the PAA secured with the PANA SA. Section 6.2.4 of [I-D.ietf-pana-threats-eval] describes a threat where an adversary modifies the Device Identifier to gain unauthorized access to the network.

The installation of the Device Identifier at the EP (independently whether the EP is co-located with the PAA or not) has to be accomplished in a secure manner. These threats are, however, not part of the PANA protocol itself since the protocol is not PANA specific.

g) Triggering a data protection protocol

Recent activities in the EAP working group try to create a common framework for key derivation which is described in [I-D.aboba-pppext-key-problem]. This framework is also relevant for PANA in various ways. First, a PANA security association needs to be created. Additionally it might be necessary to trigger a protocol which allows link layer and network layer data protection to be

established. As an example see Section 1 of [I-D.aboba-pppext-key-problem] with [802.11i] and [802.11] as an example. Furthermore, a derived session key might help to create the pre-requisites for network-layer protection (for example IPsec [I-D.ietf-pana-ipsec]).

As motivated in Section 6.4 of [I-D.ietf-pana-threats-eval] it might be necessary to establish either a link layer or a network layer protection to prevent certain thefts in certain scenarios.

Threats specific to the establishment of a link layer or a network layer security association are outside the scope of PANA. The interested reader should refer to the relevant working groups such as IPsec or Midcom.

h) Liveness test

Network access authentication is done for a very specific purpose and often charging procedures are involved which allow restricting network resource usage based on some policies. In mobility environments it is always possible that an end host suddenly disconnects without transmitting a disconnect message. Operators are generally motivated to detect a disconnected end host as soon as possible in order to release resources (i.e., garbage collection). The PAA can remove per-session state information including installed security association, packet filters, etc.

Different procedures can be used for disconnect indication. PANA cannot assume link-layer disconnect indication. Hence this functionality has to be provided at a higher layer. With this version of the draft we suggest to apply the soft-state principle found at other protocols (such as RSVP). Soft-state means that session state is kept alive as long as refresh messages refresh the state. If no new refresh messages are provided then the state automatically times out and resources are released. This process includes stopping accounting procedures.

A PANA session is associated with a session lifetime. The session is terminated unless it is refreshed by a new round of EAP authentication before it expires. Therefore, at the latest a disconnected client can be detected when its lifetime expires. A disconnect may also be detected earlier by using PANA reauthentication messages. A request message can be generated by either PaC or PAA at any time and the peer must respond with an answer message. A successful round-trip of this exchange is a simple verification that the peer is alive. This test can be engaged when there is a possibility that the peer might have disconnected (e.g., after discontinuation of data traffic). Periodic use of this exchange

as a keep-alive requires additional care as it might result in congestion and hence false alarms. This exchange is cryptographically protected when PANA SA is available in order to prevent threats associated with the abuse of this functionality.

i) Tear-Down message

The PANA protocol supports the ability for both the PaC and the PAA to transmit a tear-down message. This message causes state removal, a stop of the accounting procedure and removes the installed packet filters.

It is obvious that such a message must be protected to prevent an adversary from deleting state information and thereby causing denial of service attacks.

12. Open Issues

A list of open issues is maintained at [1].

The remaining issues for -01 version of draft are: None.

The remaining issues for -xx version of draft are: 2, 12, 16, 28, 29, 34, 35, 36 and 37.

13. Change History

Issues incorporated in PANA-01 June 2003: 1, 3, 10, 5, 6, 7 and 11.

Issues incorporated in PANA-02 October 2003: 8, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 30, 31, 32 and 33.

14. Acknowledgments

We would like to thank all members of the PANA working group for their comments to this document.

Normative References

[I-D.ietf-pana-usage-scenarios]
Ohba, Y., "Problem Statement and Usage Scenarios for PANA", draft-ietf-pana-usage-scenarios-06 (work in progress), April 2003.

[RFC2284] Blunk, L. and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[I-D.ietf-pana-threats-eval]
Parthasarathy, M., "PANA Threat Analysis and security requirements", draft-ietf-pana-threats-eval-04 (work in progress), May 2003.

[I-D.ietf-pana-requirements]
Yegin, A. and Y. Ohba, "Protocol for Carrying Authentication for Network Access (PANA)Requirements", draft-ietf-pana-requirements-07 (work in progress), June 2003.

[RFC1982] Elz, R. and R. Bush, "Serial Number Arithmetic", RFC 1982, August 1996.

[RFC2988] Paxson, V. and M. Allman, "Computing TCP's Retransmission Timer", RFC 2988, November 2000.

[I-D.ietf-eap-rfc2284bis]
Blunk, L., "Extensible Authentication Protocol (EAP)", draft-ietf-eap-rfc2284bis-06 (work in progress), September 2003.

[I-D.ietf-pana-ipsec]
Parthasarathy, M., "PANA enabling IPsec based Access Control", draft-ietf-pana-ipsec-00 (work in progress), October 2003.

[I-D.tschofenig-pana-bootstrap-rfc3118]
Tschofenig, H., "Bootstrapping RFC3118 Delayed authentication using PANA", draft-tschofenig-pana-bootstrap-rfc3118-00 (work in progress), June 2003.

[I-D.ietf-seamoby-ctp]
Loughney, J., "Context Transfer Protocol", draft-ietf-seamoby-ctp-04 (work in progress), October 2003.

[RFC2716] Aboba, B. and D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.

[I-D.josefsson-pppext-eap-tls-eap] Josefsson, S., Palekar, A., Simon, D. and G. Zorn, "Protected EAP Protocol (PEAP)", draft-josefsson-pppext-eap-tls-eap-06 (work in progress), March 2003.

[I-D.ietf-pppext-eap-ttls] Funk, P. and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)", draft-ietf-pppext-eap-ttls-03 (work in progress), August 2003.

[I-D.tschofenig-eap-ikev2] Tschofenig, H. and D. Kroeselberg, "EAP IKEv2 Method (EAP-IKEv2)", draft-tschofenig-eap-ikev2-01 (work in progress), July 2003.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

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

[I-D.ietf-aaa-eap] Eronen, P., Hiller, T. and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-02 (work in progress), July 2003.

[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.

[RFC2522] Karn, P. and W. Simpson, "Photuris: Session-Key Management Protocol", RFC 2522, March 1999.

[I-D.ietf-aaa-diameter-cms-sec] Calhoun, P., Farrell, S. and W. Bulley, "Diameter CMS Security Application", draft-ietf-aaa-diameter-cms-sec-04 (work in progress), March 2002.

[I-D.walker-aaa-key-distribution]
Housley, R., Walker, J. and N. Cam-Winget, "AAA Key Distribution", draft-walker-aaa-key-distribution-00 (work in progress), April 2002.

[I-D.puthenkulam-eap-binding]
Puthenkulam, J., "The Compound Authentication Binding Problem", draft-puthenkulam-eap-binding-03 (work in progress), July 2003.

[I-D.aboba-pppext-eapgss]
Aboba, B. and D. Simon, "EAP GSS Authentication Protocol", draft-aboba-pppext-eapgss-12 (work in progress), April 2002.

[RFC2478] Baize, E. and D. Pinkas, "The Simple and Protected GSS-API Negotiation Mechanism", RFC 2478, December 1998.

[RFC3329] Arkko, J., Torvinen, V., Camarillo, G., Niemi, A. and T. Haukka, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)", RFC 3329, January 2003.

[I-D.aboba-pppext-key-problem]
Aboba, B. and D. Simon, "EAP Key Management Framework", draft-aboba-pppext-key-problem-07 (work in progress), August 2003.

Informative References

[ianaweb] IANA, "Number assignment", http://www.iana.org.

[jb99] Juels, A. and J. Brainard, "Client Puzzles: A Cryptographic Defense Against Connection Depletion Attacks", Proceedings of NDSS '99 (Networks and Distributed Security Systems), pages 151-165, 1999.

[mitm] Asokan, N., Niemi, V. and K. Nyberg, "Man-in-the-middle in tunnelled authentication", In the Proceedings of the 11th International Workshop on Security Protocols, Cambridge, UK, April 2003.

[802.11i] Institute of Electrical and Electronics Engineers, "Draft supplement to standard for telecommunications and information exchange between systems - lan/man specific requirements - part 11: Wireless medium access control (mac) and physical layer (phy) specifications: Specification for enhanced security", IEEE 802.11i/D6.0, 2003.

[802.11] Institute of Electrical and Electronics Engineers, "Information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications", IEEE Standard 802.11, 1997.

URIs

[1] <http://danforsberg.info:8080/pana-issues/>

Authors' Addresses

Dan Forsberg
Nokia Research Center
P.O. Box 407
FIN-00045 NOKIA GROUP
Finland

Phone: +358 50 4839470
EMail: dan.forsberg@nokia.com

Yoshihiro Ohba
Toshiba America Information Systems, Inc.
9740 Irvine Blvd.
Irvine, CA 92619-1697
USA

Phone: +1 973 829 5174
EMail: yohba@tari.toshiba.com

Basavaraj Patil
Nokia
6000 Connection Dr.
Irving, TX 75039
USA

Phone: +1 972-894-6709
EMail: Basavaraj.Patil@nokia.com

Hannes Tschofenig
Siemens Corporate Technology
Otto-Hahn-Ring 6
81739 Munich
Germany

EMail: Hannes.Tschofenig@siemens.com

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

Appendix A. Adding sequence number to PANA for carrying EAP

Appendix A.1 Why is sequence number needed for PANA to carry EAP?

EAP [I-D.ietf-eap-rfc2284bis] requires underlying transports to provide ordered-delivery of messages. If an underlying transport does not satisfy the ordering requirement, the following situation could happen:

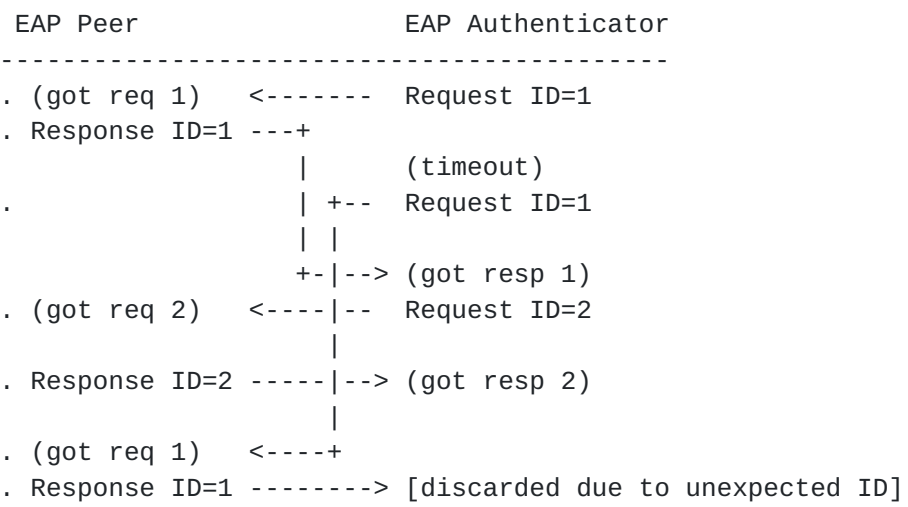


Figure 11: Undesirable scenario

In Figure 11, the second EAP Request message with Identifier=1 arrives at the EAP peer after the third EAP Request message with Identifier=2. As a result, the EAP peer accepts the second EAP Request as a new EAP Request while it is just an old EAP Request that was already responded and the authentication might be totally messed up.

This problem occurs due to the fact that EAP doesn't recognize duplicate packets in the scope of one EAP protocol run, but only in the scope of current and previous packet (i.e., request and response message matching). When EAP is running over PPP or IEEE 802 links, this is not a problem, because those link-layers have the ordering invariant characteristic.

On the other hand, the PANA design has chosen UDP as its transport. Given that UDP does not provide ordered delivery of packets and PANA does not assume any specific link-layer technology to carry EAP, PANA messages need to have a sequence number.

In the following text we describe two possible approaches for sequence number handling in PANA. The first one makes use of a single sequence number whereas the latter utilizes two. Finally a

comparison between the two approaches is provided. The method described in Appendix A.3.1 (i.e., the dual sequence number with orderly-delivery method) is suggested as the preferred method for PANA transport.

Appendix A.2 Single sequence number approach

This section discusses several methods based on using a single sequence number for providing orderly message delivery. Sequence number handling for all methods discussed in Appendix A.2 must comply to the following rules:

Rule 1: The sequence number starts from initial sequence number (ISN) and is monotonically increased by 1. The arithmetic defined in [RFC1982] is used for sequence number operation.

Rule 2: When a PAA sends an EAP message passed from EAP layer to a PaC, a new sequence number is placed in the message, regardless of whether it is sent as a result of a retransmission at the EAP layer or not.

Note: It might be possible to define other mechanisms for sequence number handling if it can be assumed that a PAA detects EAP retransmissions. However, such an assumption heavily depends on EAP implementation details in particular on EAP APIs, thus it was decided not to use such an assumption.

Appendix A.2.1 Single sequence number with EAP retransmission method

Again, the following rules must hold:

Rule 3: Use EAP layer retransmission for retransmitting EAP messages (based on a timer expiration).

Rule 4: When the PaC receives a message from the PAA, it checks the sequence number and discards the message if the sequence number is not greater than that of the last accepted message.

Rule 5: When the PAA receives a message from the PaC, it checks the sequence number and discards the message if the sequence number does not match a pending request message.

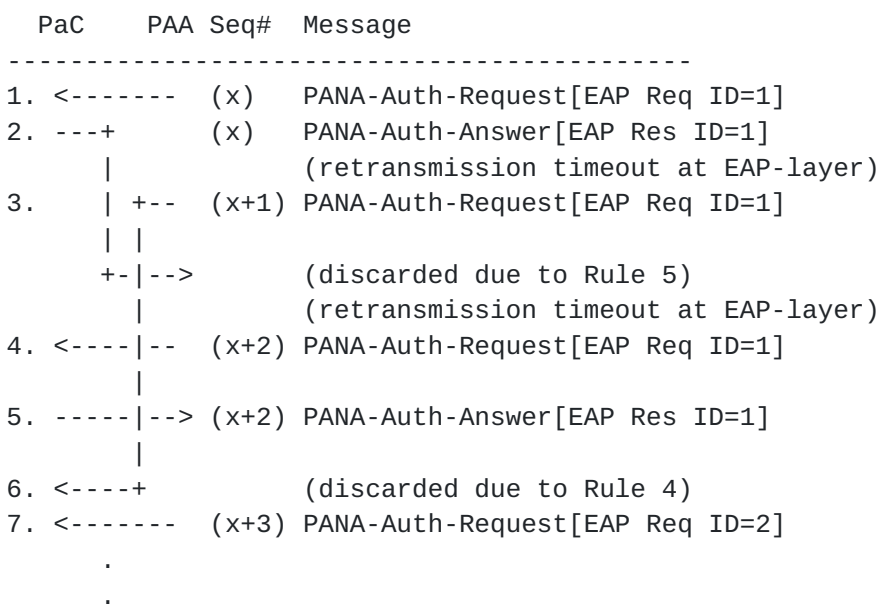


Figure 12: Example for Single sequence number with EAP retransmission

This method is vulnerable to a blind DoS attack on the sequence number since the PaC will accept quite a wide range of sequence numbers. For example, if an attacker blindly sends a bogus message to a legitimate PaC with a randomly chosen sequence number, it will be accepted by the PaC with 50% probability, and once this happens, all messages sent from the communicating PAA will be discarded as long as they have a sequence number smaller than the accepted value. The problem of this method leads to a requirement for PaC to have a narrow range of acceptable sequence numbers to make the blind DoS attack difficult. Note that the DoS attack cannot be prevented if the attacker is on the same IP link as PaC and able to eavesdrop the PANA conversation. However, the attacker needs to put itself in promiscuous mode and thus spend more resources to eavesdrop and launch the attack (in other words, non-blind DoS attack is still possible as long as sequence numbers are unprotected.)

Appendix A.2.2 Single sequence number with PANA-layer retransmission method

The next method is still based on using a single sequence number but the PANA-layer takes the responsibility of retransmission. The method uses the following rules in addition to the common rules described in Appendix A.2.

Rule 3: Use PANA-layer retransmission for retransmitting both EAP and non-EAP messages (based on a timer expiration). EAP layer retransmission is turned off. Retransmission based on timer

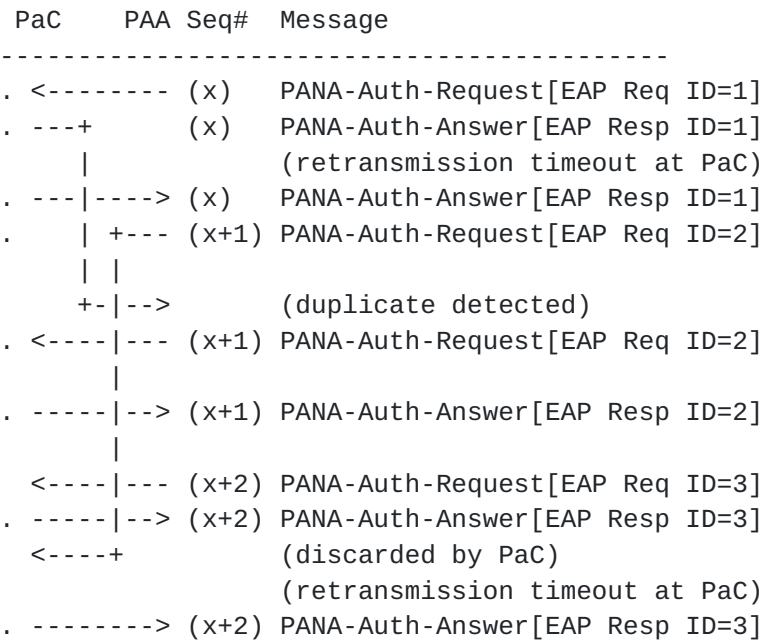
occurs both on PaC and PAA side, but not on both sides simultaneously. PAA does retransmission at least for PANA_Termination and PANA_Reauth messages, otherwise PaC takes care of retransmission.

Rule 4: When the PaC receives a message from the PAA, it accepts the message if the sequence number is equal to that of the last accepted message + 1. If the sequence number is equal to that of the last accepted message, the PaC retransmits the last transmitted message. Otherwise, it silently discards the message.

Rule 5: When the PAA receives a message from the PaC, it accepts the message if the sequence number is equal to that of the last transmitted message. If the receiving sequence number is equal to that of the last transmitted message - 1, the PAA retransmits the last transmitted message and discard the received message. Otherwise, it silently discards the message.

Rule 6: The PaC retransmits the last transmitted EAP Response until a new EAP Request message or an EAP Success/Failure message is received and accepted.

Rule 7: PAA must keep the copy of the last transmitted message and must be able to retransmit it until either a valid message is received and accepted by the PAA or a timer expires. The timer is used if no new message will be sent from the PaC.



```
 9. lost<---- (x+3) PANA-Auth-Request[EAP Succ ID=3]
                    (retransmission timeout at PaC)
10.---->lost (x+2) PANA-Auth-Answer[EAP Resp ID=3]
                    (retransmission timeout at PaC)
11.--------> (x+2) PANA-Auth-Answer[EAP Resp ID=3]
12.<-------- (x+3) PANA-Bind-Request[EAP Succ ID=3]
                    (retransmission timer stopped at PaC)
                    (deletion timeout at PAA)
                    (message (x+3) deleted at PAA)
13.lost<---- (x+4) PANA-Termination-Request
                    (retransmission timeout at PAA)
14.<-------- (x+4) PANA-Termination-Request
15.---->lost (x+4) PANA-Termination-Answer
                    (retransmission timeout at PAA)
16.<-------- (x+4) PANA-Termination-Request
17.--------> (x+4) PANA-Termination-Answer
                    (retransmission timer stopped at PAA)
```

Figure 13: Example for Single sequence number with PANA-layer retransmission

This method has an advantage of eliminating EAP layer retransmission by providing reliability at the PANA layer. Retransmission at the EAP layer has a problem with determining an appropriate retransmission timer value, which occurs when the lower-layer is unreliable. In this case an EAP authenticator cannot distinguish between (i) EAP Request or EAP Response message loss (in this case the retransmission timer should be calculated based on network characteristics) and (ii) long latency for EAP Response generation due to e.g., user input etc. (in this case the retransmission timer should be calculated based on user or application characteristics). In general, the retransmission timer for case (ii) is longer than that for case (i). If case (i) happens while the retransmission timer is calculated based on user or application characteristics, then it might frustrate an end user since the completion of the authentication procedure takes unnecessarily long. If case (ii) happens while the retransmission timer is calculated based on network characteristics (i.e., RTT), then unnecessarily traffic is generated by retransmission. Note that in this method a PaC still cannot distinguish case (i) and case (iii) the EAP authenticator or a backend authentication server is taking time to generate an EAP Request.

A problem of this method is that it is based on the assumption that EAP authenticator does not send a new EAP message until an EAP Response to the outstanding EAP Request is received. However, this assumption does not hold at least EAP Success/Failure message which does not need the outstanding EAP Request to be responded before

sending the EAP Success/Failure message. This would require timer-based retransmission not only at PaC side but also at PAA side. Another problem occurs when a new EAP message overrides the outstanding EAP Request, the PaC cannot assume any more that the sequence number of the next message to be accepted is the last accepted message + 1. So the PaC needs to accept a range of sequence numbers, instead of a single sequence number. These two additional things would increase the complexity of this method.

Appendix A.3 Dual sequence number approach

Based on the analysis of previous schemes, it is recognized that two sequence numbers are needed anyway, one for each direction. Two different methods are proposed based on this approach. Both methods have the following rules in common.

Rule 1: A PANA packet carries two sequence numbers: transmitted sequence number (tseq) and received sequence number (rseq). tseq starts from initial sequence number (ISN) and is monotonically increased by 1. The arithmetic defined in [RFC1982] is used for sequence number operation. It is assumed that the two sequence numbers have the same length for simplicity.

Rule 2: When PAA or PAC sends a new message, a new sequence number is placed on the tseq field of message. Every transmitted message is given a new sequence number.

Rule 3: When a message is sent from PaC or PAA, rseq is copied from the tseq field of the last accepted message.

Rule 4: For messages which experience a PANA layer retransmission, the retransmission timer is stopped when the message is acknowledged.

It is possible to carry multiple EAP sequences in a single PANA sequence, with using EAP Success/Failure message as a delimiter of each EAP sequence. In this case, EAP Success/Failure message needs to be reliably delivered.

Appendix A.3.1 Dual sequence number with orderly-delivery method

This method relies on EAP layer retransmission for EAP messages. This method is referred to as orderly-delivery method. The following rules are used in addition to the common rules.

Rule 5: Use the EAP-layer retransmission for retransmitting EAP Requests (based on a timer expiration). For other PANA layer messages that require a response from the peer, PANA layer has its own mechanism to retransmit the request until it gets a response or gives up. A new tseq value is always used when sending any message even when it is retransmitted at PANA layer.

Rule 6: When a message is received, it is accepted if (i) the tseq value is greater than the tseq of the last accepted message and (ii) the rseq falls in the range between the tseq of the last acknowledged message + 1 and the tseq of the last transmitted message. Otherwise, the received message is discarded.

```
   PaC    PAA  (tseq,rseq) Message
  ------------------------------------------------
  1. <-------   (x,y)       PANA-Auth-Request[EAP Req, ID=1]
  2. ------->   (y+1,x)     PANA-Auth-Answer[EAP Resp, ID=1]
  3. <-------   (x+1,y+1)   PANA-Auth-Request[EAP Req, ID=2]
  4. --->lost   (y+2,x+1)   PANA-Auth-Answer[EAP Resp, ID=2]
                            (retransmission timeout at EAP layer)
  5. <-------   (x+2,y+1)   PANA-Auth-Request [EAP Req, ID=2]
  6. ------->   (y+3,x+2)   PANA-Auth-Answer[EAP Resp, ID=2]
  7. lost<---   (x+3,y+3)   PANA-Auth-Request[EAP Req, ID=3]
                            (retransmission timeout at EAP layer)
  8.    +----   (x+4,y+3)   PANA-Auth-Answer[EAP Req, ID=3]
        |                   (retransmission timeout at EAP layer)
  9. <--|----   (x+5,y+3)   PANA-Auth-Request[EAP Req, ID=3]
  10.---|--->   (y+4,x+5)   PANA-Auth-Answer[EAP Resp, ID=3]
```

```
          |
       <--+                    (out of order. discarded)
   11.lost<---   (x+6,y+4)    PANA-Bind-Request[EAP Succ, ID=3]
                              (retransmission timeout at PAA)
   12.<-------   (x+7,y+4)    PANA-Bind-Request[EAP Succ, ID=3]
   13.--->lost   (y+5,x+7)    PANA-Bind-Answer
                              (retransmission timeout at PAA)
   14.<-------   (x+8,y+4)    PANA-Bind-Request[EAP Succ, ID=3]
                              (duplicate detected by PaC)
   15.------->   (y+6,x+8)    PANA-Bind-Answer
```

Figure 14: Example for Dual sequence number with orderly-delivery

Appendix A.3.2 Dual sequence number with reliable-delivery method

This method relies solely on PANA layer retransmission for all messages. This method is referred to as reliable-delivery method. The following additional rules are applied in addition to the common rules.

Rule 5: Use the PANA layer retransmission for retransmitting all messages (based on a timer expiration). EAP retransmission is turned off.

Rule 6: Either an ACK message is used for acknowledgment or an acknowledgment can be piggybacked with data. ACK messages are not retransmitted. An ACK message is sent if no the acknowledgement cannot be piggybacked with a data within a given time frame W.

Rule 7: When a message is received, it is accepted if (i) the tseq value is greater than the tseq of the last accepted message and (ii) the rseq falls in the range between the tseq of the last acknowledged message and the tseq of the last transmitted message. Otherwise, the received message is discarded.

Rule 8: When a duplicate message is received, the last transmitted message is retransmitted if the received message is not an ACK. A message is considered as duplicate if its tseq value is equal to the tseq of the last accepted message.

	PaC	PAA	(tseq,rseq)	Message
1.	<-------		(x,y)	PANA-Auth-Request[EAP Req, ID=1] (user input ongoing)
2.	------->		(y+1,x)	PANA-Auth-Answer (user input completed)
3.	------->		(y+2,x)	PANA-Auth-Answer[EAP Resp, ID=1]
4.	<-------		(x+1,y+2)	PANA-Auth-Request [EAP Req, ID=2]
5.	--->lost		(y+3,x+1)	PANA-Auth-Answer[EAP Resp, ID=2] (retransmission timeout at PAA)
6.	<-------		(x+1,y+2)	PANA-Auth-Request [EAP Req, ID=2] (duplicate detected by PaC)
7.	------->		(y+3,x+1)	PANA-Auth-Answer[EAP Resp, ID=2]
8.	lost<---		(x+2,y+3)	PANA-Auth-Request [EAP Req, ID=3] (retransmission timeout at PaC)

```
9. ------->   (y+3,x+1)   PANA-Auth-Answer[EAP Resp, ID=2]
                          (duplicate detected at PAA)
10.<-------   (x+2,y+3)   PANA-Auth-Request [EAP Req, ID=3]
11.---+       (y+4,x+2)   PANA-Auth-Answer[EAP Resp, ID=3]
      |                   (retransmission timeout at PAA)
12.<--|----   (x+2,y+3)   PANA-Auth-Request [EAP Req, ID=3]
      |                   (duplicate detected at PaC)
13.---|--->   (y+4,x+2)   PANA-Auth-Answer[EAP Resp, ID=3]
14.<--|----   (x+3,y+4)   PANA-Bind-Request[EAP Succ, ID=3]
15.---|--->   (y+5,x+3)   PANA-Bind-Answer
      +--->               (out of order. discarded)
```

Figure 15: Example for Dual sequence number with reliable-delivery method

Appendix A.3.3 Comparison of the dual sequence number methods

The orderly-delivery method is simpler than the reliable-delivery method in that the former does not allow sending a separate ACK while the latter does.

In terms of authentication performance, the reliable-delivery method is better than the orderly-delivery method in that the former gives more detailed status of the link than the latter, e.g., an entity can know whether a request has reached the communicating peer without before receiving a response. The reliable-delivery can reduce retransmission traffic and communication delay that would occur if there is no reliability, as described in section Appendix A.2.2

Appendix A.4 Consensus

Although it is recognizable that the reliable-delivery method would be important in terms of improvement of overall authentication latency, we believe that this is a performance problem of EAP and not a problem of PANA. It is agreed that solving the EAP problem is not the scope of PANA and simplicity is more important factor in the PANA design.

As a consequence, the orderly-delivery method is chosen as the message transport part of PANA.

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.