Network Working Group
Internet-Draft
Expires: April 20, 2006

J. Bournelle (Ed.)
M. Laurent-Maknavicius
GET/INT
R. Marin Lopez
University of Murcia
D. Forsberg
Nokia
J-M. Combes
France Telecom R&D
October 17, 2005

PANA Mobility Optimizations Analysis
draft-bournelle-pana-mobopts-analysis-00

Status of this Memo

Copyright Notice

Abstract

The PANA protocol offers a way to authenticate clients in IP based access networks. It carries EAP over UDP which permits ISPs to use

multiple authentication methods. However, in roaming environments IP clients might change of gateways and new EAP authentication from scratch may occur. This can considerably degrade performance. To solve this problem, the PANA WG is currently working on a solution based on context transfer between PANA Authentication Agents. The aim of this document is to analyze how this proposal works in a WLAN environment considering various deployment scenarios.

Table of Contents

1. Introduction

In IP based access network, PANA [I-D.ietf-pana-pana] may be used as a front-end to a AAA architecture in order to authenticate users before granting them access to the resources. For this purpose, it uses EAP which offers a variety of authentication methods.

The PANA mobility optimization [I-D.ietf-pana-mobopts] and its companion document [I-D.bournelle-pana-ctp] propose to transfer previous established context from the previous PAA to the new PAA. The goal is to avoid a reauthentication from scratch. This document analyses this proposal in WLAN environment depending on PANA deployment. The interaction with the AAA infrastructure is also considered.

2. Terminology

This document uses the following terms or abbreviations:

AR Access Router. The router to which the PaC is attached .

PaC PANA Client. A mobile node (MN) using a PANA protocol implementation to authenticate itself to the network.

PAA PANA Authentication Agent.

PANA Protocol for Carrying Network Authentication for Network Access

3. Notations

In this document, the notations PAA > AR means that the PAA is located behind the Access Router (AR). The access router is the default router for the PaC.

4. PANA overview

PANA is a protocol that carries EAP over IP/UDP to authenticate users. The PANA Authentication Agent (PAA) is the endpoint of the PANA protocol at the access network. The PAA itself might not be able to authenticate the user by terminating the EAP protocol. Instead the PAA might forward the EAP payloads to the backend AAA infrastructure.

The Enforcement Point (EP) is an entity which enforces the result of the PANA protocol exchange. The EP might be co-located with the PAA or separated as a stand-alone device. In the latter case, the SNMPv3 protocol [I-D.ietf-pana-snmp] is used to communicate between PAA and EP.

A successful EAP authentication exchange results in a PANA security association (PANA SA) if the EAP method was able to derive session keys. In this case, all further PANA messages between PaC and PAA will be authenticated, replay and integrity protected thanks to the MAC AVP.

5. IP traffic security

We only consider here PANA deployment in a Wireless LAN environment. The first hop router of the PaC is the Access Router (AR).

As noted above, the EP is the equipment on which security policies are applied to secure PaC's traffic. Depending on its location, the traffic will be protected at the layer 2 or at the layer 3.

If the EP is colocated with the Access Point (L2), either the PAA configures L2 filtering based on MAC address or the PAA may bootstrap 802.11i [802.11i] security.

If the EP is colocated in the AR, the PAA configures L3 filtering based on PaC's IP address or it provides IKE material to the EP to setup an IPsec tunnel between PaC and EP.

6. Intermediary key transfer and Domino effect

The pana-mobopts approach proposes to transfer an intermediary key between pPAA to the nPAA. This key AAA-Key-int is derived from the AAA-Key located at the pPAA. A new PANA_MAC_Key is then computed between the nPAA and the PaC based on Nonces exchanged during PANA-Start-Exchange.

According to EAP [I-D.ietf-eap-keying], the figure below illustrates the keys hierarchy in the PANA case:

```
      PaC                 pPAA                AAA/EAP
      ---                 ----                -------
      MSK                 MSK                 MSK
      EMSK                                    EMSK
      AAA-Key             AAA-Key <---------- AAA-Key

      PANA_MAC_Key        PANA_MAC_Key
```

MSK and EMSK are derived from the EAP method used between the EAP client (PaC) and the EAP server. The AAA-Key is computed from MSK and EMSK. This key is exported to the pPAA. The PANA_MAC_KEY, used to protect PANA messages, is derived from the AAA-Key as follows:

```
    PANA_MAC_KEY = The first N bits of
            HMAC_SHA1(AAA-Key, PaC_nonce | PAA_nonce | Session-ID)
```

The document [I-D.ietf-pana-mobopts] proposes to provide to the nPAA an intermediary AAA-Key-int [I-D.ietf-pana-mobopts]. This key is computed as follows:

```
     AAA-Key-int = The first N bits of
         HMAC-SHA1(AAA-Key, DiameterIdentity | Session-ID)
```

DiameterIdentity is the identifier of the pPAA and Session-ID is the identifier of the Session between the pPAA and PaC.

During the PANA-Start-Exchange (PSR/PSA), PaC and nPAA provide nonces that are used to derive a new AAA-Key:

```
    AAA-Key-new = The first N bits of
                  HMAC-SHA1(AAA-Key-int, PaC_nonce | PAA_nonce)
```

The new PANA_MAC_Key used to compute AVP MAC will be calculated from this key.

The issue with this approach is that it does not completely fulfill one of the requirements described in [I-D.housley-aaa-key-mgmt] also known as Preventing the Domino effect:

"Compromise of a single authenticator MUST NOT compromise any other part of the system, especially session keys and long-term keys. There are many implications of this requirement; however, two implications deserve highlighting. First, an authenticator MUST NOT share any keying material with another authenticator. Second, the scope of the authenticator needs to be defined and understood by all parties that communicate with it."

In our case, if the pPAA is compromised and if the attacker gets the exchanged Nonces between PaC and nPAA, it can derive the new PANA_MAC_Key.

However, even if the pPAA is compromised, only the PaC linked to the pPAA has security issues with nPAA and the attacker has to follow closed the PaC to take advantage of this security hole. It is also important to note that a PaC attached to the nPAA and having no links with the pPAA does not have security issues.

One can also argue that if we suppose homogeneous deployment of PAAs, if the attacker can compromise the pPAA, it could also compromised the nPAA.

This issue is currently not solved and further discussions are needed.

7. Deployment scenarios in WLAN

In this document, we only consider intra-domain case. This means that all equipments belong to the same administrative domain. PAAs may rely on the AAA infrastructure in order to authenticate PaCs.

7.1 EP in AP and PAA in AP

In this case, EP and PAA are located in the AP. Normally, this will not be typical deployment of PAA however it is worth mentioning it due to this case is also considered in PANA framework [I-D.ietf-pana-framework].

As the EP is located in the AP , only layer 2 security will be considered. If no security on the link is needed, enable L2 filters for PaC's MAC address would be enough. Otherwise, some kind of L2 security association will be established.

7.1.1 Layer 2 filtering

To be done.

7.1.2 802.11i

To be done.

7.2 EP in AP and PAA in AR

In this section, the EP is located in the AP and the PAA is in AR. The Figure 2 represents the architecture considered. We consider here two types of security: L2 filtering or 802.11i [802.11i]. Note that 802.11i is normally the combination of 802.1X [802.1X] for authentication, 4-way handshake to establish keying material at the supplicant (PaC) and authenticator (AP/EP) and CCMP/TKIP to protect the traffic at layer 2.

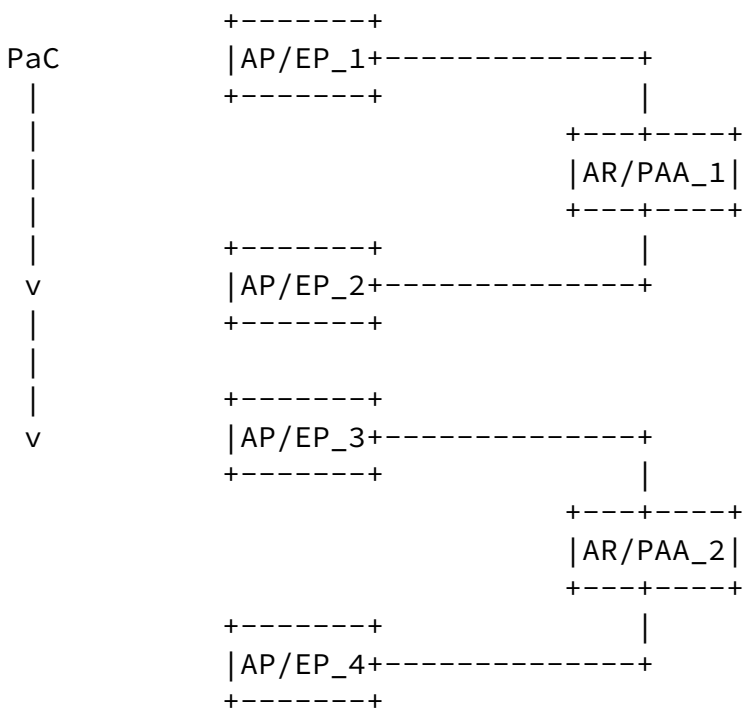


Figure 2: EP in AP and PAA in AR

7.2.1 L2 filtering

To be done.

7.2.2 802.11i

At this time, the PANA WG does not define any solution to bootstrap layer 2 security using PANA. For this reason, this section is left

for future consideration.

7.3 EP in AP and PAA > AR

In this section, we consider the case where the EP is located in AP and PAA are located inside the network (PANA multihop).

7.3.1 L2 filtering

To Be Done.

7.3.2 802.11i

At this time, the PANA WG does not define any solution to bootstrap layer 2 security using PANA. For this reason, this section is for future consideration.

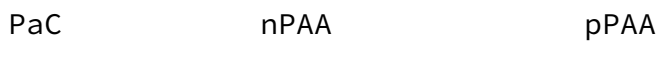
7.4 EP in AR and PAA in AR

In this scenario, PAA and EP are colocated in the access router (AR). We only consider use of pana-mobopts in reactive case.

7.4.1 Without IPsec

After the authentication phase, the PAA locally configures the EP for the PaC. We assume here that only IP filtering is applied on the EP. After an IP handover to the next AR, the PaC is detected by the EP and a new authentication is triggered. The PaC may also detect its handover and sends a PANA-Discovery message.

In both cases, the nPAA sends a PSR message to the PaC. If pana-mobopts is enabled, the PAA must be stateful and the PSR carries a Nonce (PAA_Nonce). If the PaC replies with the correct PSA, the nPAA requests the PANA context to the pPAA and then runs a PANA-Bind-Exchange with the PaC. In case of success, the nPAA configures the nEP for the PaC. After this, the nPAA could reauthenticate from scratch the PaC. This procedure is depicted in the Figure 3.



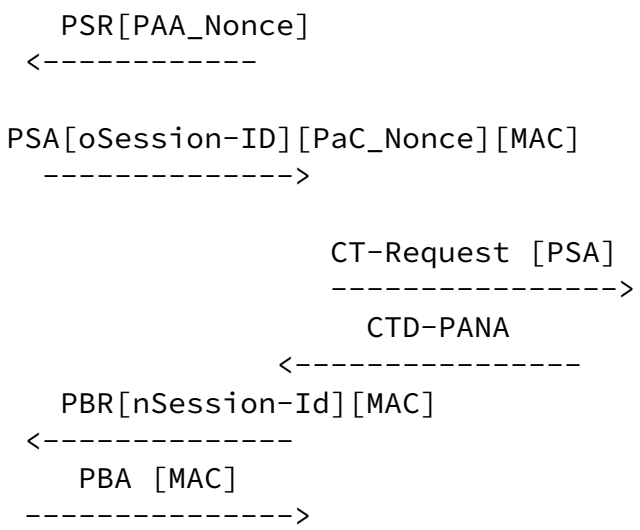


Figure 3: PANA mobopts without IPsec

7.4.2 With IPsec

In this case, IPsec is used between the PaC and the EP to secure the

communication. For this, the PAA communicates the following information to the EP (cf. [I-D.ietf-pana-ipsec])

PaC-EP Master Key

Key-Id

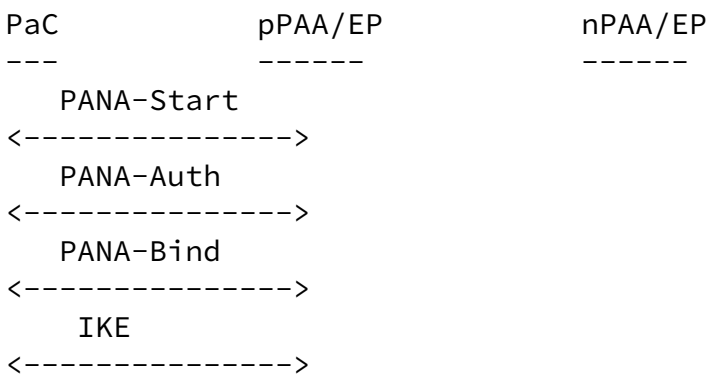
Device-Identifier of the PaC

Session-Id

Thus, after the authentication phase, the PAA binds the session with the PaC (PANA-Bind-Exchange) and in the same time provides above information to the EP. Right after, PaC and EP initiate an IKE session to configure IPsec SAs. Then, the PaC uses its IPsec tunnel to send its IP traffic to the Internet.

After an IP handover, the PaC is detected by the nEP and must be

reauthenticated. If pana-mobopts is used, after a context transfer and a PANA-Bind exchange, the PaC and nPAA share a new session. Then nPAA provides necessary information to nEP to run IKE with the PaC. Then PaC and nEP use IKE to setup an IPsec tunnel.



IP handover

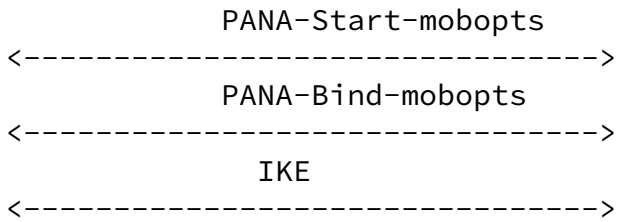


Figure 4: PANA mobopts with IPsec

Even if pana-mobopts is used, the re-establishment of the IKE session creates a latency after the handover.

7.5 EP in AR and PAA > AR

In this scenario, we consider that EP is located in AR whereas the PAA is more than one IP hop away from the PaC (PANA multihop case). This scenario is described on the Figure 5. AR/EP_1 and AR/EP_2 are connected to PAA_1 and AR/EP_3 and AR/EP_4 are connected to PAA_2.

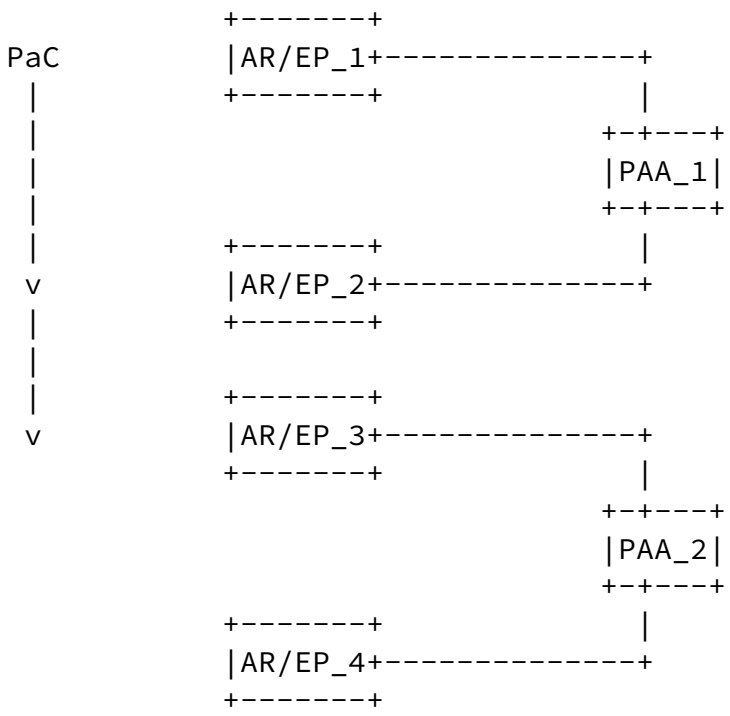


Figure 5: EP in AR and PAA > AR

7.5.1 Without IPsec

First, the PAA_1 authenticates to PaC through AR/EP_1. After the authentication phase, PAA_1 configures AR/EP_1 to authorize network access of the PaC. Then the PaC moves to AR/EP_2.

Note: A possible optimization could be that the AR/EP_2 is preconfigured by the PAA_1. This would however imply that the PAA_1 knows the PaC's address on AR/EP_2's network.

If the AR/EP_2 is not preconfigured by PAA_1, the PaC obtains a new

address and is detected by the AR/EP_2 which triggers a reauthentication. Then two situations are possible.

In the first one, the PAA_1 uses the same IP source address for the

PSR message (i.e. the address that was used during the authentication through AR/EP_1). In this case, the PaC detects this and sends a PUR message containing its new IP address to update the Device-Identifier. The PAA configures the AR/EP_2 with the correct Device-Identifier. This is depicted in Figure 6. Note that this procedure is currently not handled in PANA state machine.

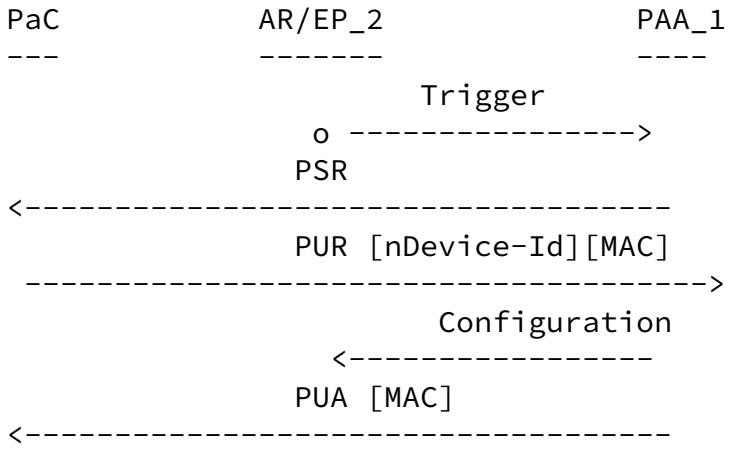
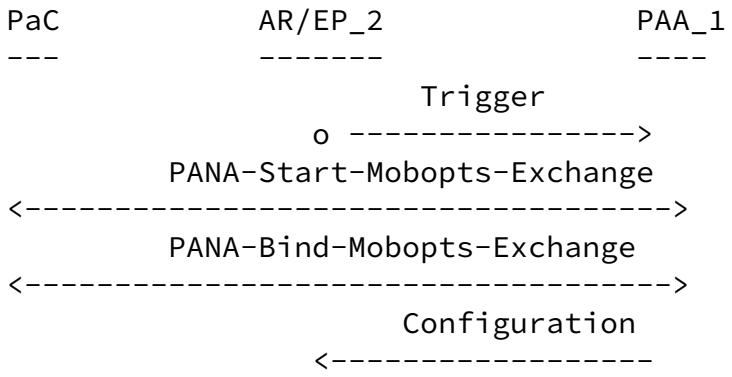


Figure 6: PAA_1 uses same IP address

In the second one, the PAA uses a different address. Thus the PaC thinks that it is a different PAA and if pana-mobopts is enabled it sends the corresponding PSA message. PAA_1 detects that it was the previous PAA (in fact itself) and locally recovers corresponding PANA context. Then it derives new keying material as described in pana-mobopts and it runs a PANA-Bind exchange with the PaC reallocating a new PANA session. After this exchange, the PAA configures AR/EP_2 and the PaC can access to the Internet through it.



In a second step, the PaC moves to AR/EP_3. In this case, the PaC can not recognize a known PAA and pana-mobopts/pana-ctp can be used here to retrieve PANA context from PAA_1.

7.5.2 With IPsec

In this case, IPsec is used between PaC and EP. The PAA provides necessary information to the EP using SNMPv3 as specified in [I-D.ietf-pana-snmp].

At the beginning, the PaC is detected by AR/EP_1 and a PANA authentication phase occurs with PAA_1. After the authentication phase, PAA_1 derives necessary keying material, binds the session with the PaC and sends to AR/EP_1 the information. The PaC and AR/EP_1 uses IKE to setup an IPsec tunnel as specified in [I-D.ietf-pana-ipsec]. Figure 8 presents the procedure.

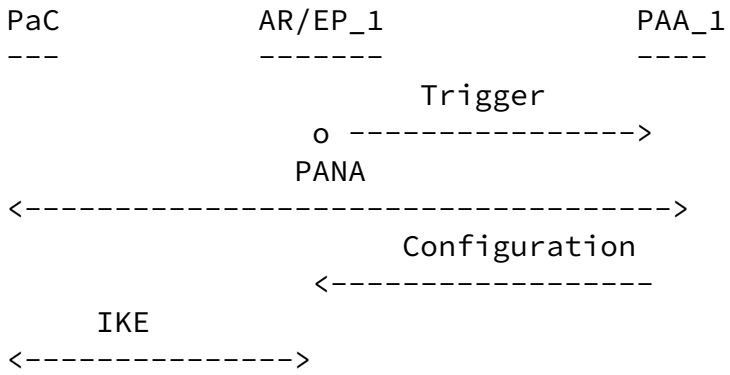


Figure 8: PAA_1 uses the same IP address

After this, the PaC moves to the AR/EP_2. It is detected by AR/EP_2 which triggers an authentication phase.

A possible optimization could be to preconfigure the AR/EP_2. In this case, only IKE could be needed.

If this optimization possible, PAA_1 can fallback in negotiation specified by [I-D.ietf-pana-mobopts] and depicted in Figure 9.

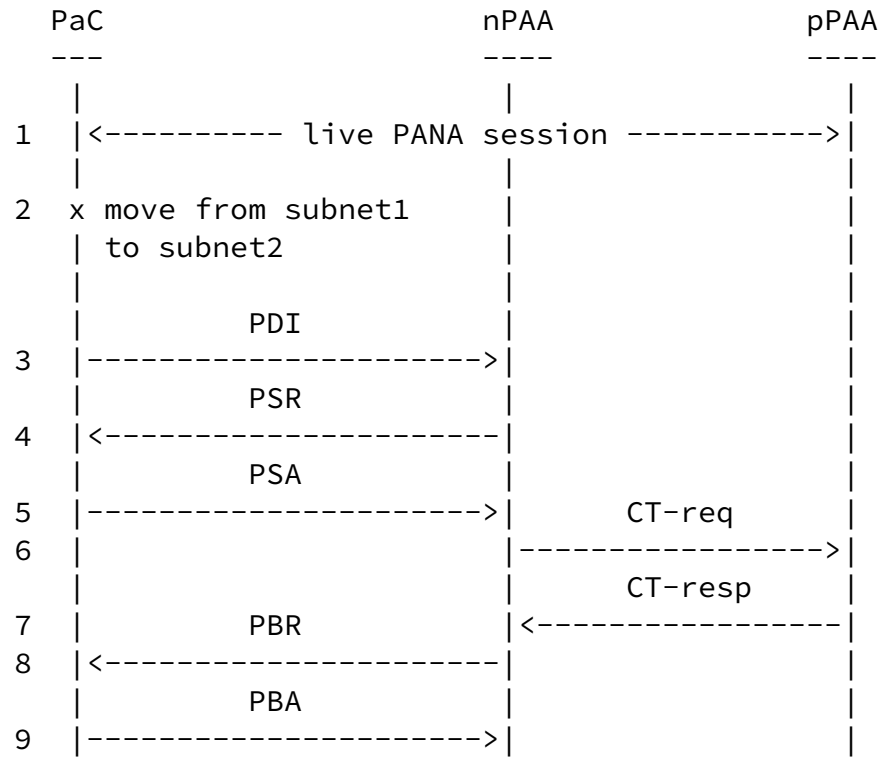


Figure 9: PANA mobopts with CxTP

However, in this case nPAA and pPAA are the same entity but working on different IP address. Thus, CT-req and CT-resp could be done through an API. The PaC does not know that it is the same PAA and thus, if pana-mobopts is enabled, it sends a PSA-mobopts. The PAA_1 receives the PSA and detects that it can locally recover the context. It computes necessary keying material and binds the PANA session with the PaC. After this, it provides the AR/EP_2 with IKE material.

Note that another alternative could also be considered. Taking into account the same PAA is attached to EPs and use the same IP address for both of them, PaC can detect this somehow (for example checking IP address included in PSR) and update the current PANA session with new PaC's IP address. This alternative is depicted on Figure 10.

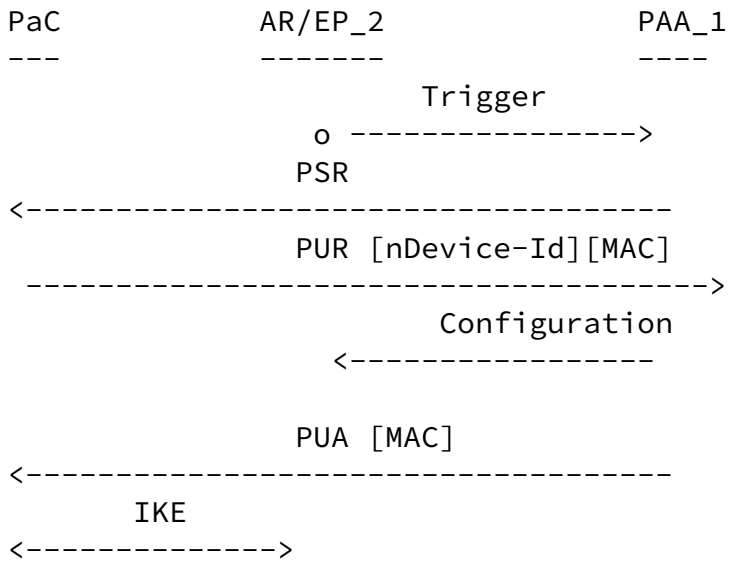


Figure 10: PAA_1 uses the same IP address

The PaC detects that it knows this PAA and responds with a PUR to update its Device-IDentifier (here the IP address). The PAA_1 replies with a PUA and sends necessary information to AR/EP_2 for IKE. Then PaC and EP run IKE to setup IPsec SAs.

Unfortunately this solution needs some modifications in PANA state machine mainly because PaC would react discarding PSR because it is in OPEN state and source IP address of the PANA PSR message is the same. Nonetheless this solution reduces signalling with respect to previous version.

8. AAA Considerations

PAAs may rely on the AAA infrastructure in order to authenticate PaC. The interaction between PANA and AAA protocols (RADIUS and Diameter) is described in [I-D.ieft-pana-aaa-interworking].

The figure below is extracted from [I-D.ieft-pana-aaa-interworking].

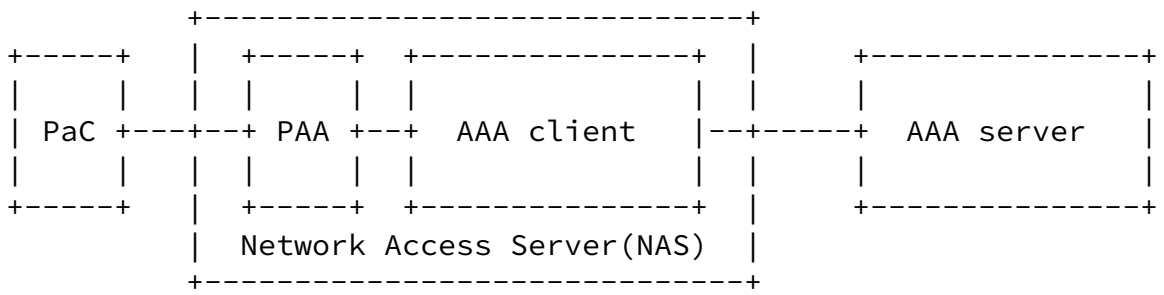


Figure 11: PANA with AAA

We assume here that the EAP server is colocated with the AAA server. In the roaming scenario, the EAP server is located in the home domain. Depending on operator's deployment, the AAA traffic is routed through a local AAA server or directly sent from the NAS to

the AAAH (using redirection functionality).

Considering Diameter, the NAS shares a session-id with the AAA server per PaC. This session-id is used in each AAA message concerning a PaC (e.g. for accounting).

8.1 Reauthentication

The home AAA server may need to contact a PaC in order to reauthenticate him or to close a session. The reauthentication mechanism is described in [RFC4005]. The AAA server sends a Re-Auth-Request (RAR) message to the NAS containing the session-id. We consider here two distinct scenarios.

In non-roaming scenario, the local AAA server needs to know the NAS in charge of the PaC. This implies that if the PaC moves during the session between different PAAs, the local AAA server must be informed of this. For this purpose, a new session must be shared between the nPAA and the AAA server.

In roaming scenario, two cases appeared. In the first case, we have a direct communication between PAA and AAAH. This case is similar

than above and the AAAH must be informed of the current PAAs. In the second case, the AAA traffic is routed through the local AAA server. In this case, we may consider that only the local AAA server needs to keep track of the current PAA.

8.2 Session Termination

While a user's session is being terminated, the NAS sends a message to the AAA server. Thus, the nPAA must know the AAA server used to authenticate the PaC and it must share a session with it.

8.3 Accounting

The accounting is an important part of the AAA architecture. For this purpose, the NAS sends accounting report to an accounting server (probably colocated with the AAA server used for authentication). The accounting process should handle PaC's handover. This means that the Accounting server should receive accouting report from the nPAA and should be able to know that it is the same PaC.

8.4 Conclusion

Considering the whole network access authentication architecture, it appears that we also need to reestablish a context between the nPAA and the AAA infrastructure to handle PaC's handover. In particular, the nPAA must re-establish a session with the AAA server that was used by pPAA. For this purpose, the pPAA could send context information to the nPAA, which can then re-establish AAA session for the PaC. Another alternative would be to have a local AAA Proxy that hides the AAA session mobility between PAAs from the AAAH.

This implies that the AAA infrastructure must also be considered while defining a solution for mobility optimization in PANA environment.

9. Conclusion

The goal of this document is to analyze pana-mobopts in WLAN environment in order to raise discussions. The 802.11i bootstrapping is not analyzed since the document is not yet submitted. It appears that considering PANA multihop, some optimizations may be possible by proactively distributing some information to EP. The PANA preauthentication is not yet analyzed in this document. It appears that the AAA infrastructure must be considered while defining a global optimization for mobility.

10. Security Considerations

This document does not define a new protocol nor mechanism. For this reason, this section is left empty.

11. References

[802.11i] Institute of Electrical and Electronics Engineer, "Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", IEEE std. 802.11i, July 2004.

[802.1X] Institute of Electrical and Electronics Engineer, "IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control", IEEE std. 802.1X-2004.

[I-D.ietf-eap-keying] Aboba, B., "Extensible Authentication Protocol (EAP) Key Management Framework", draft-ietf-eap-keying-07 (work in progress), July 2005.

[I-D.housley-aaa-key-mgmt] Housley, R. and B. Aboba, "AAA Key Management", draft-housley-aaa-key-mgmt-00 (work in progress), June 2005.

[I-D.ietf-pana-mobopts] Forsberg, D., "PANA Mobility Optimizations", draft-ietf-pana-mobopts-00 (work in progress), January 2005.

[I-D.ietf-pana-pana] Forsberg, D., "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-10 (work in progress), July 2005.

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

[I-D.ietf-pana-snmp] Mghazli, Y., "SNMP usage for PAA-EP interface", draft-ietf-pana-snmp-04 (work in progress), July 2005.

[I-D.ietf-pana-framework]
Jayaraman, P., "PANA Framework",
draft-ietf-pana-framework-05 (work in progress),
July 2005.

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton,
"Diameter Network Access Server Application", RFC 4005,
August 2005.

[I-D.ieft-pana-aaa-interworking]
Lior, A. and A. Yegin, "PANA AAA Interworking.",
draft-ieft-pana-aaa-interworking-00 (work in progress),
July 2005.

[I-D.bournelle-pana-ctp]
Bournelle, J., "Use of Context Transfer Protocol (CxTP)
for PANA", draft-bournelle-pana-ctp-03 (work in progress),
June 2005.

Authors' Addresses

Julien Bournelle
GET/INT
9 rue Charles Fourier
Evry 91011
France

Email: julien.bournelle@int-evry.fr

Maryline Laurent-Maknavicius
GET/INT
9 rue Charles Fourier
Evry 91011
France

Email: maryline.maknavicius@int-evry.fr

Rafa Marin Lopez
University of Murcia
Murcia 30071
Spain

Email: rafa@dif.um.es

Dan Forsberg
Nokia
P.O Box 407
NOKIA GROUP FIN-0045
Finland

Email: dan.forsberg@nokia.com

Jean-Michel Combes
France Telecom R&D
38/40 rue du General Leclerc
Issy-les-Moulineaux 92794
France

Email: jeanmichel.combes@francetelecom.com

Intellectual Property Statement

Disclaimer of Validity

ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

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