# STUDY OF PROTOCOL FOR CARRYING AUTHENTICATION FOR NETWORK ACCESS (PANA) AND ITS FUNCTIONALITY

## (FOR ACHIEVING NETWORK SECURITY IN THE NETWORK LAYER)

*[1] MS. SHABINA GULAM AHEMED SAYYED , [2] DR. G.R. KULKARNI*

**[1] Research Scholar, Computer Science & Engg Dept., Suresh Gyan Vihar University, Jagatpura,Jaipur,Rajastan**
**[2] Principal, Kalol Institute of Technology & Research Center , Kalol Gujrat**

***shabina_sayyed@yahoo.com,grkulkarni29264@rediffmail.com***

***ABSTRACT :*** *Nowadays networking world requires IP-device to alternative themselves before getting permission to access a network means to get authorization to use it. To achieve this authentication a protocol is needed . which provides several authentication methods and special features that link layer is not able to satisfy. Because of the absence of such mechanism like a protocol for authorization in link layer ,non standard and proprietary methods where used to get the needed functionality. Both application layer and additional layers between link-layer and network-layer where used, in addition to overloading existing network layer's protocol to achieve the functionality of missing authentication protocol . Instead of those non standard inventions a network layer protocol for authentication would be a better solution. An authentication protocol for a higher layer than link layer is necessary , When functionality of link layer authentication is not satisfying and does not meet the expected authentication and security requirements. Access control with authentication and authorization of the clients and the access networks is needed to provide secure network access. Therefore a protocol is required which work as a transport for the authentication parametes between the client and the access network.*

*PANA working groups goal was to define or identify a carrier respectively a transport for a certain payload. This payload should ideally be an existing authentication protocol which meets the current requirements of network access authentication . The working group took care of desccribed problem and defined a protocol for clients using IP protocols to authenticate themselves to an access network in order to be granted network access, called PANA. Now a client can get access to a networks backend Authentication ,Autherization and accounting (AAA) infrastructure without knowing the details about the used protocols and without having link layer specific mechanism . PANA also supports both multi-access and point to point links, as much as methods for authentication ,dynamic service provider selection and roaming clients PANA provides a protocol that allows a host and a network to authenticate each other for network access.*

*So it is not intention of PANA to develop a new security protocol and technologies belonging to such a protocol like authentication and authorization mechanism. Existing methods should be reused, such as the Extensible Authentication Protocol (EAP) and its features like key distribution and derivation Methods. The EAP may need to be extended to fulfill the need or requirements for PANA. But this extension is outside the scope of PANA. The protocol to be invented, PANA can be considered as a front end of AAA protocol or any other protocol the network uses for authentication of its clients. To understand PANA, we will first discuss about the requirements of PANA and before that we will study the description of PANA usage model, Components of PANA etc.*

**PROTOCOL OVERVIEW**

Network access authentication is a key procedure for network operator to control user access to the network service. The IETF recently finished its major work in this area by standardizing an IP based protocol named Protocol for Carrying Authentication for Network Access (PANA).We provide a fruitful analysis of PANA Architecture based on develop IETF Standard deployed on IPv4 and next generation network environments.

1. PANA [2] is an application protocol using the User Datagram Protocol (UDP) as transport, which has been specially conceived by the IETF to carry the Extensible Authentication Protocol (EAP) in order to support different authentication mechanisms for network access, regardless of the underlying network access technology.
2. EAP [4] was standardized by the IETF to provide a flexible authentication framework for network access.
3. Various solutions can be considered as an alternative to PANA. AAA protocols, DHCP, TCP and IKEv2 are considered here as potential alternatives to PANA for EAP transport. AAA protocols such as RADIUS or

Diameter do not have message formats that satisfactorily meet the requirements (see RFC 4058) for an EAP lower-layer protocol. Some header fields are too large, some too short, some are not present at all, and so on. PANA, designed from scratch with its own message format, matches the EAP transport requirements. EAP over DHCP2 has complexity problems that eliminated it as a candidate for the IETF EAP standard

4. Difference in messaging direction between EAP and DHCP
(EAP requests and DHCP requests are sent in opposite ways)
5. Difficulty with integrating (stateful) EAP authenticator and stateless DHCP relay agent
6. Applicability of PANA On emerging network (IPV4) Next Generation Network

1) On emerging network (IPV4)
2) Next Generation Network
3) Wireless multihop and smart grid
4) Mobile network

## I. INTRODUCTION OF PANA

PANA [2] is an application protocol using the User Datagram Protocol (UDP) as transport, which has been specially conceived by the IETF to carry the Extensible Authentication Protocol (EAP) in order to support different authentication mechanisms for network access, regardless of the underlying network access technology. PANA can be used in

1. Environments with physical layer security
2. Environments with link layer security
3. Environments where no lower security is available

PANA requirement:

1) Topology Knowledge: Device Identifier information can be installed at the correct devices
2) Device Identifier Installation: Security provided by DI installation is sufficient for some environments. Otherwise, DI is accompanied by cryptographic keys.
3) Disconnect Indication: Link layer disconnect indication cannot be assumed
4) Session Key Establishment: Session key needs to be available for PANA SA

Steps involved in PANA:

1) PAA Discovery: To discover the PAA's addressed dynamically by
a) (Link local) multicast UDP packet from PaC.
b) PaC sends data packets. Then EP sends a PANA_discover message to PAA, which contains PaC's unicast address and PAA sends PANA_start to PaC. In PAA Discovery step II involved to check the hop limit, so to prevent from attacks Steps: Prevent off-path attacks (Cookie, Sequence numbers) by

• Initial Sequence Number (ISN) mechanism is used to prevent blind Does and off-path attacks.
• Cookie mechanism is used to prevent non-blind DoS attack. Cookie is sent from PAA in PANA_start message, but does not create any state in PAA that would enable DoS attack. The Cookie is implementation specific by implementing as below
• Message Flow

PaC PAA Message(tseq,rseq)[AVPs]
---
1) ----------> PANA_discover(0,0)
2) <---------- PANA_start(x,0)[Cookie]
3) ----------> PANA_start(y,x)[Cookie]
(continued to authentication phase)

### A) *Literature Survey*

Up to the early 2000s there was no standard protocol to transport network access authentication information, For example

1. Using Point-to-Point Protocol over Ethernet (PPPoE) to implement an authentication protocol, but it complicates the implementation of multicast-based services over PPPoE.
2. In Mobile Internet Protocol version 4 (MIPv4) has an extension to support network access authentication that requires a foreign agent in the visited network.
3. In Wi-Fi networks captive portal, has been implemented on top of Hypertext Transfer Protocol (HTTP).This variety of choices greatly complicates the management of authentication and network access control

To solve this problem, the Internet Engineering Task Force (IETF), through the PANA Working Group (WG), has developed the Protocol for Carrying Authentication for Network Access (PANA)[2] and an associated architecture [3] to carry network access authentication regardless of the access technology.

PANA-related IETF RFCs have been produced. As a consequence of typical pre-analysis within IETF, two informational documents were delivered: one to define the requirements for PANA (RFC 4058) and another

(RFC 4016) that analyzes the security requirements and threats for PANA. Based on these initial RFCs, the PANA base specification (RFC 5191) and PANA architecture (RFC 5193) were delivered. The PANA state machine (RFC 5609), which provides a guide for developers to implement PANA, was also submitted. During the development of this initial set of specifications, several features were identified as extensions to the basic protocol functionality and therefore removed from the initial set of specifications for simplicity.

The first extension is the specification of a PAA discovery mechanism used by a PaC to Ascertain the PAA's IP address to be used during a PaC-initiated PANA authentication. RFC 5192 defines such a discovery mechanism using DHCP (v4/v6).

The second extension details the PEMK derivation algorithm (RFC 5807) that is used for Generating cryptographically independent PEMKs for different EPs.

The third extension is the so-called PANA pre-authentication (RFC 5873). The objective of PANA pre-authentication is to reduce EAP authentication latency during handoff in mobile environments.

## II. OVERVIEW OF THE EXTENSIBLE AUTHENTICATION PROTOCOL

EAP [4] was standardized by the IETF to provide a flexible authentication framework for network access. This flexibility was achieved through the definition of the so-called EAP methods, which allow user authentication based on different mechanisms such as symmetric keys or digital certificates, it presents a layered architecture where each layer processes a different part of an EAP message. An EAP authentication is based on the execution of a specific EAP method between an EAP peer and an EAP server through an EAP authenticator in the network access server (NAS) providing network access (e.g., an access router) for the user's device. Finally, the EAP server functionality is typically implemented by a backend server placed in the network, such as an authentication, authorization, and accounting (AAA) server.

A protocol referred to as EAP lower-layer protocol is used to transport EAP packets between the EAP peer and EAP authenticator. Specifically, as we analyze, PANA is an EAP lower-layer protocol. Alternatively, the communication between the EAP authenticator and EAP server is performed with an AAA protocol like RADIUS [5] or Diameter [6]. Additionally, many EAP methods also generate keying material upon successful completion of authentication. The exported keying material is composed of the Master Session Key (MSK) and the Extended Master Session Key (EMSK).Both keys are exported to the EAP lower layer in the EAP peer, whereas the EAP server exports them to the AAA layer. While the MSK is eventually provided by the EAP server to the EAP lower layer in the EAP authenticator to establish a security association with the EAP peer, the EMSK is not provided to any other entity outside the EAP server and peer.

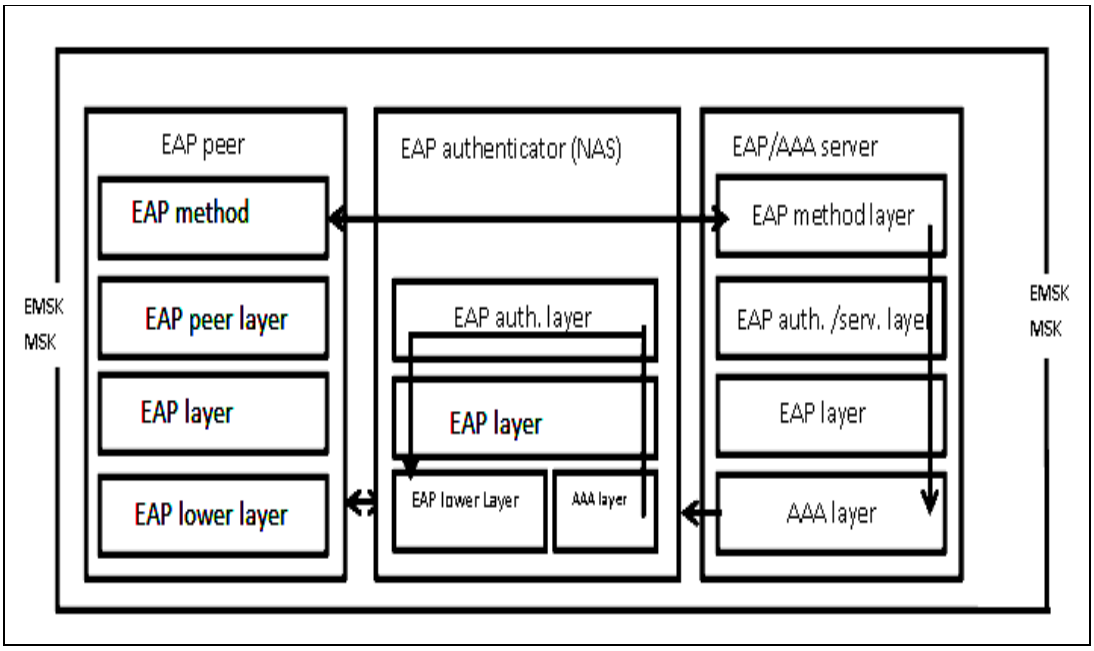
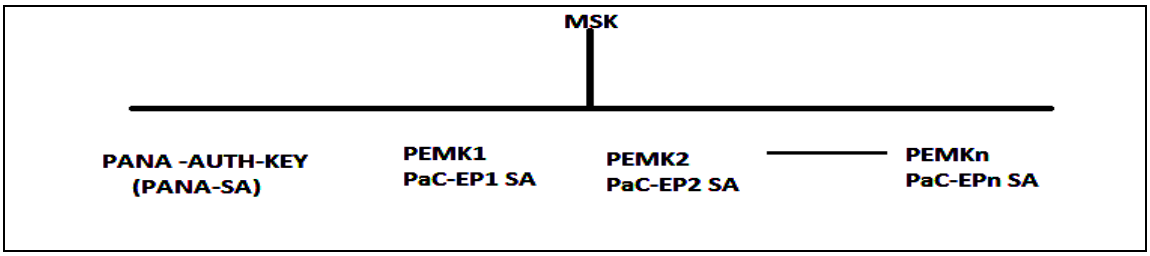



**Fig.1.** ***EAP framework***




## III. COLLABORATING EAP AND PANA

Carrying EAP over PANA

1) Authentication and authorization required for network access procedures. Steps involved

- EAP is payload of PANA (carried in EAP AVP)
- Use an appropriate EAP method depending on
- the security requirements.
- Difficult to prevent all attacks until PANA SA is established.

2) Transport Protocol Properties

- EAP requires ordered message delivery since EAP provides its own reliability and does not require the transport to be reliable.
- EAP recommends EAP methods to provide message fragmentation.
- EAP supports retransmission for EAP Requests and Retransmission timeout calculation based on RFC2988 takes congestion control into account.

3) Approach chosen by PANA

- PANA does not provide fragmentation. but we use EAP method fragmentation for EAP messages and use IP fragmentation for other messages.
- PANA provides Ordered delivery of EAP messages on top of UDP which protecting the PANA PDU after PANA SA is established.

i)Dual sequence number with orderly-delivery.
ii) PANA SA Establishment by implementing the steps
iii) EAP method must provide session key for PANA SA
iv)There is no secure tunnel established between the PaC and the PAA (e.g. via ISAKMP or TLS) outside EAP!

4) EAP Method Choice is one of the two methods
->PANA can carry any EAP authentication method.
->It is the responsibility of the user and the network operator to pick the right method, depending on the environment.
a) PANA does not enable weak methods in secure environments (a non-goal!).
b) PANA does not create a secure channel for them.
c) PANA can carry EAP-tunneling methods (PEAP, EAPTTLS).

5) Device ID Choice

1) PaC will configure an IP address before PANA if it can Network policy: EP might detect PaC's attempts and trigger PANA first
2) DI is either a link-layer address, or IP address
IP address: when PaC can configure one prior to PANA and IPsec is used for access control.
Link-layer address: otherwise.

3) Filter Rule Installation
->PANA protocol helps identifying who should gain access.
->PAA helps EP build filters based on PANA results.
->When PAA and EP are separated, a protocol is needed.

6) Device Identifier Exchange

Steps involved
->Key derived from EAP method; No algorithm negotiation because by installing this device identifier unauthorized nodes are not able to inject packets.
->Exchange data origin authenticated, replay and integrity protected with PANA SA.
->Triggering a data protection protocol because Spoofing attacks on shared links cannot be prevented by device ID based packet filters. Cryptographic protection needed. Steps:

->PAA can signal if L2 or L3 ciphering should be initiated after PANA.
->EAP established session key is indirectly used as an input to enforce link or network layer protection.
->PANA can help bootstrap link-layer/network-layer ciphering.
7) Re-authentication
->Lower-layer disconnect indication is not always available
->Garbage collection and stop of accounting required
->Prevent DI spoofing and resulting service theft after disconnect (e.g. due to roaming)
Steps: ->Soft-state principle
->Two types of re-authentication supported by PANA
->Re-authentication based on EAP
->Re-authentication based on PANA_reauth / PANA_ reauth_
ack exchange
->Both PaC and PAA can initiate re-authentication Protection by PANA SA
->Limit re-authentication rate in implementation

The role of PANA is to transport EAP messages between peer (referred to as PANA Client or PaC) and authenticator (PAA). PANA uses UDP as a transport layer, and hence the service provided to PANA may have packet losses, duplication and re-ordering. An exchange of messages in PANA is a session, which is divided into four phases:

1)Authentication and Authorization At the start of a PANA session this phase involves the exchange of EAP messages to perform authentication.

2) Access once authentication of the peer is successful, network access is provided. During this phase either PaC or PAA may test for the livens of the session (which has a limited lifetime).

3)Re-authentication May be performed to maintain the session liveness.

4) Termination Either PaC or PAA may terminate a session. If a session isn't terminated gracefully, then a timeout on the PANA session will result in the termination.

PANA communications are implemented as a series of request and answer messages. The PANA session can be initialized by either the PAA or PaC. The methods for each entity learning about the presence of the other is out side of the scope of PANA (e.g. it may be through DHCP). For a PAA-initiated-session, after it discovers the presence of a PaC, it sends an AuthRequest message to start the session (the 'S' flag indicates this message is to start the session). This initial AuthRequest is used to force a restart of the EAP session at the Peer. The PaC responds with an AuthAnswer, which results in the EAP session at the Authenticator restarting. The EAP Authenticator initiates the authentication with an EAP Request. This triggers the PAA to send an AuthRequest carrying the EAP Request method. Upon receipt of the AuthRequest, the PaC passes the EAP Request method to the EAP Peer and replies with an AuthAnswer. The AuthAnswer messages are acknowledgements to the AuthRequest messages. The PaC sends the response to the challenge in an AuthRequest (which is also acknowledged by the PAA with an AuthAnswer). This sequence of EAP requests and responses (and AuthRequest and AuthAnswer messages) may repeat until the authentication is complete. Finally the EAP Authenticator will send a Success or Failure method indicating the result of authentication. The EAP Success is shown in Figure, which is carried in an AuthRequest with the complete flag set. Once the AuthAnswer is received by the PAA, both PAA and PaC have the PANA session established and the Access phase is entered. Other relevant details of PANA include 32-bit sequence numbers are used to maintain ordering and perform error detection. The sequence numbers at PAA and PaC are independent. An outgoing request message contains a sequence number, and the corresponding answer message must have the same sequence number.

Request messages are retransmitted if an answer is not received within a specified time. The session is terminated if too many retransmissions occur. PANA messages contain 16 bytes of fixed size header (e.g. flags, message type, sequence number, session identifier) as well as a variable number of Attribute-Value Pairs (AVPs). AVPs include: the actual EAP message; authentication data; session lifetime; and other security related information. Optional piggybacking of messages allows either PaC or PAA to send a single PANA
message that represents both an answer and a request. The collaboration of PANA with EAP can be shown in Fig. 2 & 3.

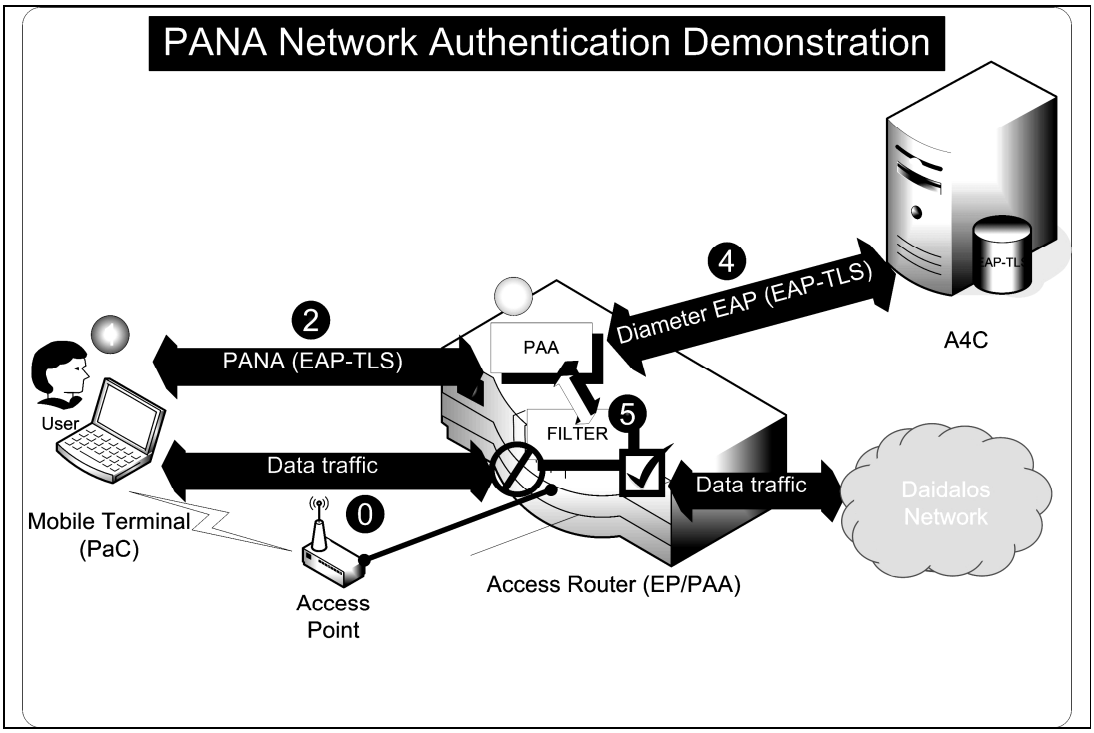



*Fig. 2 PANA network authentication*

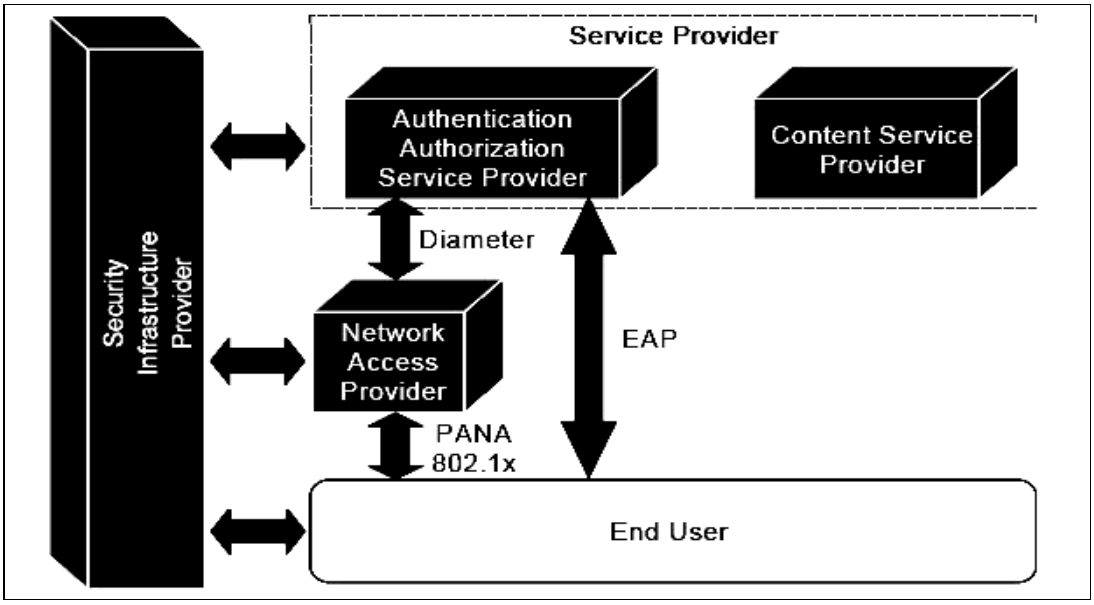



*Fig. 3 PANA with EAP*

## IV. PANA ARCHITECTURE

PANA has been designed to transport EAP between an EAP
peer and an EAP authenticator; thus, it is an EAP lower-layer protocol. Consequently, the PANA architecture [3] takes into consideration four main logical entities that are related to the EAP entities described earlier. As observed in Fig. 1, these PANA entities are:

•The PANA Client (PaC): It is the client entity of PANA. It resides in the user's device that is requesting network access and interacts with the EAP peer implementation in the same device. PaCs can be end hosts (e.g.,

laptops and cell phones), and are responsible for requesting network access and anticipating in the authentication process by using PANA.

•The PANA Authentication Agent (PAA): It is the server-side entity of PANA. A PAA is in charge of communicating with the PaCs for authenticating and authorizing them for network access by interacting with the EAP authenticator implementation on the same device. To verify the credentials and rights of a PaC, the PAA may consult a back-end AS, such as an AAA server. An AAA protocol (e.g., Diameter) is used to communicate with the PAA and the Authentication Server (AS).

•The Enforcement Point (EP): It is the entity in the access
network that performs forwarding decisions of data traffic originating from or destined to the user's device. It implements non cryptographic (IP filters) or cryptographic filters at either the network layer (e.g., IPsec) or the link layer (e.g., the four-way handshake protocol of IEEE 802.11) to selectively discard data packets depending on certain parameters associated with the user. Typically, access points or access routers play the role of an EP.

•The AS: It implements the EAP server functionality to verify the credentials provided by a PaC through a PAA. The AS functionality is typically implemented on an AAA server where the EAP server is placed. Upon successful verification of the credentials, the AS sends authorization parameters (network access lifetime, quality of service parameters, cryptographic material, etc.) to the PAA. From the implementation standpoint, the interface between a PANA entity (i.e., a PaC or a PAA) and its associated EAP entity (i.e., an EAP peer for the PaC or an EAP authenticator for the PAA) allows the local coordination between PANA and EAP state machines through a set of state variables that are accessible from both of the locally coordinating state machines. This interface is fully specified in RFC 5609 [7]. To provide flexibility in the deployment of PANA (e.g., allowing a single PAA to manage several EPs at the same time), the protocol designers considered the possibility of physically separating the network access authentication process (performed by the PAA) from the data traffic filtering functionality (implemented by the EP). Thus, once the user successfully completes a single PANA-based authentication through a specific PAA, this can provide access to the PaC through different EPs managed by the specific PAA, thus avoiding a PANA execution each time the user changes EP.

When the PAA is placed on a different device from the one implementing the EP functionality, the PAA uses a configuration network protocol (CNP), like Simple Network Management Protocol (SNMP), to transfer configuration information to the EP after a user is successfully authenticated and authorized to use the network. Otherwise, when both entities are located on the same physical entity, this process can be performed by simply using an application programming interface (API).

To provide security protection, PANA defines two types of security associations (SAs). On one hand, the PANA SA is established between the PaC and PAA in order to protect the integrity of PANA messages. On the other hand, after the PANA SA has been set, a PaC-EP SA may be established to protect data traffic between the PaC and the EP. Both PaC and PAA derive the PANA_AUTH_KEY to build a PANA SA and may derive the PaC-EP master key (PEMK) to establish a PaC-EP SA.

## V. PANA WORKING

PANA Usage Models : For PANA four different usage model can be used

1. PAA co-located with EP but separated from AR

The shape below in Fig. 4 shows the topology where the Enforcement Point (EP), which control access and the PANA Authentication Agent (PAA) are located together. The PaCs residing on different devices communicate to the PANA Authentication Agent to be authenticated. The job of PANA in this logical topology is to carry the authenticate data from PaC to PAA, which is responsible for checking this data, granting or denying network access to the PaC and sending a positive or negative message back to the client after verification of the credentials. PANA is responsible for a secure transport of those credentials and the methods to verify them.

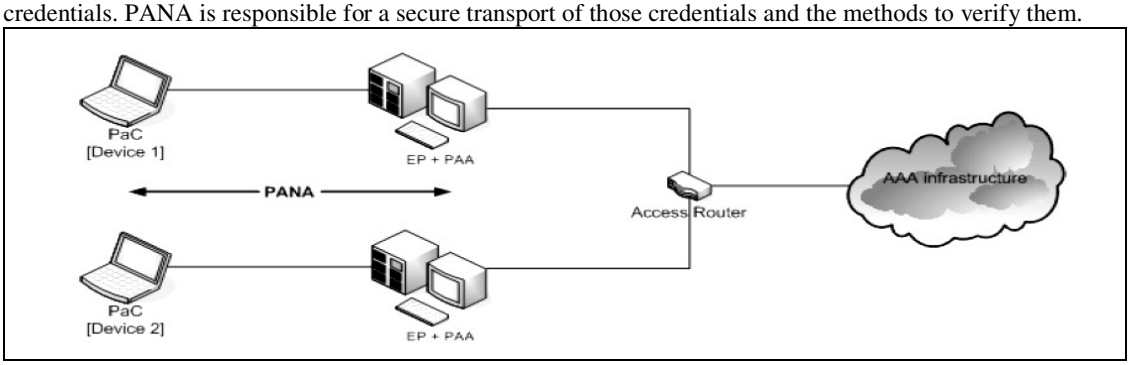



**Fig. 4** ***PAA co-located with EP but separated from AR***

2. PAA co-located with AR but separated from EP

In second model shows in Fig. 5 that PAA and the first-hop access router are located together. Both are separated from the EP which is located between themselves and a PaC on a certain device. Here the same authenticated data like in 1st model is sent from PaCs to PAA. But if the first attempt of authentication was successful, parameters for access control according to the PaC have to be distributed to the corresponding EPs. in order to grant access to the device on which the PaC is authenticated.

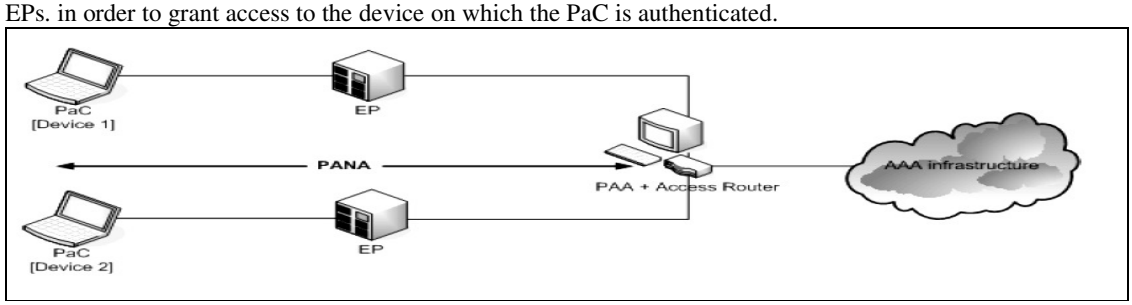



**Fig. 5** ***PAA co-located with AR but separated from EP***

3. PAA co-located with EP and AR

The fig 6 shows that EP, PAA and the access router, which provides routing and access control in this case are united in one single location. The message between PaC and AAA are still the same and has to be verified by the PAA.

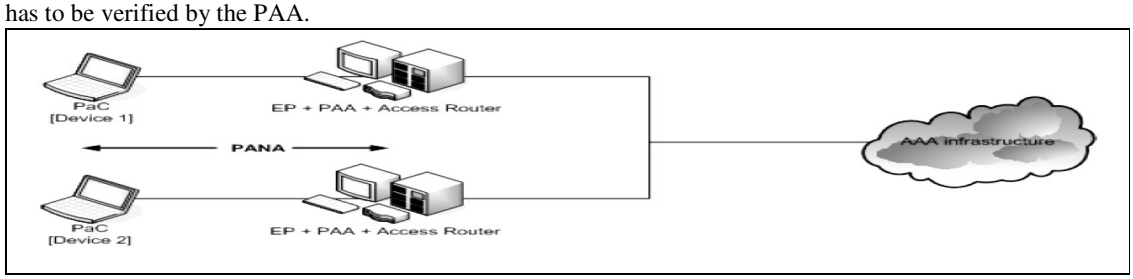



**Fig.6** ***PAA co-located with EP and AR***

4. PAA separated from EP and AR

EP, PAA and AR each are standalone instances were shown in Fig. 7. The separate PAA however has to be on the same IP range. Similar to the above models the PaC exchanges the messages with the PAA. After successful authentication of the PaC by the PAA, the access control parameters have to be distributed over a separate protocol to the corresponding EPs.

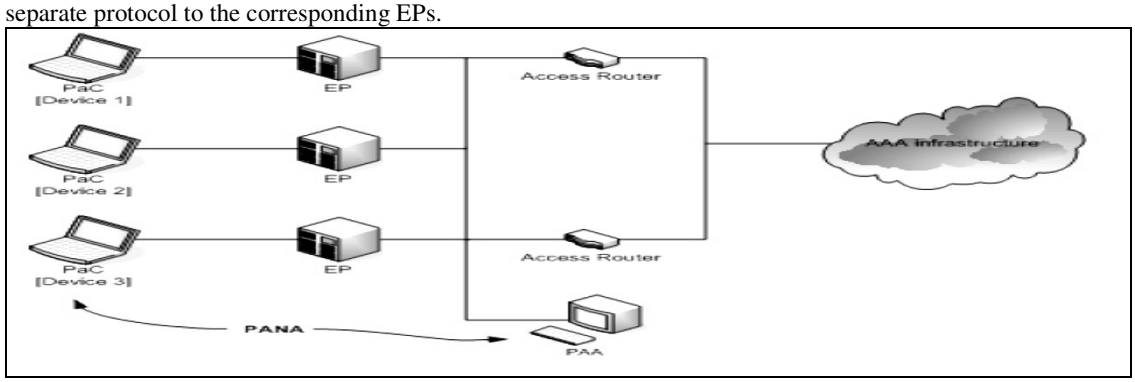



**Fig. 7** ***PAA separated from EP and AR***

association protocol, such as Internet Key Exchange (IKE) or the four-way handshake protocol of IEEE 802.11, to protect the user data transmitted between the PaC and the EP. Indeed, a distinct PEMKi is derived for each specific EPi used by the PaC so that compromising one.

## VI. PANA PROTOCOL OPERATION

PANA proposes a flexible framework where either the user or the network is responsible for starting the network access control process. So PANA authentication can be initiated by the PaC or the PAA. Thus, both entities must first know or discover each other's IP address to start the PANA execution. For example, a PAA

discovery mechanism can be based on either static configuration or with Dynamic Host Configuration Protocol (DHCP), where the PaC is not only provided with a valid IP address but also with a list of available PAAs.

Once the PaC knows the PAA's IP address (or the PAA finds out the PaC's IP address when, for example, this is configured through DHCP), the protocol operation can start. As observed in Fig. 2 & 3 a PANA execution may consist of up to four different phases. Initially, during the authentication and authorization phase, the PaC and the PAA negotiate some parameters like the integrity algorithms used to protect PANA messages (1). Additionally, during this phase, the user is authenticated by using EAP, which is transported within both PANA messages (between PaC and PAA) and an AAA protocol (between PAA and AS) (2).As an example, Fig. depicts an authentication process based on the widely employed EAP-TLS method. As observed in this figure, the PAA forwards the EAP messages to the backend AS (where the EAP server is collocated) for verification of the user's credentials. Once the authentication is successfully completed, a PANA session is established with an associated lifetime. The protocol then enters the access phase, in which the PaC is able to access the network by transmitting and receiving data through the EP(s).

When the underlying network does not provide security protection, all PANA messages transmitted from the beginning of the access phase to the end of the PANA session can be protected with integrity by using the PANA SA derived from the MSK obtained as a consequence of the successful authentication. After establishing the PANA SA, if data traffic protection is required, a PaC-EP SA is established between PaC and EP to provide confidentiality and/or integrity to user data exchanged between both entities. He required EMK is installed by the PAA on the specific EP (3).When the PANA session is about to expire, the PaC or PAA can initiate the re-authentication phase to extend the current session. For example, in Fig. , this phase is based on the fast re-authentication mechanism of EAP-TLS, which will generate a new key (MSK') to rebuild the PANA SA and potential PaC-EP SAs (4). Finally, these entities can end the PANA session by (where the EAP server is collocated) for verification of the user's credentials. Once the authentication is successfully completed, a PANA session is established with an associated lifetime. The protocol then enters the access phase, in which the PaC is able to access the network by transmitting and receiving data through the EP(s). When the underlying network does not provide security protection, all PANA messages transmitted from the beginning of the access phase to the end of the PANA session can be protected with integrity by using the PANA SA derived from the MSK obtained as a consequence of the successful authentication. After establishing the PANA SA, if data traffic protection is required, a PaC-EP SA is established between PaC and EP to provide confidentiality and/or integrity to user data exchanged between both entities. The required PEMK is installed by the PAA on the specific EP (3). When the PANA session is about to expire, the PaC or PAA can initiate the re-authentication phase to extend the current session. For example, in Fig., this phase is based on the fast re-authentication mechanism of EAP-TLS, which will generate a new key (MSK') to rebuild the PANA SA and potential PaC-EP SAs (4). Finally, these entities can end the PANA session by when the PaC desires to log out of the network access session), to remove the resources allocated by the network for the PaC. Additionally, reserved network resources are also released when the PANA session lifetime is reached. As we can observe, during each phase a different set of messages can be sent, according to the rules defined by the PANA state machines described in which have been proven to be well designed and deadlock-free.

**Table 1: PANA Related IETF RFCs**

| Documents | Content |
|---|---|
| **RFC 4016** | Associated threat analysis and security requirements for the PANA protocol |
| **RFC 4058** | The general requirement of PANA are described |
| **RFC 5191** | The PANA base specification is described |
| **RFC 5192** | New DHCPv4 and DHCPv6 option are specified. PaC can discover the available PAAs within a network |
| **RFC 5193** | The PANA framework and the general architecture are described |
| **RFC 5609** | A description of the PaC and PAA state machines is provided |
| **RFC 5807** | Specification of the PaC-EP Master Key(PEMK) derivation process for the EP and the PaC using |
| **RFC 5872** | Rules for allocating protocol fields in PANA are relaxed |
| **RFC 5873** | Extension to the PANA base Protocol to support PANA pre-authentication |
| **RFC 5873** | Extension which specifies the PANA Relay Element(PRE) functionality |

## CONCLUSION

We have provided a detail study of the PANA protocol, which is the contribution made by the IETF in the field of network access authentication. We have shown the PANA architecture and its associated entities specially connection with EAP involved in the protocol operation. We have also explained a set of PANA related IETF RFCs produced by the PANA WG. The basic function of PANA to carry EAP over UDP takes maximum advantage of EAP characteristics of lower-layer independence and authentication method independence. As a

result, PANA is gaining interest as a potential candidate for network access authentication (for basic usage) and service access authentication (for extended usage) in both existing and emerging network scenarios.

**ACKNOWLEDGMENT**

I am very much thankful to my guide Prof. G. R. Kulkarni because of his motivation and support i am try to present a paper on very interesting and very innovative topic study of PANA for achieving network security. I also thanks to the PANA workgroup who have initiated this topic and presented excellent articles on this topic .I also thanks to Pedro Moreno Sanchez (co-developer of OpenPANA) for his excellent articles from that i have learned the detail concept of PANA.

**REFERENCES**

[1] M. O'Droma and I. Ganchev, "The Creation of a Ubiquitous Consumer Wireless World Through Strategic ITU-T Standardization," IEEE Commun. Mag., vol. 48 no. 10, Oct. 2010, pp. 158–65.
[2] D. Forsberg et al., "Protocol for Carrying Authentication for Network Access (PANA)," IETF RFC 5191, May 2008.
[3] P. Jayaraman et al., "Protocol for Carrying Authentication for Network Access Framework," IETF RFC 5193, May 2008.[4] B. Aboba et al., "Extensible Authentication Protocol (EAP)," IETF RFC 3748, June 2004.
[5] C. Rigney et al., "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2865, June 2000. [6] S. Gordon, "Towards Verification of the PANA Authentication and Authorization Protocol Using Coloured Petri Nets," Proc. 10th Wksp. and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools, Aarthus,Denmark, Oct. 2009, pp. 61–80
[7] P. Calhoun and J. Loughney, "Diameter Base Protoco,"IETF RFC 3588, Sept. 2003Authentication
[8] V. Fajardo, Y. Ohba, and R. Marin-Lopez, "State Machines for Protocol for Carrying
for Network Access (PANA)," IETF RFC 5609, Aug. 2009.
[9] C. Rigney et al., "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2865, June 2000.
[10] P. Calhoun and J. Loughney, "Diameter Base Protoco,"IETF RFC 3588, Sept. 2003.
[11] V. Fajardo, Y. Ohba, and R. Marin-Lopez, "State Machines for Protocol for Carrying Authentication for Network Access (PANA)," IETF RFC 5609, Aug. 2009.
[12] C. Kaufman et al., "Internet Key Exchange Protocol Version 2 (IKEv2)," IETF RFC 5996, Sept. 2010.
[13] A. Dutta et al., "Media-Independent Pre-Authentication Supporting Secure Interdomain
Handover Optimization,"IEEE Wireless Commun., vol. 15, no. 2, Apr. 2008, pp. 55–64.
[14] "Machine-to-Machine Communications (M2M); Functional Architecture," ETSI Technical Specification 102 690 v. 1.1.1
[15] Rafa Marine Lopez," Network Access Security for the internet : Protocol for Carrying Authentication for Network Access" IEEE Communication Magazine March 2012.