AAA considerations within several NEMO deployment scenarios

Julien Bournelle[1], Guillaume Valadon[3], David Binet[2], Saber Zrelli[4], Maryline Laurent-Maknavicius[1], and Jean-Michel Combes[2]

[1] GET/INT, France
[2] France Telecom R&D, France
[3] University of Tokyo, Japan; LIP6 - UPMC, France
[4] JAIST, Japan

Abstract. Network mobility allows nodes to maintain their connections whilst attaching to different access networks. These access networks may be based on different access technologies. The NEMO Basic Support protocol is a generic protocol that can be used in different mobile environments such as bus or train. Yet, access control mechanisms and Authentication, Authorization and Accounting (AAA) architecture have to be set up according to these specific contexts. The fundamental difference, from an operator's point of view, for access control and AAA considerations, is the ownership of the Mobile Router which is the centric device for network mobility. As such, three deployment scenarios are studied. AAA architectures are proposed and security problems are highlighted for each scenario.

1 Introduction

Support of network mobility in IPv6 is now possible with the use of the NEMO Basic Support protocol [1] defined at the Internet Engineering Task Force (IETF). From an operator's perspective, this protocol allows IPv6 mobility and continuous connectivity in environments with embedded networks such as cars (cf. [2]), buses or trains. Other devices connected to a Personal Area Network (PAN) may also benefit from this solution. However, access control and security are necessary for an Internet Access operator.

Operating common AAA architectures in NEMO environnments could seem straigthforward. However, as shown in this article, their interactions raise some issues that should be considered by operators. A AAA framework generally assumes that customers use fixed equipments in a fixed infrastructure. On the contrary, within NEMO environment, users' devices may move and moreover the NAS may also be moving. Previous works exist on this topic such as those described in [3] and in [4]. The former proposes an architecture and protocols for a specific NEMO deployment scenario. The latter introduces AAA framework within NEMO environment and specify some requirements. In this article, we extend these two previous works by studying how to combine both network mobility and access control mechanisms from an operator's point of view. For

this, in the second section, three possible deployment scenarios using NEMO Basic Support are described. We think that these three scenarios covers most of the deployment scenarios. The third section gives an overview of an access control mechanism based on a AAA architecture and presents the PANA protocol used to authenticate customers. Finally, in the fourth section, we explain how to combine mobility and access control mechanisms whilst raising current challenging issues.

This paper focuses on the NEMO Basic Support and not on the Mobile IPv6 protocol. The reason is that Mobile IPv6 allows mobility for end-host and not for mobile networks. As such, it does not introduce particular features from a AAA point of view.

2 NEMO deployments from an operator's perspective

The NEMO Basic Support protocol allows a whole IP network to move whilst offering seamless connections to local mobile network nodes (MNN). For this, the NEMO protocol introduces the concept of Mobile Router (MR) and Home Agent (HA). Whilst away from its home network, the MR binds its new address, called Care of Address (CoA), to its Mobile Network Prefix (MNP) by sending signaling messages called Binding Update (BU). As a result of the registration, a bidirectional tunnel is established between the MR and the HA.

The following entities are defined to ease the categorization: the fixed Internet Service Provider (f-ISP) and the mobile Internet Service Provider (m-ISP). The f-ISP is an Internet access provider that offers Internet connectivity through a fixed infrastructure. It can be seen as a regular access provider selling Internet connectivity based on 802.11b, GPRS, 3G, or WiMAX. The m-ISP is an ISP operating moving networks. It manages MRs and HAs devices and offers its services to subscribers located inside these NEMOs. The m-ISP operates the HA of the moving networks and uses the services of f-ISP to access the Internet.

A customers can access Internet services provided by an f-ISP through a fixed infrastructure or provided by an m-ISP which deploys NEMO based infrastructure. This customer may access to the Internet through a device (laptop, phone) directly connected to the access network (of the f-ISP or of the m-ISP) or through a PAN with a Mobile Router handling the mobility for all his equipments. In the latter case, his Mobile Router is connected to the access network and his equipments are connected to the MR's ingress interface (cf. Fig. 1).

In the following sections, we describe the different usage scenarios depending on the entities (MNN, MR, AR) involved, then we define the AAA architecture that handles each case. In order to illustrate a real life scenario, we use a commercial NEMO-Bus deployment scenario using the NEMO Basic Support to offer Internet access within a bus. Issues raised in this article are still valid for other types of commercial NEMO deployments (e.g. trains,. . .).

2.1 MR-pan in the fixed infrastructure

In this scenario, the customer owns a PAN. Network mobility is managed by the MR-pan using NEMO Basic Support. This personal NEMO includes a MR and a set of MNNs attached to the MR-pan.

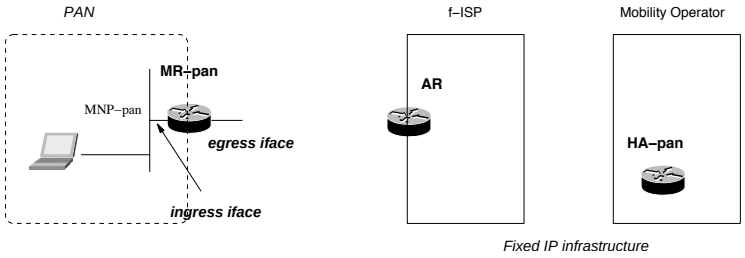

Fig. 1. MR-pan in a fixed infrastructure

On Fig. 1, the PAN customer uses his laptop to access to the Internet through the PAN's MR. The egress interface of his MR-pan obtains an address (CoA) from the fixed infrastructure and binds its MNP-pan. The laptop has an IPv6 address whose prefix is MNP-pan and uses his MR-pan as its default router. Thus its traffic is sent through the ingress interface of the MR which tunnels it to its HA-pan. This Home Agent (HA-pan) is most likely operated by a mobility operator. This mobility operator can be an operator different from f-ISP or m-ISP.

2.2 MR-bus in the fixed infrastructure

In this scenario, the end-user or customer uses a laptop to access to the Internet but we do not consider here a PAN. However, it uses a MR belonging to an operator for this purpose. This user may be connected in a bus offering Internet access. In this scenario, the MR-bus is a client for the f-ISP.

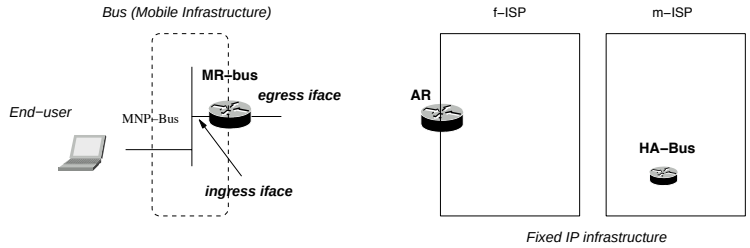

Fig. 2. MR-bus in the fixed infrastructure

On Fig. 2, the end-user obtains an address in the bus'network (whose IPv6 prefix is MNP-Bus) and uses the MR-bus as its default router. The MR-bus is operated by a m-ISP and it obtains an address for its egress interface from the fixed IP infrastructure (thus from the f-ISP). All the traffic from the mobile network is tunneled to the HA (HA-bus) of the MR-bus. Note that the ISP managing the fixed infrastructure (f-ISP) may also be the m-ISP. If not, the m-ISP uses resources from the fixed ISP and thus is considered as a f-ISP customer.

2.3 MR-pan in the MR-bus

In this scenario, we combine both two previous scenarios: we consider a MR-pan in a MR-bus. In this case, the MR-pan belongs to an end-user and the MR-bus belongs to the m-ISP or to another operator in charge of this mobile network. This case is also known as the nested case.

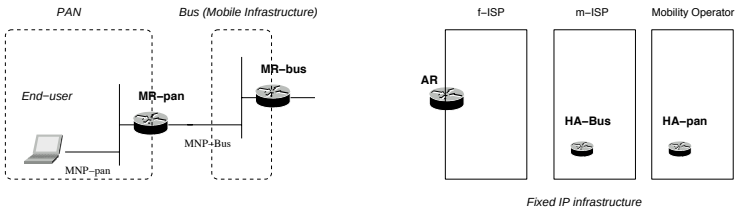

Fig. 3. MR-pan in the MR-bus

The MR-bus obtains a care-of address for its egress interface from the f-ISP and tunnels the traffic to its HA (HA-bus). The MR-pan obtains a care-of address for its egress interface in the bus' mobile network and tunnels the traffic from the end-user to its HA (HA-pan). The MR-bus may not see the traffic originated by the end-user's device if the tunnel between the MR-pan and the HA-pan is encrypted.

3 AAA overview

Regardless of the service used and the access type, ISPs have to set up some access control mechanisms. These mechanisms are generally based on the deployment of equipments and servers on specific platforms for each access operators. These platforms integrate access control means and authentication servers.

3.1 Generic AAA architecture

Fig. 4 depicts an AAA architecture where AAA stands for *Authentication, Authorization and Accounting*. The customer owns an IP client (e.g. a laptop or

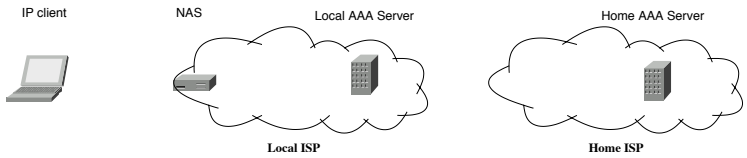

Fig. 4. Generic AAA architecture

MR-pan) and has a contract with an ISP called "home ISP" in order to get access to the Internet. To be authenticated in the visited network, the equipment has some credentials and sends them to a local *Network Access Server* (NAS), owned by the visited ISP, located at the edge of the network. The NAS relies on a local AAA server for authentication, but also for authorizing a client to access some services (such as Internet access). During authentication and authorization procedures, the local AAA server communicates with the home AAA server. Note that the local ISP also performs accounting in its own network for billing purposes as well as obtaining information on the current usage of resources. After AAA operations, the NAS receives configuration information from the AAA server that may be used to configure a security equipment performing firewalling or IPsec [5].

To summarize, the operators need at least three components for securing access to their networks:

- A protocol used between the client and the NAS. As an example, PANA or 802.11i can be used here.
- A protocol used between the NAS and local and home AAA servers. It is generally called a AAA protocol.RADIUS [6] is currently the most widely used.
- An authentication method between the client and the AAA server. The EAP [7] framework allows to use a wide variety of methods.

3.2 An example of client to NAS protocol: PANA

In NEMO environments, multiple access technologies may be used. As an example, the MR-bus could be connected to AR through WiMAX whilst offering Internet access to its passengers thanks to 802.11b/a/g. The protocol used between the client and the NAS authenticates the client based on long term credentials. The NAS relies on a AAA server for authentication purposes. After authentication succeeded, the NAS applies security polices based on a layer 2 or layer 3 identifier depending on the protocol. As an example, 802.11i would set up security at the layer 2 level.

To illustrate a AAA in a NEMO environment, we use PANA, the *Protocol for Carrying Authentication Network Access* [8] as the protocol to be used between the client and the NAS. We choose so because PANA is an IETF standardized protocol which is layer 2 agnostic. Moreover as it carries EAP packets, any authentication methods can be used. The PANA Authentication Agent (PAA)

is located in the NAS while the PANA Client (PaC) is in the client requiring access. The PANA framework also introduces the Enforcement Point (EP) which is the equipment where security policies are applied.

It is important to note that the issues raised in section 4.1, 4.2 and 4.3 are not dependent of PANA and are still valid if another protocol for authentication is used.

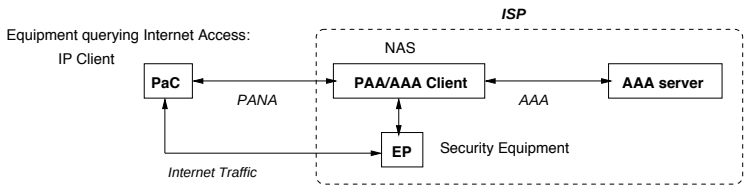

Fig. 5. PANA-AAA Framework

Fig. 5 shows the PANA-AAA architecture. The client uses PANA with the NAS. The NAS uses a AAA protocol with the AAA server. As PANA carries EAP packets, the AAA protocol must be either RADIUS-EAP [9] or Diameter-EAP [10]. After the authentication, the PAA configures the EP. Then the PaC sends its IP traffic through the EP to the Internet. It is up to the ISP to decide which security policy to use. As an example, the PANA protocol enables to bootstrap an IPsec tunnel between PaC and EP. The security policy uses a device identifier of the PaC such as its IP address or MAC address.

4 Introducing AAA in specific NEMO environments

In this section, we study how to introduce AAA mechanisms in the three scenarios described in section 2. One assume here that PANA is the protocol used between clients and NAS but other protocols may be used. Concerning AAA protocol, RADIUS or Diameter could be used. To simplify explanations, we assume that PAA is co-located in access router. Moreover, we do not put the customer's home AAA server on figures in order to avoid overloading them. This home AAA server is always contacted in order to authenticate the end-user.

4.1 MR-pan in the fixed infrastructure

In the scenario described in section 2.1, the end-user is granted access to the Internet through a laptop located behind his MR-pan. All the traffic seen by the f-ISP carries the source IP address of the MR-pan's egress interface. It is thus mandatory for the PAA to authenticate this IP address to correctly configure security policies.

Fig. 6 shows location of PaC and PAA. The PaC must be colocated with the MR-pan because it is the MR-pan's address that must be authorized to

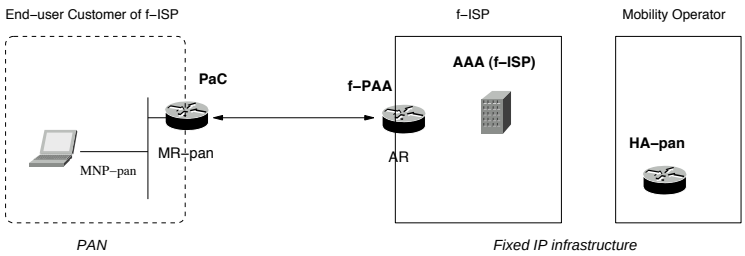

Fig. 6. MR-pan scenario

access to the Internet. Thus, the PAA authenticates the egress interface of the MR-pan and only traffic initiated by this interface is authorized. Basically, after the PANA authentication process, the MR-pan registers its CoA to its HA and establishes the bidirectional tunnel that handles its laptop's traffic.

Non explicitly authorized equipments One issue of this model is that a non-authorized equipment can access to the Internet. Indeed, the client uses its laptop whose source address belongs to the PAN whereas it is the MR-pan egress interface address which has been authorized. The MR-pan may hide its MNNs' traffic to the f-ISP if it encrypts the tunnel used with its HA-pan. However, the IPv6 prefix used in the MR-pan may be explicitly authorized by the operator managing the HA-pan.

A consequence is that one can imagine that a client could deliberately (or not!) let other people access through its personal MR-pan. This is an accounting issue and can be considered as a business model issue for the operator. One can notice that this issue already exists in current ISP deployment by using NAT features.

4.2 MR-bus in the fixed infrastructure

In the scenario described in the section 2.2, the MR-bus is operated by a m-ISP and uses resources of the f-ISP. We consider here that m-ISP is a different operator than the f-ISP. The m-ISP provides Internet access to its local customers through its MR-bus. To provide this service, the MR-bus must be authenticated by the fixed infrastructure. In the same time, the m-ISP needs to authenticate local customers in the bus.

Fig. 7 represents this scenario. All the traffic from the bus' mobile network uses the IP address of the MR's egress interface and is tunneled to the HA-bus. For this reason, the MR's egress interface must be authenticated by the PAA belonging to the f-ISP (noted f-PAA on the figure). The m-ISP must install a PaC on the MR-Bus's egress interface (noted Bus-PaC). While the egress interface is authenticated, the m-ISP can afford Internet service.

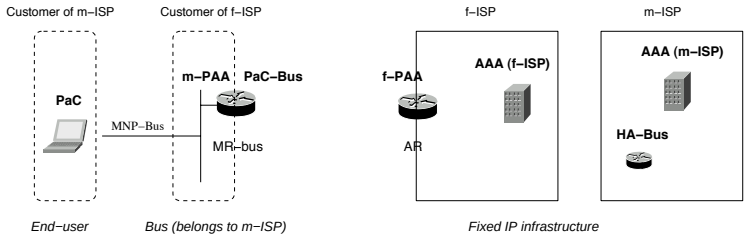

Fig. 7. MR-bus in the fixed infrastructure with AAA

For the same reason than for the f-ISP, the m-ISP should install a PAA in the MR-bus (noted m-PAA). This PAA will authenticate devices connected to the ingress interface. Thus, in this scenario, the NAS is moving.

AAA traffic security If the m-PAA relies on a AAA server for authentication, all the AAA traffic will be tunneled to the HA-bus and then delivered to the m-ISP's AAA server. This AAA server will then have to contact home ISP's server of local customers. This means that the AAA traffic may go through the air interface between MR-bus and the AR. For this reason, the m-ISP should ensure that his AAA traffic is correctly protected. In particular, the integrity, authentication and confidentiality must be ensure.

f-ISP and m-ISP agreements As the m-ISP offers Internet services based on f-ISP resources, there should be strong agreement between the two entities. In a sense, the f-ISP relies on the m-ISP authentication system to protect its network. Another aspect is relative to resource allocation, it appears that the MR-bus may need some extra bandwidth to provide correct Internet services in the bus. Based on the identity provided during the authentication of Bus-PaC, the f-ISP may configure its equipments for this.

Loss of connectivity Another issue concerns the authentication in the bus. If the m-PAA relies on a AAA server located in the fixed infrastructure, it may not be able to authenticate clients if the bus looses its connectivity. This issue is irrelevant here since we are considering authentication for network access. However, one can imagine that the m-ISP deploys some IP-based services in the bus and that it relies on the authentication for network access to authorize these services. In this case, this issue is relevant and needs to be considered.

4.3 MR-pan in the MR-bus

This scenario is quite similar to the previous one and is described in section 2.3. The only difference is that the single visiting node is replaced with an entire visiting sub-network.

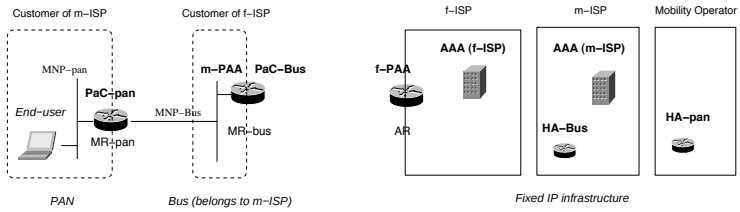

Fig. 8. Nested case with AAA

The PaC-bus is authenticated by the f-PAA. Then PaC-pan is authenticated by the m-PAA. Thus this scenario combines problems from the two above scenarios.

Nested case and availability of local services In addition to the issues highlighted earlier, there is however an additional one to consider. Considering that the m-ISP wants to provide some IP based services (such as a Web server) located in the NEMO-Bus, it will only allow IP traffic whose source address belongs to the mobile network (thus based on MNP-Bus). If we consider the end-user of Fig. 8, his laptop will have an IP address belonging to its PAN and this address will not be authorized on the bus' mobile network. The reason is that the m-PAA only authenticates and authorizes the address of the MR-pan's egress interface. Thus the end-user will not be able to access these local services. Moreover, the traffic will be routed through HA-bus, then HA-pan and then should come back through HA-bus to finally access the local services. This issue is tied to Route Optimization in the NEMO protocol [4].

5 Conclusion

In this article we considered three possible NEMO deployment scenarios from an operator's point of view: a Personal Area Network (PAN) using a NEMO-enabled mobile router (MR-pan) accessing to the Internet through a fixed access router, a bus offering Internet access through a NEMO-enabled mobile router (MR-bus) in it and finally a combination of these two scenarios. At the same time, it raises issues that must be solved or at least known before commercial deployment of NEMO Basic Support. The first issue is that only the egress interface of a Mobile Router is authenticated. As a result, IP traffic coming from the mobile network can access the Internet while it has not been explicitly authorized. Secondly, for similar reasons, a laptop behind a MR-pan is disallowed access to local services in a bus as services are restricted to authorized users directly connected to the MR-bus. These issues need to be considered and solved in order to deploy the NEMO Basic Support protocol on current IP infrastructures. Finally, different actors could take part in network mobility and this can lead to new business models that have some impacts on the AAA architecture.

Acknowledgements

The authors would like to express their acknowledgements to the Nautilus6 project [11] and in particular to the members of the n6aaa group for the discussions that leads to this article.

We also thank Thierry Ernst (Keio University/WIDE Project) for his careful review of this article and for his support.

References

1. V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. Network Mobility (NEMO) Basic Support Protocol. Request For Comments 3963, IETF, January 2005.
2. Thierry Ernst and Keisuke Uehara. Connecting Automobiles to the Internet. In *3rd International Workshop on ITS Telecommunications (ITST)*, Seoul, South Korea, November 2002.
3. S. Zrelli and T. Ernst and J. Bournelle and G. Valadon and D. Binet. Access Control Architecture for Nested Mobile Environments in IPv6. *4ème Conférence sur la Sécurité et Architectures Réseaux, SAR2005*, June 2005.
4. C. Ng and T. Tanaka. Usage Scenario and Requirements for AAA in Network Mobility Support. http://www.mobilenetworks.org/nemo/drafts/draft-ng-nemo-aaa-use-00.txt, 2002.
5. S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. Request For Comments, IETF, November 1998.
6. C. Rigney, A. Rubens, W. Simpson, and S. Willens. Remote Authentication Dial In User Service. Request For Comments, IETF, June 2000.
7. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). Request For Comments, IETF, June 2004.
8. D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin. Protocol for Carrying Authentication for Network Access. draft-ietf-pana-pana-10.txt, IETF, July 2005. Work in progress.
9. B. Aboba and P. Calhoun. RADIUS support for EAP. Request For Comments, IETF, June 2003.
10. P. Eronen, T.Hiller, and G. Zorn. Diameter Extensible Authentication Protocol (EAP) Application. Request For Comments, IETF, August 2005.
11. WIDE Nautilus6 Working Group Web Page, As of September 2004. http://www.nautilus6.org.