Internet Draft
Document: draft-ng-nemo-aaa-use-00.txt

C. W. Ng
Panasonic Singapore Labs

T. Tanaka
Matsushita Communications
Industrial

Expires: April 2003

October 2002

Usage Scenario and Requirements for AAA in Network Mobility Support

Status of this Memo

Abstract

This memo set out the basic Authentication, Authorization, and Accounting (AAA) model for Network Mobility Support (NEMO), and described various usage scenarios. From the scenarios, a set of AAA requirements in NEMO is drawn.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [2].

Table of Contents

1. Introduction

The problem of Network Mobility Support (NEMO) is identified in various previous works [3,4,5,6,7]. This document attempts to explore the usage scenarios and requirements for Authentication, Authorization, and Accounting (AAA) in the NEMO problem space. Since NEMO entails various mobile devices accessing the Internet using network resources that are in different administrative domains, AAA

is an important consideration for a NEMO solution.

In this document, we focus mainly on access control in NEMO. Since NEMO infrastructure is by and large wireless in nature, access control is a critical aspect for large-scale deployment of support for NEMO. Such large-scale NEMO deployments are usually found in

commercial applications, where Internet Service Providers (ISP) erect fixed and mobile access routers and allow subscribers to attach devices to the access routers for Internet connection. Examples of such commercial applications include providing Internet access in trains, ships, and aircrafts.

Access control is needed in these networks in order to protect the interest of the paying subscribers. If there is no access control, significant portions of the network resources may be used by unauthorized users, thereby affecting the quality of service provided to other legitimate subscribers.

The need for access control exists in all networks that allow unknown devices to connect to the network, and to identify itself to gain access to services and resources provided in the network. Access control function is usually provided by a gateway or router device, generally known as a Network Access Server (NAS). Excellent work on requirements for NAS can be found in [8]. It is not the objective of this document to duplicate previous effort in defining NAS requirements. Instead, this document explores specific requirements that arise due to characteristics that are unique to a network in motion. To this end, this document first presents the overview of operations in a network in motion. Since a NEMO solution does not exits (yet), this document assumes the operation to be based on a reverse tunneling link between the mobile router in a mobile network and the home agent in the home domain of the mobile router. Following this, we describe possible usage scenarios of mobile networks. From the usage scenarios, basic AAA requirements are drawn out.

1.1. Terms Used

It is assumed that readers are familiar with the NEMO terminology described in [9].

1.2. Assumptions

In this document, the following assumptions are made:

1. There exist an entity in the NEMO solution that resides in the home domain of the mobile network node which provide functionality similar to the home agent in the Mobile IP specification.

2. This document assumes there is no need for local fixed nodes (LFN) and local mobile nodes (LMN) to be authenticated by the mobile router they attached to. This is because the LFNs and LMNs belongs to the same administrative domain as their MR, and are always attached to the same mobile network.

2. Overview of Operation

2.1. Overview of Visiting Mobile Nodes Operation

Access control of NEMO depends very much on the resources required for NEMO solution. To identify the resources required, we have to model the general sequence of operation. This model is applicable whether the node is a mobile host or a mobile router. We will use the term Visiting Mobile Node (VMN) to meant both host and router. The sequence of operation is as follows:

(1) VMN starts up and performs auto-configuration to use a link-local address.
(2) VMN obtains a global Care-of-Address (CoA) through router solicitation, or Dynamic Host Configuration Protocol (DHCP) [10].
(3) VMN discovers its Home Agent (HA) at its home domain.
(4) VMN sends the HA the appropriate binding updates.

2.2. Resources Needed for NEMO Operation

AAA is required in NEMO for two basic reasons:
(1) to control the access of and to account for the use of network resources in the foreign domain, and
(2) to control the access of and to account for the use of network resources in the home domain.

Network resources in the foreign domain that a VMN requires includes a CoA, and the access to the wireless network channel. AAA for the

use of foreign resources is generally performed in a "link-local" manner, utilizing access protocols such as IEEE 802.1x [11] to gain access to the wireless network channel, and protocols such as DHCP [10] to get a CoA. Since the link-layer and pool of IPv6 addresses generally belongs to the same administrative domain, AAA for the allocation of CoA is usually not required after granting access to the link-layer network.

Network resources in the home domain that a VMN requires are the use of HA, and the network bandwidth it consumes at the home domain for the support of NEMO. Since the lowest layer where the VMN can connect to the home network is at the IP layer, AAA operations for the use network resources in the home domain must be carried out in the IP layer.

2.3. Overview of AAA Operation

A plausible scenario for AAA operations is that two types of AAA protocols will be used: a "link-local" AAA protocol, and a "global" AAA protocol. The "link-local" AAA protocol is usually employed at

link-layer, and usually takes place over a single network hop. Examples include IEEE 802.1x [11], PANA [12], or other EAP-variant protocols [13]. The "global" AAA protocol is normally employed at the IP layer, and usually takes place over multiple network hops. Examples include Diameter [14], or RADIUS [15].

There are two main elements in AAA for NEMO. The first is the MR performing AAA negotiations with the access router, and the second is the MR handling AAA negotiations from a VMN. We will describe them separately in the following sub-sections.

2.3.1. AAA Operation between MR and Access Router

Generally, a MR will initiate an access request by sending relevant messages to the access router it attached to in the foreign domain using a "link-local" AAA protocol. The access router can then contact the AAA server in the same domain to check the credentials provided by the MR. The AAA server in the foreign domain may or may not have enough information to verify the credentials. If the AAA server in the foreign network does not have sufficient information, it can contact the AAA server in the home domain of the MR to complete the verification process. Since the two AAA servers are

located in different domains, a "global" AAA protocol will have to be used for the communications between them. This is depicted in Figure 1 below.

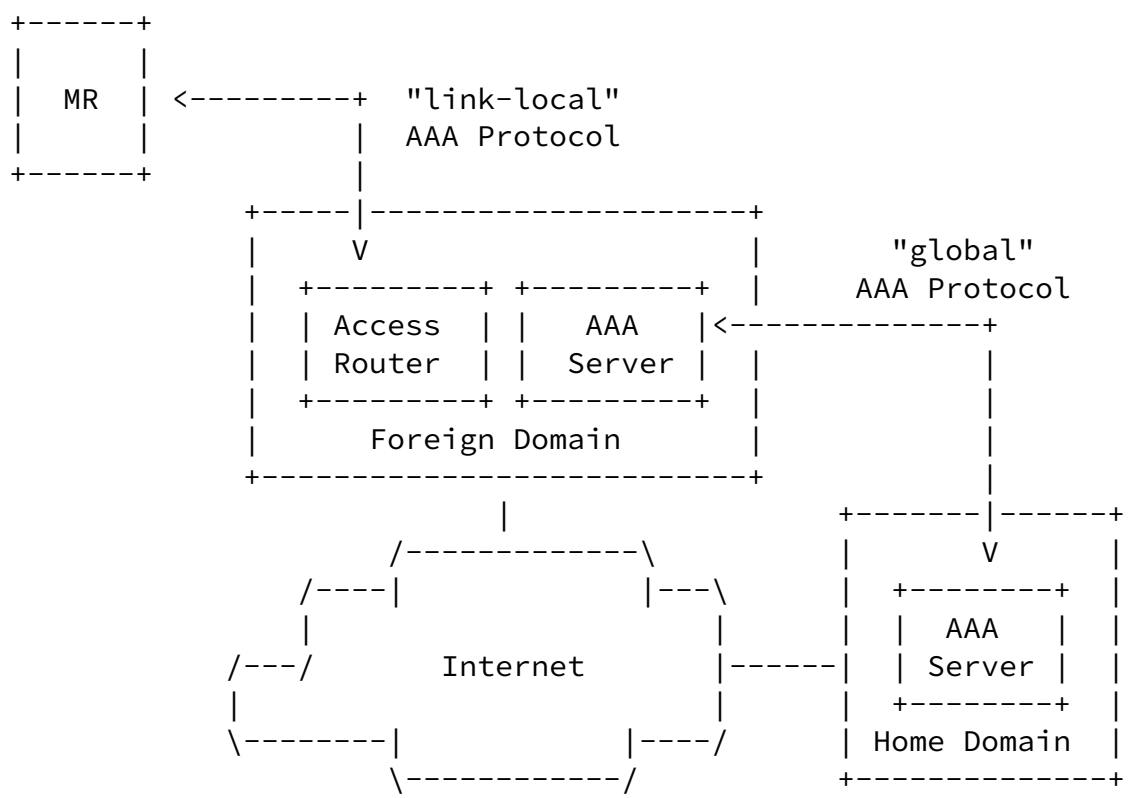

Figure 1: AAA Operation between MR and Access Router.

2.3.2. AAA Operation between VMN and MR

When a MR allows a VMN to attach to its local mobile network based on some access control policy, the MR is essentially behaving as a Network Access Server, or NAS. As such, we basically model the mobile router as NAS in this document, and draw heavily from work done in IETF NASREQ Working Group [16].

The VMN will first initiate an access request by sending relevant messages to the MR it attached to using a "link-local" AAA protocol. The MR will normally not have enough information to verify the credentials of the VMN. Thus it will have to contact an external AAA server to perform the actual authentication and authorization. This external AAA server can be located anywhere in the global Internet.

Hence, the communications carried out between the MR and the AAA server will employ one of the "global" AAA protocol. This is depicted in Figure 2 below.

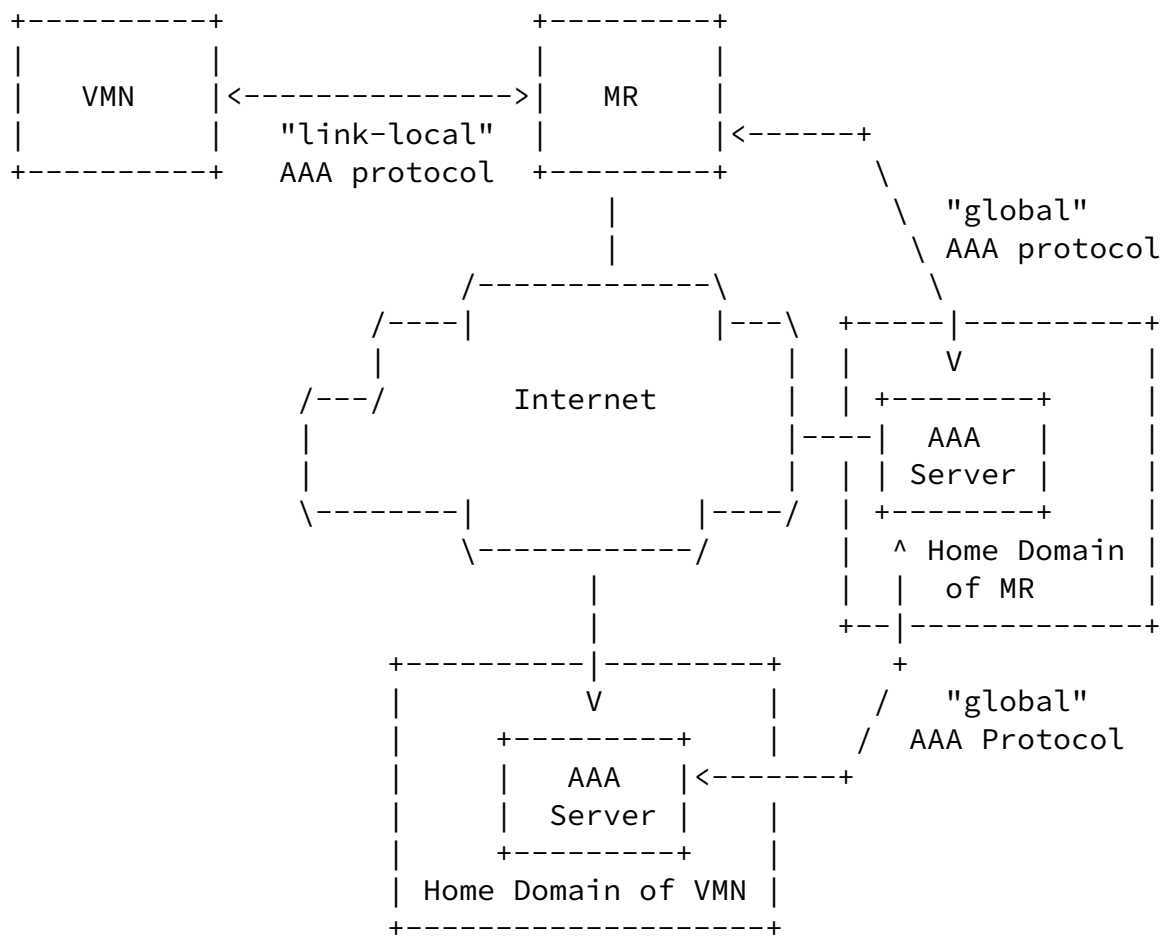

Figure 2: AAA Operation between VMN and MR.

2.4. Home Resources vs Foreign Resources

The previous discussion only illustrates the access request for foreign resources. To gain access to home resources, the MR/VMN will typically has to discover its HA in the home domain, and send binding updates to its HA. Access control on the use of home resources can then be carried out by the HA after the reception of the binding

updates. This can be done with the HA consulting an AAA server. Since the main operation of access control of home resources is not carried out by the nodes in the mobile network, we will focus on the access control of foreign resources in the remaining sections of this document.

3. Usage Scenario

In this section, we describe several usage scenarios of NEMO. In our descriptions, we will focus more on the AAA aspects of NEMO rather than the routing solution. A total of five scenarios are presented, classified according to the administrative domains of the access routers (ARs), top-level mobile routers (TLMRs), nested visiting mobile router (VMR), and mobile network nodes (MNNs), as shown in Table 1 below. AD-1 and AD-2 are used to differentiate distinct administration domains controlled by different Internet Service Providers (ISP) or companies, and USER refers to the domain of individual subscribers (or roaming subscribers) to AD-1.

Table 1: Administrative Domains (AD) in Different Scenarios

	AR	TLMR	VMR	MNN
Scenario 1	AD-1	AD-1	None	USER
Scenario 2	AD-2	AD-1	None	USER
Scenario 3	AD-1	USER	None	USER
Scenario 4	AD-1	AD-1	USER	USER
Scenario 5	AD-2	AD-1	USER	USER

In scenarios 1 and 2, the subscribers are individual VMH attached to MR in a foreign domain. The difference between scenarios 1 and 2 is that in the first scenario, the MR and the AR it attached to belong to the same administrative domain, while in scenario 2 they belong to distinct administrative domains.

In scenarios 3, 4, and 5, the subscribers are moving networks themselves. The difference between these scenarios is that in scenario 3, the subscribers attach directly to fixed AR, while in

scenarios 4 and 5 the subscribers attach to a MR. For scenario 4,

the MR and the AR it attached to belong to the same administrative domain, while in scenario 5 they belong to distinct administrative domains.

Each scenario is described in greater details in the following sub-sections. Examples of each scenario, and the AAA operations required are also presented.

3.1. Scenario 1

In this scenario, subscribers are using their mobile devices to connect to MRs that belongs to an Internet Service Provider (ISP). The MRs have their points of attachment to the Internet via an AR that belongs to the same ISP. Two distinct types of administrative domains are present: one for the AR and MRs, and one for each mobile network nodes (MNN). This is illustrated in Figure 3 below.

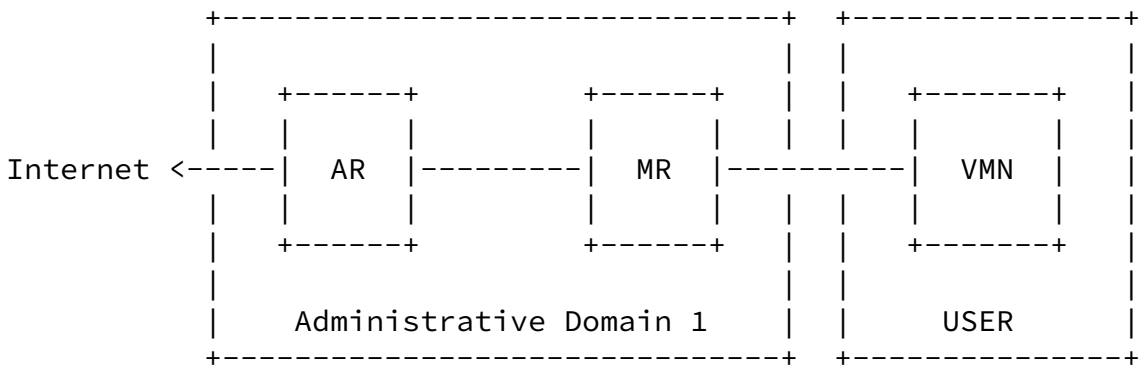

Figure 3: Scenario 1

3.1.1. Example

An example of such scenario will be the train network. A railway company may collaborate with an ISP to provide each cabin of the trains with a MR. Along the routes of the trains, the same ISP could erect fixed ARs for the MRs of the train to connect to the Internet. Passengers can then access the Internet via the MRs in the cabins. Thus, each cabin (or possibly the entire train) can be treated as a single mobile network.

In this case, the ISP/railway company owns both the ARs and the MRs. The access devices of the subscribers (i.e. the passengers) are then the MNNs.

3.1.2. AAA Operations

Since the MR for each mobile network belongs to the service provider of the AR, the access authentication of the MR by the access routers is straightforward. Each handover of the MR between the ARs may require access authentication. No special consideration for NEMO is necessary.

However, the MNNs (i.e. subscribers) will have to be authenticated by the MR. Two different possibilities arise: (1) the MNN is a subscriber with the service provider of the train network, and (2) the MNN is a roaming subscriber with another ISP.

For the first case where the MNN is a subscriber of the local ISP, the AAA process would typically be the following:

- The MNN makes a "link-local" access request to the MR.
- The MR consults the local AAA server to check the credentials of the subscriber.
- The MR replies the request.

For the second case where the MNN is a roaming subscriber, the AAA process would typically be the following:

- The MNN makes a "link-local" access request to the MR.
- The MR consults the local AAA server to check the credentials of the subscriber.
- The local AAA server consults the home AAA server of the MNN to check the credentials of the subscriber.
- Response is passed back from home AAA server, to local AAA server, to MR back to the subscriber.

3.2. Scenario 2

This scenario is an extension of the previous one where the MRs may not belong to the same administration domain as the ARs. In this case, 3 distinct types of administrative domains are present: an administrative domain for the ARs, an administrative domain for MRs, an administrative domain for each MNNs. This illustrated in Figure 4 below.

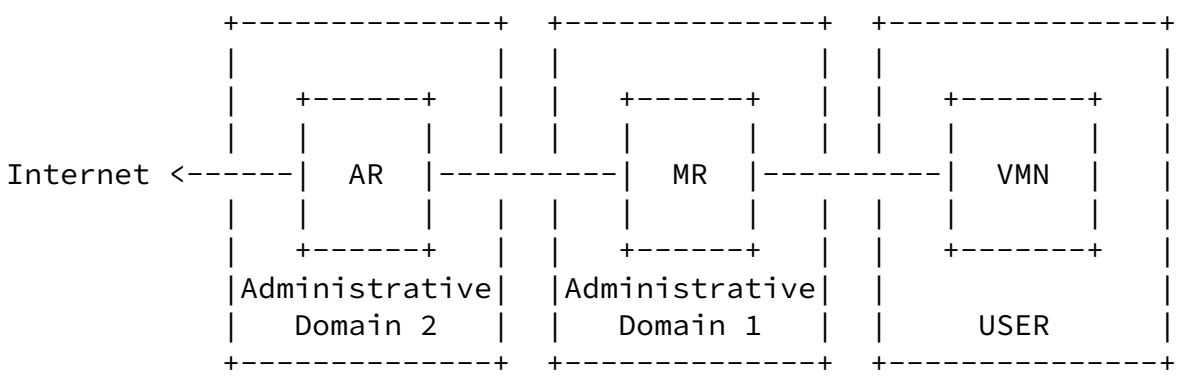

Figure 4: Scenario 2

3.2.1. Examples

An example of this scenario is again the train illustration. Here, the train may travel along a route where the available ARs belong to a different ISP. Other examples include ships and planes.

3.2.2. AAA Operations for MR

Since the AR and MR belong to different administrative domains, each handover of MR between different ARs may require AAA request/response negotiations. Such negotiations may employ standard mobile IP type operations. A typical AAA negotiation will be:

- The MR makes a "link-local" access request to AR.
- The AR consults the local AAA server to check credentials of MR.
- The local AAA server consults the home AAA server of the MR to check credentials of MR.
- Response is passed back to the local AAA server, AR and MR in that order.

3.2.3. AAA Operations for MNNs

For the MNN, there are again two possibilities: a subscribing MNN or a roaming MNN. For both cases of MNN, it needs only be authenticated by the MR once when the MNN first attaches to the MR.

For the first case where the MNN is a subscriber of the train network, the AAA process would typically be the following:

- The MNN makes a "link-local" access request to the MR.
- The MR consults the local AAA server to check the credentials of the subscriber.
- The MR replies the AAA request.

For the second case where the MNN is a roaming subscriber, the AAA process would typically be the following:

- The MNN makes a "link-local" access request to the MR.
- The MR consults the local AAA server to check the credentials of the subscriber.
- The local AAA server consults the home AAA server of the MNN to check the credentials of the subscriber.
- Response is passed back from home AAA server, to local AAA server, to MR back to the subscriber.

3.3. Scenario 3

This scenario is the case where the mobile network belongs to a single administrative domain, but its access to the Internet via an AR in a foreign domain. The mobile network does not allow VMNs to attach to its mobile router. (In this document, we shall refer to such mobile network as a private network). This is illustrated in Figure 5 below.

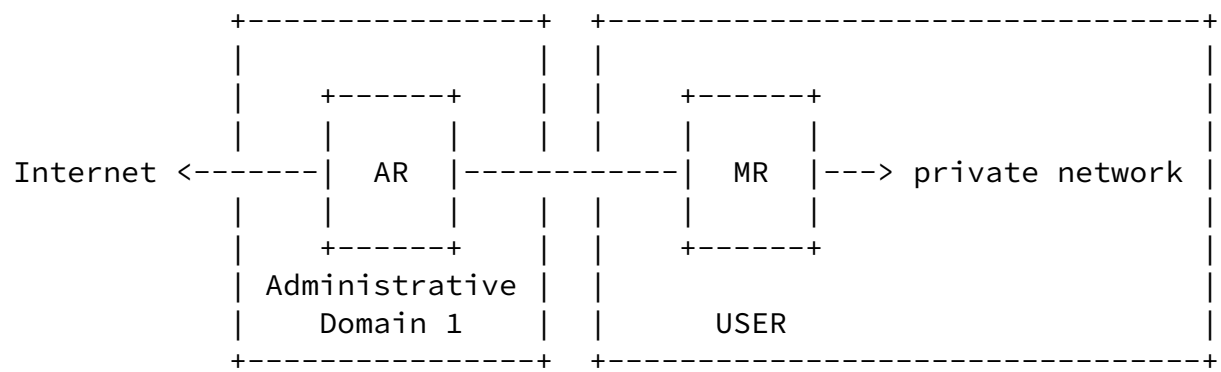

Figure 5: Scenario 3

3.3.1. Examples

One example of this scenario is the car network, where sensors, laptops, and navigation systems are fixed nodes on the mobile car network. The vehicle would have a MR to roam through the AR provided by the ISP along major streets.

Another common example is the Wireless Personal Area Network (W-PAN). The equipment used by a person formed a bluetooth-based mobile network, with the 802.11b-enabled laptop/PDA, or a GPRS-enabled handphone acting as the MR.

3.3.2. AAA Operations

For this scenario, there is no need for AAA between the MR and the MNNs. The MR simply assumes that any node on the sub-net is an authorized node of the network. (Here, we ignore the situation of a nearby third-party node trying to sneak in an unauthorized access.) The only requirements that are relevant are the AAA negotiations between the AR and MR, and this will be similar to the previous scenario (scenario 2).

A typical AAA negotiation will be:

- The MR makes a "link-local" access request to AR.
- The AR consults the local AAA server to check credentials of MR.
- The local AAA server consults the home AAA server of the MR to check credentials of MR.
- Response is passed back to the local AAA server, AR and MR in that order.

3.4. Scenario 4

This scenario is the nested extension of Scenario 1 plus Scenario 3. Here, a mobile network attaches itself to a higher level mobile

network (NEMO-1). The higher level MR (MR-1) and the AR belongs to a single administrative domain, and the lower level mobile network (NEMO-2) belongs to a single subscriber. This is illustrated in Figure 6 below.

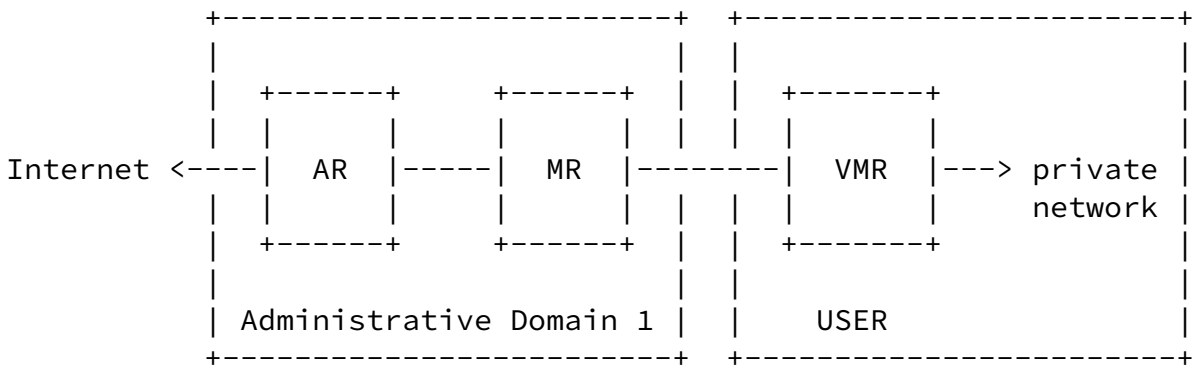

Figure 6: Scenario 4

3.4.1. Examples

One example of this scenario is again the train. Here the MR-1 are installed on the trains and the ARs belong to the same railway

company or ISP. The passenger, however, may bring in a W-PAN network onto the train. Thus the W-PAN forms the NEMO-2, which attaches itself to NEMO-1, the mobile network in the cabin of the train.

3.4.2. AAA Operations

In this scenario, there are two distinct administrative domains: one encompassing the ARs and MR-1, and the other encompassing NEMO-2. Since MR-1 for each NEMO-1 belongs to the service provider of the AR, the access authentication of the MR by the AR is straightforward (as in Scenario 1). Each handover of the MR between the AR may require access authentication. In addition, there is no need for AAA negotiations within NEMO-2, since this is usually a privately owned network (eg. WPAN). Thus the only case we have to consider is the AAA negotiations between MR-1 and MR-2.

A typical AAA negotiation will be:

- The MR-2 makes a "link-local" access request to MR-1.
- The MR-1 consults its home AAA server to check credentials of MR-2.
- The home AAA server of MR-1 consults the home AAA server of MR-2 to check credentials of MR-2.
- Response is passed back to the home AAA server of MR-1, MR-1 and MR-2 in that order.

3.5. Scenario 5

This scenario is the nested extension of Scenario 2 plus Scenario 3. Here, a mobile network attaches itself to a higher level mobile network (NEMO-1). The higher level mobile router (MR-1) and the AR belongs to different administrative domains, and the lower level mobile network (NEMO-2) belongs to a single subscriber. This is illustrated in Figure 7 below.

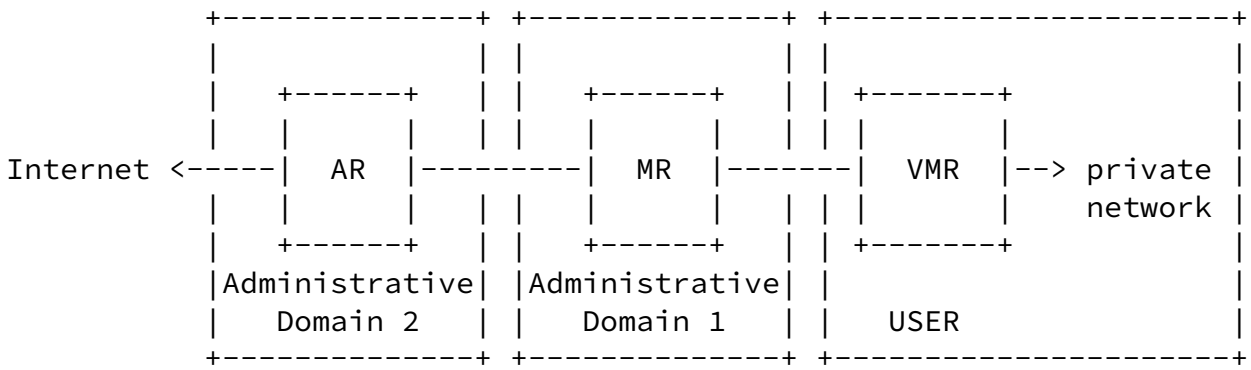

Figure 7: Scenario 5

3.5.1. Examples

One example of this scenario is again the train. Here the MRs on the trains and the access routers belong to different railway companies or ISP. The passenger bring in a wireless PAN network onto the train. Thus the W-PAN is the lower level mobile network (NEMO-2), the cabin of the train is the higher level mobile network (NEMO-1).

3.5.2. AAA Operations

In this scenario, there are 3 different types of administrative domains: one for the AR, one for NEMO-1, and one for each NEMO-2. Again, no AAA negotiation is necessary within NEMO-2 as it is solely owned by a single administrative agent.

AAA negotiations between AR and MR-1 is similar to those depicted in Scenario 3. A typical AAA negotiation will be:

- The MR-1 makes a "link-local" access request to AR.
- The AR consults the local AAA server to check credentials of MR-1.
- The local AAA server consults the home AAA server of MR-1 to check credentials of MR-1.
- Response is passed back to the local AAA server, AR and MR-1 in that order.

When MR-2 first enters the influence of NEMO-1, it will have to perform AAA negotiation with MR-1. This is similar to scenario 4. A typical AAA negotiation will be:

- The MR-2 makes a "link-local" access request to MR-1.
- The MR-1 consults its home AAA server to check credentials of MR-2.
- The home AAA server of MR-1 consults the home AAA server of MR-2 to check credentials of MR-2.
- Response is passed back to the home AAA server of MR-1, MR-1 and MR-2 in that order.

4. AAA Requirements

From the usage scenario, we can identify the set of requirements described below. It must be noted that the requirements specified are by no means exhaustive. Since a NEMO solution has yet to be specified, these requirements are merely spelt out to generate further discussion within the NEMO working group. When a NEMO solution is eventually specified, AAA requirements by NEMO can be rapidly generated by building on top of this document.

(1) The AAA servers MUST be able to share, or dynamically establish security associations with external authorities that are able to verify the credentials provided by the client.

This requirement is a direct induction from the need for AAA servers of ARs/MRs to consult home AAA servers of mobile network nodes for verifications of client's credentials. Since these AAA servers usually belong to different administrative domains, it is necessary for AAA operations to provide a mechanism for AAA servers in two different domains to establish a security relationship between each other.

(2) The VMN or MR MUST be able to provide complete, unforgeable credentials without having to contact its home agent.

Since VMN or the MR would initiate network connectivity from a foreign domain, it is necessary for it to be able to provide credentials without having first granted access to NEMO resources. Thus it has to be able to provide credentials sufficient for verifications without the ability to contact any other nodes in its home domain.

(3) Intermediate nodes MUST not be able to learn any information which may enable them to reconstruct and reuse the credentials.

This requirement protects the AAA servers from replay attacks. It is necessary for the ARs/MRs to be able to process the credentials provided by the MRs/VMNs and yet unable to reconstruct the credentials independently at a later time, so that malicious AR/MR cannot use the credentials to launch a replay attack against the home AAA server. It also serves to protect the MRs/VMNs from the visited NEMO.

In addition, to the above requirements, the following security requirements need to be considered.

(4) AAA request and response operations between the ARs/MRs and the respective AAA servers MUST prevent eavesdropping.

Any AAA operations MUST prevent the confidential information passed between the AR/MR and the corresponding AAA server from being known by eavesdroppers in the network. This is especially needed since NEMO typically operates in a wireless environment.

(5) AAA request and response operations between the ARs/MRs and the respective AAA servers MUST NOT be vulnerable to denial-of-service attack.

Since AAA operations typically entail cryptographic computations in the nodes involved, it is necessary to consider denial of service attacks by consuming CPU and memory resources to process illegitimate AAA requests, thereby preventing authentication of a legitimate mobile network node.

(6) AAA request and response operations between the ARs/MRs and the respective AAA servers MUST NOT be vulnerable to man-in-the-middle attack.

Since AAA operations may involve more than two nodes and operate over multiple hops, it MUST prevent communications between two legitimate nodes from being spoofed by an attacker in the middle.

The following are the set of requirements for NEMO in considerations to AAA operations.

(7) MR that supports attachment of VMN on its internal link SHOULD implement AAA client capability to be able to contact MR's home AAA server to check on credentials provided by the visiting nodes.

It is generally not expected for MR to implement a full AAA server for scalability reasons. However, MR should be configured to consult an AAA server (possibly an AAA server from the MR's home domain) for verifications of credentials from the VMN.

(8) MR that support attachment of VMN on its internal links SHOULD NOT change its AAA policy for the said VMNs during a continuous session, even when the MR has undergone a handover between AR of different administrative domains.

It is expected for handover of MR should be transparent to VMNs behind the MR. Thus, a change in administrative domain of the AR should not be propagated to nodes behind the MR.

5. Security Considerations

This document illustrates the usage scenarios of NEMO AAA operations, and specifies the NEMO AAA requirements. Because AAA is security driven, security considerations are spelt out in the requirements.

6. Acknowledgement

The authors wish to express their sincere gratitude to Thierry Ernst and Keisuke Uehara of the WIDE Project for their constructive comments to the initial draft of this document.

References

1 Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

2 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

3 Soliman, H., and Ernst, T., "NEMO (NEwork Mobility) Charter", http://www.nal.motlabs.com/nemo/nemo-charter.txt.

4 Soliman, H., and Pettersson, M., "Mobile Networks (MONET) Problem Statement and Scope", Internet Draft, draft-soliman-monet-statement-00.txt, Feb 2002, Work In Progress.

5 Ernst, T., and Lach, H., "Network Mobility Support Requirements", Internet Draft, draft-ernst-monet-requirements-00.txt, Feb 2002, Work In Progress.

6 Lach, H. et. al., "Mobile Networks Scenarios, Scope and Requirements", Internet Draft, draft-lach-monet-requirements-00.txt, Feb 2002, Work In Progress.

7 Kniventon, T. J., and Yegin, A. E., "Problem Scope and Requirements for Mobile Networks Working Group", Internet Draft, draft-kniventon-monet-requiremetns-00.txt, Feb 2002, Work In Progress.

8 Mitton, D., and Beadles, M., "Network Access Server Requirements Next Genreration (NASREQNG) NAS Model", IETF RFC 2881, July 2000.

9 Ernst, T., and Lach, H., "Network Mobility Support Terminology",

Internet Draft, draft-ernst-monet-terminology-01.txt, Jul 2002, Work In Progress.

10 Droms, R., et. al., "Dynamic Host Configuration Protocol for Ipv6 (DHCPv6)", Internet Draft, draft-ietf-dhc-dhcpv6-25.txt, Jun 2002, Work In Progress.

11 IEEE 802.1 Working Group, "Port-Based Network Access Control", IEEE 802.1x Standard, June 2001.

12 Patil, B. et. al., "Charter of Protocol for Carrying Authentication for Network Access", IETF PANA WG Charter, May 2002.

13 Blunk, L., and Vollbrecht, J., "PPP Extensible Authentication Protocol", IETF RFC 2284, March 1998.

14 Calhoun, P. R. et. al., "Diameter Base Protocol", Internet Draft, draft-ietf-aaa-diameter-12.txt, July 2002, Work In Progress.

15 Rigney, C. et. al., "Remote Authentication Dial In User Service (RADIUS)", IETF RFC 2865, June 2000.

16 IETF NASREQ WG, "Network Access Server Requirements Working Group Charter", http://www.ietf.org/html.charters/nasreq-charter.html.

Author's Addresses

Chan-Wah Ng
Panasonic Singapore Laboratories Pte Ltd
Blk 1022 Tai Seng Ave #04-3530
Tai Seng Industrial Estate
Singapore 534415
Phone: (+65) 6554 5420
Email: cwng@psl.com.sg

Takeshi Tanaka
Wireless Solution Laboratories
Matsushita Communication Industrial Co Ltd

5-3, Hikarinooka, Yokoshuka-shi, Kanagawa
239-0847, Japan
Phone: +81-468-40-5494
Email: Takeshi.Tanaka@yrp.mci.mei.co.jp