AAA Requirements from Mobile IP

Gopal Dommety, Cisco Systems

Steve Glass, Sun Microsystems

Stuart Jacobs, GTE Laboratories

Basavaraj Patil, Nortelnetworks

Charles E. Perkins, Nokia Research Center

Presentation available at:

http://www.iprg.nokia.org/~charliep/txt/ietf46/aaa.ps

AAA - Authentication, Authorization, and Accounting

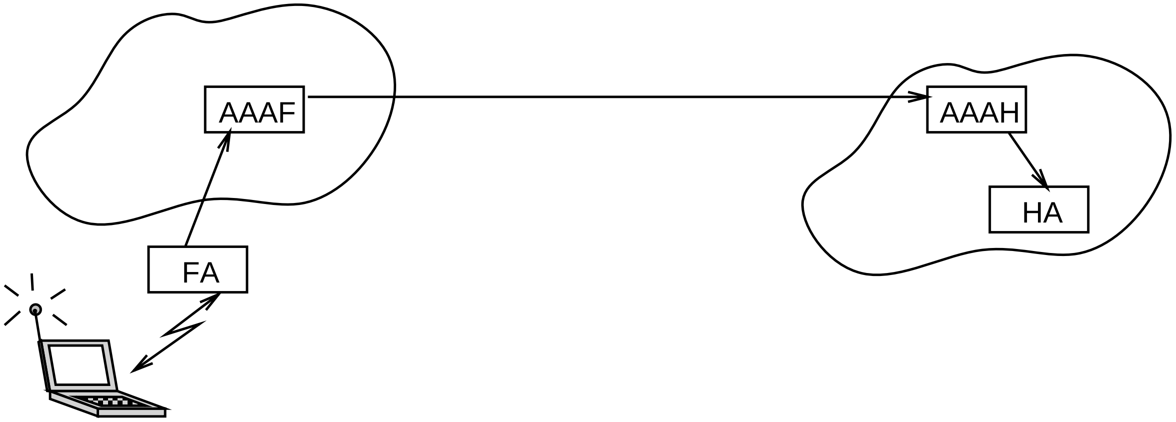
Mobile IP agents use AAA to handle authorization for connectivity

- Mobile Nodes authenticated by trusted agents in their home domain
- Connectivity authorized by administrative agents in the foreign domain, which serve *many* foreign agents
- Accounting initiated by foreign agents, which are trusted by the administrative agents in the foreign domain

draft-ietf-mobileip-aaa-reqs-01.txt breaks down requirements into three classes:

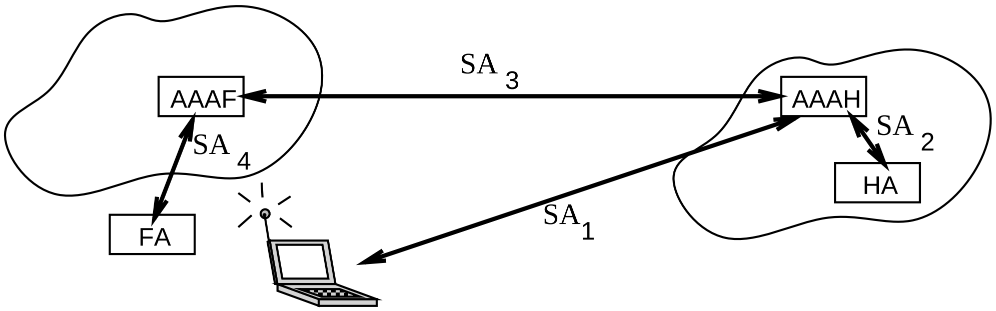
- Relevant requirements from the general model (shown later)
- Relevant requirements from IP addressing
- Relevant requirements from Mobile IP

Interactions between Mobile IP and AAA



- Mobile Node authenticated by AAA in its home domain
- Authentication invoked by simple Mobile IP extensions
- AAA protocol should not have to parse Mobile IP messages
- Mobile IP protocol should not have to parse AAA messages

Trust Relationships – Generic Model



- Home AAA trusts Mobile Node

- Visited AAA trusts Home AAA

- Visited Foreign Agent trusts Visited AAA

- Home Agent trusts Home AAA

MN NAI extension

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |  Network Access Identifier ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

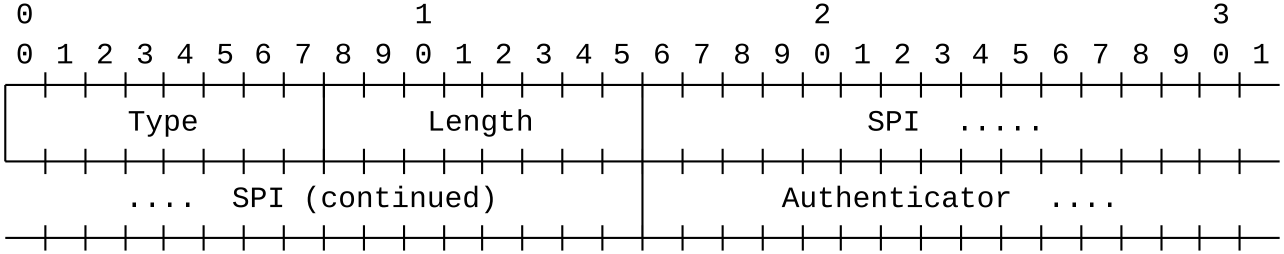
The NAI is standardized in RFC 2486.

Requirements:

- AAA *MUST* be able to use the NAI to identify a mobile node (instead of its IP address)

- AAA must be able to handle delivery of an IP address to the mobile node.

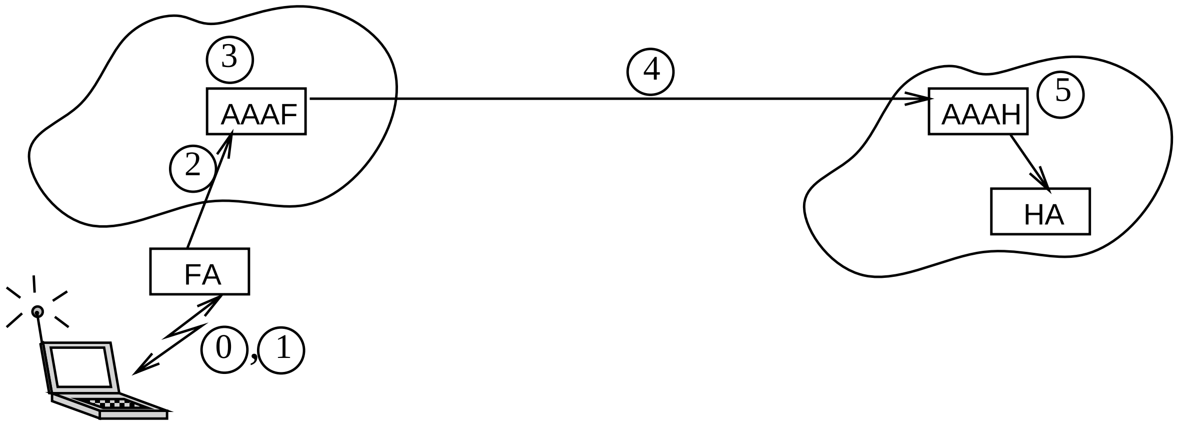
MN-AAA Authentication



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |          SPI  .....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   ....  SPI (continued)        |        Authenticator  ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The mobile node includes a *MN-AAA* authentication extension along with the challenge string from the FA challenge.

Protocol Overview



0. Foreign agent (FA) advertises challenge

1. Mobile node (MN) adds NAI, Challenge Response etc., to Mobile IP registration request

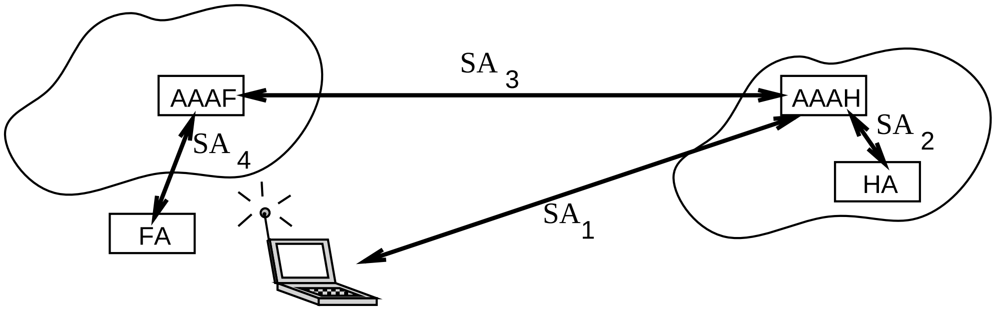
2. FA invokes AAA protocol with its local AAA server (AAAF)

3. AAAF ("proxy") parses NAI, finds MN's home server address (AAAH)

4. AAAF invokes AAA protocol and awaits approval by AAAH

5. AAAH checks MN credentials and *may* allocate a home address for the mobile node

Step 6: Key Generation



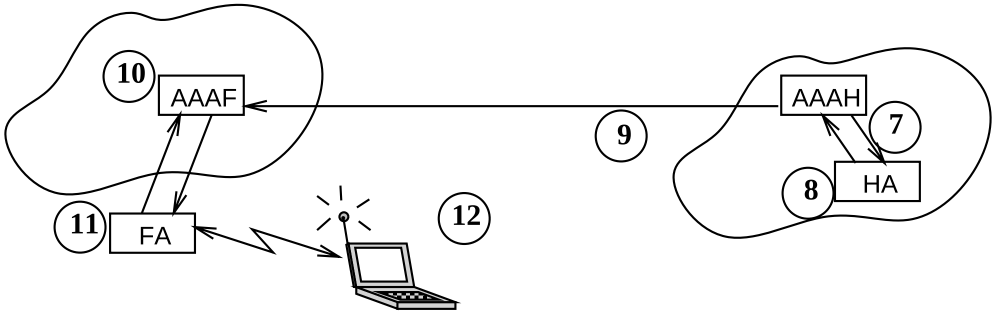
AAAH generates:

- K_1: MN ↔ FA
- K_2: MN ↔ HA
- K_3: FA ↔ HA

AAAH encrypts:

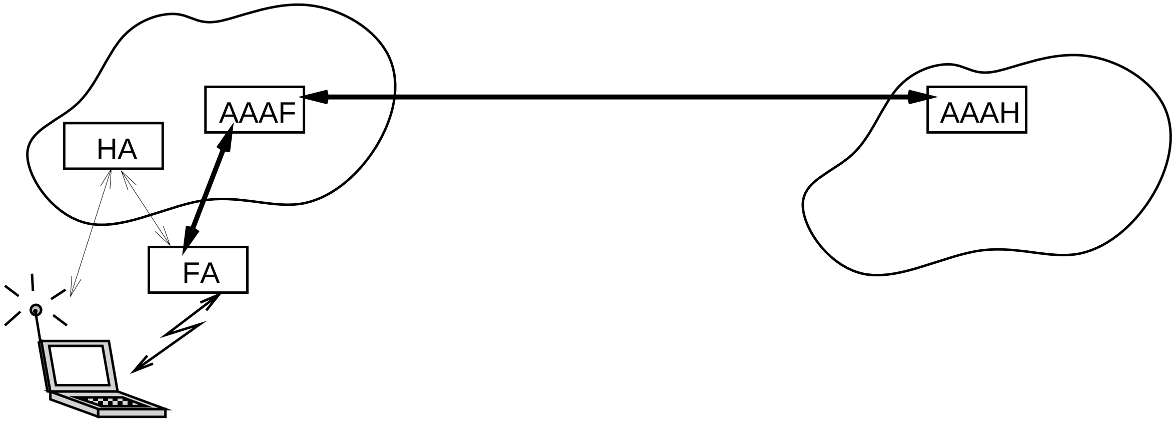
- K_1 & K_2 using SA_1 → MN
- K_1 & K_3 using SA_3 → FA
- K_2 & K_3 using SA_2 → HA

Protocol Overview, continued



7. AAAH relays Mobile IP information to HA with K_2, K_3
8. HA creates registration reply using K_2, and K_3 for FA.
9. HA sends results to AAAH, which proxies request to AAAF
10. AAAF decrypts K_1 & K_3 using SA_3, re-encrypts using SA_4
11. FA decrypts K_1 & K_3 using SA_4, checks registration reply and FA↔HA authentication, adds MN↔FA using K_1
12. MN decrypts K_1 & K_2 using SA_1, checks registration reply, and MN↔FA authentication

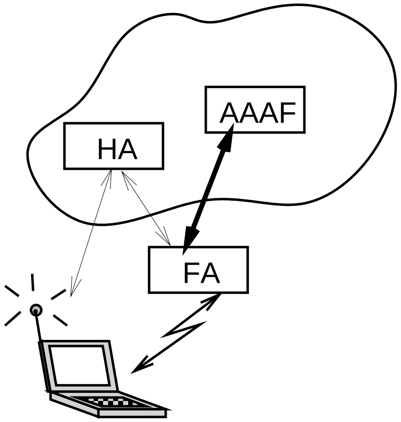
AAA Model with Local Home Agent



Advantage: local home agent does not require long-distance negotiations for Mobile IP re-registration

Disadvantage: Communications with correspondent nodes in home domain or any other domain becomes more difficult.

AAA Model with Local Everything



Advantage: Offers Mobile IP in the local area

Disadvantage: Communications with correspondent nodes in home domain or any other domain becomes more difficult.

Disadvantage: Mainly suited for local payments, since no authorization available based on mobile node's identity

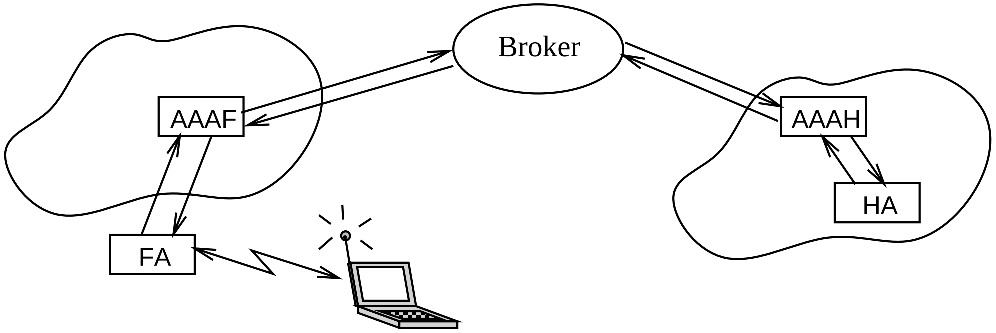
General Tasks for AAAF and AAAH

- enable authentication for Mobile IP registration
- authorize the mobile node (once its identity has been established) to use at least the set of resources for minimal Mobile IP functionality, plus potentially other services requested by the mobile node
- initiate accounting for service utilization
- use AAA protocol extensions specifically for including Mobile IP registration messages as part of the initial registration sequence to be handled by the AAA servers.

Key Distribution by AAAF

- identify or create a security association between MN and home agent (HA)
- identify or create a security association between mobile node and foreign agent, for use with subsequent registrations at the same foreign agent
- identify or create a security association between home agent and foreign agent
- participate in the distribution of the security association (and Security Parameter Index, or SPI) to the Mobile IP entities
- validate certificates provided by the mobile node
- accept an indication from the foreign agent about the acceptable lifetime for its security associations
- condition their acceptance of a Mobile IP registration authorization depending upon whether broadcast or multicast is needed

Using Brokers



- Brokers provides scalable economic infrastructure for inter-domain AAA (in particular, for Mobile IP)

- Bilateral relationships *may* override need for brokers in particular cases

Using a security broker should be enabled, if the AAAF and AAAH do not already share a security association SA_3

AAA Requirements – Broker Model

- Negotiating service by a trusted third party
- Negotiating service parameters
- Reliable accounting in the face of packet loss
- Passing encrypted data between AAA servers
- Secret information must not be divulged to any third parties
- Verification of message integrity is required for messages handled by third parties.

AAA Requirements – Pre-existing Contracts

- Trust relationship between foreign agent and foreign AAA
- Trust relationship between home agent and home AAA
- Foreign agent has to be able to keep state for pending registration/credentials-checking
- AAA must not restrict the scalability of Mobile IP registrations at any particular foreign agents.
- Confirmation when service begins
- Support for prepaid network cards and cyber cafes
- Either *bill-before-service* or *service-before-bill*

AAA Reqs – Mobile IP Authentication

- Arbitrate trust between the home agent and the mobile node
- Arbitrate trust between the home agent and the foreign agent
- Mobile node has to be able to verify the credentials of the foreign domain
- Foreign agent has to be able to verify mobile node credentials without requiring mobile node to first contact home domain
- Authentication information SHOULD be available from AAA agents in 1 second or less.
- Challenge authentications *may* be less time-critial
- Foreign and Home AAA servers must simultaneously handle huge numbers of Mobile IP registrations (from different FAs).
- AAA must maintain the mobile node's ability to register with multiple home agents.

AAA Requirements – Mobile IP Authorization

- Authorization for link access
- No constraint on Mobile IP protocol regarding resource categorization
- Authorization for default router service
- Authorization for various tunnel protocols (Minimal, GRE)
- Authorization for reverse tunneling/home agent decapsulation
- Authorization for clock synchronization
- Authorization for smooth handoff
- Authorization for firewall traversal

AAA Reqs – Mobile IP vs. Accounting

Mobile IP doesn't have anything to say about accounting.

However, accounting requirements within the scope of AAA include information to enable charging for the following resources and services:

- Connection time to some degree of accuracy (per minute, per second)
- Address allocation, distinguishable by routability
- Location-sensitive home agent allocation
- Registration processing requirements
- Number of packets
- Key generation
- Bandwidth requirement

Accounting modes could be either *incremental* or *running totals*.

TBD

IPv6?

Smooth handoff problems

Tunneling requirements (esp. for private addresses)

Encryption services requested at Mobile IP registration time

QoS requirements specified at Mobile IP registration time