AAA Requirements from Mobile IP

Gopal Dommety, Cisco Systems

Steve Glass, Nokia Telecommunications

Stuart Jacobs, GTE Laboratories

Tom Hiller, Lucent

Basavaraj Patil, Nortelnetworks

Charles E. Perkins, Sun Laboratories

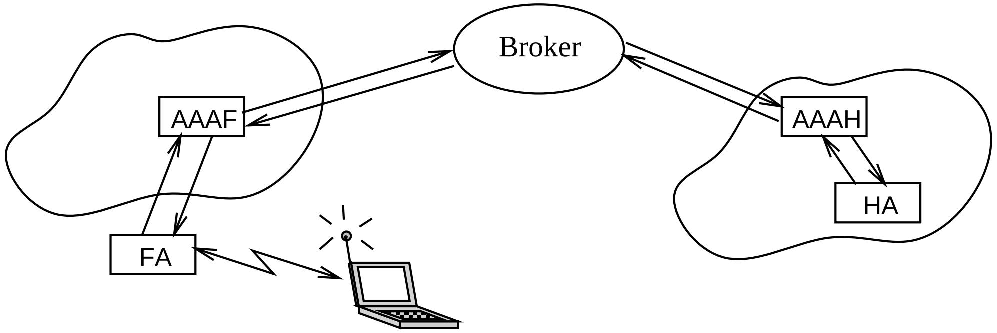
http://www.svrloc.org/~charliep/txt/ietf45/aaa.ps

AAA - Authentication, Authorization, and Accounting

AAA is used by Mobile IP agents to handle

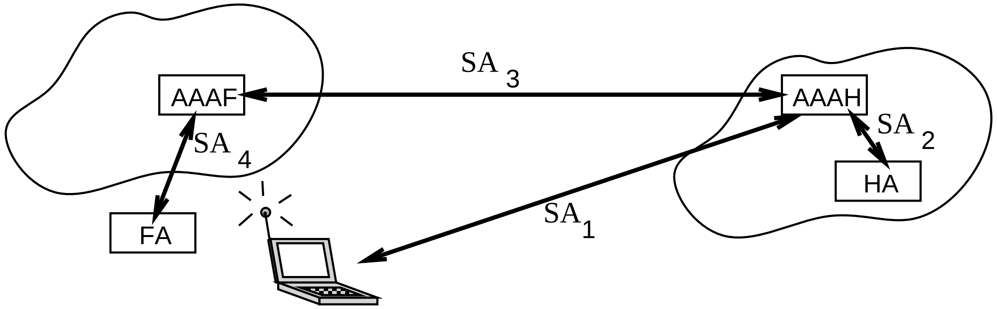
- Mobile Nodes authenticated by trusted agents in their home domain
- Connectivity authorized by administrative agents in the foreign domain
- Accounting initiated by foreign agents, which are trusted by the administrative agents in the foreign domain

Interactions between Mobile IP and AAA



- Mobile Nodes authenticated by AAA in their home domain
- Connectivity authorized by AAA in the foreign domain
- Acct'g initiated by foreign agents
- AAA w/brokers provides economic infrastructure for inter-domain mobility
- Bilateral relationships *may* preempt need for brokers
- Authentication invoked by simple Mobile IP extensions

Trust Relationships



- Home AAA trusts Mobile Node

- Visited AAA trusts Home AAA

- Visited Foreign Agent trusts Visited AAA

- Home Agent trusts Home AAA

MN NAI extension

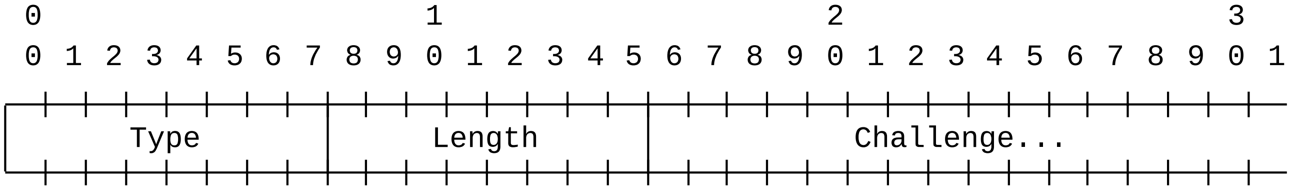
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     | Network Access Identifier ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+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

The mobile node is able to identify itself using its NAI (Network Access Identifier) instead of its IP address.

The NAI is standardized in RFC 2486.

This extension is going through working group Last Call.

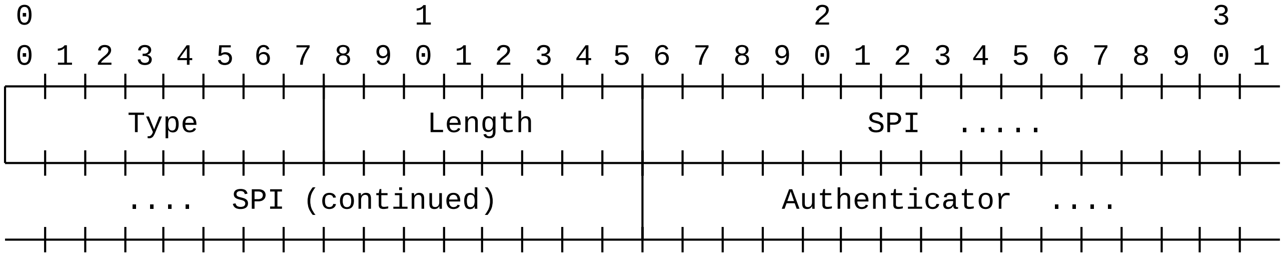
FA Challenge Extension



```
 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     |         Challenge...
```

The Foreign Agent includes the FA Challenge extension in its Agent Advertisements. The mobile node includes the same challenge string in an extension to the Registration Reply

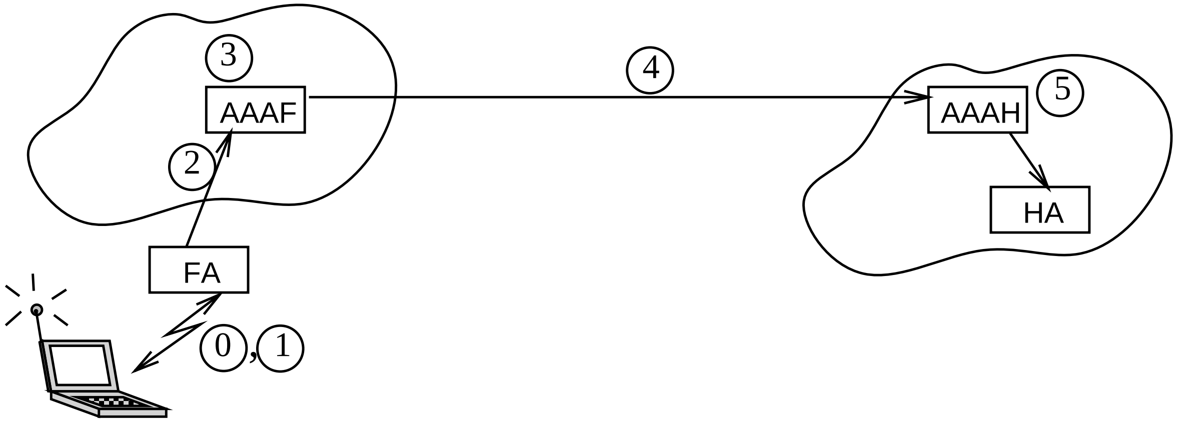
MN-AAA Authentication



```
 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  ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

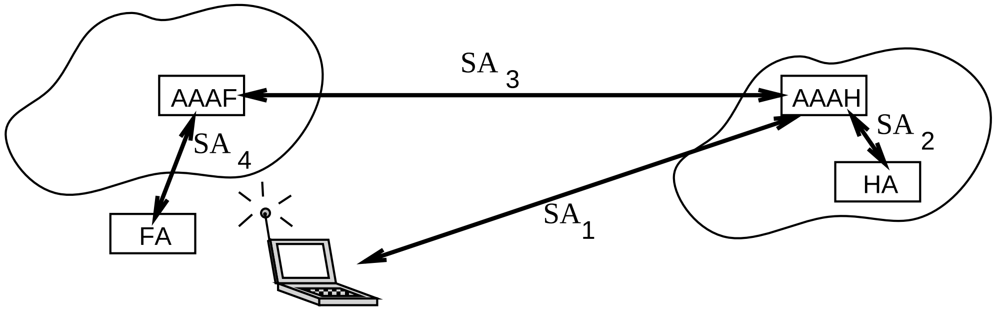
The mobile node includes a *MN-AAA* authentication extension along with the challenge string from the FA challenge.

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



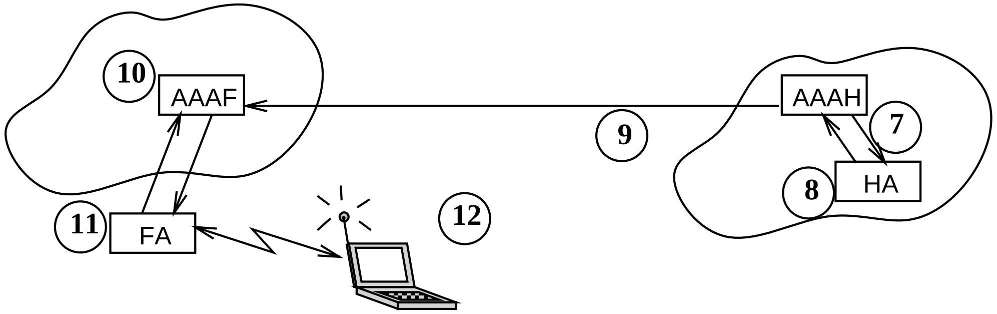
AAAH generates:

- 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

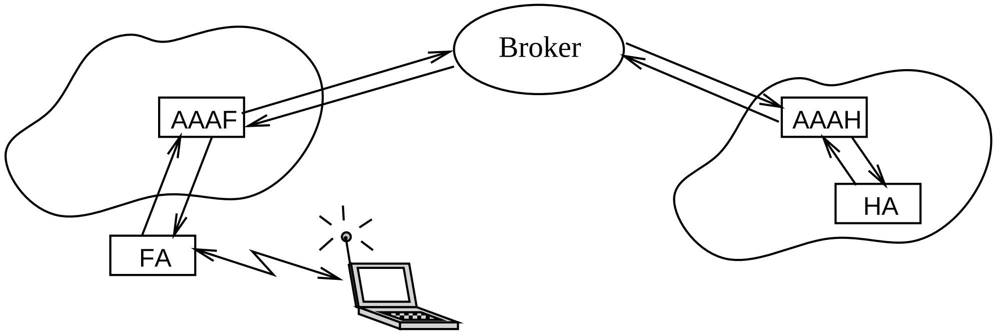
11. FA decrypts K_1 & K_3 using SA_4, checks registration reply and FA↔HA authentication, adds MN↔FA using K_1

12. MN decrypts K_1 & K_2 using SA_1, checks registration reply, and MN↔FA authentication

AAA 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*

Using Brokers



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
- Secret information must not be divulged to any third parties
- Verification of message integrity is required for messages handled by third parties.

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

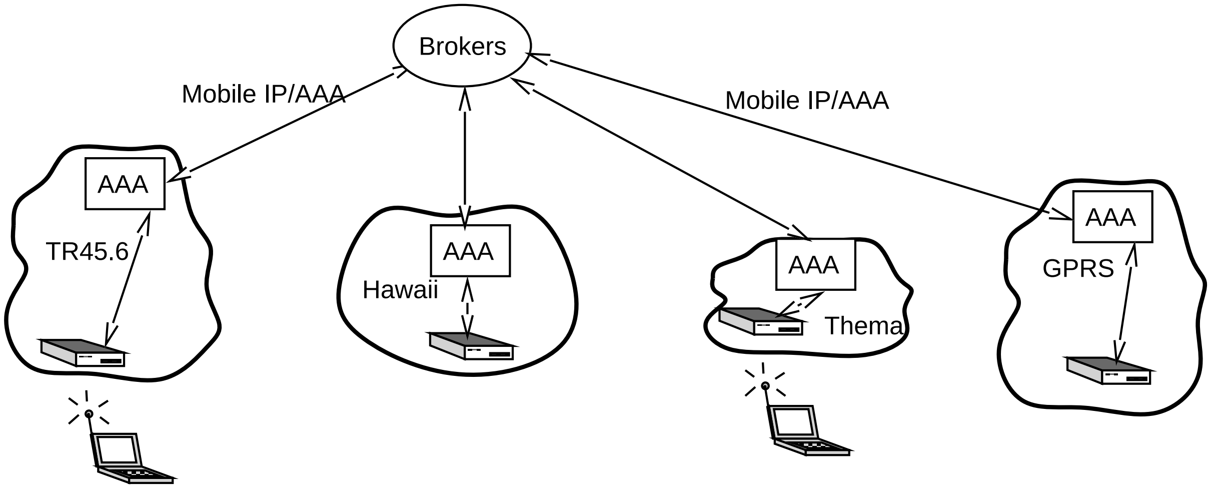
Mobile IP doesn't have anything to say about accounting.

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*.

Overall Vision



Mobile IP can provide the best technology for new deployments of wireless technology.

Mobile IP, with AAA, can also provide the backbone connectivity for wireless providers, no matter what local or legacy protocols are used.

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