AAA Extensions for Mobile IP

Charles E. Perkins

Advanced Network Development

Sun Microsystems

Menlo Park, CA 94025

cperkins@eng.sun.com

http://www.svrloc.org/~charliep

Pat Calhoun

Advanced Network Development

Sun Microsystems

Menlo Park, CA 94025

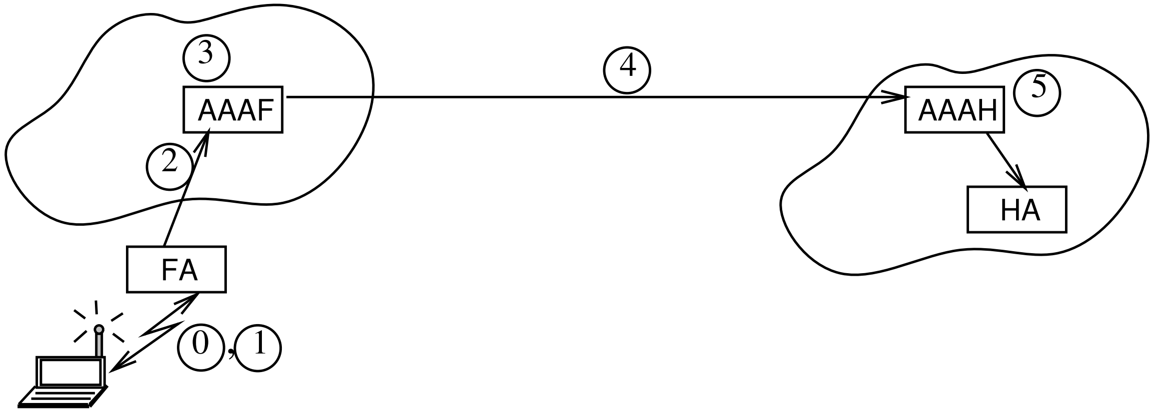
pcalhoun@eng.sun.com

AAA - Authentication, Authorization, and Accounting

DIAMETER (a follow-on to RADIUS) is used by Mobile IP agents to handle

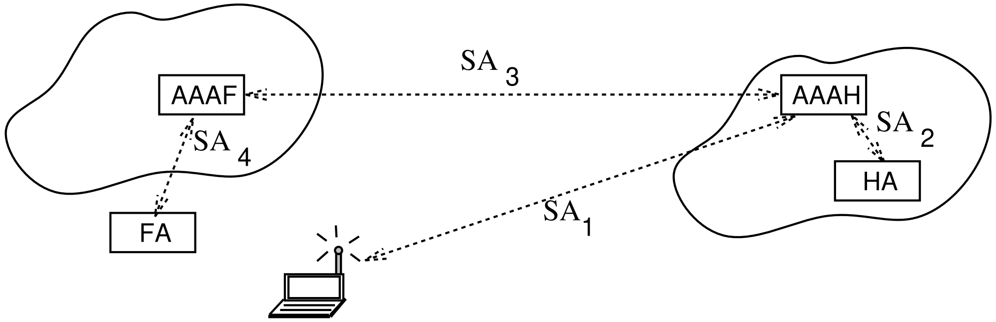
- Mobile Nodes authenticated by trusted agents in their home domain
- Connectivity authorized by administrative agents in the foreign domain
- Accounting initiated by foreign agents, which are trusted by the administrative agents in the foreign domain

Protocol Overview



0. Foreign agent (FA) advertises challenge
1. Mobile node (MN) adds NAI, Challenge Response etc., to Mobile IP registration request
2. FA sends DIAMETER AVPs with registration request to Foreign AAA (AAAF)
3. AAAF ("proxy") looks up NAI, finds MN's home server address (AAAH)
4. AAAF sends DIAMETER request, awaits approval by AAAH
5. AAAH authenticates request; it *may* allocate a HA and IP address for MN

Step 6: Key Generation



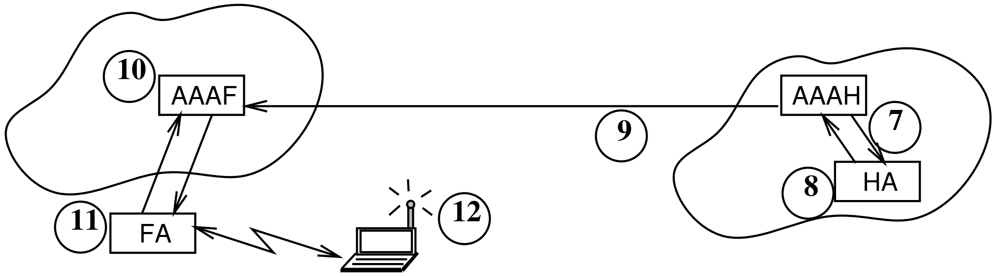
AAAH generates:

- K_1: MN $\leftrightarrow$ FA
- K_2: MN $\leftrightarrow$ HA
- K_3: FA $\leftrightarrow$ HA

AAAH encrypts:

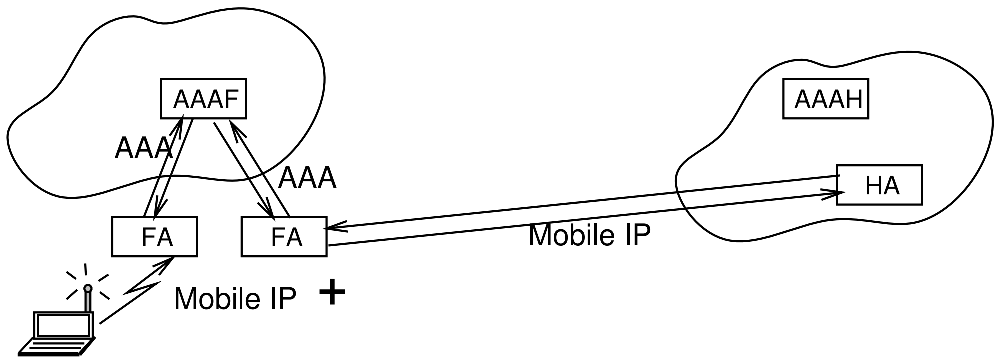
- K_1 & K_2 using $SA_1 \rightarrow$ MN
- K_1 & K_3 using $SA_3 \rightarrow$ FA
- K_2 & K_3 using $SA_2 \rightarrow$ HA

Protocol Overview, continued



7. AAAH issues DIAMETER request 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

Local Handoff



FA advertises NAI as well as challenge

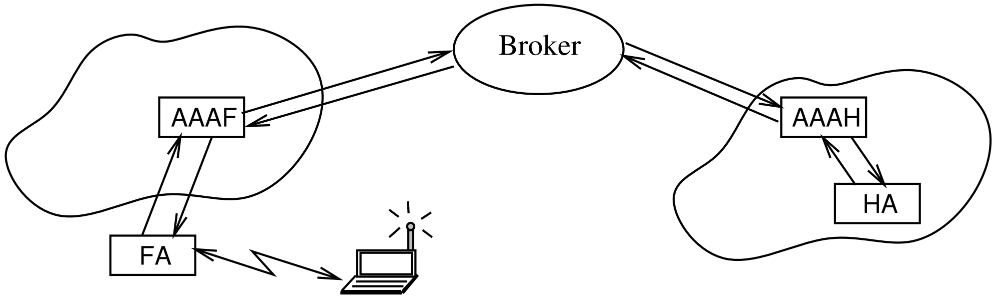
Mobile Node checks whether new NAI is in same domain as old NAI

Mobile Node supplies previous FA as well as unforgeable response

FA sends request to AAAF

AAAF *may* re-encrypt previous registration key and send it to new FA, without contacting AAAH

Using Brokers



It is possible to use a broker, if the AAAF and AAAH do not already share a security association SA_3

Regionalized Registration

A GFA lives at the top of a FA hierarchy

If GFA has no valid key for MN, it contacts AAAF

The FAs do not expose their structure to the MN

Self-Configuring Agent Hierarchy

A GFA sends a distinguished, externally addressable COA in a *regionalized router advertisement*

Other FAs are then enabled to send theirs

Question: What is the correct TTL for advertisements

Answer: a *regionalized router solicitation*

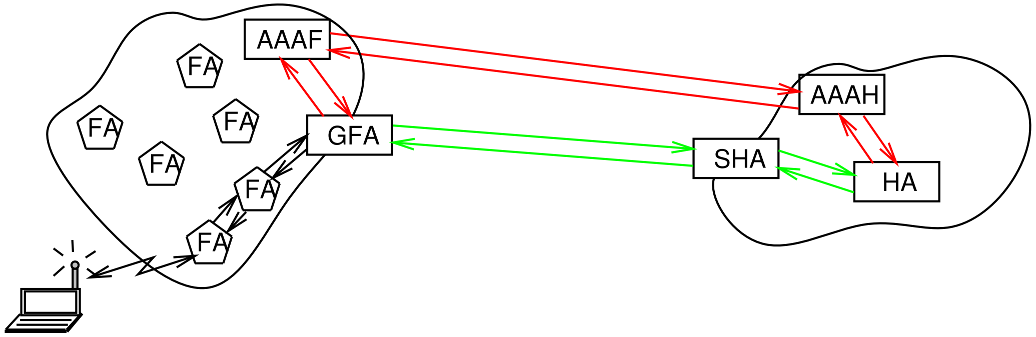
Flexible HA allocation

HA inhabits the path from correspondent node to MN

If HA can live nearby the MN, the detour is minimized.

Must be enabled by MN, and approved by AAAF

Private Addresses



Private Addresses should be hidden

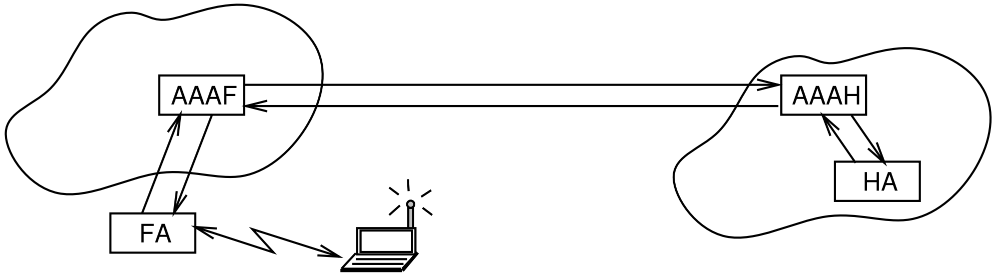
If HA has private address, a Surrogate HA is needed

If HA has private address, MN does too

If one FA has private address, all FAs in hierarchy do too

$\rightarrow$ (COA == 0) in advertisement!

AAAF↔AAAH Accounting



- After successful registration reply, FA sends Accounting Start Record to AAAF
- AAAF proxies Start Record to AAAH.
- Foreign Agent MAY send interim Accounting Records (perhaps every 5 minutes) containing cumulative information.
- Foreign Agent sends Accounting Stop Record upon receipt of notification from new FA.

Features

Regionalized Registration

Private Addresses handled

Generates session keys for Mobile Node and Mobility Agents

Eliminates unnecessary Internet traversals

Challenge/Response integrated with Registration Request

Automatic IP address allocation for mobile nodes

Automatic HA allocation in either home or foreign domain

Centralizes AAA functions in administrated services

Broker certification (e.g., IPASS, GRIC)

Clear separation between Mobile IP function and AAA function