DHC WG   G. Tsirtsis
                                             Flarion Technologies
Internet Draft   J. Privat
                                                      Northstream

Title: draft-ietf-dhc-aaa-ra-00.txt
Expires : June 2001   January 2001

Triggering AAA from DHCP Relay Agents
draft-ietf-dhc-aaa-ra-00.txt

Status of this Memo

Abstract

    Recently there has been interest in using DHCP for configuring
    clients accessing the Internet through some form of high-speed access
    technology such as cable or ADSL [DHC-AGENT]. In addition, although
    DHCP was initially designed for configuring fixed hosts, proposals
    are being made to enhance DHCP to support roaming/mobile clients
    [DHC-ENHANCE]. These two trends have put in evidence the need for a
    coupling between AAA and DHCP. Some initial requirements for DHCP/AAA
    have been proposed in [DHC-AAA].

    This document proposes a different model in which AAA procedures are
    invoked not from a DHCP server but from a DHCP relay agent to make
    sure that ALL the Internet Access features supported by the PPP model
    can be replicated in a DHCP based Internet Access environment.

[1](#). Introduction

   Traditionally DHCP has mainly been used in intranets such as
   corporate or campus networks. Recently there has been interest in
   using DHCP for configuring clients accessing the Internet through
   some form of high-speed access technology such as cable or ADSL [DHC-
   AGENT].

   In addition, although DHCP was initially designed for configuring
   fixed hosts, proposals are being made to enhance DHCP to support
   roaming/mobile clients [DHC-ENHANCE]. These two trends have put in
   evidence the need for a coupling between AAA and DHCP. Some initial
   requirements for DHCP/AAA have been proposed in [DHC-AAA].

   This document proposes a different model in which AAA procedures are
   invoked not from a DHCP server but from a DHCP relay agent. The
   reason is that if DHCP is to replace PPP in some environments, there
   will be a strong requirement to make sure that ALL the Internet
   Access features supported by the PPP model can be replicated in DHCP-
   based Internet Access scenarios.

   However, there are fundamental differences between PPP-based and
   DHCP-based Internet access.
   On the one hand, PPP terminates on the Access Router (or Network
   Access Server-NAS) which becomes the Policy Enforcement Point between
   the network and the client. Typically the NAS is at the same time a
   PPP terminator, AAA client and possibly DHCP relay agent. This is a
   very powerful model since the NAS is the most sensible point at which
   to apply services such as Accounting, Resource Allocation,
   Authentication and many others.
   On the other hand, DHCP runs from the client to the DHCP server which
   is inside the Access Network and possibly several routers away from
   the Access Router. In the absence of PPP, the Access Router, as it
   stands at the moment, does not have a way to trigger the AAA
   functions that PPP based networks have. Although, DHCP relay agents
   will typically be operating in the Access Routers, these are
   considered to be very simple, and most importantly transparent,
   devices.

   We propose in this document that DHCP relay agents be used as AAA
   triggers intercepting and conveying relevant information from clients
   to AAA servers. This allows the PPP Internet Access model to be
   replicated in a non-PPP environment.

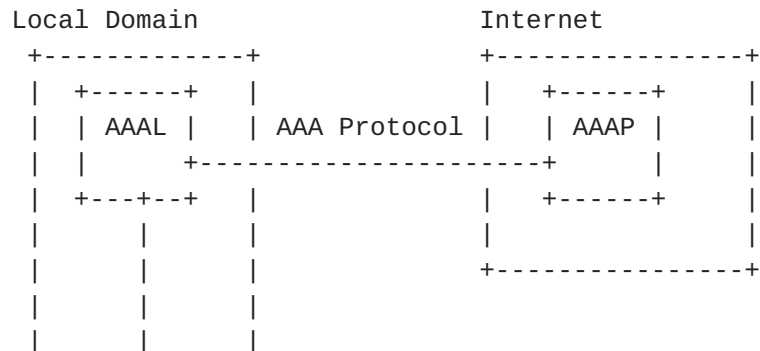## 2. Currently proposed model: AAA from DHCP server
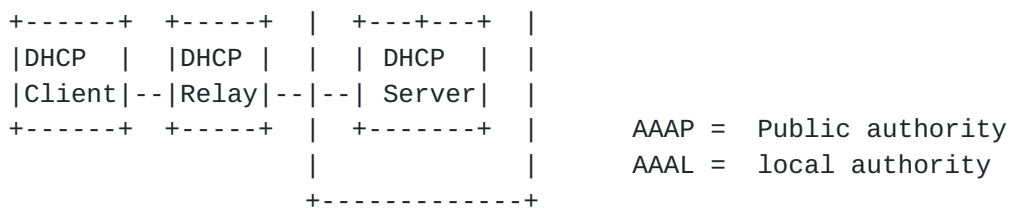
2.1 Description

   The currently proposed model for DHCP based roaming and mobile IP as
   described in [DHC-AAA] and [MOBILEIP-AAA] is shown in Figure 1. In
   this model the AAA procedure is invoked from the DHCP server.

```
                     Local Domain                   Internet
                  +-------------+             +----------------+
                  |  +------+   |             |  +------+      |
                  |  | AAAL |   | AAA Protocol|  | AAAP |      |
                  |  |      +---------------------+      |      |
                  |  +---+--+   |             |  +------+      |
                  |      |      |             |                |
                  |      |      |             +----------------+
                  |      |      |
                  |      |      |
       +--------+ |  +---+---+  |
       | DHCP   | DHCP | DHCP |  |
       | Client |-------|--| Server|  |
       +--------+ |  +-------+  |      AAAP =  Public authority
                  |      |      |      AAAL =  local authority
                  +-------------+
```
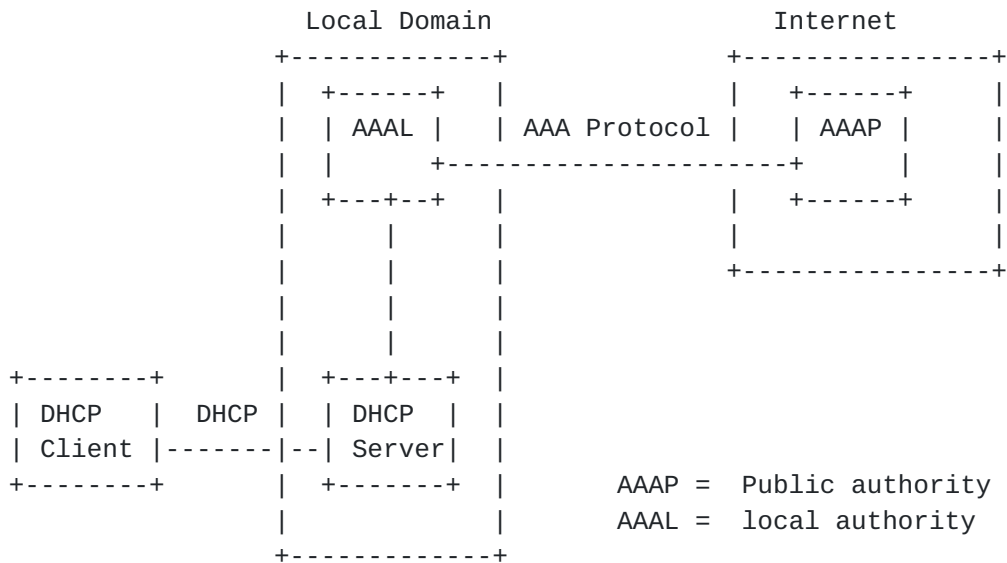
             Figure 1: DHCP/AAA Current Model

   Even with the use of a DHCP Relay Agent the above picture does not
   change fundamentally but only becomes Figure 2.

```
                     Local Domain                   Internet
                  +-------------+             +----------------+
                  |  +------+   |             |  +------+      |
                  |  | AAAL |   | AAA Protocol|  | AAAP |      |
                  |  |      +---------------------+      |      |
                  |  +---+--+   |             |  +------+      |
                  |      |      |             |                |
                  |      |      |             +----------------+
                  |      |      |
                  |      |      |
```

```
      +------+  +-----+  |  +---+---+  |
      |DHCP  |  |DHCP |  |  | DHCP  |  |
      |Client|--|Relay|--|--| Server|  |
      +------+  +-----+  |  +-------+  |        AAAP =  Public authority
                         |             |        AAAL =  local authority
                         +-------------+
              Figure 2: DHCP/AAA Servers Model with Relay Agent
```

2.2 Limitations

The above model is fine for traditional use of DHCP in corporate and
other such networks were a level of trust already exists between the
clients and the network. DHCP is, however, increasingly being used in
other environments such as residential access over Cable modems or
possibly xDSL and mobile networks.
These new types of applications for DHCP have different requirements
and characteristics in terms of security and trust. Before DHCP was
considered in the above types of networks, PPP had been applied
successfully providing similar functionality. PPP has a fundamental
difference to DHCP in the way it treats new clients. All checks
happen from the Access Point, i.e: the first point of attachment for
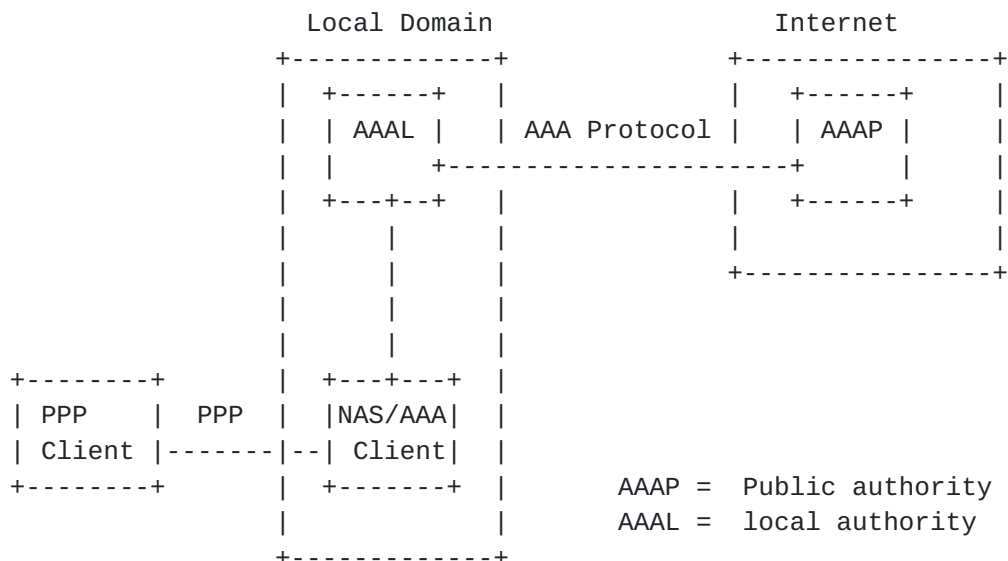the client, for example the NAS. Figure 3 shows this PPP model.

```
                            Local Domain                 Internet
                       +-------------+          +----------------+
                       |  +------+   |          |  +------+      |
                       |  | AAAL |   | AAA Protocol |  | AAAP |      |
                       |  |      +---------------------+      |      |
                       |  +---+--+   |          |  +------+      |
                       |      |      |          |                |
                       |      |      |          +----------------+
                       |      |      |
                       |      |      |
       +--------+      |  +---+---+  |
       | PPP    |  PPP |  |NAS/AAA|  |
       | Client |------|--| Client|  |
       +--------+      |  +-------+  |        AAAP =  Public authority
                       |             |        AAAL =  local authority
                       +-------------+
```

Figure 3: PPP Model

3 New model: AAA from DHCP Relay Agent

3.1 Description

   If DHCP is to replace PPP in some environments, a similar model is
   needed so the client details are checked on the first node of
   attachment (CMTS, DSLAM, etc...). This would produce the layout of
   Figure 4. This is consistent with the approach followed in [DHC-
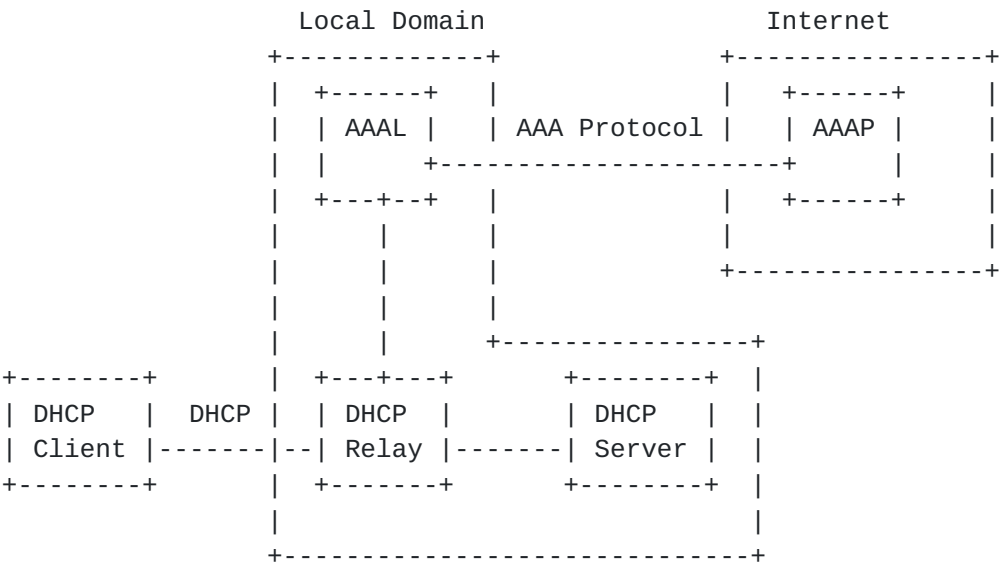   AGENT] in that the access point is the first trusted point in the
   provider network.

                         Local Domain   Internet
                    +-------------+   +----------------+
                    | +------+ | | +------+ |
                    | | AAAL | | AAA Protocol | | AAAP | |
                    | | +----------------------+ | |
                    | +---+--+ | | +------+ |
                    | | | | |
                    | | | +----------------+
                    | | |
                    | | +---------------+
        +--------+ | +---+---+   +--------+ |
        | DHCP | DHCP | | DHCP | | DHCP | |
        | Client |-------|--| Relay |-------| Server | |
        +--------+ | +-------+   +--------+ |
                    | |
                    +-----------------------------+

              Figure 4: DHCP Relay Agent Model

3.2 Advantages

   The major benefit from this new model is the ability to enforce
   policy. In Figure 2, the DHCP server can only Authenticate the client
   details but not much else. In the PPP model, because the AAA check
   takes place at the NAS, it is possible to get detailed, customized
   configuration for the client and dynamically configure an access list

on the NAS's interface to restrict/allow certain functions and
resources.
It could be argued that this customization is also possible in the
currently proposed model (AAA from DHCP server). Once a user identity
has been established using AAA, looking up access control lists and
storing usage information could be done using LDAP or other existing
means to communicate with databases/directories. However there is
value for a provider in reusing as much as possible the same existing
AAA mechanisms as currently deployed.

[4](#). **Impact on DHCP**

[4.1](#) **Authenticating a user**

   Discussion:
   In order to authenticate a user, a AAA server needs to be passed some
   information of the form username/password. How does the AAA client
   get this information? Does it get it through DHCP (either through
   existing options or through a new one) or does it get it through a
   separate challenge sent by the access point?
   Note that once an access point gets the username/password
   information, it can use it for the Agent Remote ID sub-option
   proposed in [DHC-AGENT].

[4.2](#) **Relay Agent behavior**

   Discussion:
   Clearly, the relay agent behavior needs to be specified when
   triggering AAA from DHCP messages.
   The relay agent needs to know:
   Which DHCP message triggers a AAA check.
   Which DHCP message triggers the download of policies (such as an
   access list) on the access point? Note that in order to install
   access lists, some information is required such as the IP address
   given to the client.
   What action to take if no response is received from the AAA server
   (timer, notification sent back to client).

   The Relay agent must be able to terminate service to a client if not
   authorized by a AAA server.

[5](#) **Security considerations**

   Authentication is presently being added to the DHCP protocol [DHC-
   AUTH]. This allows DHCP clients and servers to authenticate each

other. Our purpose differs in that we want to authenticate and
authorize a user before he accesses a provider network, to apply
policy to customize this access connection and to account for the
service. However it may be possible to re-use some elements of this
authentication framework when coupling AAA to DHCP.

[6](#). Acknowledgements

The authors would like to thank Alan O'Neill, who initiated this
work.

[7](#). References

[DHC-AAA] [draft-ietf-dhc-aaa-requirements-00.txt](#)
[MOBILEIP-AAA] [RFC 2977](#), Mobile IP Authentication, Authorization and
Accounting Requirements
[DHC-AGENT] [draft-ietf-dhc-agent-options-12.txt](#)
[DHC-ENHANCE] [draft-ietf-dhc-enhance-requirements-00.txt](#)
[DHC-AUTH] [draft-ietf-dhc-authentication-15.txt](#)

[8](#). Authors

George Tsirtsis
Flarion Technologies
Phone: +44 20 88260073
Email: G.Tsirtsis@Flarion.com

Jerome Privat
Northstream
Phone: +33 4 97 23 40 45
Email: jerome.privat@northstream.se