draft-ietf-dhc-dhcproam-00.txt
Internet Draft

B. Mukherjee
B. Gage
Y. Liu
Nortel Networks

February 2001

Extensions to DHCP for Roaming Users
<draft-ietf-dhc-dhcproam-00.txt>

Status of this Memo

1. Abstract

This draft defines enhancements to DHCP so that it can be used by access networks as an initial configuration protocol for nomadic users. The authentication mechanism described here interacts with existing public Authentication, Authorization, and Accounting (AAA) mechanisms, thus enabling per customer authentication and authorization across multiple domains. In addition, we describe a mechanism that enables the client to authenticate the network to prevent attacks on an end host from a bogus network access point.

2. 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].

3. Introduction

Providing authenticated IP access to subscribers across administrative domains is expected to be a vital functionality of next generation access networks. Such access networks are expected to perform authentication, authorization, accounting (AAA) [3] in addition to IP parameter configuration for its subscribers. The mechanisms described here address the requirements for accessing these networks in a flexible and extensible manner using the existing AAA infrastructure to perform the actual authentication. Similar motivations were expressed in proposing requirements for extending DHCP to new environments [4]. We expect that the proposed mechanisms will allow DHCP to be used as a secure yet easy to administer initial configuration protocol in commercial access networks as opposed to its present usage as means of configuring a pool of trusted hosts in a LAN.

3.2. Overview

This document defines mechanisms for authentication in access networks by means of DHCP. In order to be authorized for using the access network, the user must submit credentials via DHCP authentication messages. In response, the access network may indicate that a user has been authorized by providing configuration parameters to the user's mobile host. The user may also verify the access network's credentials as a part of the process. The authentication messages also provide a framework for negotiating other parameters, some of which may aid in enhancing the security of the system.

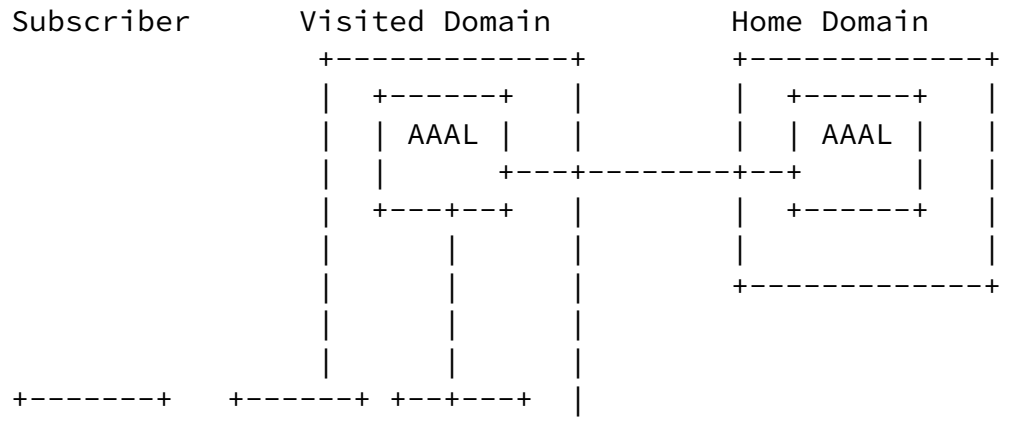
Any proposed security mechanism should allow flexible authentication between the network and its subscribers with scope for negotiation about the mechanisms to be used and the type of ciphers (e.g., ssl handshakes [5]). This is because the networks and their users may support only a few of the possible wide range of security mechanisms available. This may be due to internal constraints of the hosts (e.g., CPU cycles may be a bottleneck in case of a mobile user) or the security level the hosts desire (e.g., the network may only allow users that perform per message authentication). Furthermore no assumptions can be made about the local security requirements of visited domains. Thus a flexible mechanism that allows the security parameters to be negotiated and established is desirable. The

security mechanisms defined here can be used to create trust relationships between the network and the client that may be used then for accountable usage of the network resources.

4. Network Model

Throughout this document we use the example of an access network in order to demonstrate how the authentication additions in DHCP may be of use in new environments. The model of the network used by this draft is depicted in the Figure 1 below. This is similar to the model described in the draft on AAA requirements for DHCP [3]. The

model assumes that the users may roam and thus their initial interaction with the accessed network is overseen by a public AAA mechanism. The public AAA infrastructure consists of local AAA authorities in each of the access networks. These local AAA servers communicate among each other through a hierarchy of public AAA servers, and security associations exist between the local AAA server and the DHCP servers. The public AAA servers have inter domain security associations through the public AAA servers that allow them to authenticate users from visited domains. Thus upon presenting the right information a user can authenticate himself to a visited network, obtain the right levels of authorization and at the same time be accountable for the use of the network. This model allows the network access provider to leverage the existing AAA mechanisms to perform user authentication and accounting in a scalable manner across domains instead of using localized mechanisms.



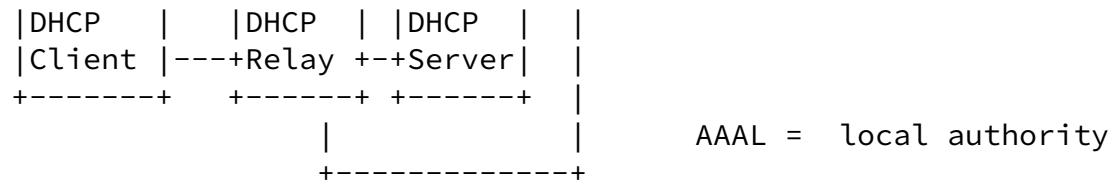


Figure 1: DHCP's interaction with AAA

5. Related Work

The DHCP working group of IETF has in the past expressed the need for DHCP to support AAA functions [3] and be extensible to different environments than ethernet LANs [4]. These are the principal motivations behind our work.

5.1 Requirements for using DHCP in new environments

The draft [3] had proposed that DHCP use the public AAA server infrastructure to perform AAA for roaming nodes and had set out the requirements for the same. Leveraging the AAA infrastructure provides a network service provider with a scalable way of ensuring access security because it does not require every DHCP server to have a pre-established security association with every DHCP client it may ever talk to. Using the public AAA infrastructure, the DHCP servers will be able to provide access to nodes from visited domains and bill them through their local service providers. Most major ISPs presently use AAA servers which support RADIUS or TACACS+ for customer accounting [6]. In this draft we describe mechanisms that allow DHCP to extensibly interface with this AAA infrastructure thus meeting the requirements set out by the requirements draft [3].

5.2 Mobile IP and PPP

There are other commonly used protocols like PPP and mobile IP, which are used for related functions. We contend that none of the above protocols are as suited for initial registration and configuration as DHCP. For instance, PPP's registration model assumes a point-to-point connection and is requires explicit link configuration before entering into IP authentication and configuration. This leads to considerable delay and overhead in providing access to the mobile host. Moreover when the host roams the physical layer parameters may change and may cause PPP to

restart configuration to reinitialize its link layer. Mobile IP based registration depends on the availability of the 'home-agent' and is tied in to that particular mobility solution. New generations of wireless networks may use and deploy several other types of mobility solutions. Thus there exists the need for a general-purpose protocol for registration and configuration that is not tied in to other functions or environments. DHCP is a natural choice because it exclusively deals with registration and configuration of nodes, independent of other functions being handled in a particular scenario. The draft [4] argues in favor of using DHCP as a general-purpose registration and configuration mechanism. In our proposal we address several of the requirements listed in this draft[4].

5.2. DHCP message authentication option.

The DHC WG has produced a draft that describes an authentication method for DHCP messages [7]. This involves a replay detection method as well as a keyed hash that allows the receiver of the message to authenticate the source. The mechanism relies on a shared secret between the two negotiating authorities. For the case of servers providing service to local clients, the above mechanism may be sufficient. But in the more general case of the clients roaming across domains it is not possible to create all the possible key associations before hand. Possible solutions to this problem were discussed in the DHC WG meeting on June 1998. It may be possible to use the public key infrastructure to authenticate the client and the server and then use Diffie-Hellman to generate a shared secret that

---

can then be used to authenticate messages. But a potential problem is that an uninitialized client may not be able to contact a trusted PKI node, resulting in an asymmetrical security relationship against the client. For instance, the server's certificate may have been revoked by the PKI authority and the client has no means of finding that out. In this document, the authentication mechanism leverages the AAA infrastructure to not only authenticate the client and the server in a symmetric fashion, but also to allow the network to initiate the AAA functions at the same time. In addition, the extra set of messages and the state allow the use of additional security mechanisms, like re-keying, that cannot be completed by piggybacking on the present set of DHCP messages. Another proposal was to create a IPSEC security association between the client and the server. Setting up a valid security association with an uninitialized client may not be possible without a valid IP address and a configured stack.

5.3. Dynamic Registration and Configuration Protocol

Another protocol, called Dynamic Registration and Configuration Protocol (DRCP)[8], was proposed in order to address the need for new features in a registration and configuration framework like DHCP. However DRCP requires every client to be a router. The DRCP protocol allows the servers to send advertisement messages that allow the clients to send discover messages to the servers using unicast. The protocol however does not specify any mechanisms for performing AAA functions or security mechanisms.

6. DHCP with Extensible Authentication

Adding authentication to DHCP allows the client and the server to establish mutual trust before configuration is effected. From the perspective of an access network, authentication mechanisms in DHCP allow easy configuration of subscriber devices as well as protection against certain theft of service attacks. A simple approach to prevent unauthorized access is that the configuration of the mobile host be completed only after the user is authenticated. The underlying assumption being that the configuration step is the one that allows a client to act as a fully functional host and access the network and its resources, and if this step fails to complete the mobile will be incapable of using the network. The threat scenario that this addresses is when a user attempts to access the IP services of the network without presenting valid credentials (e.g., user-id or password).

However the authentication mechanism used by the access networks must be scalable as each of the access networks are expected to be extensive. Thus pre-establishing security association between every client and the DHCP servers[9] in the access network may not be a viable option. In addition, the home and visited systems are expected to interact with each other in order to provide access to roaming users of other access networks. This would mean that for

visiting users the access network would need a mechanism to create a security association between the users home domain and itself.

From the perspective of the subscriber, DHCP should allow access across different service provider domains. From the perspective of the service provider there is a need for an authentication mechanism in order to provide service to subscribers roaming from other networks.

This document describes an optional extension to the DHCP protocol to include an authentication phase and to add authentication messages to DHCP. To support this option, the DHCP client must be modified to include a new state and to send new messages and options for authentication. The DHCP relay agent may remain the same, and does not need to be altered for the authentication phase. The DHCP server must also be modified to process the DHCP authentication messages and to forward the required messages to the AAA components.

6.1. Authentication Messages and Options

This option adds two new authentication messages to the set of existing DHCP messages:

DHCPAUTHREQ Request for authentication information (e.g. request for challenge response).
DHCPAUTHRESP Response to a DHCPAUTHREQ

The value of message type for new messages is left as TBD until assigned by IANA.

The messages are generic in nature and thus allow the DHCP server and client to establish the required credentials using any authentication protocol they predetermine or negotiate. The authentication phase may be completely skipped to remain backward compatible but the DHCP server may enforce a policy that makes authentication mandatory for certain (groups of) mobiles. The new messages function as means of transporting authentication information to and from the network's AAA mechanisms. In doing so we are able to leverage the existing AAA infrastructure to perform inter-domain authentication and authorization.

This document defines new message types for authentication, as opposed to piggybacking security information upon existing messages, in order to make the process flexible and extensible. For example, there are instances like the challenge-response protocols where the present sequences of DHCP messages are unable to fulfill the functionality. In addition challenges for re-keying in mid-session cannot be fitted in the existing messages without causing the client to restart the configuration procedure. The separate messages also allow the authentication protocol to be symmetrical, allowing the server to authenticate the client and the client, if necessary, to authenticate the server. The need to be extensible was also

propounded in other initial access protocols like PPP, which itself

has an extensible authentication protocol [10].

Several new options are defined to carry authentication information within the DHCPAUTHREQ and DHCPAUTHRESP messages as well as in other DHCP messages like DHCPREQUEST and DHCPACK. The client uses the DHCPREQUEST message to present its Network Access Identifier (NAI)[11] and to request the use of an (or possibly a set of) authentication mechanism by setting the appropriate option fields. The server can then query its local AAA mechanism about the security parameters supported for the given NAI. The DHCP server then can use the authentication request message (DHCPATHREQ) to ask the client to present it with authentication information that will be relayed on to the AAA mechanism. The option fields are thus used to indicate the choice when negotiating and then to carry actual data during the security exchange. The authentication mechanisms may be a challenge response handshake protocol (CHAP) [12], digital signature, plain password etc. The current set of option types that may be used are listed below:

Option #	Option Type
TBD	NAI
TBD	PAP
TBD	CHAP
TBD	Signature

Table 1: Authentication Options

6.2 The DHCP Server

The DHCP server model is relatively simple as compared to [7], as it need not manage and process keys or any client specific authentication information by itself. The DHCP server receives the user identification (e.g. NAI) from the client in a DHCPREQUEST; if the client is supporting a password protocol (e.g. PAP), the DHCPREQUEST may also include the password. The DHCP server then contacts the local AAA server (e.g. using RADIUS) with the DHCP client information and asks the AAA server if it can configure the client. For a network that uses a challenge response protocol for authentication, the server issues the challenge with a DHCPAUTHREQ message, receives the challenge response from the client through a DHCPAUTHRESP message and forwards the response to the AAA server for client authentication.

If the client chooses to authenticate the network, the DHCP server also needs to respond to DHCPAUTHREQ messages with a DHCPAUTHRESP message for the client. If a challenge-response protocol is used by the client for network authentication, the DHCP server must ask the AAA server to create a response for the challenge. Extensions to existing AAA protocols to support this function are beyond the scope of this document.

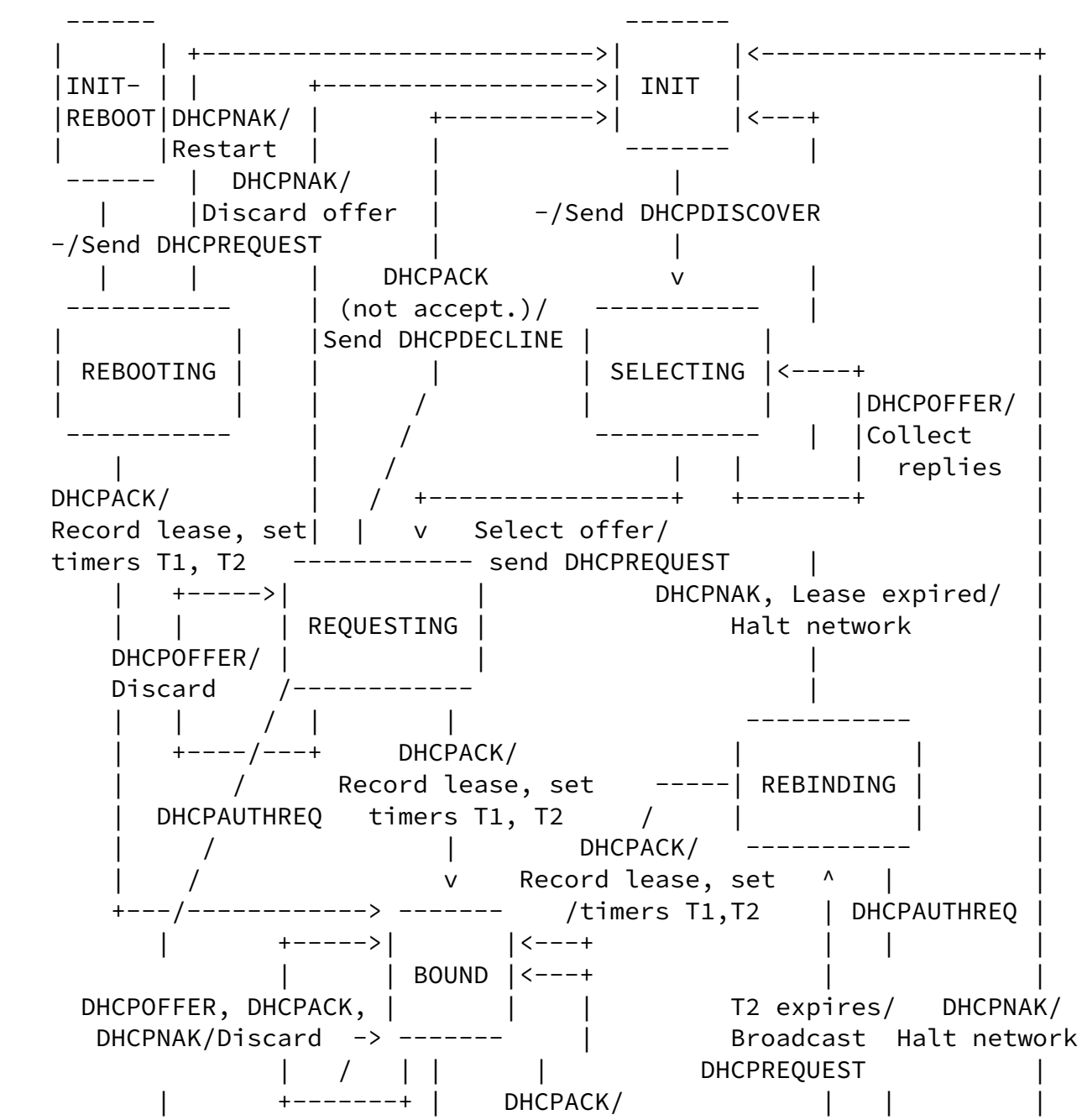
6.3. The DHCP Client

The DHCP client needs to be modified to incorporate the optional authentication mechanisms. First, it requires a new state in the client's state machine called AUTHENTICATING. This state is entered upon the receipt of a DHCPAUTHREQ message or when the client sends out a DHCPAUTHREQ message. The client MUST respond to a DHCPAUTHREQ message received when it is in the states REBOOTING, REQUESTING, RENEWING, REBINDING and AUTHENTICATING. The client MAY send DHCPAUTHREQ when it is in the BOUND or AUTHENTICATING state.

The client MUST respond to the DHCPAUTHREQ message with the message DHCPAUTHRESP. Both of these messages carry authentication options as described above. If the server had issued the challenge, the client MUST depart from the AUTHENTICATING state upon the receipt of a DHCPACK or a DHCPNACK message. The client MUST return to the bound state if the server responds with a DHCPACK but if the message received is DHCPNAK it MUST go back to the INIT state.

If the client had sent the DHCPAUTHREQ, the client MUST leave the AUTHENTICATING state and enter the BOUND state when a valid DHCPAUTHRES is received. If a valid DHCPAUTHRESP is not received, the client MUST enter the REBIND state and obtain new configuration parameters. The lease timers MUST be set as per the security requirements such that the server and the client cannot delay the response to the AUTHREQ messages indefinitely. Upon the expiry of the T1 and T2 timers the authenticating client MUST enter the REBINDING and RENEWING state respectively. The remaining state transitions are the same as described in RFC 2131[13].

The DHCP client also needs to be augmented with an authentication module that can manage keys, respond to challenges or encrypt messages. The specific functions of the authentication module is implementation dependent. The following is the state diagram for the client with the new state AUTHENTICATING as well as the new messages DHCPAUTHREQ and DHCPAUTHRES.


INIT-REBOOT
DHCPNAK/Restart
DHCPNAK/Discard offer
-/Send DHCPREQUEST
DHCPACK (not accept.)/Send DHCPDECLINE
INIT
-/Send DHCPDISCOVER
REBOOTING
SELECTING
DHCPOFFER/Collect replies
DHCPACK/Record lease, set timers T1, T2
Select offer/send DHCPREQUEST
DHCPNAK, Lease expired/Halt network
REQUESTING
DHCPOFFER/Discard
DHCPACK/Record lease, set timers T1, T2
DHCPAUTHREQ
REBINDING
DHCPACK/Record lease, set timers T1,T2
DHCPAUTHREQ
BOUND
DHCPOFFER, DHCPACK, DHCPNAK/Discard
T2 expires/Broadcast DHCPREQUEST
DHCPNAK/Halt network
DHCPACK/

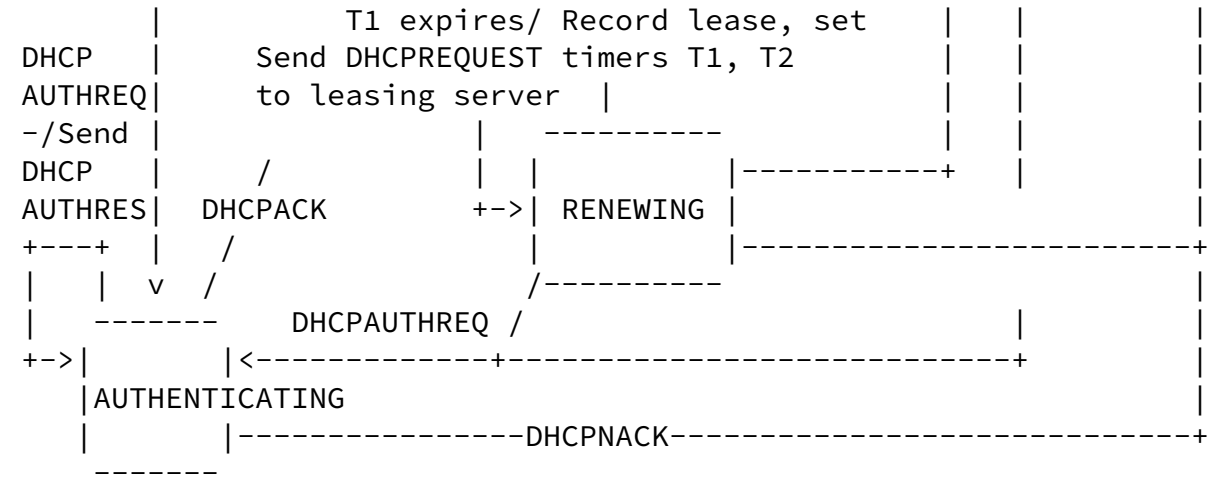


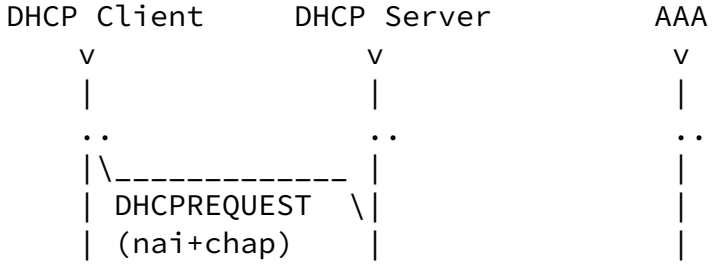
Figure 2: State-transition diagram for DHCP clients

6.4. Interworking with AAA Servers

The AAA mechanisms described here are similar to the ones already deployed and used by ISPs to serve PPP users. A AAA protocol like RADIUS can be employed with no modification to support client authentication by the network. The RADIUS protocol however needs to be modified in order to support network authentication by the client. These modifications are beyond the scope of this document.

6.5. Illustrations

To see the use of the authentication mechanisms described here, consider the case of a subscriber connecting to an access network and requesting configuration using DHCP. Figures below show the message flow between DHCP components of a network and their interaction with the AAA components. In the first case the network authenticates the client and in the second case the client authenticates the network. The last illustration shows how the initial configuration of a typical host would work when both the client and the network are being authenticated.



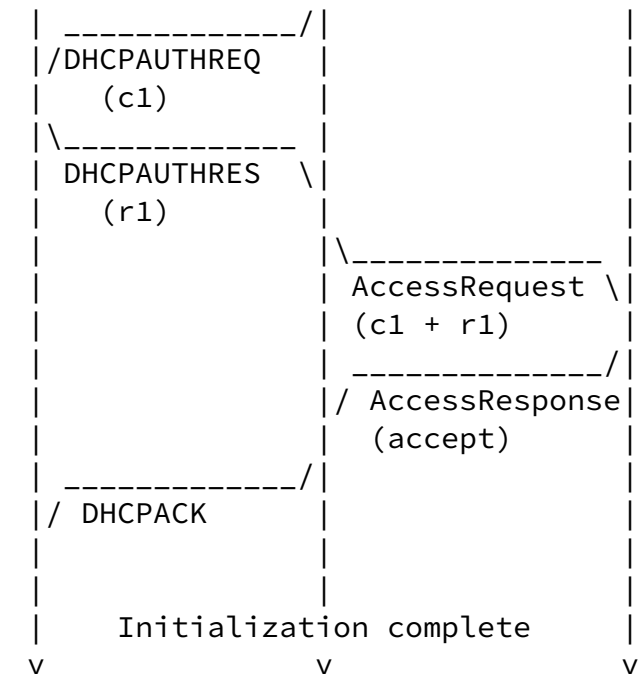
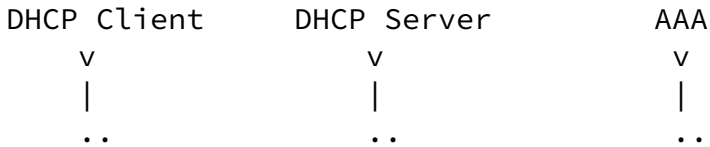


Figure 3: Authentication of the client

In Figure 3, the Client starts by sending the NAI in the appropriate option field. It also indicates its preference to perform CHAP authentication by including the CHAP option field. The server can

check that it does indeed support the requested authentication method and thus sends an authentication request message with the challenge in the CHAP option. The client can now use a key shared with its home AAA authority to respond to the challenge. Upon receiving the response, the DHCP server can then contact the local AAA server using, for example, a RADIUS Access Request message containing the challenge that was sent to the client and the response received from it. The AAA server may in turn contact the client's local AAA server. The AAA authority can then verify if the client's response to the challenge was correct using the shared key. The DHCP server, upon receiving the access response, will send a DHCPACK if the client authentication succeeded or DHCPNAK otherwise. Finally the DHCP client can verify and accept the parameters sent to it in the DHCPACK message.



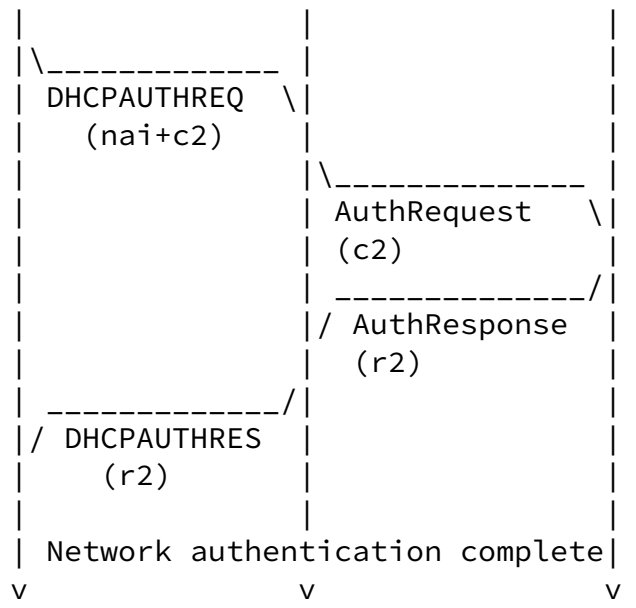
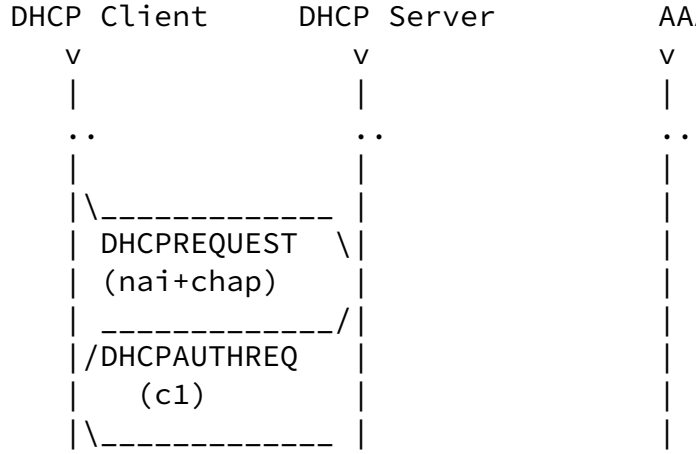


Figure 4: Authentication of the network

As shown in Figure 4, the client may also require authentication of the network and sends its own challenge to the network in a DHCPAUTHREQ message. The DHCP server may forward that request to the AAA server who will then use the key it shares with the client to respond. The Client upon confirming that the response was correct will reenter bound state and resume normal operation. Otherwise, if the response to the challenge was incorrect, it may reject the parameters it was given and restart configuration.



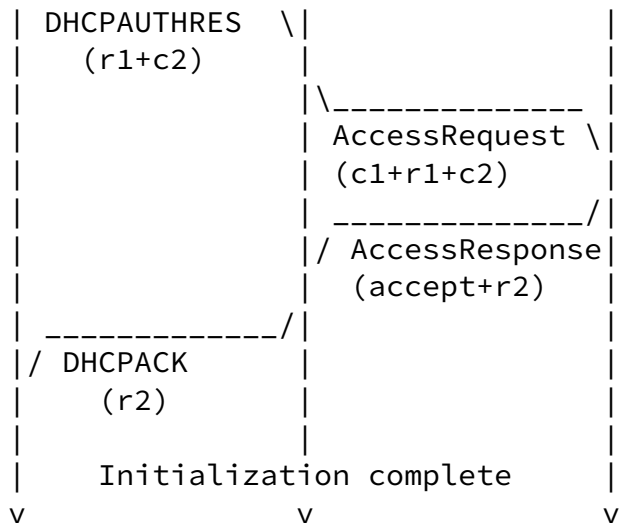


Figure 5: Authentication of the client and the network

During initial configuration when both sides may want to establish trust the two steps above may be combined as shown in Figure 5. In this case, the network's challenge is contained in its DHCPAUTHREQ message and the client's response is contained in its DHCPAUTRES message. The client's challenge is also contained in its DHCPAUTHRES message and the network's response to the challenge is contained in its DHCPACK message.

For re-authenticating, challenges can be sent using the DHCPAUTHREQ and DHCPAUTHRESP messages at any time without the need for reconfiguration or rebinding.

7. Security Considerations

The purpose of this document is to describe a mechanism for authenticating DHCP clients and servers. It does not cover other possible security attacks such as IP spoofing.

8. 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 S. Das, A. McAuley, A. Baba, Y. Shobatake, _Authentication, Authorization, and Accounting Requirements for Roaming Nodes using DHCP_, Internet Draft <draft-ietf-dhc-aaa-requirements-00.txt>, March 2000.

4 S. Das, A. McAuley, A. Baba, Y. Shobatake, _Requirements for Extending DHCP into New Environments_, Internet Draft <draft-ietf-dhc-enhance-requirements-00.txt>, March 2000.

5 K. Hickman, "The SSL protocol", Netscape Communication Corp., February 1995

6 C. Munroe, "http://www.uu.net/press_center/hot_tech_topics/vpn/vpn-whitepaper.pdf", White Paper, May 2000.

7 R. Dorms, W. Arbaugh, "Authentication for DHCP Message", Internet Draft <draft-ietf-dhc-authentication-14.txt>, July 2000.

8 S. Das, A. McAuley, A. Baba, Y. Shobatake, "Dynamic Registration and Configuration Protocol (DRCP)", Internet Draft <draft-itsumo-drcp-01.txt>, July 2000.

9 B. Volz, S. Gonczi, T. Lemon, R. Stevens, "DHC Load Balancing Algorithm", Internet Draft, <draft-ietf-dhc-loadb-03.txt>.

11 L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol(EAP)", RFC 2284, March 1998.

11 Aboda, Beadles, "The Network Access Identifier" RFC 2486, January 1999

12 W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

13 R. Dorms, "The Dynamic Host Control Protocol", RFC 2131, March 1997

10. Acknowledgments

We Acknowledge the help of Kris Ng and all the members of the Advanced Wireless research group at Nortel Networks.

11. Author's Addresses

Biswaroop Mukherjee
Nortel Networks,
Ottawa, ON,
Canada.
Email: biswaroo@nortelnetworks.com

Bill Gage
Nortel Networks,
Ottawa, ON,
Canada.
Email: gageb@ nortelnetworks.com

Yajun Liu

Nortel Networks,
Ottawa, ON,
Canada.
Email: yajun@nortelnetworks.com

Full Copyright Statement