B. Mukherjee
B. Gage
Y. Liu
J. Melzer
Nortel Networks
October 2000

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

Status of this Memo

1. Abstract

This draft proposes enhancements to DHCP so that it can be used to securely provide dynamic configuration to roaming mobile hosts. The problem has two major aspects: 1) adding extensible, inter-domain, user and network authentication functionality to DHCP and 2) to allow DHCP to function without relying on link layer specific mechanisms. The first feature would allow authenticated and audited visited network usage for roaming users while the second feature would allow DHCP to be used in the new environments like the wireless data networks. The authentication mechanism proposed here interacts with existing public Authentication, Authorization, and Accounting (AAA) mechanisms, thus enabling per customer authentication authorization and accounting across multiple domains. In addition, we propose a mechanism that enables the client to authenticate the DHCP server that has provided it with configuration parameters. We also describe a mechanism that allows DHCP to work independent of link layer broadcasts and addressing.

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 a subscriber, across administrative domains, is expected to be a vital part of the functionality of the next generation access networks. In addition users and devices are accessing networks from a variety of environments, from the office desktop to the wireless pagers. As a result, the access networks of the future are expected to operate over a wide variety of link layers. Such access networks are expected to perform authentication, authorization, accounting (AAA) [3] in addition to IP parameters configuration for its subscribers. We believe that DHCP can be used as an initial configuration protocol for the nodes that access such networks. The mechanisms proposed here attempt to address the requirements of such networks in a flexible and extensible manner. In this draft we propose mechanisms that allow DHCP to interface with the existing AAA infrastructure that allows the network to perform the AAA functionality in a flexible manner. Also, in order to use DHCP in new environments the protocol must have mechanisms that allow it to function without relying on layer two (e.g., ethernet) specific features. In this draft we show how using link local IP addresses the DHCP client and relay communicate, removing the reliance on link layer specific mechanisms. In past the DHC working group has also indicated similar concerns and has drafted requirements for AAA to aid roaming nodes using a dynamic address configuration protocol. The WG has also drafted the requirements for extending DHCP to new environments [4]. This draft addresses several of these requirements.

3.1. Motivation

It is clear that network access providers would require means to prevent the unauthorized and unbilled use of their network resources. Paying customers would also like to be billed only for their own usage and not those of unauthorized users. Also the new link layers being deployed especially in the wireless networks, make it imperative for DHCP to not rely on any features of the link layer like broadcast. The proposed additions would allow DHCP to be used by commercial access networks as a secure and flexible initial configuration protocol for subscribers, as opposed to its common present use as a means for configuring a pool of trusted clients in a local LAN.

3.2. Overview

One of the goals of this work is to propose mechanisms for user authentication to the access network by means of DHCP. To be

authorized for using the access network, the user must submit credentials to the network 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. In order for DHCP and the proposed mechanisms to be useful for new environments, we also introduce mechanisms that allow DHCP to function without relying on layer two specific features. The authentication messages may also provide a framework for negotiating other parameters, some of which may aid in enhancing security or in providing better performance to the user.

The 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 mechanisms that allows the security parameters to be negotiated and established is desirable. The security mechanisms being proposed here can be used to create trust relationships between the network and the client that may be used later 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 proposed additions in DHCP may be of use in new environments. The model of the network that this draft assumes 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 authentication is done via a public AAA mechanism. The public AAA infrastructure is assumed to consist of local AAA authorities in each of the access networks. It is assumed that these local AAA servers communicate among each other through a hierarchy of public AAA servers, and there exist security associations between the local AAA server and the DHCP servers. We also assume that 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 in a visited network and then enjoy its use. This model also 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. Furthermore, we do not assume that the client connects to the access network through ethernet. This is because we believe

that access networks may use different link layers with properties different from ethernet. As a result DHCP mechanisms cannot rely on ethernet broadcasts.

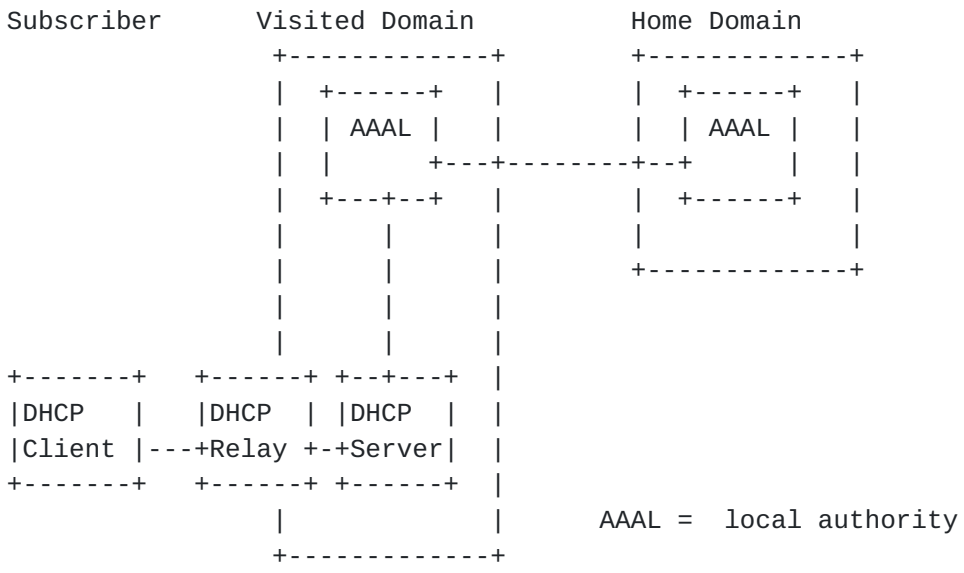

Figure 1: DHCP's interaction with AAA

5. Related Work

The DHCP working group of IETF has in the past expressed the need for DHCP to perform 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 (e.g., UUNET and QUEST) presently use AAA servers which support RADIUS or TACACS+ for customer accounting [6]. In this draft we propose mechanisms that allow DHCP to extensibly interface with this AAA infrastructure thus meeting the requirements set out by the requirements draft [3].

The reason for desiring new features in DHCP, like cross-domain AAA,

is that DHCP is being increasingly proposed as a solution for new environments, such as commercial access networks. Some requirements

for extending DHCP into new environments are listed in [4]. In this draft, DHCP is proposed as a general-purpose framework for performing registration and configuration of nodes in a network, as opposed to being a mechanism for configuring fixed nodes on an internal LAN. 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 confiuration. 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]. We also describe a method by which link local addresses are used for initial DHCP messages so that the protocol does not rely on link layer specific mechanisms of ethernet. We believe that these mechanisms are steps in making DHCP into a flexible intial configuration protocol, propounded by 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 was 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 our proposal, the authentication mechanism leverages the AAA infrastructure to not only authenticate the client and the

server in a symmetric fashion, but also allows 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 an 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. Some of the motivations for DRCP were the same as ours, like the need for a layer two independent protocol. On the other hand unlike DRCP our model does not require 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. Furthermore the request step is skipped. The protocol however does not specify any mechanisms for performing AAA functions or security mechanisms, whereas this is one of our primary motivations.

5.4. Using link local IP addresses

DHCP clients can automatically select an IP address in the case that no server responds to its address requests. The draft [9] suggests that this should be used only as an emergency measure. The client is supposed to pick an IP address that is valid only in the local subnet, called LINKLOCAL address. The IANA has specified the address range for IPv4 LINKLOCAL as 169.254/16. The client also needs to check if the address picked is already under use. We use the link local address in a different manner. In order to be independent of the link layer (and its addresses), we do not rely on the use of link layer addresses for even the initial message exchange between the uninitialized DHCP client and the network. This is indeed a requirement in certain scenarios where the existance of a unique link layer adress cannot be guaranteed (e.g., wireless). Also, future link layers may use addressing schemes that may not allow the network to easily map the link layer address to the client. Hence we propose that the DHCP use only IP layer addresses. The client can assign itself a LINKLOCAL IP address and then use that in conjunction with a IP multicast address set aside for DHCP server/relay [10] to communicate with the network, until it has obtained full configuration including an 'global' IP address. In our proposal, as our network model does not assume that all the hosts in the network can be reached by link level broadcasts, we use the

relay agent and a randomized address selection algorithm at the client to eliminate the duplicate assignment of the initial LINKLOCAL IP addresses.

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, which is our prime motivation, 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 in the access network may not be an option. In addition the access networks 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. On both counts the present message authentication draft falls short of providing a solution.

On one hand from the perspective of the subscriber, DHCP should allow access across different service provider domains. On the other hand from the perspective of the service provider there is a need for an authentication and accounting mechanism. We propose that DHCP use the existing AAA mechanisms to authenticate the users potentially across network domains and then initiate accounting using the same.

We propose that the DHCP protocol be extended so as to include an authentication phase and add authentication messages to DHCP. In our proposal the DHCP client is 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 is also modified to process the DHCP authentication message and forward the required messages to the AAA components.

6.1. Authentication Messages and Options

We propose that two new authentication messages be added 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 assined by IANA.

The messages are meant to be generic in nature and thus allow the DHCP server and client to establish the required credentials using any protocol they predetermine or negotiate. In fact the authentication phase may be completely skipped to remain backward compatible. But the 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 networks AAA mechanisms. In doing so we are able to leverage the existing AAA infrastructure as well as perform inter domain authentication and accounting.

The authentication messages can be sent by either the client or the server, whenever the user or the network wish to establish or (re-establish) a security relationship. We choose new message types for authentication as opposed to piggybacking security information upon other messages, as we believe that the specialized messages would make the process flexible and extensible. Moreover, there are instances like the challenge response protocols, where the present sequence of DHCP messages are unable to fulfill the functionality. For instance future challenges for re-keying in mid-session cannot be fitted in the existing messages without causing the client to restart the configuration procedure. Further if a security protocol that involves negotiation or requires more messages to be exchanged, the present set of messages will no longer be adequate. That is why we propose the new set of messages that allow extensible authentication. The need to be extensible was also propounded in other initial access protocols like PPP, which has an extensible authentication protocol [11].

We also propose options in order to carry authentication information within the messages DHCPAUTHREQ, DHCPAUTHRESP as well other DHCP messages like DHCPREQUEST. The client is expected to present its Network Access Identifier (NAI)[12] and 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 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)

[13], 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: Proposed options for security

6.2 The DHCP Server

The DHCP server model we propose is relatively simple as compared to [7], as it need not manage and process keys or any client specific authentication information by itself. Instead it contacts the local AAA server with the client information, like NAI and password (PAP) and ask the AAA server if it can configure the client or not. For a network that requires a challenge response protocol for authentication the server needs to be able to issue challenge messages with a DHCPAUTHREQ message, receive the DHCPAUTHRES response from the client and forward to the AAA for client authentication. The server also needs to respond to DHCPAUTHREQ messages with a DHCPAUTHRESP message for the client. It may ask the AAA to create a response for the challenge and then send it using the DHCPAUTHRESP message.

6.3. The DHCP Client

The DHCP client needs to be modified to incorporate the authentication mechanisms proposed. We add in a state in the clients 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. We choose not to allow the client to send challenges in the other states as it adds unnecessary complexity. The client MUST respond to the DHCPAUTHREQ message by the message DHCPAUTHRESP. Both of these messages carry authentication options as described in 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 on the other hand the client had sent the DHCPAUTHREQ the client MUST leave the AUTHENTICATING state and enter the BOUND sate when a valid DHCPAUTHRES is received. Otherwise 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[14]. 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 proposed client with the new state authenticating as well as the new messages DHCPAUTHREQ and DHCPAUTHRES.

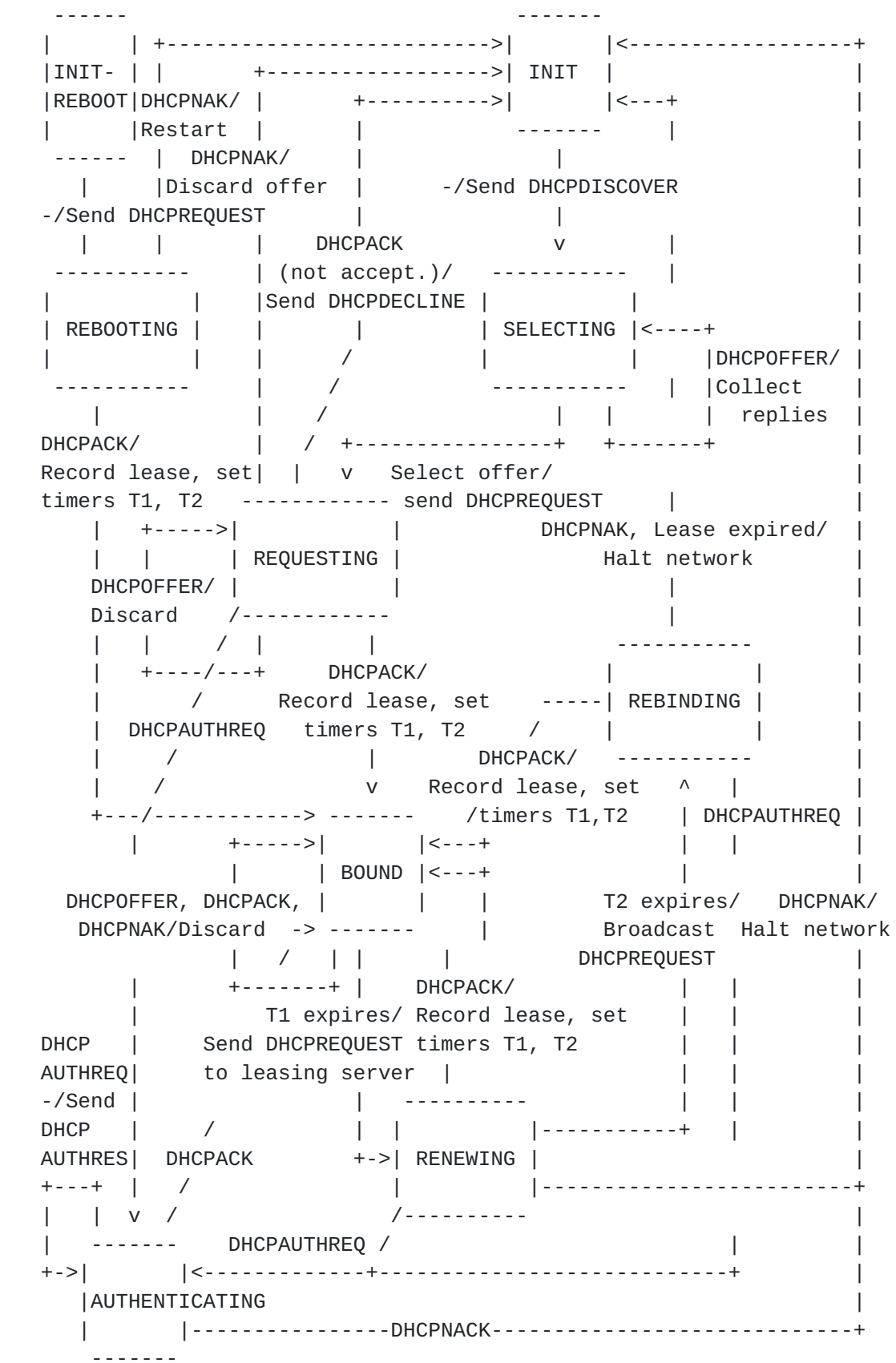
INIT-REBOOT
DHCPNAK/ Restart
DHCPNAK/ Discard offer
-/Send DHCPREQUEST
DHCPACK (not accept.)/ Send DHCPDECLINE
INIT
-/Send DHCPDISCOVER
REBOOTING
SELECTING
DHCPOFFER/ Collect replies
DHCPACK/ Record lease, set timers T1, T2
Select offer/ send DHCPREQUEST
DHCPNAK, Lease expired/ Halt network
REQUESTING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

Figure 2: State-transition diagram for DHCP clients

6.4. AAA

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 the DHCP interaction described here. The RADIUS server however needs to be modified in order to support network authentication by the client. The server needs the added functionality to respond to a challenge that may have been sent by a client. Note that the key management and challenge response functions are already available in the server for client authentication.

6.5. Illustrations

To see a possible 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 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 intial configuration of a typical host would work when both the client and the network authenticate themselves.

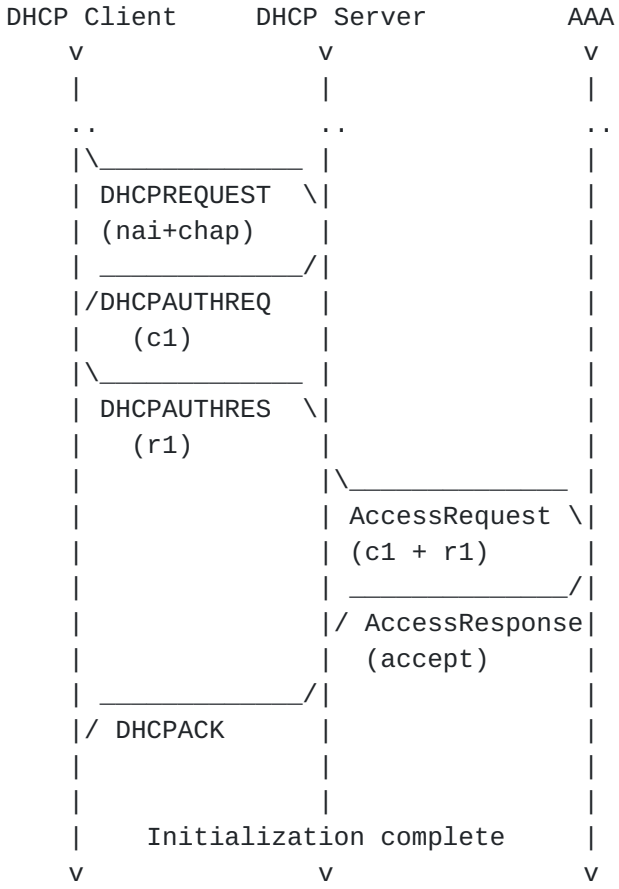

Figure 3: Authentication of the client

In the above scenario, the Client starts by sending the NAI in the appropriate predefined 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, with an Access Request message containing the challenge that was sent to the client, the response received from it. The AAA server may in turn contact the clients 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.

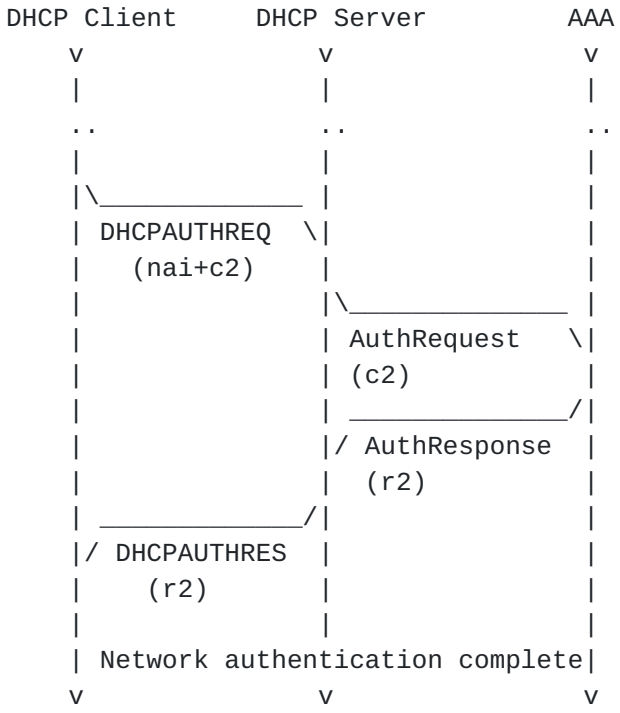

Figure 4: Authentication of the network

The client may also require authorization from the network, and send 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. As an aside note that, the popular AAA protocol, RADIUS, does not respond to challenges at this time. But

it is expected that means for authenticating the network will be in incorporated the future.

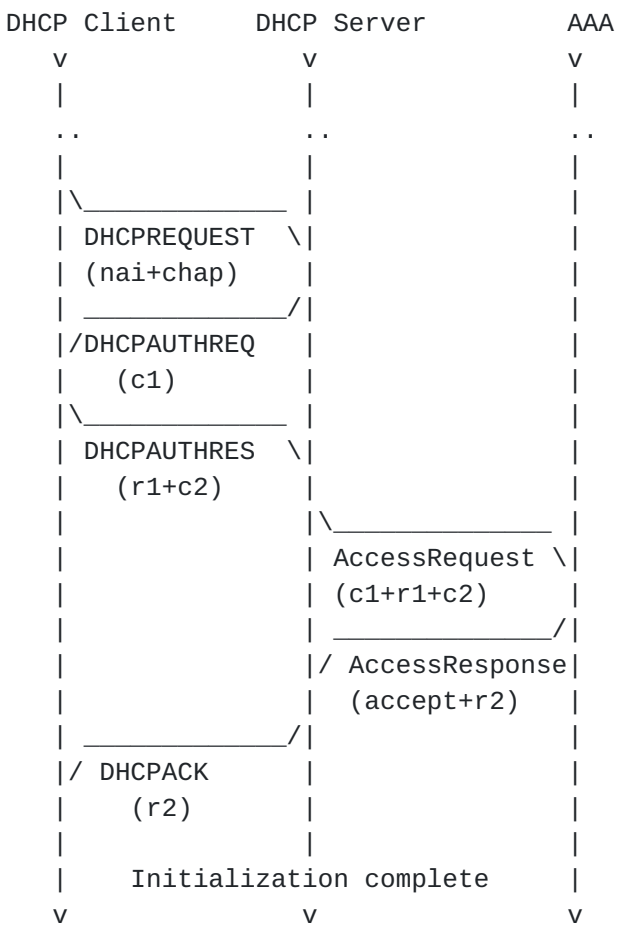

Figure 5: Authentication of the client and the network

During initial configuration when both sides may want to establish trust the two steps above may be combined as shown above. For the future messages the client and the server may choose a session key and use the message authentication header proposed to the DHC working group [7]. Or the challenge response procedure can be repeated every time the lease is about to expire. For re-authenticating, challenges can be sent using the DHCPAUTHREQ and DHCPAUTHRESP messages at any time and new session keys may be generated. The session key may also be used as the client's ticket to the services of the network. The key may be propagated to the appropriate elements of the network and the client may be required to use it for verifying service requests. For instance, a managed network may require that the client use the key to sign its bandwidth reservation requests, that will be verified at policy decision points that allow disallow the reservation requests.

6.6. Trust relationships and Security Associations

There are several trust relationships and security associations (SA) that are involved in the process above.

1. DHCP client to DHCP server
2. DHCP server to AAA server
3. AAA server to DHCP server
4. DHCP server to DHCP client
5. DHCP client to AAA server
6. AAA server to DHCP client

In our network model we assume that the existence of per-session security associations between the DHCP server and the AAA infrastructure and vice versa (i.e., the SAs 2 and 3 are pre-established).

The subscriber and thus the DHCP client is identified by AAA using a predefined key or password(say K1). When the DHCP server sends a challenge to the client, it uses K1 to respond to it. The DHCP server then sends the challenge and response to the AAA server, where the trust relationship 5 can be established. Also using the pre-established SAs 2 and 3 the trust relationship 1 is established (i.e., the DHCP server is told to trust the DHCP client by AAA).

Now all that remains is for the network to authenticate itself to the client. The client can send a challenge to the AAA server, with whom it shares the key K1 and use the response to establish the trust relation 6 and by extension the trust relationship 4. In order to avoid going to AAA for every interaction a session key K2 can be generated and be shared between the DHCP client and the server as most future interactions may just require the trust relations 1 and 4. Using the Message authentication proposal of the DHC working group[7] the key K2 can ensure that the renewals are authenticated.

7. Link Local Addresses for Initial Access

An issue when trying to extend DHCP into new environments is that it relies on ethernet broadcasts to allow unconfigured nodes to exchange messages with DHCP relay and or server as well as other clients for ARP requests. A DHCP client implementation must either be able to form a link-layer broadcast as in ethernet or send a link-layer unicast packet in the absence of a unicast IP address. In some environments it may be impossible or inadvisable to send link-layer broadcasts. In these cases servers or relays, which receive broadcast packets must be able to unicast responses by direct interaction with the link layer. This makes the DHCP implementation link layer dependent. This may be a problem when different types of link layers with different capabilities are being deployed. We propose that a non-broadcast IP address be used to isolate DHCP from any link-layer specific features of the link

layers.

In view of the new link layer protocols that are being proposed and deployed, it is imperative that DHCP not rely on the link layer being ethernet like. In particular, we believe that broadcasts may not be a feature of all the link layer protocols. It cannot be assumed that all the hosts on the IP layer subnet will be able to receive packets as broadcasts. As a result we need broadcast-independent mechanisms that allow the DHCP client to reach the DHCP server/relay and vice versa. We also need the address conflicts to be resolved without using link layer broadcast.

In order to insure reachability of the uninitialized client and the DHCP server/relay, we propose that the DHCP client, upon initialization, assign itself a link local IPv4 address form the range 169.254/16 which is registered with the IANA as the LINKLOCAL net [10] and the DHCP server/relay listen to the IPv4 multicast address 224.0.0.12 assigned to it in the RFC1884 [10]. The client sends out packets intended for the DHCP server/relay to the multicast address 224.0.0.12. and the server/relay replies back to the link local IP address that the client has chosen. In order to ensure that there are no address conflicts, when a DHCPDISCOVER message is received, the DHCP Relay Agent MUST test to see if the source address is already in use. If the network address appears to be in use, the Relay Agent MUST silently discard the DHCPDISCOVER message. If the DHCP client does not receive a response to the DHCPDISCOVER message within its timeout period, it MUST choose another address, and try again. The client MUST keep choosing addresses until it either receives a response to its DHCPDISCOVER message, or it has tried more then the autoconfig-retry count. The autoconfig-retry count is implementation specific, and should be based on the algorithm used for choosing an IP address. This retry count is present to make sure that DHCP Clients auto-configuring on busy auto-configured network segments do not loop infinitely looking for an IP address. After successfully obtaining configuration information, the client changes its IP address to the one given out by the DHCP server to complete the process.

8. Security Considerations

Security assumptions for the mechanisms described here are described in section 6.6.

9. 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 R. Troll, _Automatically Choosing an IP Address in an Ad-Hoc IPv4 Network_, Internet Draft, <draft-ietf-dhc-ipv4-autoconfig-05.txt>, March 2000.
10 R. Hinden, S. Deering, "IP Version 6 Addressing Architecture", RFC 1884, December 1995.
11 L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol(EAP)", RFC 2284, March 1998.
12 Aboda, Beadles, "The Network Access Identifier" RFC 2486, January 1999
13 W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.
14 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,
100 Constellation Cr.,
Napean, ON,
K2G 6J8, Canada.
Email: biswaroo@nortelnetworks.com

Bill Gage
Nortel Networks,
100 Constellation Cr.,
Napean, ON,
K2G 6J8, Canada.
Email: gageb@ nortelnetworks.com

Yajun Liu

Nortel Networks,
100 Constellation Cr.,
Napean, ON,

K2G 6J8, Canada.
Email: yajun@nortelnetworks.com

Jordan Melzer
Email: jmelzer@usc.edu

Full Copyright Statement