Network Working Group
INTERNET-DRAFT
Internet Engineering Task Force
draft-ietf-dhc-aaa-requirements-00.txt
Date: March 8, 2000
Expires: August, 2000

Subir Das
Anthony McAuley
Telcordia Technologies
Shinichi Baba
Yasuro Shobatake
Toshiba America Research Inc.

Authentication, Authorization, and Accounting Requirements for Roaming Nodes using DHCP

Status of this memo

Abstract

The AAA working group is currently defining the requirements for Authentication, Authorization, and Accounting (AAA). This draft lists the AAA requirements to aid roaming nodes using a dynamic address configuration protocol such as DHCP. The node may or may not be using Mobile IP [3] (with co-located care-of-address) or other dynamic address binding protocol.

1. Introduction

A network providing communication services to nodes from foreign domains, must use Authorization, Authentication, and Accounting (AAA) services [1,2]. A dynamically roaming node places stronger requirements on AAA than a static node. Moreover, next generation network applications will raise the requirements on IP network even higher. The Mobile IP [3] Working Group is currently specifying the requirements for a roaming node using Mobile IP with Foreign Agents [4]. This document specifies the requirements for a roaming node who obtains an address using DHCP [5] [17] or similar node configuration protocol (e.g., DRCP [6]).

Recent drafts [7,8] specify how to add authentication to DHCP messages. This allows clients to verify DHCP servers or servers to verify DHCP clients. It does not, however, specify the interaction with a AAA protocol to allow roaming users to access networks in multiple administrative domains.

The document is independent of whether the roaming node uses dynamic address binding. The roaming node getting an address through DHCP [5] and once authenticated via AAA [1, 13,14] may also use Mobile IP with co-located addresses, dynamic DNS updates [9,10], or any other dynamic address binding techniques [15,16]. The document does not discuss the pros and cons of how best to support roaming users, only to ensure that the AAA protocol is sufficiently flexible to support both nodes using Mobile IP with Foreign Agents and nodes using DHCP (with or without Mobile IP).

Since many of the requirements for DHCP are similar to those for Mobile IP with Foreign Agents, we borrow heavily from the Mobile IP requirements document [3, 4].

1.1 Requirements Terminology

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 [REQ].

2. Basic Model

Figure 2 shows that our general model is very much similar to that described in [4]. The only change is that we do not assume the AAA authentication is necessarily done in a home domain. We assume, more generally, that the roaming node authentication is done in a (possibly distributed) Public AAA (AAAP), which is similar to AAA broker model. The reasons for using the AAAP are discussed in section 4. Each DHCP client might use a different AAAP that can check its credentials, or they may share the same AAAP (even if they are from different domains).

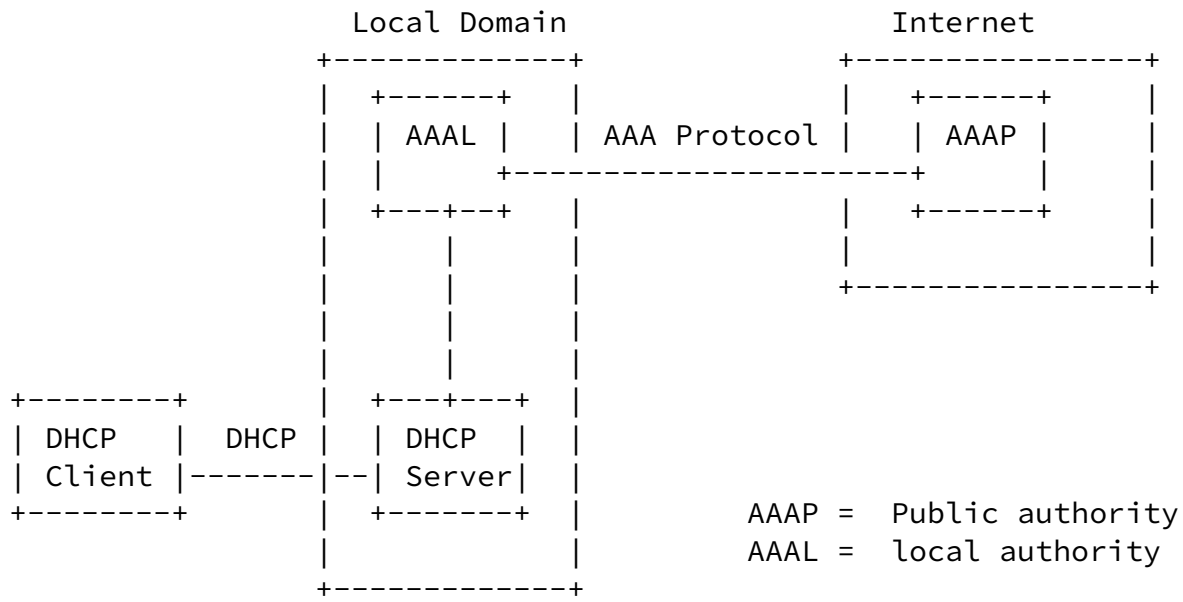

Figure 1: AAA Servers Model

DHCP server does not have direct access to the data needed for authentication. So it is expected that the server will consult the

local authority (AAAL) for verification. Since the server and the local authority are in the same domain it is assumed that they will have strong security associations. Alternatively, they may be co-located. On the other hand, AAAL itself may not have enough information stored locally to complete the transaction. However, AAAL is expected to be configured with enough information to negotiate the client's verification with corresponding AAAP. Sometimes client may notify its own AAAP for verification via its registration message (e.g., Client's NAI [11]). The local AAA and public AAA should have sufficient security relationships and access control so that they can negotiate the authorization and enable the client to have the requested resources. Once this is over, DHCP

server will be notified about the successful negotiation and the server can provide the requested resources to the client. If it is not authorized, server will be informed to terminate the service to the client.

3. Requirements

Based on the above scenarios, the following specific requirements for AAA can be ascertained.

- Either the DHCP Server and AAAL are co-located or they share a security relationship.
- The DHCP server should be configured to obtain authorization from a trusted local AAA server (AAAL).
- The local authority (AAAL) has to share, or dynamically establish, security relationships with public authorities (AAAP) that are able to check client credentials.
- The client must have a security association with its public authority (AAAP).
- Nobody can reconstruct and reuse the credentials that the client uses.
- The DHCP server MUST be able to terminate service to the

client based on policy determination by the AAA server.

- The DHCP server should be able to handle requests for many clients simultaneously.

- The client may resend a request if it does not get a reply in some time, so the AAA entities must be designed to operate correctly and efficiently with multiple requests for the same client.

- The DHCP server has to keep state for pending client requests while the local authority contacts the appropriate external authority.

- Support replay protection and optional non-repudiation capabilities for all authorization and accounting messages.

- AAA server need not know any IP address of the client and it identifies clients by other means, e.g., Network Access

Identifier (NAI).

- Client NAI domain allows AAAL to easily determine the AAAP.

- The local AAA server MUST support anonymous access.

- There is no requirement for AAA to transport `DHCP or other node configuration messages'.

- AAA must complete in one round trip. A major component of the setup latency is the time taken to traverse the wide-area Internet that is likely to separate the AAAL and the AAAP.

- AAA must allow a node to register once in its domain and move among subnets in the same domain without requiring more AAA. After the initial registration, the AAAP and AAAL would not be needed.

- Support accounting information via AAAP servers providing accounting clearinghouse and reconciliation between serving and home networks.

- AAA MUST support message privacy and integrity.

4. Reasons for using Public AAA

AAA servers model in [4] shows a configuration in which the local and the home authority have to share trust. This configuration causes a quadratic growth in the number of trust relationships as the number of AAA authorities (local AAA and home AAA) increases. This has been identified as a problem by the roamops working group [12], and any AAA proposal MUST solve this problem. Using public AAA (AAAP) solves many of the scalability problems associated with requiring direct business/roaming relationships between every two administrative domains. A public AAA may play the role of a proxy between two administrative domains which have security associations with the AAAP, and relay AAA messages back and forth securely.

The AAAP enables the local and home domains to cooperate without requiring each of the networks to have a direct business or security relationship with all the other networks. Thus, AAAPs offer the needed scalability for managing trust relationships between otherwise independent network domains. Use of the AAAP does not preclude managing separate trust relationships between domains, but it does offer an alternative suitable for commercial environments.

5. Security Considerations

This draft defines the AAA requirements for roaming nodes using DHCP or similar type of node configuration protocol. Since AAA is security driven, most of this documents addresses the security considerations AAA must make on behalf of roaming nodes using node configuration protocols.

6. Acknowledgements

The requirements in section 3 were taken from a draft submitted by

S. Glass, S. Jacobs, and C. Perkins of the Mobile IP working group. We would like to acknowledge their work.

The authors acknowledge the contributions of other members of the ITSUMO (Internet Technologies Supporting Universal Mobile Operation) team from Telcordia (P. Agrawal, J.C. Chen, A. Dutta, D. Famolari, S. Madhani, F. Vakil, P. Ramanathan, H. Sherry and R. Wolff) and Toshiba America Research Incorporated (T. Kodama).

References

[1] S. Farrell, J. Vollbrecht, P. Calhoun, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege and D. Spence, "AAA Authorizatiopn Requirements," <draft-ietf-aaa-authorization-reqs-01.txt>, October 1999.

[2] J. Arkko, "Requirements for Internet-scale Accounting Management," <draft-arkko-acctreq-00.txt>, August, 1998.

[3] C. Perkins, "IP Mobility Support," RFC 2002, October 1996.

[4] S. Glass, S. Jacobs, C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements," <draft-ietf-mobileip-aaa-reqs-00.txt>, October, 1999.

[5] R. Droms, "Dynamic Host Configuration Protocol," Request for Comments 2131, March, 1997.

[6] A. McAuley, S. Das, S. Baba, Y. Shobatake, "Dynamic Registration and Configuration Protocol (DRCP)," <draft-itsumo-drcp-00.txt>, October, 1999.

[7] R. Droms, "Authentication for DHCP Messages," <draft-gupta-dhcp-auth-12.txt>, October, 1999.

[8] V. Gupta, "Flexible Authentication for DHCP Messages," <draft-ietf-dhc-authentication-12.txt>, October, 1998.

[9] A. Gustafsson, "A DNS RR for encoding DHCP information,"

<draft-ietf-dnsind-dhcp-rr.00.txt>, October, 1999.

[10] M. Stapp, Y. Rekhter, "Interaction between DHCP and DNS," <draft-ietf-dhc-dhcp-dns-11.txt>, October, 1999.

[11] B. Aboba and M. A. Beadles, "The network access identifier," RFC 2486, January 1999.

[12] B. Adoba and G. Zorn, "Criteria for evaluating roaming protocols," RFC 2477, December 1998.

[13] J. Wang and R. Wang, "Cellular network Authentication, Authorization, and Accounting requirements," <draft-wang-aaa-cel-req-00.txt>, October, 1999.

[14] M. Beadles and et.al., "Criteria for evaluating AAA protocols for network access", <draft-ietf-aaa-na-reqts-01.txt>, October 1999.

[15] H. Schulzrinne and et. al., "SIP: Session initiation protocol," RFC 2543, March 1999.

[16] E. Wedlund and H. Schulzrinne, "Mobility support using SIP", Proc. The second ACM International workshop on Wireless Mobile Multimedia, ACM/IEEE, pp 76-82, August, 1999.

[17] A. McAuley, S. Das, S. Baba, Y. Shobatake, " Requirements for Extending DHCP into New Environments," <draft-dhc-enhance-requirements-00.txt>, March, 2000.

7. Authors' Addresses

Subir Das
MCC 1D210R, Telcordia
445 South Street, Morristown, NJ 07960
Phone: +1 973 829 4959
email: subir@research.telcordia.com

Anthony J. McAuley
MCC 1C235B, Telcordia
445 South Street, Morristown, NJ 07960
Phone: +1 973 829 4698
email: mcauley@research.telcordia.com

Shinichi Baba
Toshiba America Research Inc.
P.O. Box 136 Convent Station, NJ 07961-0136
Phone: +1 973 829 4759
email: sbaba@tari.toshiba.com

Yasuro Shobatake
Toshiba America Research Inc.
P.O. Box 136 Convent Station, NJ 07961-0136
Phone: +1 973 829 3951
email: yasuro.shobatake@toshiba.co.jp