Network Working Group
INTERNET DRAFT
Category: Informational
Date : 16 June 2003

Farid Adrangi
Victor Lortz
Jose Puthenkulam
Intel Corporation

RADIUS Issues in Public Wireless LAN Roaming Scenarios

draft-adrangi-radius-issues-in-pwlan-roaming-00.txt

Status of this Memo

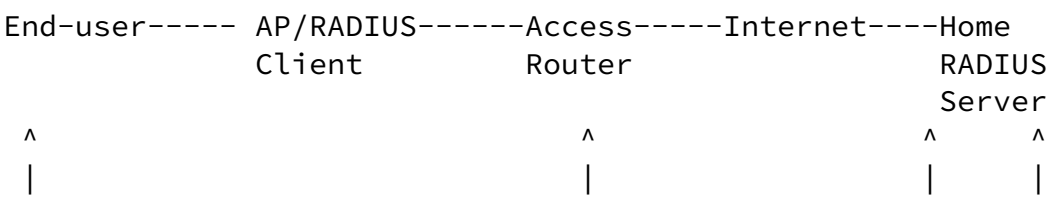
Abstract

There are a number of IETF drafts that describe use of RADIUS in a variety of scenarios. However, in the context of Public Wireless LAN (PWLAN) deployments, there are still some areas where either use of RADIUS is unclear or not covered. To address this problem, we first need to generate a list of RADIUS issues significant to public wireless LAN roaming (authenticating and obtaining service on a network operated by or affiliated with a home providerÆs ôroaming partnerö). Once these issues are understood and analyzed, we can take appropriate actions to solve them. This document describes some of RADIUS issues encountered in PWLAN deployments and roaming scenarios.

Table of Contents

1. Introduction

A PWLAN network is comprised of three main components that work together to provide users with wireless access to the public network. These components are: the Access Points (AP), the Router which links to the Internet and the Authentication Server (AS). Currently, there are two standard protocols used to implement an AS, which are : 1) RADIUS [1] 2) DIAMETER [2] IETF Protocols. However, we will only focus on use of RADIUS protocol hereafter in this document. The following diagram shows a simple RADIUS-based PWLAN network architecture.



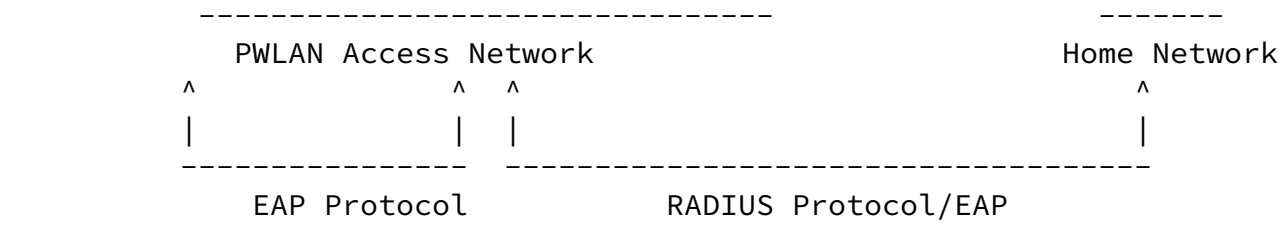


Figure 1.0

Authentication exchanges are carried out between the end-user (authenticating peer) and the home RADIUS server (authentication server) through the AP/RADIUS-Client acting as a bridge. From the end-user to the AP/RADIUS-Client, the protocol is EAP [3] over wireless. On the back-end, the protocol used is RADIUS. This is also referred to as ôEAP over RADIUSö [4].

In the roaming context, the network topology depicted above becomes slightly complicated. Two new components, visited RADIUS proxy and intermediary RADIUS proxy, are introduced to the network. Simply put, these two components are basically a RADIUS server used in a particular roaming scenario. There are three possible roaming scenarios: 1) Roaming within the home network û the AP/RADIUS client directly communicates with the home RADIUS server. 2) Roaming within a foreign network which has direct roaming agreement with the home network û the AP/RADIUS client communicates with the home RADIUS server through the visited RADIUS proxy located in the foreign network. 3) Roaming within a foreign network which has an indirect roaming agreement with the home network û the AP/RADIUS client communicates with the home RADIUS server through the visited RADIUS proxy and 1 or more intermediary RADIUS proxies managed by the roaming partners. The following diagram depicts the network topology that supports the above roaming scenarios.

```
End-user-- AP/---Visited--Access--Internet--RADIUS--RADIUS--Home
           RADIUS  RADIUS   Router          Proxy...Proxy   RADIUS
           Client  Server/                                 Server
```

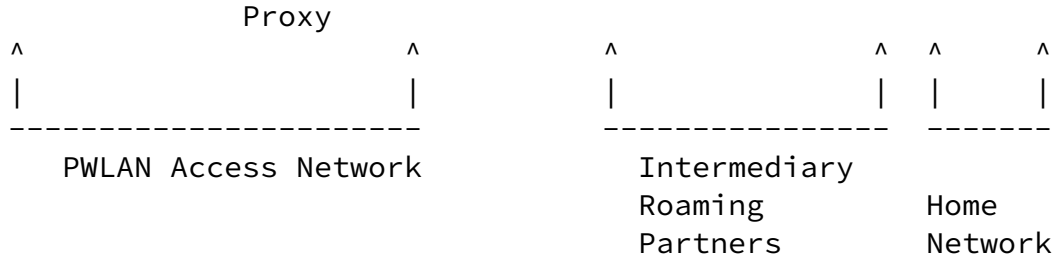


Figure 2.0

This document lists RADIUS issues encountered in the context of the aforementioned roaming scenarios. At this point, this document does not provide or suggest any solution to the issues.

2. Terminology

Access Point (AP)
ôA Station that provides access to the distribution services via the wireless medium for associated Stations.ö

Network Access Server (NAS)

ôThe device providing access to the network. Also known as the Authenticator (IEEE 802.1X or EAP terminology) or RADIUS client.ö

RADIUS server
ôThis is a server which provides for authentication/authorization via the protocol described in [1], and for accounting as described in [6].ö

RADIUS proxy
ôIn order to provide for the routing of RADIUS authentication and accounting requests, a RADIUS proxy can be employed. To the NAS, the RADIUS proxy appears to act as a RADIUS server, and to the RADIUS server,

the proxy appears to act as a RADIUS client.ö

3. General Issues

This section describes a list of current issues in no particular order in terms of importance or priority.

3.1 The lack of Identity for Accounting Purposes with privacy protection

In some cases the userÆs identity may not be known to the AP/RADIUS-client (For example, the authenticating peer uses a tunneled authentication protocol, such as PEAP [5], which protects the userÆs identity). This can be a problem as the AP/RADIUS-Client needs to know the userÆs identity for RADIUS accounting [6] purposes or other things.

3.2 The lack of Standard ôFilter Profilesö

Typically RADIUS server relays information about session authorizations through the Filter-ID attribute which contains pointers to certain ôfilter profilesö. Examples of a filter profile are ômail-onlyö, ôlocal-netö, ôFull-netö, and ôAccess-to-multimedia-servicesö which correspond to various account types and help the RADIUS client to enforce restriction on a session. Filter profiles for authorizing commonly used services are not standardized and therefore there is a need for standardizing most common filter profiles or providing standard attributes for this functionality. The main reason behind this is to ensure interoperability between RADIUS client, RADIUS proxy, and RADIUS server implementations from different vendors.

3.3 The Problem with RADIUS Proxy Routing

There is no consistent mechanism by which RADIUS proxies can determine the next hop in an interoperable manner.

3.4 The lack of a method to specify the Access Network Location

---

The RADIUS server needs the Access Network Location Identifier (probably BSSID) and name for Management and Accounting purposes.

3.5 The lack of a method to specify the type of clientÆs IP address

There is a need to specify whether a public or a private IP address type should be assigned to the client by the wireless network. The RADIUS server determines this based on the service profile that it is going to authorize for the user. For example,

if the user is being authorized for services that are not NAT friendly (e.g., H.323 based services), then the RADIUS server can request for a public address to be assigned to the user.

3.6 The problem of differentiating between access service types

There is a need for the RADIUS server to distinctly identify ôwirelessö NASes from other types like Dialup and Ethernet for Management and Accounting purposes.

3.7 The lack of a method to relay the Mobile IP Home Agent address to the NAS

There is a need for the RADIUS server to convey the Mobile IP Home Agent address to the RADIUS client for subsequent use in DHCP.

3.8 The lack of an interoperable method to express quality of service parameters to the NAS

There is a need for the RADIUS server to convey the quality of service parameters for each user to the NAS in an interoperable manner.

4. Acknowledgements

The authors would like to thank Mark Montz of HP, Serge Manni of Sprint, Ed Van Home of Cisco, Bernard Aboba of Microsoft, and Blair Bullock of iPass for their contribution.

5. References

[1] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[2] Calhoun, P., "Diameter Base Protocol", draft-ietf-aaa-diameter-17 (work in progress), January 2003.

[3] Blunk, L. and J. Vollbrecht, "PPP Extensible

Authentication Protocol (EAP)", RFC 2284, March 1998.

[4] Aboba, B. and P. Calhoun, "RADIUS Support for Extensible Authentication Protocol (EAP)", Internet draft (work in progress), draft-aboba-radius-rfc2869bis-18.txt, April 2003.

[5] Andersson, H., et al., "Protected EAP Protocol (PEAP)", Internet draft (work in progress), draft-josefsson-pppext-eap-tls-eap-05.txt, September 2002.

[6] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

AuthorsÆ Addresses

Farid Adrangi
Email: farid.adrangi@intel.com Phone:+1 503-712-1791
Victor Lortz
Email: victor.lortz@intel.com Phone:+1 503-264-3253
Jose Puthenkulam
Email: jose.p.puthenkulam@intel.com Phone:+1 503-264-6121

Full Copyright Statement

assigns.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.