

54. IWK
Internationales Wissenschaftliches Kolloquium
International Scientific Colloquium



**Information Technology and Electrical
Engineering - Devices and Systems, Materials
and Technologies for the Future**



Faculty of Electrical Engineering and
Information Technology

Startseite / Index:

<http://www.db-thueringen.de/servlets/DocumentServlet?id=14089>

Impressum

Herausgeber: Der Rektor der Technischen Universität Ilmenau
Univ.-Prof. Dr. rer. nat. habil. Dr. h. c. Prof. h. c.
Peter Scharff

Redaktion: Referat Marketing
Andrea Schneider

Fakultät für Elektrotechnik und Informationstechnik
Univ.-Prof. Dr.-Ing. Frank Berger

Redaktionsschluss: 17. August 2009

Technische Realisierung (USB-Flash-Ausgabe):
Institut für Medientechnik an der TU Ilmenau
Dipl.-Ing. Christian Weigel
Dipl.-Ing. Helge Drumm

Technische Realisierung (Online-Ausgabe):
Universitätsbibliothek Ilmenau
[ilmedia](#)
Postfach 10 05 65
98684 Ilmenau

Verlag:  Verlag ISLE, Betriebsstätte des ISLE e.V.
Werner-von-Siemens-Str. 16
98693 Ilmenau

© Technische Universität Ilmenau (Thür.) 2009

Diese Publikationen und alle in ihr enthaltenen Beiträge und Abbildungen sind urheberrechtlich geschützt.

ISBN (USB-Flash-Ausgabe): 978-3-938843-45-1
ISBN (Druckausgabe der Kurzfassungen): 978-3-938843-44-4

Startseite / Index:
<http://www.db-thueringen.de/servlets/DocumentServlet?id=14089>

THE IMPLEMENTATION OF RADIUS AUTHENTICATION IN PUBLIC WIRELESS NETWORKS

Dusan Vuckovic, Dragan Jankovic

Faculty of Electronic Engineering, Nis, Serbia

ABSTRACT

This paper presents the means of user authentication in wireless networks when the strong network protection is required. It is also intended to help implement RADIUS user authentication on wireless networks in the environments where different operating systems are used. The concept of RADIUS authentication is explained along with procedures for connecting Wireless Access Points with GPL Linux firmware and Captive Portal to Microsoft's Network Policy Server and Windows Server 2008 Active Directory users database.

Index Terms – Wireless, Authentication, Accounting, RADIUS, LDAP, Active, Directory

1. INTRODUCTION

RADIUS (Remote Authentication Dial-In User Service) was originally established as a set rules and services for user authentication management in dial-up, intranet and VPN networking environments. It gained much of its popularity in contemporary, widely spread wireless internet connections world. RADIUS protocol defines authentication, authorization and accounting (AAA) in centralized fashion. The RADIUS Authentication and Authorization are defined in RFC 2865 [1], while the Accounting part is defined in RFC 2866 [2]. Implementations of RADIUS specification vary and are vendor independent. There is an integrative Microsoft solution, various other proprietary and open source solutions. This paper tackles the problem of implementation of RADIUS server in corporate intranet wireless environment through combining Microsoft technology on the back-end side with an open source solution on the side of the access client and server.

Situations like this one may be found in academic institutions, often open for experimenting with new solutions and technologies, and in public wireless networks. Academic institutions are the perfect example of heterogeneous environment and situation where RADIUS component can be located on a Linux platform, Microsoft Active Directory can be used as a LDAP base with student accounts and Data Base server could be MySQL on a Unix platform used for Accounting.

2. THE RADIUS CONCEPT

As a relatively simple client-server type protocol, RADIUS is responsible for user authentication, authorization and account management related to network accessing clients. It is designed to reside on a centrally positioned server and acts as a secure layer between network access points (typically IEEE 802.11) and the back-end database of user accounts [3]. It is the network accessing client that initiates communication towards the RADIUS server, and the responses it gets include access permission or denial, depending on the evaluation of the connection request (defined by username and password, or a certificate the user provides). In addition, the server can determine the set of privileges to which the specific client (user) is authorized. There can also exist RADIUS proxies, assigned to route connection requests between other components, namely clients, servers and other RADIUS proxies.

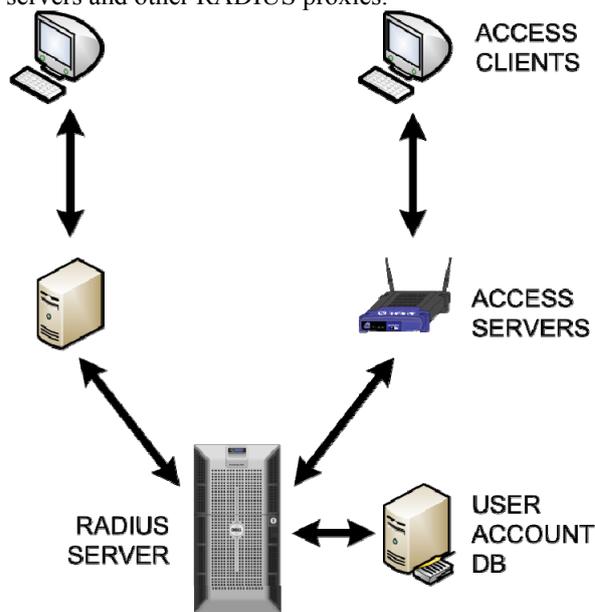


Figure 1. Various RADIUS implementations

3. THE PARTS OF RADIUS

In general, a system using RADIUS includes access clients, access servers (which act as clients from the RADIUS point of view), RADIUS servers, user account databases and, optionally, RADIUS proxies, as shown in Fig. 1.

An access client is any entity that connects to the network (e.g. LAN, VPN or intranet). An access server provides network access; this category includes wireless access points, switches and network access

servers (NASs). Access server acts as a client to RADIUS server by sending it connection requests and account-related messages. RADIUS server processes what is sent by its client (or RADIUS proxy) and decides on the connection of each user according to a set of rules. In early versions of RADIUS servers the data on users was kept in a file within the servers. Later versions introduced database access, detaching the user account database from the server, thus allowing the use of SQL, Kerberos, LDAP or Active Directory. User account database keeps record of user accounts and their properties – authorization and connection parameters. Routing of connection and accounting messages between servers and clients is provided by RADIUS proxies. This situation occurs when multiple RADIUS servers are used within the same network, or when RADIUS components from different vendors are used. Proxies can be chained, which, in turn, may result in somewhat ambiguous role distribution between components.

The sequence of events triggered by reception of a connection request from the network accessing client begins with the RADIUS-enabled NAS creating an Access-Request Message and sending it to the RADIUS server. Server then evaluates the message and, if required, sends the Access-Challenge message (requiring more data on user) to the access server, to which the access server responds with a new Access-Request message. RADIUS server accesses user account database, verifies user credentials and sends Access-Accept or Access-Reject message back. Upon receiving the message, if the connection is approved, completes the connection procedure and sends Accounting-Request message to the RADIUS server, to which it responds with the Accounting-Response message.

4. RADIUS MESSAGES

RADIUS components communicate by six types of RADIUS messages, all sent by UDP protocol on ports 1812 (authentication) and 1813 (accounting) by default. Clients use a dynamically allocated UDP port for both (in most cases this is configurable). Older versions use ports 1645 and 1646, respectively. TCP is not used. Access-Request type of message carries information that identifies the network access client, credentials for authentication and optional special requirements. Once received by a RADIUS server, it is checked whether it comes from a known RADIUS client. Access-Challenge message type is the server's response when additional information about the accessing client is needed. Access-Accept informs the client that the user is authorized and authenticated, while Access-Reject denies the connection (e.g. if the account is not active). Accounting-Request and

Accounting-Response are exchanged after the connection is approved.

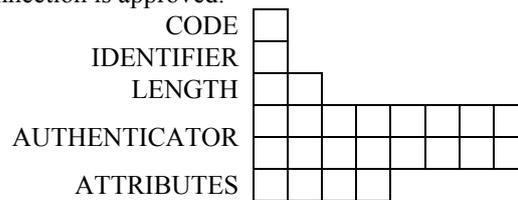


Figure 2. RADIUS message format

RADIUS messages are sent using UDP where each UDP message contains one single RADIUS message. RADIUS messages have common structure, as shown in Figure 2.

Code (1 byte) indicates RADIUS message type. Identifier value is created by the sender; this field enables the client (or the proxy) to match the responses with respective requests. Length field indicates the length of the entire RADIUS message, while Authenticator carries information about the RADIUS client (ensuring that client and server share the same Shared Secret) [4]. Attributes field is of variable size and contains attributes related to the specific user (e.g. authentication, authorization, information, configuration details for the messages etc). Attributes have the Type-Length-Value form (with the exception of vendor-specific attributes) and their order needs to be preserved if the message has multiple instances.

5. TRAFFIC AND SECURITY ISSUES

Due to interception and analysis susceptibility, RADIUS traffic needs to be secured, which includes Strong Shared Secrets, Message-Authenticator Attributes and Internet Protocol Security (IPSec). Strong Shared Secret authenticates RADIUS messages using the Authenticator field in the response message header and encrypts attributes. RFC 2865 recommends full 128 bit information entropy. If keyboard characters (5.8 bits of entropy) are used, a random sequence should be no less than 22 characters long. Incoming Access-Request messages are not cryptographically verified by default (only the sender's IP address is verified), thus can be spoofed. To avoid this RADIUS server can require Message-Authenticator attribute in order for data to be confidential across complete RADIUS message, IPSec should be implemented using Encryption Security Payload (ESP) and algorithms like Triple Data Encryption Standard (3DES). Possible attacker is, in this way, forced to decrypt IPSec protection of the message prior to analyzing its contents.

6. IMPLEMENTATION MODELS

Depending on network infrastructure and different needs, RADIUS server may be implemented in different manners. One of the things that should be seriously taken into account is the type of the software installed in the network. Whether it is about Open Source solutions, Windows, or any other solution, the best help one can get is to have a homogenous network. The biggest problem arises when trying to add RADIUS authentication to the existing Windows infrastructure. Slight differences in a way that RADIUS connects to Open LDAP, or Microsoft Active Directory user database make this task very difficult.

One implementation involves completely Open Source solutions like Open LDAP as user's database, FreeRADIUS as RADIUS server and any access point that supports this kind of user authentication. When using this configuration, some users may experience problems after the installation of Microsoft Windows XP Service Pack 2 (SP2), where Protected Extensible Authentication Protocol (PEAP) connection does not authenticate successfully. This failure occurs during an authentication attempt to a third-party Remote Authentication Dial-In User Service (RADIUS) server. The cause of this problem lies in a different method that third-party RADIUS server uses to calculate the Extensible Authentication Protocol (EAP) Type:Length:Value format (EAP-TLV) id than the method that Windows XP uses [5].

Another use case would involve Microsoft Active Directory as LDAP users database, Wireless access points that support RADIUS authentication and finally Microsoft Internet Authentication Service

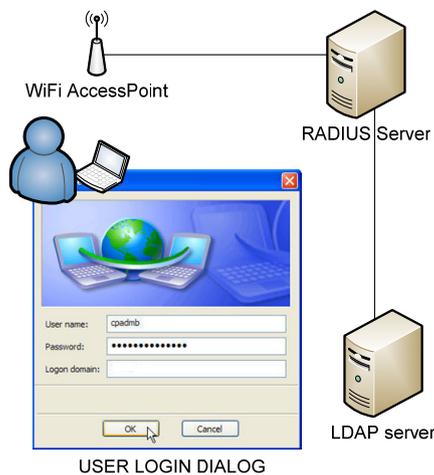


Figure 3. Simple RADIUS implementation

(IAS) in Windows Server 2003, or new Network Policy Server (NPS) in Windows Server 2008 as a RADIUS instance. As described in Figure 3. After the client connects to access point, login dialog should be presented, so the user can enter their credentials. Those credentials are encrypted and sent via IAS or NPS RADIUS server to Active Directory (LDAP) for authentication.

In this connection model, Linux users reported problems regarding the login dialog. Some Linux distributions do not show login dialog at all, denying

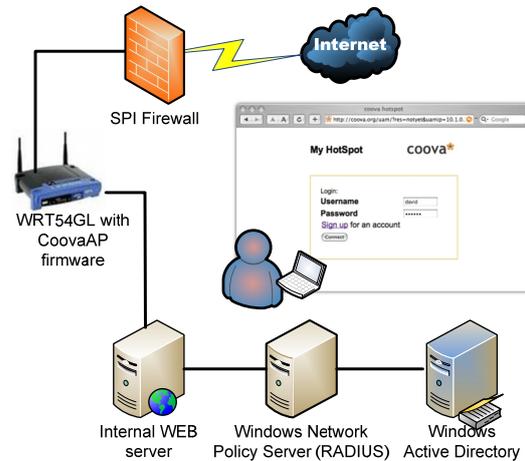


Figure 4. Full RADIUS implementation with Captive Portal

the user Wi-Fi access.

In order to avoid instantiation of a login dialog and any other problems connected to cross platform use, captive portal must be used. This portal is a simple web page that will be presented no matter what platform is used.

7. UNIVERSAL SOLUTION

The key for successful user authentication in networks which include both Linux and Windows Servers and Clients is the use of so called "Captive Portal". The Login dialog's been replaced with a CGI or PHP script that resides on a web server (shown in Fig. 4.) After successful connection to an Access Point, and immediately after starting any Web browser, the user is redirected to a web page, hosted on another web server which asks for user's username and password. That way, no login dialog's been activated and login process is Operating System independent [6].

The only problem in this constellation is that too many servers are involved in a single user authentication process. Single request ends up at web server, RADIUS server, LDAP server and back. DHCP server is also involved, since after initial association with access point user gets one IP address, to keep him for going out of the so called "garden". After the access's been granted, DHCP server delivers new valid IP address to allow user internet access.

To simplify login process it is useful to have access point, web server and DHCP server at one place. That's where customized firmware may be used. Linksys's WRT54GL is the most customizable Wireless Router ever built. Its own firmware is under GPL license, so there are various distributions that can be uploaded into device to suite specific needs. In this case the distribution of Open WRT -White

Russian firmware called CoovaAP is perfect solution.

includes multiple accounts that have to be created, to

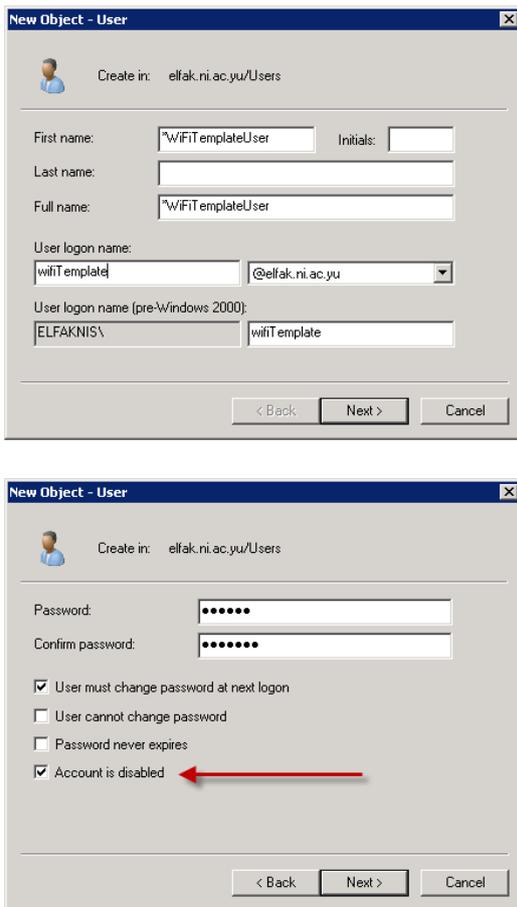


Figure 5. Template User Account

Not only does it have built in web server, it already has several pre built login CGI scripts that can be customized. That way, after the access point association, user's been internally redirected to a web server with IP address from local DHCP server, and after the user enters credentials, RADIUS server's been contacted.

This setup works very well when Free RADIUS and Open LDAP are used, but connection to an existing Active Directory infrastructure can be a problem, especially when connecting to the new Windows Server 2008.

Since the typical situation includes already formed LDAP base with user account, and RADIUS comes as an extra it is necessary to connect RADIUS to existing infrastructure. In order to authenticate the user through Active Directory, several tweaks must be made. These tweaks are not obvious and are the result of excessive research.

8. CHANGES IN ACTIVE DIRECTORY

To authenticate users from Active Directory, several preparations have to be done. First, new group WiFiUsers has to be created. Only members of this group will be authenticated. Since the typical situation

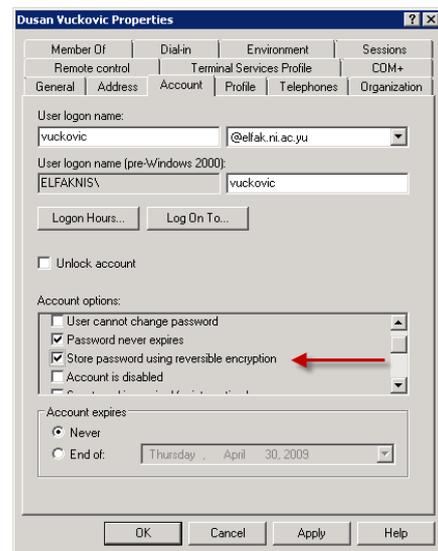


Figure 6. Reverse Encryption Filed

simplify the user accounts creation process, one template account should be created.

The creation of the template account is done in the exact same manner like any other user account with one slight difference. Fig. 5 explains the naming convention with asterisk in front of the account's name, and account disabled checkbox which has to be checked. This way, simple right click and copy option over the template account will make copy which will require only basic data to be filled, and the account will be automatically member of designated Wi-Fi Users group.

After the creation of new user account, one more step is of utmost importance. All user passwords must be stored using the reverse encryption process. This option, located in user account properties, Account tab, shown in the Fig. 6, must be turned on in order to interpret received password from Network Policy Server.

9. NETWORK POLICY SERVER CONFIGURATION

There are certain steps one should follow when configuring Network Policy Server. First and most important is to add new RADIUS client, so the Server may expect RADIUS messages from that IP addresses.

Fig. 7 illustrates setup steps for one new client, with friendly name WiFi M1. Its IP address is entered and shared secret which has to be the same as in CoovaAP firmware. This is the password AP and NPS uses to identify themselves.

One final step is to create network policy that will allow only members of one Active Directory group to be authenticated. Fig. 8 illustrates creation of one network policy that does that. Also, regarding the

authentication method used, only CHAP should be

10. CONCLUSION

Although user identification process looks like very simple task it is far beyond that. Without the use of expensive third party applications, and along with difficulties of incorporating this system into existing network infrastructure, it requires lots of man hours to make it work. Numerous different configurations exist, and are followed with numerous problems. This paper is intended to help implement user authentication in public networks where diversity in Operating Systems and client programs is strongly encouraged.

Proposed implementation clarifies the setup configuration in public environment where user accounts are stored in Microsoft Active Directory 2008, and authentication is done by using Network Policy Server. The idea was to unify the login process so it'll be platform independent. Even though the credentials check process is done exclusively by Microsoft Software, Access Points use GPL Linux Software and solution for credential forwarding is proposed in a form of CoovaAP firmware. Another optimization is the existence of embedded Captive Portal on Access Point which increases efficiency by removing web server from equation.

This configuration gives more flexibility to RADIUS as de facto standard in user Authentication, Authorization and Accounting. Combined with new powerful solutions implemented in Microsoft Windows 2008 Server, authentication of wireless users will become more secure, easier to implement and faster.

11. REFERENCES

- [1] C.Rigney, S.Willens, A. Rubens, "Network Working Group, RFC2865", June 2000, pp. 22-62
- [2] C.Rigney, "Network Working Group, RFC2866", June 2000, pp. 10-23
- [3] J. Davies, *Deploying Secure 802.11 Wireless Networks with Microsoft Windows*, Microsoft Press, 2004, pp. ch4pg1 – ch4pg28
- [4] J. Davies, *Windows Server 2008 TCP/IP Protocol and Services*, 2008, pp. ch17pg1-ch17pg30
- [5] Microsoft Knowledge Base, article KB885453, <http://support.microsoft.com/kb/885453>
- [6] S. R. Fitri, H. Syarif, "Integrating Web Server Applications With LDAP Authentication: Case Study on Human Resources Information System of UI", *Communications and Information Technologies 2006. ISCIT '06. International Symposium on*, Oct. 18 2006-Sept. 20 2006, pp. 307-312

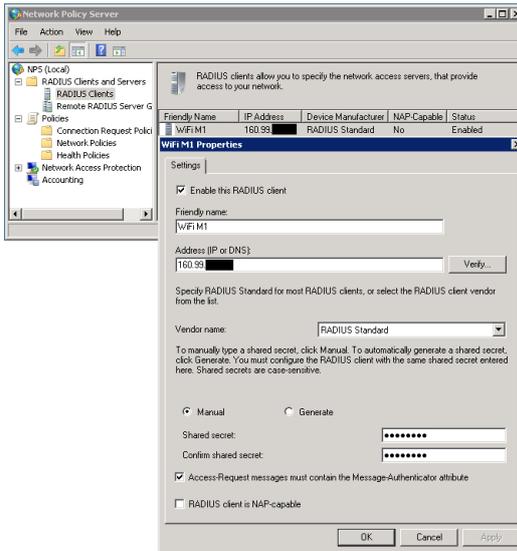


Figure 7. Adding New Client in NPS

enabled, and not PAP, MS-CHAP and MS-CHAP v2.

This should conclude the configuration process. After this, if everything is done right, user credentials

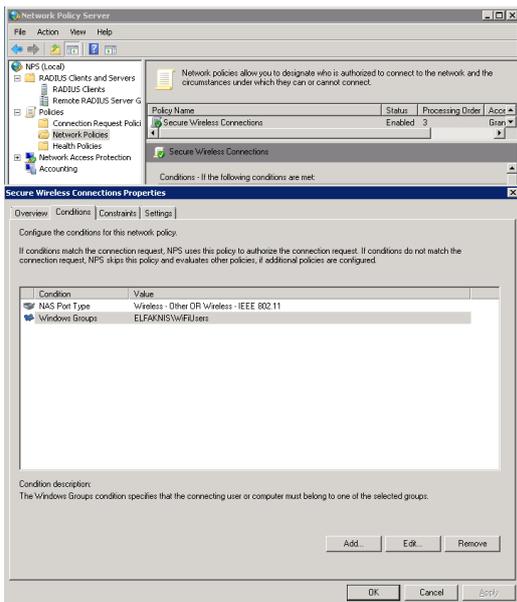


Figure 8. Network Policy Creation

will be forwarded to NPS which acts as middleware between access point and backend Active Directory Server.