

INVESTIGATING THE BUSINESS VALUE OF
UNIFIED HOTSPOT SOLUTIONS FOR HOSPITALITY
AND HOTELS

A case study of holiday apartment agency

Vladislav Alekseev

Bachelor's Thesis
School of Business and Culture
Degree Programme in Business Information Technology
Bachelor of Business Administration

2016

School of Business and
Administration
Bachelor of Business Administration
Information Technology

Author	Vladislav Alekseev	Year	2016
Supervisor	Johanna Vuokila		
Commissioned by	Lapland University of Applied Sciences		
Title of Thesis	Investigating the business value of "Unified Hotspot solutions for Hospitality and Hotels."		
Number of pages	43		

Nowadays, many people cannot imagine their lives without the Internet. Some people use it for leisure, others for doing business, but whatever they use the Internet for, all of them need a stable and well-secured access to the Internet. It is extremely important, while people are spending time on vacation, in hotels or apartments. For the owners of such business it is also necessary to provide the guests with the Internet connection. One of the most popular systems used by the owners is Hotspot – secured Wi-Fi access point. Exploring the technologies of Hotspot building and creating of such system are the objectives of this study. Reaching these objectives as a goal was inspired by current situation with Wi-Fi access in case company, which needs some improvement.

Data for this research was collected with the help of action research and case study. These methods allowed to concentrate on both – the specific problems and the theoretical part. Moreover, the most of company guests were surveyed.

"The Unified Wireless Hotspot Solutions" is an example of how the owners of various public institutions can improve their business and attract more customers. UHS is a convenient and easy-to-use solution for owners of Hotels, Holiday Apartments, various Hostels, Cafes and other places with high attendance where internet access is an important part of the business and customers` comfort. With UHS, any user can expand his Hotspot network easily and improve the service quality , without being an expert in IT field.

Key words: Hotspot, APs (Access Points), OpenWRT firmware, Open Source, Public Networks, Remote Router Management

CONTENTS

FIGURES AND TABLES.....	5
SYMBOLS AND ABBREVIATIONS	7
1 INTRODUCTION	8
1.1 Motivation and Background	8
1.2 Scope and Objectives	8
1.3 Thesis Structure.....	9
2 RESEARCH QUESTIONS AND METHODOLOGY	10
2.1 Research Questions	10
2.2 Research Methods.....	11
3 INTRODUCTION TO UNIFIED HOTSPOTS SYSTEMS	12
3.1 What is Unified Hotspots Systems.....	12
3.2 General Audience and User Requirements	12
3.3 Benefits of UHS Using	17
3.4 Case Company.....	17
4 DEVELOPMENT ENVIRONMENT AND TECHNOLOGIES, REQUIRED EQUIPMENT.....	18
4.1 Linksys WRT54GL.....	19
4.2 Main Server on Ubuntu Server 16.04 Operation System.....	20
4.3 FreeRadius Server.....	21
4.4 MySQL Database Usage	24
4.5 PHP Script Language Usage	25
4.6 Daloradius Application Usage.....	26
4.7 System Security and OpenVPN Routing.....	27
4.8 ChilliSpot Package.....	28
5 DEVELOPMENT AND IMPLEMENTATION	29
5.1 Access Point Design and Implementation.....	29
5.2 DD-WRT Firmware Installation and Configuring	30
5.3 FreeRADIUS Server Configuration	31
5.4 Installing and Configuring MySQL Database	32
5.5 Configuring Freeradius	33
5.6 Configuring DaloRADIUS.....	34
5.7 Hotspot Login.....	36
5.8 ChilliSpot Configuration	37

6 CONCLUSION.....	41
BIBLIOGRAPHY	43

FIGURES AND TABLES

- Figure 1 Internet Usage Questionnaire
- Figure 2 Age of Users
- Figure 3 Internet Usage
- Figure 4 Most Popular Devices for Internet Access
- Figure 5 Guests Succeed with Speed and Strength of the Wi-Fi Connection
- Figure 6 The Unified Hotspot System
- Figure 7 Linksys WRT54GL
- Figure 8 Authentication and Authorization Operations in the RADIUS Server
- Figure 9 Accounting Processes
- Figure 10 DaloRADIUS GUI
- Figure 11 OpenVPN Principle
- Figure 12 The Scheme of ChilliSpot Functioning
- Figure 13 Wi-Fi Plan, First and Second Floors
- Figure 14 The dd-wrt.v24_std_generic.bin Firmware Uploading
- Figure 15 Database Table
- Figure 16 Successful Test of NGINX Server
- Figure 17 Running Freeradius Server
- Figure 18 Running NGINX Server
- Figure 19 DD-WRT General Network Settings
- Figure 20 Overview
- Figure 21 ChilliSpot Configuration

Figure 22 Scheme of Components Communication Inside of UHS

Table 1 Minimum Hardware Requirements for the UHS Server

SYMBOLS AND ABBREVIATIONS

UHS	Unified Hotspot System
OSS	Open Source Software
SPI Firewall	Stateful Packet Inspection Firewall
OpenVPN	Open Virtual Private Network
CPU	Central Processing Unit
RAM	Random-access memory
SSD	Solid-State Drive
SSH	Secure Shell Protocol
WPA	Wi-Fi Protected Access
SPI	Serial Peripheral Interface
DHCP	Dynamic Host Configuration Protocol
Telnet	Teletype Network
WinSCP	Windows Secure Copy

1 INTRODUCTION

In this chapter motivation, background, limitations are described. The sources are reviewed. Scope and objectives are presented as well.

1.1 Motivation and Background

As a trainee in a holiday accommodation agency, I am engaged in a network security. Today, the hotel business cannot dispense with the provision of internet connection to their customers, if the representatives of this business want to be competitive. That, in turn, raises a number of problems related to the organization of the Internet connection, and with the organization of the safety of this compound.

Hence, there is my personal motivation. Creating the optimal solution for networking in hotels gives me the necessary understanding of the already existing technologies in this field.

Therefore, I decided to explore this subject in detail. This study aims to describe the optimal solution for the network in the hotel business, as well as using technologies.

1.2 Scope and Objectives

This study takes into consideration the system of wireless networks in hotels and apartments. However, this research focuses mainly on the creation of Hotspots and the benefits of their use in the hospitality business.

The main objective of this study is to explore technologies that allow to create so-called Hotspots. In this particular case, it means UNIX distribution called DD-WRT.

The second objective is the description and justification of the Unified System Hotspots use and make a description of both the technology and the process of creating such a system.

1.3 Thesis Structure

Chapter 2 of this thesis describes the research questions and methods. Chapter 3 explains the essence of United Hotspot system and benefits of its use. In addition, there is information about the case company and the description of used technologies and devices. Chapter 4 narrates the process of creating such a system. Chapter 5 is the conclusion, which summarizes what has been stated in the thesis.

2 RESEARCH QUESTIONS AND METHODOLOGY

This chapter describes the research questions, which means, that questions are described from the perspective of how they can help to achieve the goals of the research. In addition, the research methods are reviewed as well.

2.1 Research Questions

The thesis research addresses to three research questions. These questions are listed below:

1. What is “Unified Hotspot”? What is the difference between “Unified Hotspot” and other traditional Hotspots?

This question enables the researcher to gain understanding of the topic. This question is also important because the case company will get understanding of the differences between traditional Hotspots and Unified Hotspots. By reading this research, the customer will understand what benefits he can get from this system.

2. What is the Open-Source software and DD-WRT firmware?

The answer to this question explains why it is preferable to use Open-Source software in Unified Hotspots and how it will help in developing... **чего?**. In addition, the reader will understand the benefits of DD-WRT firmware for the AP.

3. What is the business value of adopting Unified Hotspots? How can Unified Hotspots contribute to business value in the case company?

This question will explain how the Unified Hotspots system may impact on case company and how this system will promote the business growth. As well as what the targeted clientele is for the particular system.

Answers to these questions provide the necessary theoretical basis for creating Hotspot system. In addition, the answer to the third question leads to practical results of such a system, which is necessary for this study.

2.2 Research Methods

The first method used is a case study. This method allows to use the vast types of informational sources. Additionally, the method allows to consider the topic of this research with different perspectives that is necessary while studying both the technical side of creating a Hotspot system and the possible benefits for business. (Denscombe 2010, 30 – 31.)

The second used method is an action research, which is applied to this research for finding a way to solve a particular problem. This method is relevant since the research is conducted to generate an implement plan for a new technology. (Denscombe 2010, 6). The analysis of various literature sources is utilized to collect required information for the thesis work. In addition, an empirical study is also applied – the collected data from results of Hotspots installation is included in this research. The quantitative research method is used to measure the business value of Unified Hotspot System in business. Mostly this is a data from conducted surveys of the clients of holiday apartment agency.

3 INTRODUCTION TO UNIFIED HOTSPOTS SYSTEMS

This chapter contains the definition and idea of Unified Hotspot Systems. In addition, technical means needed for creating such a system are described. Moreover, this part of research contains the results of requirements and wishes of the users study, advantages of Unified Hotspot Systems, as well as information about a case company.

3.1 What is Unified Hotspots Systems

Unified Hotspot Systems is the idea of an optimal system of connection to the Internet in hotels / apartments / other places of recreation. The idea is a system of so-called hotspots, i.e. Wi-Fi access points, usually located in public places. (Melania 2016.) The system is structured as a single access point, but with different allowance for different users. The user has to pay for the internet - either physically, at the reception or with a credit card on the Web page of the Unified Hotspot Systems, then he gets a randomly generated password, that allows to use the Internet. The system can use multiple routers to provide a permanent Internet connection, for example, on different floors of the same building.

3.2 General Audience and User Requirements

The creation of any product for the market does not dispense with exploring the opinions of customers. Therefore, this part of the research was devoted to the opinion of users and benefits of Unified Hotspot Systems.

To explore the requirements of users for the Internet in hotels and private apartments a survey was made. With the help of a case company, interviewers distributed questionnaires among the company guests. These questionnaires were issued for 79 guests, responses were received from 58. An example of a questionnaire is shown below in Figure 1.

INTERNET USAGE QUESTIONNAIRE

Name and Address of the Holiday Apartment: _____; Number of guests: _____

<p>1. Year Group</p> <p><input type="radio"/> 18-25</p> <p><input type="radio"/> 25-35</p> <p><input type="radio"/> 35-50</p> <p>2. How often do you use the Internet ?</p> <p><input type="radio"/> Everyday</p> <p><input type="radio"/> Once a day</p> <p><input type="radio"/> More than once a day</p> <p>3. What do you like doing most online ? How often do you use ?</p> <p>(Put the following number near your answer: Everyday=1; Once a day=2; More than once a day= 3)</p> <p><input type="radio"/> Music, Video ___</p> <p><input type="radio"/> Gaming ___</p> <p><input type="radio"/> Social Networking (Facebook, VK.COM, Myspace), Instant Messenger (WhatsApp, SnapChat, Skype) ___</p> <p><input type="radio"/> News, Web browsing ___</p> <p><input type="radio"/> File Sharing ___</p> <p>4. What kind of gadgets for internet access did you use ?</p> <p><input type="radio"/> Laptop</p> <p><input type="radio"/> Tablet</p> <p><input type="radio"/> Mobile phone</p>	<p>5. Did you have any difficulties with Log In ?</p> <p><input type="radio"/> NO</p> <p><input type="radio"/> YES</p> <p>If, yes specify: _____</p> <p>6. If you use Wi-Fi, what room/place do you use it in ?</p> <p><input type="radio"/> Living Room</p> <p><input type="radio"/> Bedroom</p> <p><input type="radio"/> Dining Room</p> <p><input type="radio"/> Kitchen</p> <p><input type="radio"/> Balcony</p> <p>7. How you success with strength of the Wi-Fi signal ?</p> <p><input type="radio"/> Good signal in whole apartment</p> <p><input type="radio"/> Good signal, but sometimes connection was lost</p> <p>Specify in what rooms/places: _____</p> <p><input type="radio"/> Bad signal in whole apartment</p> <p>8. How you success with speed of the Wi-Fi connection ?</p> <p><input type="radio"/> Fast</p> <p><input type="radio"/> Good</p> <p><input type="radio"/> Slow</p>
--	---

Figure 1. Internet Usage Questionnaire

While developing the questions for this questionnaire were considered targets of the research. Because of needs to obtain from respondent the sufficiently clear answers, it was decided to choose structured questions, i.e. questions with a choice of response, therefore they allow respondent to reduce the time for an answer. In addition, this kind of questions does simplify the processing of the data, since the answers are already known. (Parasuraman A., 1991)

The first question refers to the age group of Internet users. The question is important, because knowledge of most active Internet users age group gives indirect information about anticipated activity of the guests. Therefore, it gives expectation concerning spent traffic, which heads directly to the cost of the new system. Answers take into account only the age groups from 18 to 50, because representatives of this age group mainly visit holiday apartments.

Second and third question have the same reason as first question. Revealing the frequency of Internet usage and what is the main reason for respondents to connect the Internet are important to find out what kind of hardware the owner

of apartments need and which Internet rate. Different purposes and frequency of use eventually require a different cost.

The fourth question provides researchers with information about needs in wireless connection. Usually, laptops have Ethernet cable port and for owners of the laptop, the apartments could have provided just with cables. But it is a rare situation, when such port presences on the mobile devices, therefore owners of smartphones or tablets definitely need a wireless connection. Another issue is a quantity of these owners, will it be significant enough to spend money for effective Wi-Fi system or not.

Questions number 5, 7 and 8 refer to the current situation with Internet in apartments and revealing the core of problems. Is there any problems with login or with the speed or strength. Analysis of the data from these questions is performing with results from question number 6, which provides with information concerning the places, where Wi-Fi is mostly using by the guests. Such data helps to find out is their connection between low and weak Internet connection and router location.

Based on results of this questionnaire following charts were created. These charts represent basic user requirements.

Figure 2 presents the age groups percentage of Internet users among the guests. This figure was created in the form of a bar chart.

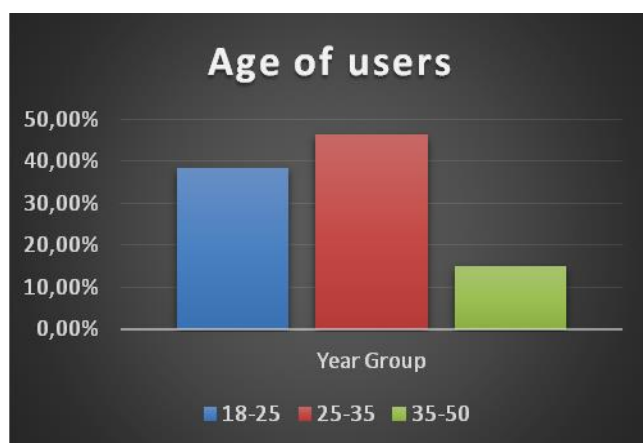


Figure 2. Age of users

As seen from this chart, almost half of users are people 25-35 years old and almost 40% of people 18-25. That is the most active age group of Internet users. (Pew Research Center, 2013)

The following statistics provide information about the purpose of Internet use in percentages. Appendix 3 is prepared as a radial diagram.

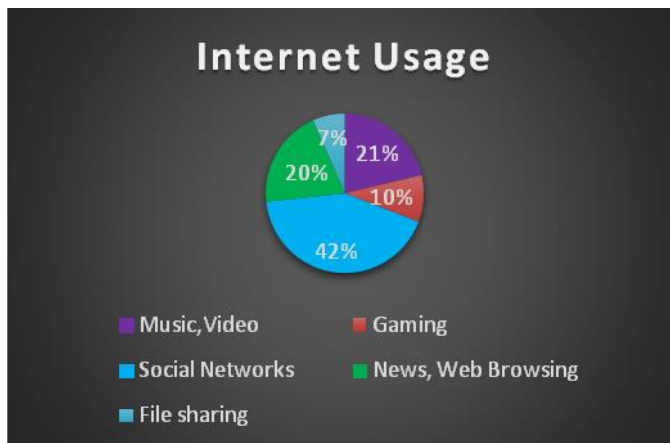


Figure 3. Internet Usage

This chart shows that 62% of the guests use internet connection for social networking, browsing and reading the news. These goals do not require large traffic costs, and therefore the apartment owner could choose not the most expensive tariff Internet connection. Appendix 4 is a chart showing the percentage of the most popular devices for Internet usage. Because it is important to find out how necessary is Wi-Fi connect for the guests.

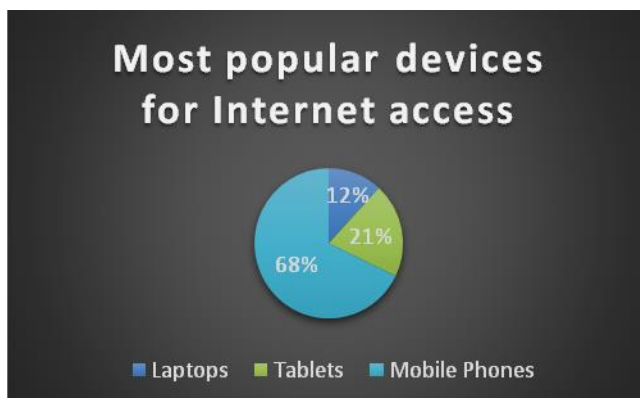


Figure 4. Most popular devices for Internet access

Based on this chart it is clear that use of Wi-Fi connection is necessary. Despite the fact that most of the guests using laptops, which are usually equipped with an entry for Ethernet cable, 32% of users are using mobile devices and tablets which mainly using wireless Internet connection methods.

Nevertheless, to justify the creation of UHS, results of research about satisfaction with the Internet connection in a variety of apartments were needed. Figure 5 shows a bar chart the of customer evaluations of Internet connection speed in different rooms.

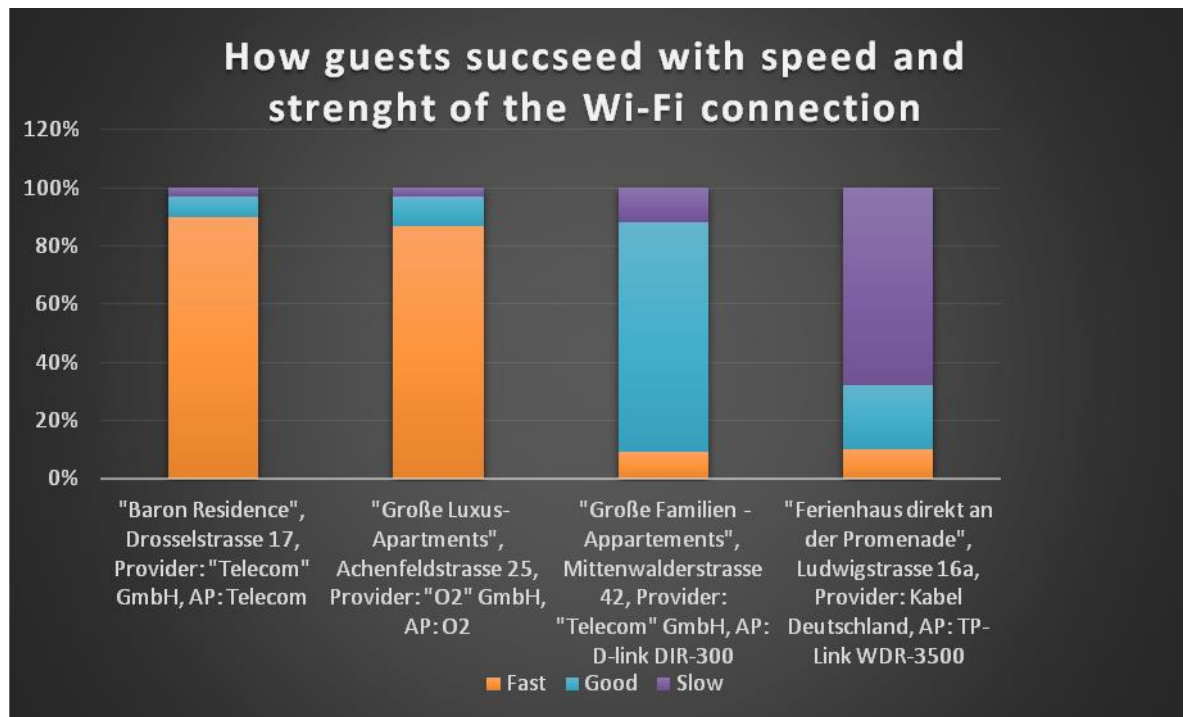


Figure 5. Guests succeed with speed and strenght of the Wi-Fi connection

The results of this part of the survey point to certain problems with the Internet connection, as not all apartments are matching the guest's requirements about speed and strength of the Wi-Fi connection. The main difference between the first two apartments, i.e. "Baron Residence" and Apartments "Große Luxus-Apartments" from the others is that they are one-storied. "Große Familien-Apartments" and "Ferienhaus direkt an der Promenade" each have two floors. Only one router is distributing Wi-Fi connection inside each of these apartments and it is clear that not in all parts of the apartment signal and speed meet user requirements.

3.3 Benefits of UHS Using

The above statistics show that the users need quick and easy access to the Internet, preferably on all floors of the hotels / apartments. In turn, for the owner of such business, it is important to be able to restrict access to the Hotspot and provide only to customers. In addition, it means to have an ability to restrict traffic and not to give access to restricted resources. Moreover, the owner should be able to do it simply and remotely.

The main advantages of the Unified Hotspot systems are the ease of use and connectivity. Chapter 4 in detail describes the process of creating such a system, and it is simple enough for even a person not versed in network settings. In addition, the system provides a number of useful properties, such as restricting access to certain websites, providing access throughout the hotel/ apartment and limiting access to persons who are not clients of the organization.

3.4 Case Company

Case company is located in Garmisch-Partenkirchen, Germany, and offering various holiday apartments in the town. Until recently, the Internet was provided through a password to a specific router in each apartment, which explains the company's desire to create a unified system of the access to Internet and to facilitate technical maintenance.

4 DEVELOPMENT ENVIRONMENT AND TECHNOLOGIES, REQUIRED EQUIPMENT

In this chapter, all of the major aspects such as hardware and firmware components of the system will be described. The whole Unified Hotspot System is based on just two parts which provide a lasting communication between user and hotspot system. The first it is an Access Point with pre-installed DD-WRT firmware, it serves as a special secure gateway and second, it is a network server which has all necessary information for the user login procedure. The system functioning starts from a modem what every customer should have for the internet access, that will give an ability to connect his Hotspot access point through his private network to the UHS server.

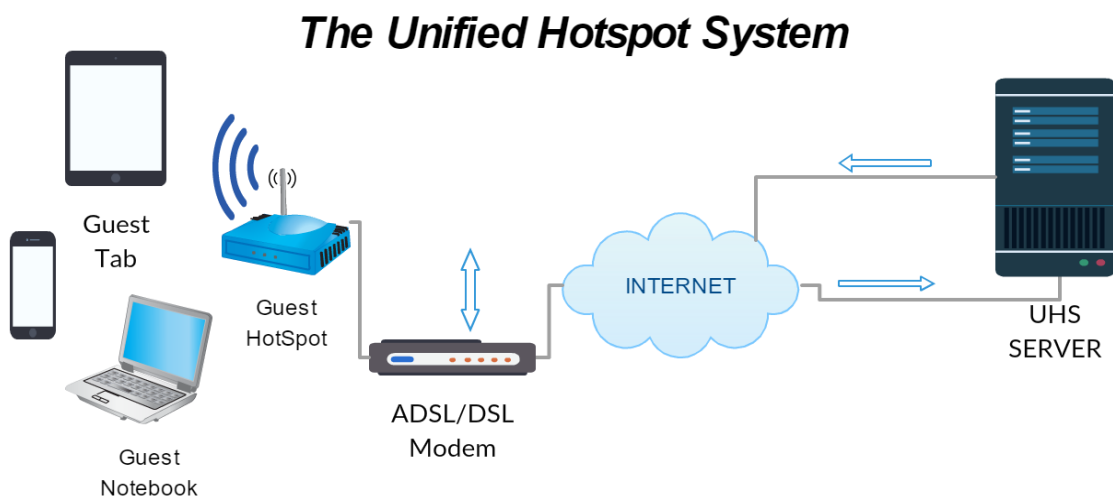


Figure 6. The Unified Hotspot System

Figure 6 shows the communication between Hotspot user and UHS system. Guest connect his device to the Hotspot, then access point redirects him to login the web-portal which is located in UHS server, after successful authorization server allows AP to grant the user with an Internet access. This method of authorization is more secure and allows to the customers provide their guests with internet access without pre-shared key, what may be the reason for the unauthorized access to the private network.

4.1 Linksys WRT54GL

The Access Point play a general role in User-UHS connection. The main AP requirement is that the Wi-Fi router should be supported by dd-wrt firmware. At the present time, the Linksys WRT54GL router it is a most reliable and trouble-free device. It was created specially for the clients who prefers to use so called non-cutted router firmware, it is cheap and quite flexible in usage. The main criteria for choosing a router as a Hotspot AP were:

- Comparably low cost
- Availability of easy OSS installing
- Possibility to backup the OS, in case of accident or incorrect installation
- Decent security
- Possibility to connect via different devices, such as printers, PC, laptops, smartphones and tablets
- Opportunity to expand device functionality
- Administration through SSH protocol



Figure 7. Linksys WRT54GL

Linksys WRT54GL fulfills all these criteria. The cost is about €70, it supports configuration of the OSS, browser-based utilities and Linux distributions. It is also has an SPI firewall, which is useful for UHS security. In addition, there is an

opportunity to configure the router through the SSH protocol, it means that the system administrator can change the settings or apply firmware updates remotely.

4.2 Main Server on Ubuntu Server 16.04 Operation System

The second component of UHS it is the main server. The Ubuntu Server 16.04 operation system is used as a general operation system. It is a well-supported and secure Linux-common OS based on Debian and has a wide range of benefits such as ability of remote administration via SSH protocol, Device Mapper Multipathing which can be used in UHS system expansion, high data protection and OpenVPN tunnel support for secure User-Internet, Router-Server communications. The main server requirements separates on two criteria it is hardware requirements which may vary from the quantity of customers and software requirements.

Table 1 Minimum hardware requirements for the UHS server

A type of the Server	CPU Intel x86, AMD64 or ARM processor architecture	RAM	SSD
Standard	1 GHz	512 MB	1 GB
Minimal	300 MHz	192 MB	700 MB

Table 1 presents minimum hardware requirements for the system server (Ubuntu Server Guide 2016). These values will be sufficient for a small network, for instance, for 5 Hotspot Access Points, but all these parameters should be increased depending on quantity of hotspot users.

Required software for the UHS server are:

- FreeRadius server
- OpenVPN server
- MySQL database and MySQL server
- PHP5

When all parts of the server are properly configured and all requirements and recommendations are compiled customer will get fast and productive server able to serve thousands of customers.

4.3 FreeRadius Server

Most of the servers in the public networks contains Radius server, which gives an ability to maintain user profiles in a central database which every remote server can share. FreeRadius it is a RADIUS server with open source code which is a free alternative for commercial RADIUS servers. This server can work on operation systems which have small memory and servicing several millions of users, it is fast, flexible and customizable system. Server with Radius – it is the central controller, whose job is to allow or deny access to the Wi-Fi network for the pair login/password on behalf of the account. The work of FreeRadius server based on AAA protocol - Authentication, Authorization and Accounting (The FreeRadius Technical Guide 2014, 8-9).

The main Authentication and Authorization operations in the RADIUS server are:

- receiving a network access request including user credentials (username and password or security certificate) from the NAS
- Checking information using authentication schemes such as CHAP, EAP or PAP for the user's credentials verification
- Returning one of the responses to the NAS (Access-Reject, Access-Challenge, Access-Accept). Where Access-Reject - user denied access to network; Access-Challenge – request an additional information from the user; Access-Accept – user have access to the requested network
- Checking information using authentication schemes such as CHAP, EAP or PAP for the user's credentials verification
- Once NAS give an internet access permit to the user, an Accounting operation starts (Rigney, Willens, Rubens & Simpson June 2000, 17-23).

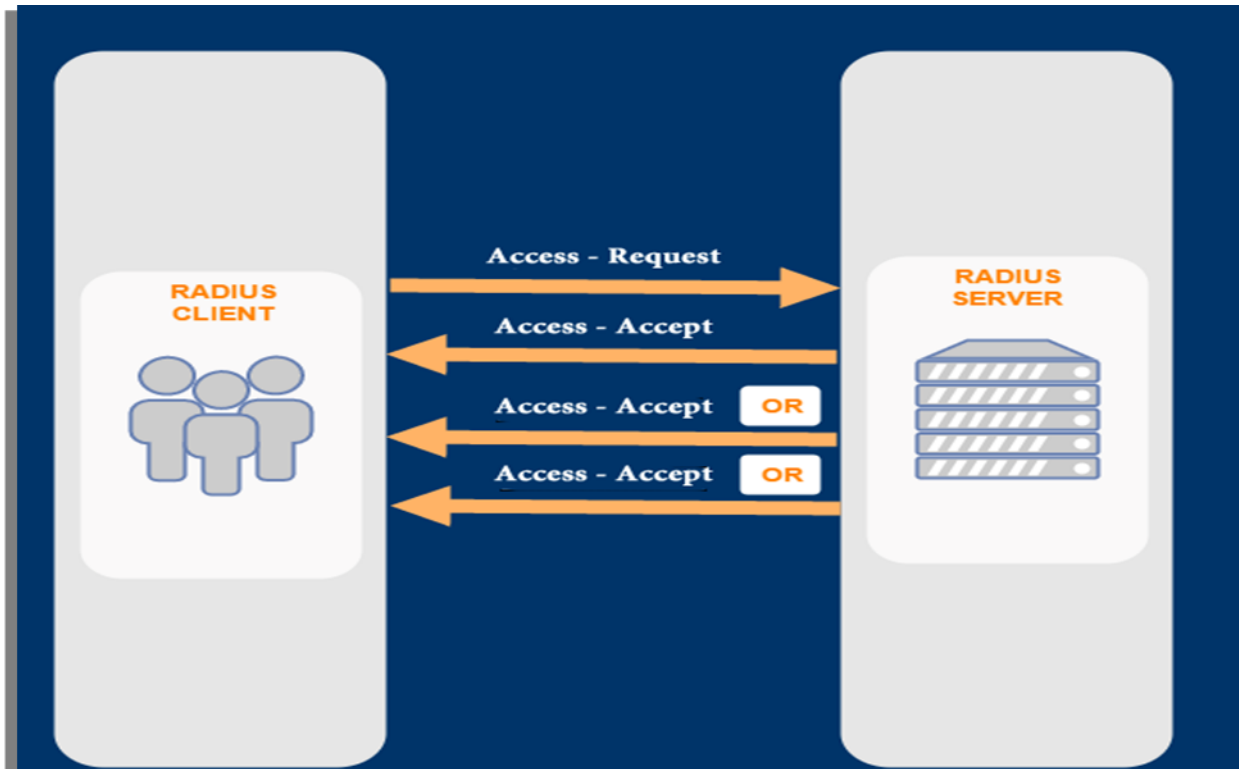


Figure 8. Authentication and Authorization operations in the RADIUS server

The main Accounting operations in the RADIUS server are:

- Accounting-Response – packages sent by FreeRadius server to the client to report that Accounting-Request has been received and recorded successfully.
- Accounting-Response – packages sent by FreeRadius server to the client to report that Accounting-Request has been received and recorded successfully.

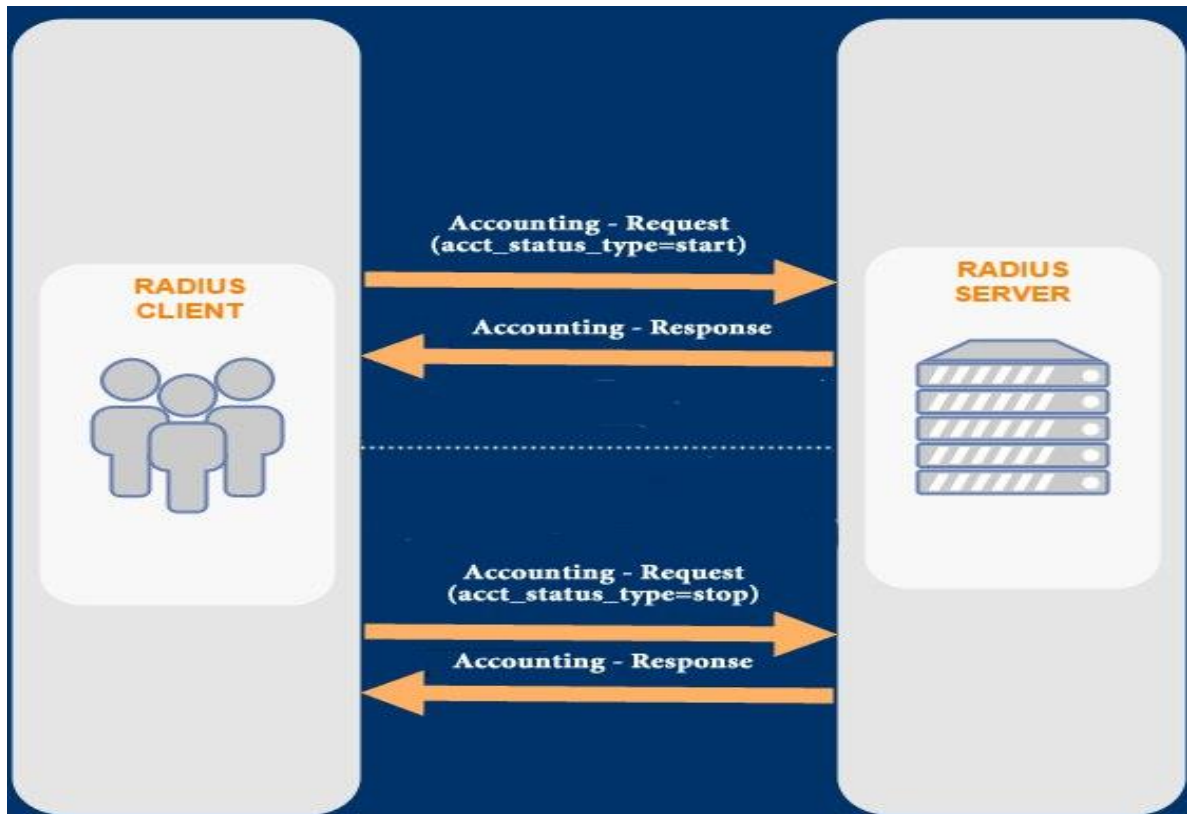


Figure 9. Accounting processes

Figure 9 shows a detailed example of the FreeRadius Accounting operations. In the connection between Radius Client and Radius Server every Accounting-Request should be accompanied by the special attributes and values. FreeRadius attributes contains specific authentication, authorization and accounting details for the client's request and server's response.

List of possible attributes		List of possible values	
40	Acct-Status-Type	1	Start
41	Acct-Delay-Time	2	Stop
42	Acct-Input-Octets	3	Interim-Update
43	Acct-Output-Octets	7	Accounting-On
44	Acct-Session-Id	8	Accounting-Off
45	Acct-Authentic	9-14	Reserved for Tunnel Accounting
46	Acct-Session-Time	15	Reserved for Failed
47	Acct-Input-Packets		
48	Acct-Output-Packets		
49	Acct-Terminate-Cause		
50	Acct-Multi-Session-Id		
51	Acct-Link-Count		

Table 1. Request Attributes in Accounting Operation

Table 1 contains the main set of accounting operation attributes.

- Accounting-Request package containing an “Acct-Status-Type” attribute with the value "start". NAS sent to the RADIUS server a command to run the user's network access.
- Accounting-Request package containing an “Acct-Status-Type” attribute with the value "stop". NAS sent to the RADIUS server a command to stop the user's network access (RFC2866 C.Rigney & Livingston June 2000).

4.4 MySQL Database Usage

The Unified Hotspot System it is complex work of various systems which are used together for providing permanent and reliable internet access for the user. Generally, UHS based on FreeRadius Server and for the proper server functioning several packages such as: MySQL Database, PHP and daloRADIUS application are required. Communicating with each other all these packages creates specified gateway to grant an authorized user with secured Internet access.

Database it is a structured collection of data, it stores various physical files with all needed information in separate tables. This kind of structure can significantly increase the speed of the system and the logical model of MySQL with an object such as databases, tables and rows offers a flexible programming environment (Oracle 2016).

Databases contain critical information about the client, users, different system data, all these files at stake if any malefactor may attack the file structure. It means, that the database security issue should be on the first place after package installation. There are some useful security recommendations for securing initial MySQL accounts:

- Provide all accounts with a password. The root accounts have all privileges in the system, if these root accounts have empty passwords, every user can connect to the MySQL server as root without a password and will get all privileges.
- Configure the operation system's firewall

- Change database privileges. Only administration accounts, for instance, root need to be granted the super, process, file privileges, other users should have only select, update, insert, delete privileges.
- Delete all history. During the installation processes, there is a lot of sensitive information that can be used by malefactor to obtain an access to the database.

System with user Authentication, Authorization and user Accounting needs a stable and fault-tolerant database where all necessary user information will be stored and will be available at any time. MySQL database plays a central role in FreeRadius server work, every action with FreeRadius client starts from reading databases.

4.5 PHP Script Language Usage

PHP – Hypertext Preprocessor

PHP it is a script language wide used for web application development, nowadays it is the most popular language in Hosting field through which a lot of dynamic websites being developed.

There are some advantages of PHP for the FreeRadius server:

- PHP can communicate with multiple database systems such as MySQL, PostgreSQL, Microsoft SQL Server
- It has automatized HTTP-header sending
- It works with cookies and sessions
- It can manage the files, which is uploaded to the server
- There is an ability to create GUI applications with PHP language
- Using PHP from the command line (The PHP Group 2016)

The advantages 4, 5 and 6 are an integral part of UHS. Before the user gets access to the internet through the FreeRadius server, he needs to pass authentication on the server. For this purpose, there is the main authentication web page where the user can put his credentials. The main page is written on

PHP language, which gives to the user a capability to communicate with FreeRadius server and upload various files or information. PHP language it is an universal language which can be used in most operation systems. Ubuntu 16.04 operation systems supplied without any graphical user interface, it means that in some cases where GUI is required user cannot manage the system or program in a proper way. Advantage 6 it is an example of flexibility PHP in usage. (The PHP Group 2016)

4.6 Daloradius Application Usage

Daloradius it is a FreeRadius web platform based on PHP script language which in UHS play the general role in communication between Administrator and Unified Hotspot Systems. Given web application it is a combination of abilities for MySQL database administrating and Hotspot managing. Daloradius has web graphical user interface, that helps to UHS operator make the system changes: add/delete users, manage the user databases, realize billing/ticketing system, setting the new Access Points without Ubuntu Terminal Using.

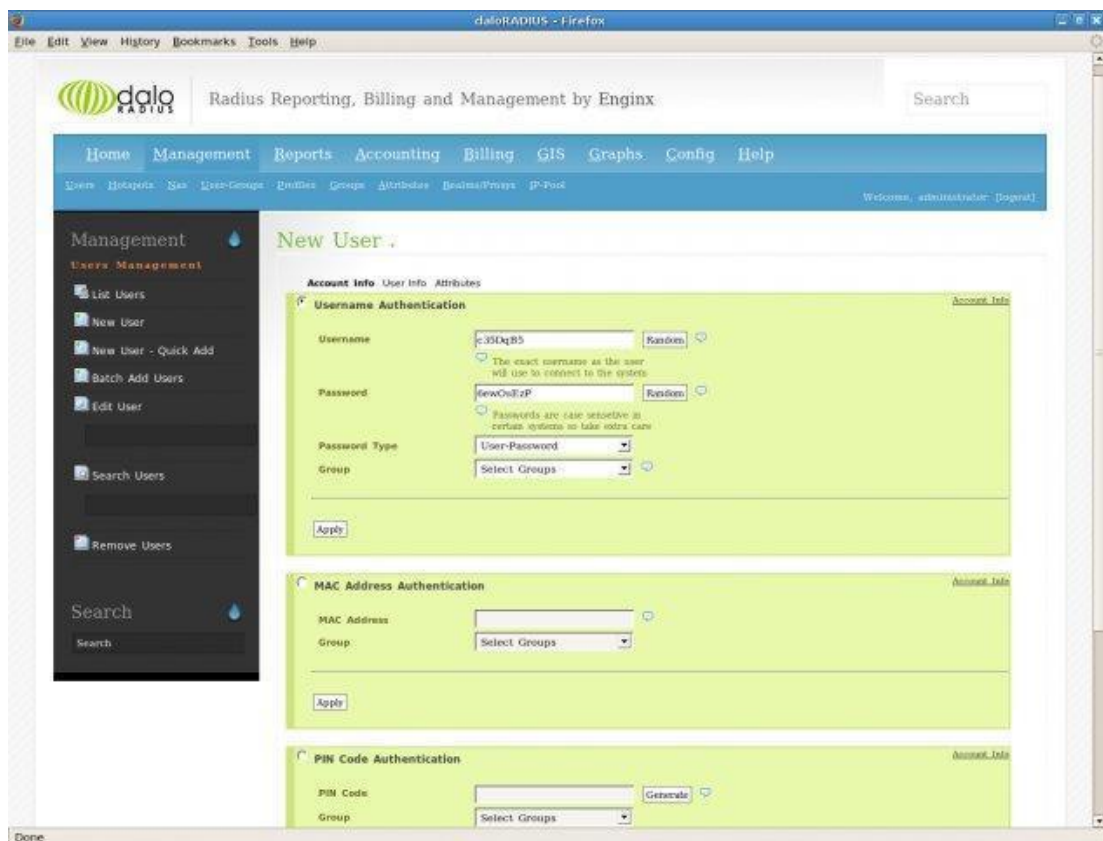


Figure 10. Daloradius GUI (Liran Tal's Enginx 2016).

4.7 System Security and OpenVPN Routing

Wi-Fi access points give the ability to receive an internet access in a short time from all devices which have a Wi-Fi module and special software (Phones, Tablets or Computers), Public APs clients don't need to use the Ethernet cords and other things to have an Internet connection. Security of this wireless connections has an essential meaning, while when the customers using any of APs they want to have secure and stable connection with no risk for their private information. Another important point, that not only AP's customer should have a secure connection, but also an AP's owner must be protected from unauthorized access to the network. In addition, for communication inside the system, the Hotspot router and FreeRADIUS server also should have a well-protected connection, because there is the risk of interception of information by a malefactor.

For that reasons, an OpenVPN technology is used in the Unified Hotspot Systems. This technology represents a special secure from point to point or, in our case, also a router-server tunnel. OpenVPN protects IP packages exchange between remote networks or hosts and users. All data which transfers through this virtual private network are encrypted by SSL or TLS cryptographic protocols. The tunnel system based on symmetric encryption, which means that both sides of the tunnel encrypt all traffic by sending special encryption and decryption keys

It gives highly protected and trouble proof data transmission inside the network. Next advantage is that an option to change the user IP address. When a client inside of the secure tunnel, his public ip automatically changes to the VPN IP, the OpenVPN server generates a new VPN IP for every user which is a great solution for private data protection. Furthermore, it helps UHS clients keep his private networks safe, because all data traffic is located in different tunnels. If some of the guests will break some Internet usage policies, especially will try to download any content with copyrights infringement, the owner of the access point does not bear any responsibility for the guest actions. It allows to avoid unpleasant situations when the owners of the Internet connections receiving

finer for copyright infringement or other unlawful acts in a public network (Hosner 2004).

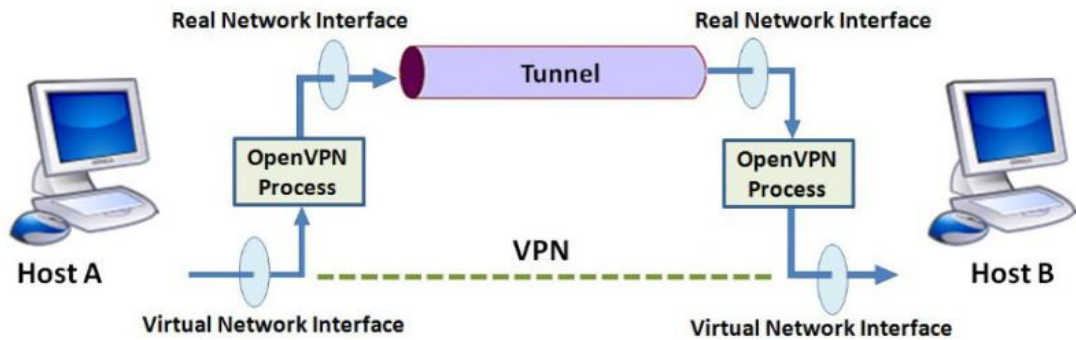


Figure 11. OpenVPN working principle

Figure 11 shows the working principle of OpenVPN tunnel in action. (viktor.net.wordpress.com)

4.8 ChilliSpot Package

ChilliSpot is an open source captive portal which is used for authenticating users of the WI-FI connection. This DD-WRT's pre-installed package allows to build a custom access controller which is connecting NAS (Access Point) with a FreeRADIUS server, sending and receiving authentication requests, granting users with an internet access. (chillispot.org).

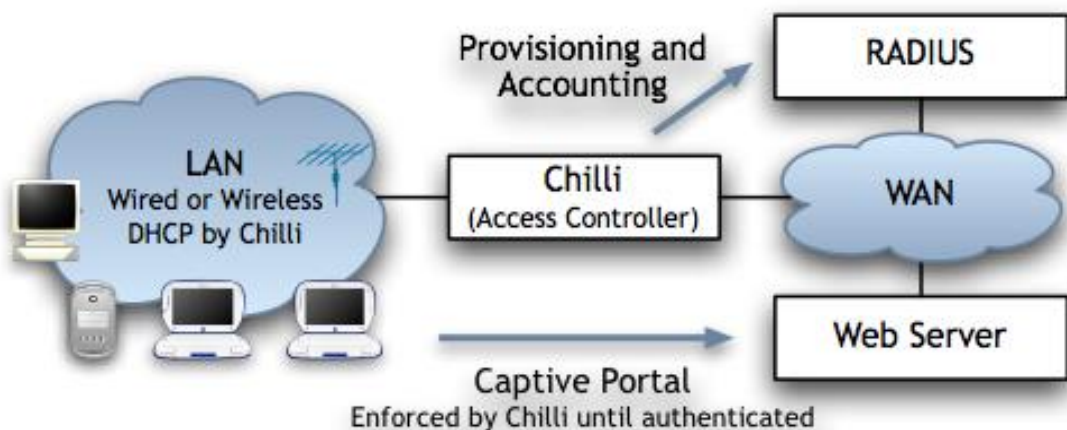


Figure 12. The scheme of ChilliSpot functioning (coova.org)

Figure 12 shows the work of Chilli Access Controller and how it is communicating with another UHS components.

5 DEVELOPMENT AND IMPLEMENTATION

This chapter describes the process of Unified Hotspot System developing and has set of recommendations which suggest how to make the network planning for the AP Access Points installation, how to install and connect all APs in union network, various firmware, hardware settings and configuration recommendations. Specifically, the installation and configuration of DD-WRT firmware on the router and installation of RADIUS server.

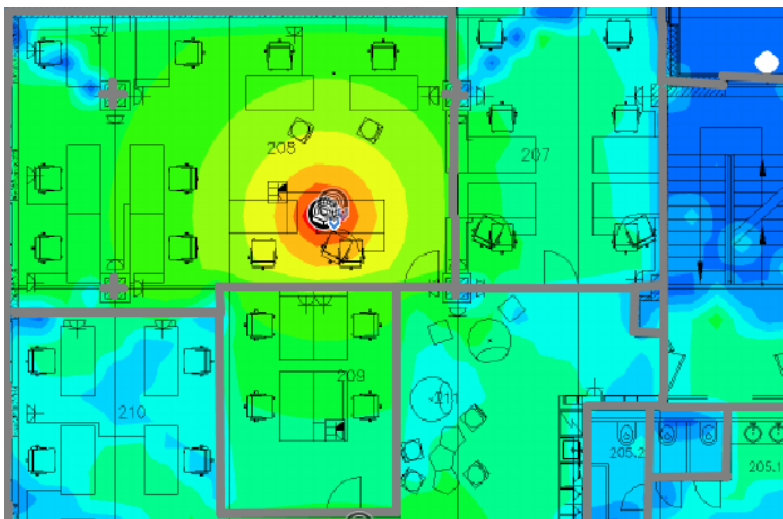
5.1 Access Point Design and Implementation

Access point planning may begin in many ways, but generally, it begins with an expressed desire to provide connections to a specific area where some users will participate in a focused activity. (Wireless LAN Design Guide, 2013)

There are three most important things which the net designer should know:

- 1) The footage of apartments.
- 2) Approximate quantity of internet users and the user needs.
- 3) The wall material and its width.

With this information, he can make the user requirements and find the solution for a stable and fast Wi-Fi network. Based on this three questions was made a research in one of apartment “Baron residence, Drosselstrasse 17” and was collected all needed information. Figure 7 shows a professional network plan of first and second floors of the building which was made with “TamoGraph Site Survey” program.



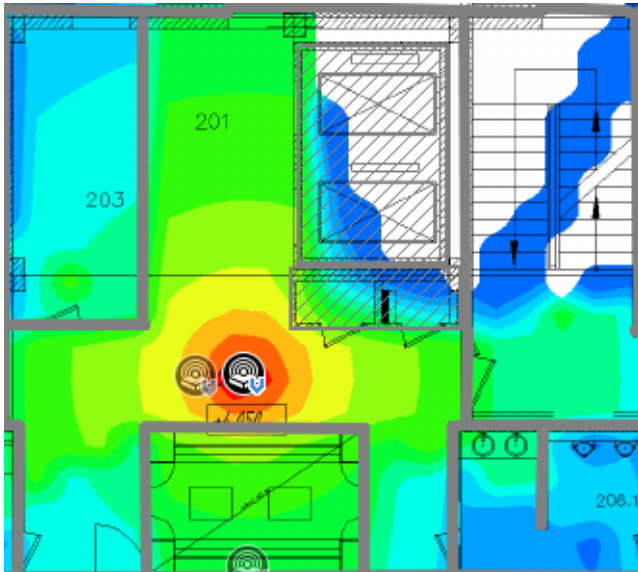


Figure 13. Wi-Fi plan, first and second floors

The total footage of the first floor is 93 sq.m and the second floor is 62 sq.m, according to the footage, used network equipment are Internet router Linksys WRT54GL and Ethernet cables “Mediabridge Cat-6a”, the program made the counting and gave the advice for the best Hotspot point implementing. Figures above shows how strong the Wi-Fi signal in different places of the apartment: red area - strong, stable signal, orange and yellow – strong signal, green – stable signal with insignificant loss of speed, blue – weak signal with significant loss of speed. From the program report user can see that for the best signal quality one AP in the middle of the apartment for each floor it is enough for the given footage of apartments.

5.2 DD-WRT Firmware Installation and Configuring

The start of the system installation should begin with Access Point installation and configuration. Later, based on the router configurations FreeRADIUS server will be installed. For the firmware installation, it is necessary to download the right firmware from the dd-wrt router database. The official website www.dd-wrt.com provides sufficiently detailed instructions for each supported by this distribution router. There it is possible to find all the necessary information about preinstalled software and the hardware of the router and links to download the actual dd-wrt.

The general steps in router flashing:

1. Identifying and downloading DD-WRT Firmware from the router database on www.dd-wrt.com website, the newest version for the Linksys WRT54GL router is “dd-wrt.v24_std_generic.bin”.
2. Connecting router using a network cable and using the browser through the default IP which is <http://192.168.1.1> opening dd-wrt GUI.
3. In tab **Administration and Firmware Upgrade** uploading the dd-wrt.v24_std_generic.bin image. Figure 8 is showing the firmware upgrade interface.

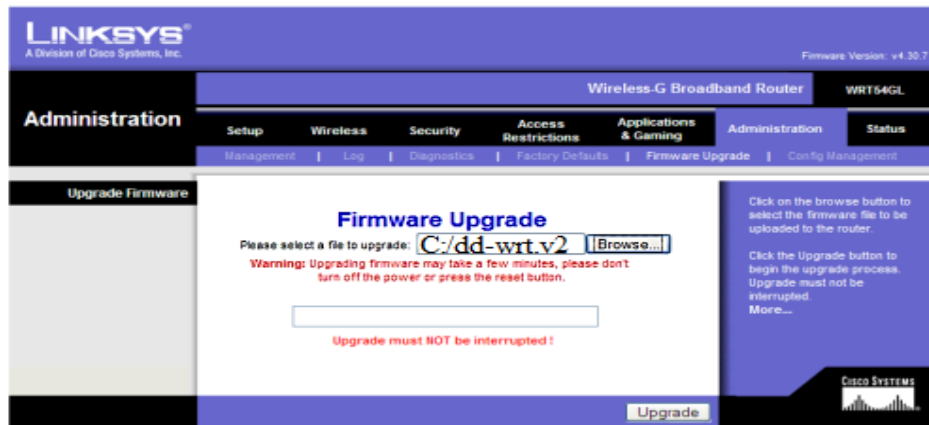


Figure 14. The dd-wrt.v24_std_generic.bin firmware uploading

4. Waiting for the automatic router reboot (dd-wrt.com).

5.3 FreeRADIUS Server Configuration

The start of the system installation should begin with FreeRADIUS server configuration, due to the fact, that it serves as a basis for the system installation.

1. Log in to the system as a root user and Install FreeRADIUS server, freeradius mysql support and radius utils

```
# sudo apt-get install freeradius freeradius-mysql
freeradius-utils
```

2. For communication with a radius server the ChilliSpot portal uses the special ports 1812 and 1813, which should be opened in the

server system. Check the status of the freeRADIUS server and open needed ports

```
# sudo service freeradius status
# sudo ufw allow 1812/udp
# sudo ufw allow 1813/udp
```

5.4 Installing and Configuring MySQL Database

1. Install MySQL

```
# sudo apt-get install mysql-server
```

2. Log into MySQL Root

```
# sudo mysql -u root -p
```

3. Create new database with name "radius", give a permissions, quit

```
# mysql > CREATE DATABASE radius;
# mysql > GRANT ALL PRIVILEGES ON radius.* to
radius@localhost IDENTIFIED BY "password";
# mysql > \q
```

4. Import command files schema.sql and nas.sql. This files fill prepar the "radius" database to usage by FreeRADIUS server

```
# sudo mysql -u root -p radius <
/etc/freeradius/sql/mysql/schema.sql
# sudo mysql -u root -p radius <
/etc/freeradius/sql/mysql/nas.sql
```

5. Get an access to radius database, and create a user with a name and password. Quite

```
# sudo mysql -u root -p
# show databases;
```

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| radius |
| sys |
+-----+
```


Figure 15. Database table

```
# mysql > use radius;
# mysql > INSERT INTO radcheck (UserName, Attribute,
Value)
    -> VALUES ('Alpin', 'Password', 'Alpinpassword');
# mysql > \q
```

5.5 Configuring Freeradius

1. Get an access to sql.conf and set the following configurations on 36, 38, 39 and 108 text lines.

```
# sudo nano /etc/freeradius/sql.conf
# Connection info:
server = "localhost"
login = "radius" # database name
password = "23041995" # your password to access
# uncomment to become
readclients = yes
```

Ctrl+O – to save and Ctrl+X for exit.

2. Change the file "default"

```
# sudo nano /etc/freeradius/sites-enabled/default
```

Uncomment the "sql" option for the following sections on. With this step we are given the permissions to use MySQL database.

```
# Accounting (text line 406)
# Session (text line 457)
# Post-Auth-Type (text line 475)
```

3. In "radiusd.conf" uncomment the following option

```
# sudo nano /etc/freeradius/radiusd.conf
# $INCLUDE sql.conf (text line 743)
```

4. Stop FreeRADIUS server and run debug mode

```
# sudo service freeradius stop
# sudo freeradius -X
```

5. Test the connection

```
# sudo radtest Alpin Alpinpassword localhost 18128
testing123
```

This message means that FreeRADIUS configuration was successfully installed.

```
# Sending Access-Request of id 134 to 127.0.0.1 port 1812
    User-Name = "Alpin"
    User-Password = "Alpinpassword"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 18128
Message-Authenticator 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port
1812, id=68, length=20
```

5.6 Configuring DaloRADIUS.

Here described how to set a connection between daloRADIUS and FreeRADIUS.

1. Download, extract and rename the original file daloRADIUS. Then move it to another directory.

```
# wget
http://sourceforge.net/projects/daloradius/files/daloradius/daloradius0.9-9/daloradius-0.9-9.tar.gz
# tar xvfz daloradius-0.9-9.tar.gz
# sudo mv daloradius-0.9-9 daloradius
# sudo mv daloradius /var/www
# sudo cp -R
/var/www/daloradius/contrib/chilli/portal2/hotspotlogin
/var/www/daloradius
# sudo chown -R www-data:www-data /var/www/daloradius
# sudo chmod 644
/var/www/daloradius/library/daloradius.conf.php
```

2. Setting the connection

```
# sudo mysql -u root -p radius <
/var/www/daloradius/contrib/db/mysql-daloradius.sql
```

3. Configure the daloradius.conf.php file

```
# sudo nano
/var/www/daloradius/library/daloradius.conf.php
# Configuration section

$configValues['CONFIG_DB_ENGINE'] = 'mysqli';
$configValues['CONFIG_DB_HOST'] = 'localhost';
$configValues['CONFIG_DB_PORT'] = '3306';
$configValues['CONFIG_DB_USER'] = 'radius';
$configValues['CONFIG_DB_PASS'] = 'LapinAMK';\\ Here
should be radius database password.
$configValues['CONFIG_DB_NAME'] = 'radius';
```

4. Modify file opendb.php

```
# sudo nano /var/www/daloradius/library/opendb.php
# This configuration should me in the end of the file
# $dbSocket->query("SET SESSION sql_mode = ''");
```

5. Install nginx HTTP server, that needs for daloRADIUS package.

```
# sudo apt-get install nginx
# sudo nano /etc/nginx/sites-available/radius \make a
new file
```

Add the following code:

```
# The hotspot won't let you use it
# if not SSL
server {
    listen 443 ssl http2;
    root /var/www/daloradius;
    index index.php hotspotlogin.php;
    server_name radius.example.co;
    include /etc/nginx/ssl/globalssl.conf;
    include /etc/nginx/snippets/statics.conf;
    location / {
        try_files $uri $uri/ =404;
    }
    location ~ /\.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php7.0-fpm.sock;
        fastcgi_param SCRIPT_FILENAME
$document_root$fastcgi_script_name;
    }
    location ~ /\.ht {
        deny all;
    }
}

server {
    listen 80;
    server_name radius.example.co;
    return 301 https://$server_name$request_uri;
```

Test the system

```
# sudo nginx -t
```

```
-available/radius
ubuntu@ubuntu-standard:/etc/nginx/sites-available$ sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Figure 16. Successful test of nginx server

5.7 Hotspot Login

1. Adding an UAM Secret

```
# sudo nano
/var/www/daloradius/hotspotlogin/hotspotlogin.php

# $uamsecret = "LapinAMK"; \\ This secret key will be used
in Chillispot settings.
```

2. Testing. After all configurations, we need to test our system

```
# sudo service freeradius start
# sudo service freeradius status
```

```
ubuntu@ubuntu-standard:~$ sudo service freeradius status
● freeradius.service - LSB: Radius Daemon
  Loaded: loaded (/etc/init.d/freeradius; bad; vendor preset: enabled)
  Active: active (running) since Fri 2016-12-02 07:54:43 UTC; 2 days ago
    Docs: man:systemd-sysv-generator(8)
  CGroup: /system.slice/freeradius.service
          └─562 /usr/sbin/freeradius

Dec 02 07:54:40 ubuntu-standard systemd[1]: Starting LSB: Radius Daemon...
Dec 02 07:54:40 ubuntu-standard freeradius[520]: * Starting FreeRADIUS daemon
Dec 02 07:54:43 ubuntu-standard freeradius[520]: ...done.
Dec 02 07:54:43 ubuntu-standard systemd[1]: Started LSB: Radius Daemon.
```

Figure 17. Running freeradius server

Figure 17 shows that the testing of freeradius server was successful.

```
# sudo service nginx restart
# sudo service nginx status
```

```
● nginx.service - A high performance web server and a reverse proxy server
  Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
  Active: active (running) since Mon 2016-12-05 01:01:28 UTC; 31min ago
    Main PID: 7794 (nginx)
  CGroup: /system.slice/nginx.service
          └─7794 nginx: master process /usr/sbin/nginx -g daemon on; master_process on
              └─7795 nginx: worker process
                  └─7796 nginx: worker process
                      └─7797 nginx: worker process
                          └─7798 nginx: worker process

Dec 05 01:01:28 ubuntu-standard systemd[1]: Starting A high performance web server and a reverse proxy server...
Dec 05 01:01:28 ubuntu-standard systemd[1]: Started A high performance web server and a reverse proxy server.
```

Figure 18. Running NGINX server

Figure 18 shows that the testing of nginx web server was successful.

Next step is to add a NAS client into the system and finish chillispot configuring

3. Open clients.conf and past the following code before “client localhost” line

```
client ddwrt {
    ipaddr = 192.168.178.43 \\ access point ip
    secret = LapinAMK
    require_message_authenticator = yes
}
```

Now all needed servers are configured and we need to configure ChilliSpot portal.

5.8 ChilliSpot Configuration

When installation of DD-WRT is complete, the system is ready for configurations which will connect customer’s AP with a FreeRADIUS server.

Following steps of configuration and FreeRADIUS server installation:

1. Connect the router to the ADSL/DSL Modem. Login to DD-WRT. Navigating to <http://192.168.1.1>, in **Administration** field, making user and password configuration.
2. In **Setup** tab set **Wan Setup** for the internet access, **Router IP** and **DHCP** info are already set by default.

Network Setup	
Router IP	
Local IP Address	192. 168. 1. 1
Subnet Mask	255. 255. 255. 0
Gateway	0. 0. 0. 0
Local DNS	0. 0. 0. 0
Network Address Server Settings (DHCP)	
DHCP Type	DHCP Server
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Start IP Address	192.168.1. 100
Maximum DHCP Users	50
Client Lease Time	1440 minutes
Static DNS 1	0. 0. 0. 0
Static DNS 2	0. 0. 0. 0
Static DNS 3	0. 0. 0. 0
WINS	0. 0. 0. 0
Use DNSMasq for DHCP	<input checked="" type="checkbox"/>
Use DNSMasq for DNS	<input checked="" type="checkbox"/>
DHCP-Authoritative	<input type="checkbox"/>

Figure 19. DD-WRT General Network Settings

3. Checking the overview of the system. Figure 9 shows how it displays using research router.

The screenshot shows the DD-WRT control panel interface. At the top, it displays the firmware version (DD-WRT v24-sp2 (10/10/09) std), the time (14:28:45 up 0 min, load average: 1.21, 0.39, 0.13), and the WAN IP (192.168.178.43). The navigation menu includes Setup, Wireless, Services, Security, Access Restrictions, NAT / QoS, Administration, and Status. The main content area is titled 'System Information' and is divided into several sections:

- Router:**

Router Name	DD-WRT
Router Model	Linksys WRT54G/GL/GS
LAN MAC	<u>C0:56:27:36:E7:85</u>
WAN MAC	<u>C0:56:27:36:E7:86</u>
Wireless MAC	<u>C0:56:27:36:E7:87</u>
WAN IP	192.168.178.43
LAN IP	192.168.1.1
- Services:**

DHCP Server	Enabled
WRT-radauth	Enabled
WRT-rflow	Disabled
MAC-upd	Disabled
CIFS Automount	Disabled
Sputnik Agent	Disabled
- Wireless:**

Radio	Radio is On
Mode	AP
Network	Mixed
SSID	AleksaSpot
Channel	6
TX Power	71 mW
Rate	54 Mbps
- Memory:**

Total Available	12.7 MB / 16.0 MB
Free	2.2 MB / 12.7 MB
Used	10.5 MB / 12.7 MB
Buffers	1.5 MB / 10.5 MB
Cached	4.5 MB / 10.5 MB
Active	3.9 MB / 10.5 MB
Inactive	2.2 MB / 10.5 MB
- Wireless Packet Info:**

Received (RX)	0 OK, no error
Transmitted (TX)	0 OK, 13 errors
- Space Usage:**

CIFS	(Not mounted)
MMC	(Not mounted)

Figure 20. Overview

This part of installation is important, mostly for checking that router is working. In addition, routers memory should not be fully filled.

4. In the tab **Wireless** make the configuration of SSID name, for the guests' comfort Wi-Fi Hotspot should be set as an open Wi-Fi network, in **Wireless Network Configuration** should be configured as "unbridged" usage
5. In the tab **Services**, subtab **Hotspot**, make configuration of ChilliSpot package. In this step it's important to separate Wi-Fi network from the LAN Bridge, it will configure the Captive Portal functionally only to the connections through Wireless network.

DD-WRT (build 13064) · × Can't reach this page +

← → ↻ | 192.168.1.1/apply.cgi | ☆ ≡

ChilliSpot

ChilliSpot Enable Disable

Separate Wifi from the LAN Bridge Enable Disable

Primary Radius Server IP/DNS // FreeRADIUS server IP

Backup Radius Server IP/DNS // FreeRADIUS server IP

DNS IP // DNS for resolving Domains, Google DNS

Remote Network // AP IP

Redirect URL // Redirecting page

Shared Key //Key from freeradius/clients.conf file

DHCP Interface eth1 - WLAN interface

Radius NAS ID

UAM Secret // Key from doloradius.conf.php file

UAM Any DNS

UAM Allowed

MACauth Enable Disable

Additional ChilliSpot Options

Figure 21. ChilliSpot configuration

Then settings should be applied, and router rebooted. When every step of installation and configurations done from a proper way, the UHS system will be an ideal combination of cost effectiveness and performance choice among other Hotspot solutions.

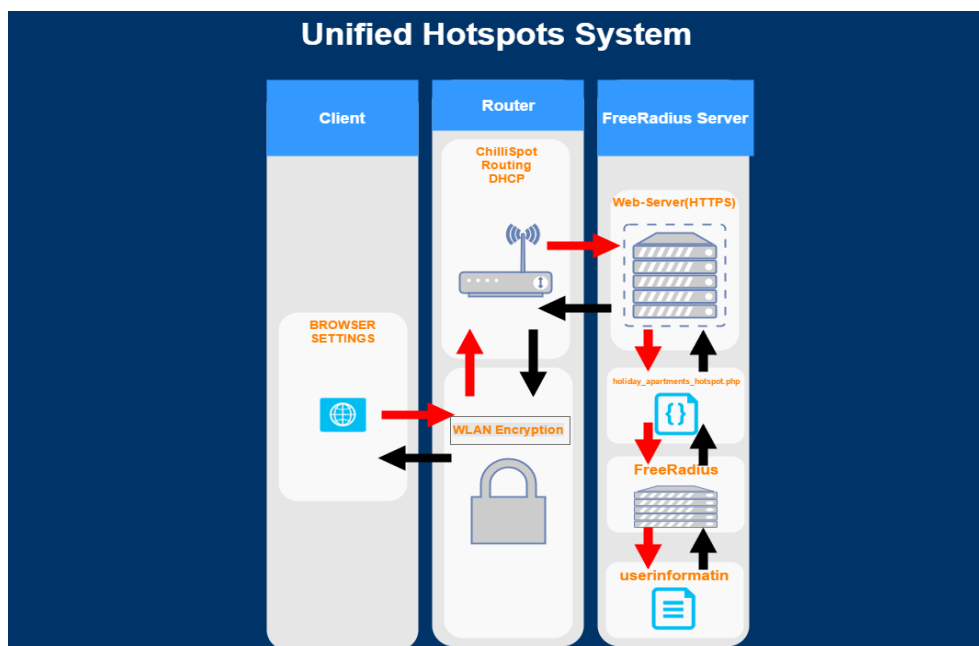


Figure 22. Scheme of components communication inside of UHS

The figure above represents the diagram, which explains how Unified Hotspot System works. The first user is trying to reach any web-site through the system client (Access Point). This request is moving through the router, supported with decent encryption and with pre-installed ChilliSpot. The request goes further to web-server, which is generating a web page. This web page, constructed using FreeRadius user will see instead of web-site he/she tried to reach. On this web page, according to requirements of the owner, user will be asked for user credentials for internet usage.

6 CONCLUSION

To summarize the results of this research, it is necessary to return to the beginning and state the objectives. There are two main objectives: to explore the Hotspots technology and DD-WRT in specific and creation of Unified Hotspot Systems. In order to reach these objectives three research questions were given and answered in this research.

1. What is Unified Hotspot? What different from other tradition Hotspots?

The answer to this question lies in the word “unified”. The essence of the UHS is that it combines several hotspots in one system and allows to use a variety of routers as a single access point, thus allowing to extend the zone of connection to the Wi-Fi for guests, using any number of routers to provide a stable signal. There is also the possibility to administer, view connected users, and the restrictions for some sites. In traditional hotspot is usually only one router and no administration possibilities, though there is the possibility of limiting visits to specific sites.

2. What is the Open-Source software and DD-WRT firmware?

Open source software is a type of software that is free for distribution and has the open code, which can be modified by user (opensource.com). This type of software is ideal for research purposes, as it is free and allows to, if it is required, customize the system. DD-WRT is a Linux-based operation system for the routers, which is flexible and allows installing various extensions. For research goals, an extension called Freeradius was needed to allow the creation of Hotspots.

3. What is the business value of adopting Unified Hotspots? How can Unified Hotspots contribute to business value in the case company? At a sufficiently low price of the system, it provides a safe and modern internet connection for guests of case company. There will not be problems with connection because of incomplete coverage of the apartments by Wi-Fi zone, because the owner could apply more than one router and provide it as one single system. Also, because

of UHS, the owner of the apartment can be sure that unauthorized users do not connect to his/her Wi-Fi.

BIBLIOGRAPHY

Chillispot.org 2004. Chillispot AAA Official Documentation
<http://www.chillispot.org/chilli.html>

Coova.org 2016. Scheme of Coova Captive Portal
<http://coova.github.io/CoovaChilli/>

Hosner Charlie 2004. SANS Institute. OpenVPN and the SSL VPN Revolution
<https://www.sans.org/reading-room/whitepapers/vpns/openvpn-and-the-ssl-vpn-revolution-1459?show=1459.php&cat=vpns>

Canonical Ltd. Ubuntu 2016. Ubuntu Server Guide - Ubuntu 16.04
<https://wiki.ubuntu.com/DocumentationTeam/SystemDocumentation/UbuntuServerGuide>

Rigney C. & Livingston June 2000. RFC2866. RADIUS Accounting
<https://tools.ietf.org/html/rfc2866>

Rigney C., Willens S., Rubens A., Simpson W. June 2000. RFC2865. Remote Authentication Dial In User Service (RADIUS)
<https://tools.ietf.org/html/rfc2865#page-17>

Denscombe M 2010. The good research guide: for small scale research projects. 4th ed. Maidenhead: McGraw-Hill Open University Press. 300.72 DEN & e-book.

Parasuraman A 1991. Addison-Wesley Publishing Company Inc. Marketing Research - 2nd Edition.

DD-WRT 2015. Installation guide
www.dd-wrt.com/wiki/index.php/installation

Linksys 2016. Linksys WRT54GL WIRELESS-G wireless router, Accessed 4 November 2016
<http://www.linksys.com/us/p/P-WRT54GL/#product-features>

Liran Tal's Enginx 2016. NGINX server
www.ngx.com

Network RADIUS SARL 2014. The FreeRADIUS Technical Guide
<http://networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf>

Oracle 2016. MySQL 5.6 Reference Manual.
<http://dev.mysql.com/doc/refman/5.6/en/what-is-mysql.html>

Opensource.com 2016. What is open source?
www.opensource.com

Pew Research Center 2013. Social Media Use By Age Group Over Time Referenced 04.11.2016
<http://www.pewinternet.org/data-trend/social-media/social-media-use-by-age-group/>

Pinola M 2016. Wi-Fi Hotspot Definition. Accessed 4 November 2016
<https://www.lifewire.com/wi-fi-hotspot-definition-2377357>.

The PHP Group 2016. PHP Introduction
<https://secure.php.net/manual/en/intro-whatcando.php>

The PHP Group 2016. PHP Features
<http://php.net/manual/en/features.php>

Viktornet.wordpress.com 2016. The principle of OpenVPN tunnel in action.
<https://viktornet.wordpress.com/2014/06/12/securing-wireless-communication-using-radius-and-vpn-technology/>

WinSCP.net 2016. WinSCP SSH Client for Windows
https://winscp.net/eng/docs/free_ssh_client_for_windows#what_is_ssh_client

Cisco 2013. Wireless LAN Design Guide for High Density Client Environments in Higher Education.
http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1250-series/design_guide_c07-693245.pdf