


Opikhalov Dmitry
RADIUS server
as centralized authentication

Bachelor's Thesis
Information Technology

May 2015



DESCRIPTION

		Date of the bachelor's thesis 28.05.2015
Author(s) Opikhalov Dmitry	Degree programme and option Information Technology	
Name of the bachelor's thesis RADIUS server as centralized authentication		
Abstract The purpose of this thesis was to examine the field of authentication and authorization for wireless users connected to Central Authentication Server. The topic has gained certain popularity over the last decade because of the constant growth of wireless users. Knowing the basics of this particular topic field that the topic will prepare myself for the future work placement. The thesis defines AAA protocols and protocol's idea, authentication protocols and security standards. The practice explains by steps the implementation in to the private network of the RADIUS protocol that was chosen as an AAA protocol. DHCP, DNS, SQL servers' and Active Directory's basic ideas were discussed and put into practice. Also some additional topics that are under very heavy development were touched during the study like virtualization. As the result the private network was created, where RADIUS server authenticates wirelessly connected users. The accounting has helped to gather the outcome of how RADIUS behaves and which decisions were made for the specific user. However, this thesis can be used as a background for future more advanced development or lab needs.		
Subject headings, (keywords) Windows Server 2012 R2, RADIUS protocol, Centralized Authentication		
Pages 64 p. + 2 p. appendices	Language English	URN
Remarks, notes on appendices		
Tutor Matti Koivisto	Employer of the bachelor's thesis Mikkeli University of Applied Sciences	

LIST OF ABBREVIATIONS

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AD	Active Directory
AD CS	AD Certificate Services
AD DS	AD Domain Services
AES	Advanced Encryption Standard
AP	Access Point
ARPANET	Advanced Research Projects Agency Network
AS	Authentication Server
AVP	Attribute-Value Pair
CA	Certification Authority
CAuth	Centralized Authentication
CCMP	Counter Mode CBC-MAC Protocol
CHAP	Challenge-Handshake Authentication Protocol
CMD	Command Prompt
DAC	Discretionary Access Control
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DAuth	Distributed Authentication
DC	Domain Controller
EAP	Extensible Authentication Protocol
FAQ	Frequently Asked Questions

GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IAS	Internet Authentication Service
ISP	Internet Service Provide
IP	Internet Protocol
KDC	Key Distribution Center
MAC	Mandatory Access Control
MD	Message Digest
MIC	Message Integrity Check
MIT	Massachusetts Institute of Technology
MS-CHAP	Microsoft Challenge-Handshake Authentication Protocol
NAS	Network Access Server
NIC	Network Interface Card
PAP	Password Authentication Protocol
PC	Personal Computer
PEAP	Protected Extensible Authentication Protocol
PPP	Point-to-Point or Peer-to-Peer Protocol
PSK	Pre-Shared Key
OS	Operating System
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-based Access Control
RC4	Rivest Cipher 4
RFC	Request For Comments
SCTP	Stream Control Transmission Protocol

SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSID	Service Set Identifier
SSO	Single Sign-On
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TGT	Ticket Granting Ticket
TGS	Ticket Granting Server
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time-to-live
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
XTACACS	Extended TACACS

CONTENTS

LIST OF ABBREVIATIONS.....	1
1 INTRODUCTION	6
2 AUTHENTICATION, AUTHORIZATION AND ACCOUNTING.....	7
2.1 Authentication.....	9
2.1.1 Centralized vs. Distributed Authentication.....	10
2.1.2 Single Sign-On.....	11
2.2 Authorization and Access Control	11
2.3 Accounting.....	13
3 SECURITY PROTOCOLS	13
3.1 TACACS family protocols.....	13
3.2 RADIUS	15
3.3 DIAMETER base protocol.....	18
3.4 Kerberos	18
3.5 Point-to-point Authentication Protocols	20
3.5.1 EAP	21
3.5.2 PAP	22
3.5.3 CHAP	22
3.5.4 MS-CHAP	22
3.5.5 MS-CHAPv2	22
3.6 Wi-Fi security standards.....	23
3.6.1 WEP	23
3.6.2 WPA	23
3.6.3 WPA2	24
4 CREATING WINDOWS ENVIRONMENT	24
4.1 OS Installation	25
4.2 MS SQL server	27
4.3 Active Directory implementation.....	29
4.4 Establishment of Network Policy Server as RADIUS.....	30
4.5 DHCP on Virtual Machine	32
5 IMPROVING AND TESTING.....	36
5.1 Single Point Setup	37

5.2	Sharing	39
5.2.1	Prepare to share	40
5.2.2	Share	45
5.3	DHCP policy	48
5.4	Accounting.....	51
5.5	Final Testing	53
6	CONCLUSION AND FUTURE WORK	56
	BIBLIOGRAPHY	58
	APPENDICES.....	65

1 INTRODUCTION

In the modern society, many things are dependent on the Internet and its utilization. For the past 30 years, the Internet has evolved dramatically and nowadays we can resolutely say that all the devices can be divided into two groups: the ones that require services and the ones that provide these services. The first ones are the clients, including each and every one of us that has ever used a simple browser. The second ones are the servers which may also include some of us, mainly because of the file sharing we do from time to time. However, when mentioning servers we will still talk about computers, but about these which have a purpose greater than a personal one. Servers are there to fulfill the needs of the clients' wishes and to respond on their queries whenever. Thus, servers are very essential part of the network. They supply others with crucial services, and their availability and quick performance are the keys to have a reliable and go-to services.

There are many kinds of servers, and the most used ones are: web servers, mail servers and gaming servers. Most of the time these services are combined into one machine as long as it does not have an effect on the machine's performance. But the main idea behind each and every one of them is to provide some particular type of service.

One of the examples is the authentication server. It is playing one of the most important roles on the Internet among others. And, I am not saying that just to show the importance of the topic, but to increase the attention to the purpose that it serves. Every one of us has an identity. In the modern world the terms "fake ID" and "catfish" are quite popular, especially when using the Internet, and the authentication server is there to solve the problem of unauthorized access to the desired services. In order to get to the services this type of server asks for the user's credentials which it compares to the database it has and makes a verdict based on the comparison. If the identification and authorization are successful, the server allows the user to receive the services he wished for, according to the priorities the user has.

Authentication is needed both in wired and wireless networks. In wireless networks authorization is much more important, because in wired networks the access is limited in a way through wires, while wirelessly any capable device can connect to the server and without proper authentication it can do serious damage by intruding into the system. Wires chain you in a way, and therefore people aim to get as much freedom as possible and they tend to break the "shackles" down. In

other words, this explains the sudden boom of wireless technology at the beginning of the 21st century, which makes this particular topic, the significance of which will not disperse with years, quite interesting and indispensable.

The aim of the study is to understand and research the field of authentication and how the access control is managed, to build a real RADIUS server and test its different versions and options. The main idea of the theoretical part of the study is to go through the idea of the AAA server and its parts. After that I am going to overview the most popular authentication protocols and their advantages and disadvantages in comparison to each other. And finally, I will define security algorithms and their characteristics.

As for the practical part, I am going to create, with the help of third-party software, an authentication server which is connected via a router and a switch to the network of wireless access points. The clients of the wireless local area network will be authenticated against the user database of the authentication server which is securely stored on the server. The created server must be scalable and flexible, i.e., the amount of access point can be easily expanded or reduced by the administrator of the network.

2 AUTHENTICATION, AUTHORIZATION AND ACCOUNTING

AAA or “triple A” is a short term for authentication, authorization and accounting. It is a term that defines the security concept for protocols that ensures that only the allowed users can gain an access to the network or some particular resources on the network and keeps log of what they have done over the time they had an access to the network.

Ventura (2002, 6) defines AAA as follows: “AAA essentially defines a framework for coordinating these individual disciplines across multiple network technologies and platforms. In practice, an AAA server with a database of user profiles and configuration data communicates with AAA clients residing on network components, such as Network Access Server (NAS) and routers, to provide distributed AAA services.”

In practice, an AAA server with a database of user profiles and configuration data communicates via one of the AAA protocols with AAA clients, usually NAS, to provide distributed AAA services. As Jimmy Ray Purser (2013) acknowledged, the most simple and understandable way

to explain AAA is as follows: authentication is for a device, authorization is for a user and accounting is for tracking what the user has done with that device on the network. But, there are more steps in the technology itself, and next I will introduce all of them.

The first thing is identification. “We can define identification as the act of claiming an identity, where an identity is a set of attributes that distinctly determines the entity,” says Pasupathinathan (2009, 2). It means that somebody is trying to gain an access and the system has to be informed of exactly who is trying to do so. Everybody must have a unique identifier. If the system could successfully acknowledge that there is a user with the given attribute, the system goes to the second step, and that would be the authentication of the user.

Authentication successively provides the mechanism that confirms the identity of a user that has been stated to the server (Jing 2008, 6). At the authentication stage, the user must prove of who he claims to be. Simply, the user must verify himself by providing the information that only he can possess. And as long as the user’s identity was confirmed, the system will now estimate the permissions that his account has.

This process is called authorization. This is the core of access control. Authorization usually relies on ACL, which stands for Access Control List, (or its analogue) or compares the levels of significance on the network, and based on these either grants for the user an access to the resource or denies the entry. This activity, when every time the user is trying to reach something on the network and the decision is supposed to be made whether to grant the permission or reject the request, is called access approval. It is important to consider “access approval” process as a separate one, because depending on its decisions the last process - accounting, which records all the things that the user has done for the session, can rely on them and provide more detailed information for the system administrator.

Accounting itself is the most useful tool of them all. The log files that are created by this process can serve as the evidence, if something happens on the network. Internet Service Providers are also using these files for billing purposes. System administrators can monitor designated target for possible violations and create statistics as well. Next sections analyze authentication, authorization and accounting separately and in more detail.

2.1 Authentication

Authentication plays a huge role in the process of granting access to resources, because it prevents users that do not belong to the network from gaining access to the resources and also ensures that the ones that do belong can get resources' availability according to the permissions they have. As mentioned earlier, its main idea is to provide the proof of whom you are claiming to be. According to Bartik (2014) there are three types of credentials:

- What-you-have or material proof (badge, card or some other physical token that proves your identity);
- What-you-know or knowledge verification (something that you have memorized and only you can know, such as a PIN code);
- What-you-are or biometric proof (fingerprints, eyes, voice - making the chance of falsification to appear to be really small because of its uniqueness).

Usually in the cyber environment the most common proof is a password which is associated with the username you have typed. Nevertheless, nowadays the case of impersonating is very common, and many services can provide additional security level via your mobile phone: SMS or one-time passwords. Therefore, this means that authentication is here to limit the possibility of impersonation by providing more steps into the authentication process, depending on the importance of the information. Hence, if you have very sensitive data and you do not want it to become public, you have to protect it with more than one method, which leads us to multifactor authentication.

This means that you must confirm your identity at least twice or even several times, and in addition to these three types of credentials, two new ones were nearly established: where you are trying to authenticate from and something that you do. The first one is dependent on your location with the help of an IP address. For example, if the IP belongs to a particular country or belongs to a company's private network, the process of authentication is simplified and the process of authorization continues. Whereas the second way, what-you-do, relies on the certain ways of doing things, e.g. handwriting, which is a bit hard to implement into the PC world, or the way you type. The keystroke analysis (keystroke dynamics) is a developing technology whose major idea is to authenticate user by comparing of his typing patterns, which is quite hard to

steal, and it is always good to have an additional layer of security. (Monrose & Rubin 2000, 351 - 352.)

There are quite many protocols for this process, but I aim to focus on the most used ones, such as Kerberos, TACACS+, RADIUS and DIAMETER, which is claimed to be a possible replacement for RADIUS. Even though I will be concentrating more on authentication in the thesis, it is quite important to understand how the decision is made for authenticated users and according to what rules the access is granted.

2.1.1 Centralized vs. Distributed Authentication

When the process comes to the point where the user should be authenticated, there are two possibilities: distributed and centralized authentication methods. The names of both methods clearly explain where exactly the authentication is managed. With Centralized Authentication (CAuth) users are connecting to the server that provides the access to resources and services once they are authenticated and authorized. With Distributed Authentication (DAuth) every device has a local database of these users who can gain an access. CAuth is easily managed at one place, it provides flexibility and scalability, but requires quite a powerful server to handle all the traffic and requests. DAuth is more secure, because the device does not rely on a third party and makes the decision on its own. In addition, it does not require separate hardware (cost saving), but whenever there is a need to change user's parameters, the administrator must do it manually on each device one by one. Thus, this method does not scale well. (Todorov 2007, 39-42.) Nevertheless, the choice on which method to use is always dependent on the type of the network (Figure 1).

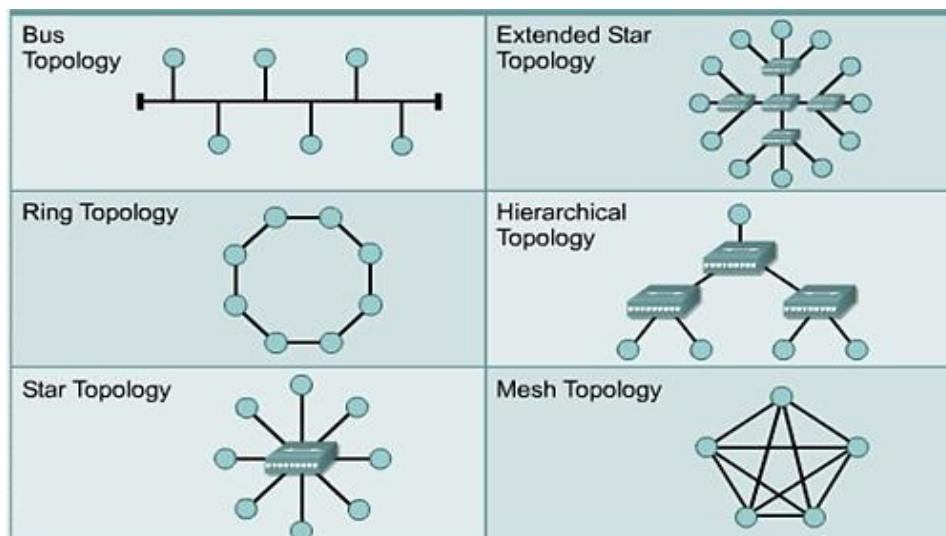


FIGURE 1. Types of networks (TANAMA 2015)

2.1.2 Single Sign-On

Single Sign-On (SSO) is often confused with CAuth, because people do not know the exact idea of the purpose and the service they bring. SSO is simply how authentication is carried out and CAuth and DAuth is where authentication takes place. But it is quite common nowadays to combine the SSO system and CAuth together for faster and not an idling service. That is why people consider these two techniques to be the same. (Salazar 2014.) According to Cao (2014, 5) Shirey (2000, 160) has defined SSO as a system which allows the users that has been already authenticated once to access other applications without repeating the process of authentication, too.

2.2 Authorization and Access Control

As long as the number of users and their devices is increasing every day, the cyber access control plays tremendous role in our lives. People pay more attention to it, because they want to be safe and secured from intrusions that might appear over the Internet. For that security reason, there are many methods to protect your data and to limit access to your system mostly via access control. Child (2004, 7) defines access control as “method whereby administrators make certain that only authorized users can gain access to specific resources or services”. Among them are

access control lists (ACLs), which is a mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and by stating, either implicitly or explicitly, the access modes granted to each entity (Shirey 2007, 11).

There are two types of ACLs: networking ACLs which are usually associated with switches and routers to control the traffic through established interfaces, and filesystem ACLs which are present to manage file permissions. Nevertheless, the filesystem ACLs sometimes are quite hard to manage in flexible systems, and therefore, there are few other options to control access by creating policies to our files. According to Messer (2014a) these include the following:

- Mandatory Access Control (or MAC) is considered to be a very secure method where access is granted based on the security labels which are associated with users and the resource. The users are not allowed to put or modify these labels on the resource they create. It will be determined by the system administrator. The model that is used with this method will determine how users will interact with the resource they are trying to reach, according to the label they have. The system of labels can vary from public to top secret.
- Discretionary Access Control (or DAC) is considered to be the least restrictive method, where users own the files and put the access regulations to other users for the objects they possess. This method is very flexible, although certain problems arise while using this method. The most threatful one is that a user can execute the malware file without even knowing that he is doing it.
- Role-Based Access Control (or RBAC), as stated in the name, grants permission for using the resource, when your role on the network is stated as approved. Usually this option is very flexible, because it allows the system administrator to create policies for a bunch of people, and if one from the group was excluded, he immediately loses the privileges that the group had. And, as long as the system decides whether a user is the member of one or another group, the level of security is quite high.
- The most restrictive access security concept, mostly used in firewalls, is “Implicit deny”. It means that all access is denied by default unless you have been granted one.

By using access control we maintain four simple tasks: allowing, denying, limiting and revoking access. These options cover many setups and outputs which may occur. (Andress 2014, 42.)

2.3 Accounting

Accounting is defined as the act of collecting information on the resource usage for the purpose of trend analysis, auditing, billing or cost allocation. Larsson (2003, 16) states: “Accounting is the act of keeping records of a particular user's usage of a resource.” And an accounting protocol itself is simply used for conveying data to an accounting server (Niemi 2002, 4). In other words, it is basically a “report system” which holds all the information concerning users’ activities: who has connected to the server (login), from where (the IP address), and what exactly did he do (time spent, resources used, accessed services)? The RADIUS protocol does not provide accounting, while it comes as a separate feature. That is why, accounting has been given its own port to communicate and the communication itself is managed independently (Tuomimäki 2003, 7). However, accounting is excluded from the scope of this thesis.

3 SECURITY PROTOCOLS

There are dozens of security protocols. And thus, I am going to concentrate more on these that provide authentication services, and they are:

- TACACS and its successors
- RADIUS
- DIAMETER base protocol
- Kerberos

All of these protocols have got their own reputation and all are well-known to system administrators. Nevertheless, each of them has its own advantages and disadvantages. In addition, the working principles of every single protocol will be discussed in the following sections and afterwards, the most popular authentication methods will be defined and explained along with Wi-Fi security standards.

3.1 TACACS family protocols

TACACS or Terminal Access Controller Access Control System is the historical remote authentication protocol which was developed in the 80s and was originally created to control access to dial-up lines for ARPANET. It runs with UDP connection on port 49. It is not that

common nowadays, because its heirs are more secure and provide more practical service. (Finseth 1993, 7.)

The first example of improved TACACS protocol is Extended TACACS (XTACACS). This protocol was introduced and developed since by Cisco in 1990. Although XTACACS did separate the tasks of authentication, authorization and accounting and provided additional support for accounting and auditing, it still sent usernames and passwords in plain text, as TACACS did. This protocol is not compatible with the original version. (Ballad et al. 2011, 278.)

TACACS+ is the modern version of TACACS family protocols, and it was also designed and managed by Cisco. This protocol is not compatible with TACACS and XTACACS, because the only thing they have in common is the name. It provides authentication via centralized server which has an AAA framework to rely on for granting access to network devices such as routers, switches, and firewalls (Jia Zhou 2008, 7). Mainly, it runs on TCP via port 49, which explains that it is a connection-oriented protocol and there is no need for transmission control. Also, with this protocol you the packet loss will not be an issue, but because it takes time to check it, this process makes TACACS+ slower in comparison with RADIUS. TACACS+ separates all AAA processes, and also allows other authentication protocols, like Kerberos, to be present. Separating these three tasks makes a TACACS+ server more flexible and scalable. Furthermore, there is a reduction in the load on one device. In comparison to its predecessors, TACACS+ encrypts all the traffic that goes between the client and the server. (Ballad et al. 2011, 279.) Figure 2 shows the TACACS+ authentication sequence.

TACACS+ can include up until 15 different access levels, configured by the administrator, which provides certain hierarchy on the access gaining process and simplicity in the organization. TACACS+ mostly provides central authorization, while with RADIUS each network device is supposed to carry authorization policies. But from the deployment side, TACACS+ server installation is supposed to be as close to the user database as possible, preferably on the same machine or at least in the same internal network. This kind of emplacement reduces security risks, increases the performance of the system and simplifies administration. (tacacs.net 2011.)

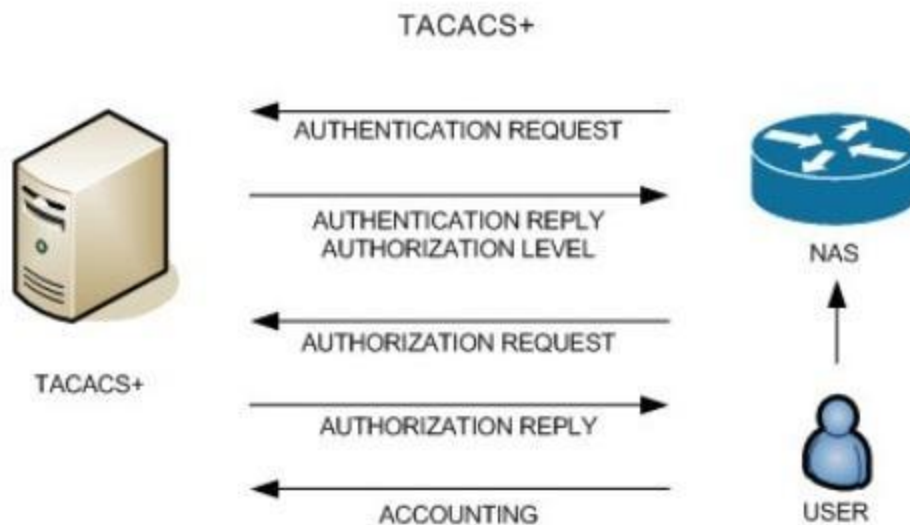


FIGURE 2. TACACS+ authentication sequence (tacacs.net 2011)

3.2 RADIUS

RADIUS is an AAA protocol and the main alternative for TACACS+ for providing centralized access. The major difference between these two is that RADIUS uses UDP protocol (ports 1812/1645 - for authentication, ports 1813/1646 - for accounting) for communication between NAS, or "RADIUS client" and the RADIUS server. There is no transmission control because of the UDP deployment, which makes it less reliable and packet loss may occur. But, if we are going to take a look at it from the other side of this problem, overall performance increases significantly, because the packets are not that "heavy" and they are handled more easily by the networking devices. (cisco.com - 12433 2006.) Figure 3 explains how the RADIUS authentication sequence works.

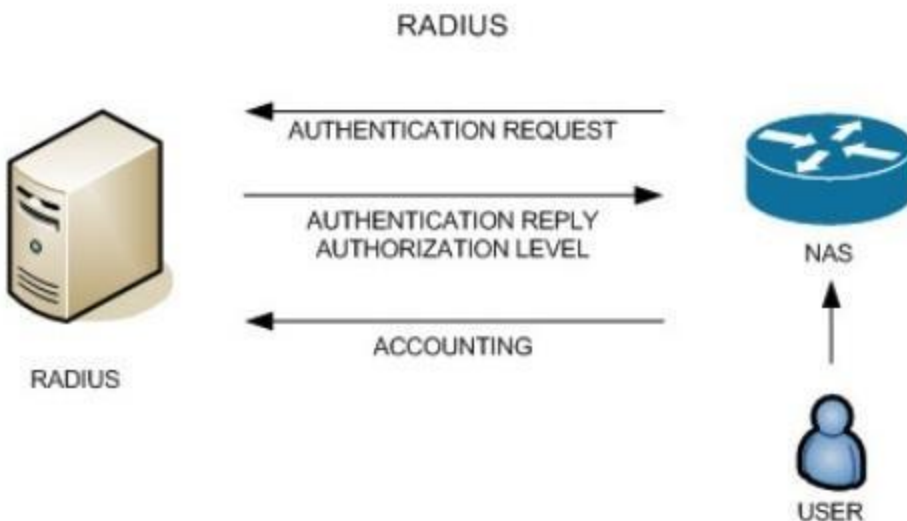


FIGURE 3. RADIUS authentication sequence (tacacs.net 2011)

The advantage of RADIUS over TACACS+ is its ease of use and the authentication time response. Also, if the request to primary authentication server fails, the server does not need to wait for the reply packets (UDP is connectionless). However, the retransmission timers must be set, or the user simply can try to authenticate with the help of a secondary authentication server, if it is available. RADIUS is supported by many vendors. Some limitations are included, which means that it is quite interoperable, but only as long as the same attributes are in use. In order to compensate that TACACS+ offers multi-protocol support.

However, RADIUS has some disadvantages, which are the following:

- It only runs on IP networks, while TACACS+ is supported on Apple, NetBIOS and X.25, as well as on IP networks (cisco.com - 13838, 2006).
- Authentication and authorization processes are combined together for RADIUS, which makes it more vulnerable and affects the performance. Instead, in TACACS+ every process is standalone and separated from each other, meaning that it can use other methods for authentication, authorization and accounting. Also, it can put these processes to different servers, which will provide flexibility and the reduction of network load, if necessary. (Zadjmool 2007.)

- The only encryption here goes for password, when the packets themselves are sent between clients and the server in a plain text, which makes it easy to eavesdrop, if there are intruders present. And, that means that it claims for additional encrypting. In TACACS+ the whole packet is encrypted, excluding the header (Woland 2014).
- RADIUS does not save the logs of the commands that were used by the administrator, which means that if two administrators have logged in at the same time, it is impossible to determine who typed which command later on. TACACS+, on the other hand, stores the full log of commands that has been entered. (tacacs.net, 2011b.)

On one hand, the RADIUS protocol is more useful for granting access to resources, such as file and print sharing, or accessing the network (the type of connection itself can vary: VPN access, wireless access, local access). On the other hand, TACACS+ is more secure and can be used for accessing the network devices, like firewalls and routers, in other words, for device administration. Also, it is necessary to mention that RADIUS works only with stateless mode. That means that packets sent do not rely on previous sessions and every packet is by itself, which means that every packet is heavier, because the server must send same information over and over again. This flaw does not exist in a stateful mode.

Stating that, I want to refer to a part of RFC for RADIUS and why UDP is, in this case, very good for the particular usage. Rigney et al. (2000, 11) state: “The stateless nature of this protocol simplifies the use of UDP. Clients and servers come and go. Systems are rebooted, or are power cycled independently. Generally this does not cause a problem and with creative timeouts and detection of lost TCP connections, code can be written to handle anomalous events. UDP however completely eliminates any of this special handling. Each client and server can open their UDP transport just once and leave it open through all types of failure events on the network.” This might be one of the reason people do prefer RADIUS over TACACS+, UDP does not establish the perfect and reliable connection, but also eliminates the unnecessary steps for better communication.

3.3 DIAMETER base protocol

DIAMETER base protocol is an advanced version of the RADIUS protocol. The irony in the name indicates the possibility for it to be two times better, and its appearance is completely based on improving the predecessor's limitations. The protocol was developed at the end of the 20th century and later on it was standardized by IETF in 2003. DIAMETER has evolved into connection-oriented protocol, and now it runs over TCP or SCTP (Calhoun et al. 2003, 7). DIAMETER is aimed more at roaming users. DIAMETER consists of two parts: base protocol and DIAMETER applications (set of extensions, such as Mobile IP, NASREQ, and accounting) and the base protocol is not meant to be used separately, but as the base for these applications. Each command has its own Attribute-Value Pair (AVP), similar to RADIUS attributes, which makes DIAMETER compatible with RADIUS. (Goswami 2003, 105-106.)

DIAMETER can run both the stateful and stateless mode of authorization. In the stateful mode the server during the whole session keeps the connection and stores the information about the session, and all the packets relate to each other (Niemi 2002, 48). Whereas the RADIUS protocol can operate only in the stateless mode, which I have mentioned and explained earlier.

3.4 Kerberos

Kerberos was introduced by MIT in order to protect the UNIX-based system. Kerberos as protocol has been developed and improved several times. The first time Microsoft has used Kerberos version 5.0 as an open standard with Windows 2000 release. (De Clercq 2004, 133-134.) Nowadays the most definite advantage of Kerberos is that it is suitable for many operating systems (OSs), which means that even if the server runs Windows, Linux, or Mac OS, all of these will be able to authenticate to the central Kerberos system without any troubles (Král 2011, 16). The main idea of Kerberos is to provide authentication policies for users and devices over an unsecure network by means of secret keys which are never sent over the network (Neuman et al. 2005, 6).

The name of the protocol comes from mythology where that was a name for hellhound, the three-headed dog, which was guarding the gates of the underworld. The three heads stand for the three major authorities of the Kerberos system: Key Distribution Center (KDC), Authentication

Service (AS) and Ticket Granting Service (TGS). All of them play essential role for the whole process. Nevertheless, I prefer to think about the idea of the key points differently, namely of the three passwords that are involved in the process. All three keys are possessed by KDC: one is for communicating with the user, the second is for AS, and the third one is for KDC itself. None of the passwords are sent over the network. Either symmetric or asymmetric encryption algorithm can be used. Either way passwords will not be sent over the network anyway.

Kerberos belongs to the family of Single Sign-On methods which allow the user to log into the system once and later on the application handles the authentication issue. Time frames are quite important for this process to operate duly. Thus, the client's and server's machines have to be synchronized, even with a bit more than 5-minute-shift (the default time that can be changed if preferred differently) shift clients will not be able to authenticate. All the tickets that are provided by KDC have Time-To-Live (TTL) timers. The main ticket which allows users to stay out of trouble of authenticating themselves every time, is Ticket Granting Ticket (TGT), which is hashed with KDC's private key and cannot be decrypted by users, so that the server itself will know that it has already authenticated the user. It includes the most essential information about the user, and by default, it lasts for 10 hours (can be changed, if desired). KDC usually listens to requests via TCP or UDP on port 88. The client might try the UDP first, but if for some reason the server will not be able to handle that request, it will ask for the client to try again, but over the TCP connection, so that the client is claimed to be able to send TCP requests anyway. The client sends an authenticator (includes data and time which creates some time frame on handling the identification, but also prevents the attacker from replaying it later on) to Key Distribution Center. (Messer 2014b.) Figure 4 explains the process of Kerberos authentication.

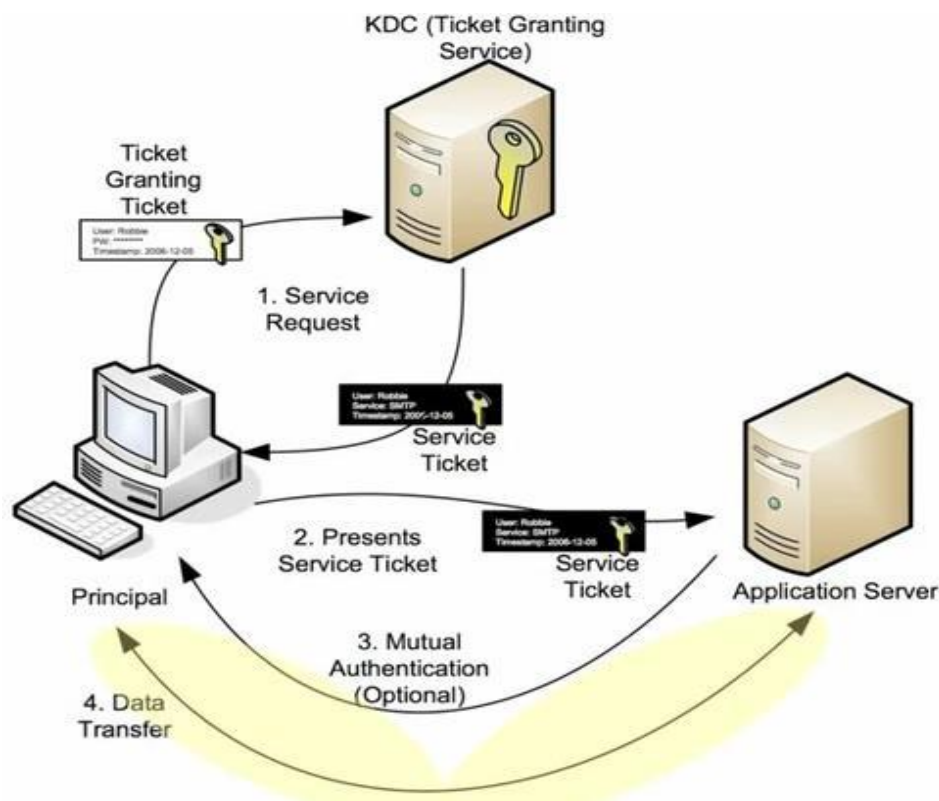


FIGURE 4. Kerberos authentication sequence (Messer 2014b)

3.5 Point-to-point Authentication Protocols

Before I will go into details, I must point out that authentication protocols bring the trust between the nodes. That is why they work between peers and called PPPs. Nevertheless, Extensible Authentication Protocol is the most difficult one among others. Therefore, I will use it to demonstrate the message flow between EAP peer (the device that is trying to connect to the network), EAP authenticator (an edge of the network that is usually represented by Wireless Access Point - WAP) and Authentication server (the entity that determines whether to grant an access or not). EAP flow chart can be found in Appendix 1. On the picture the reader can clearly see that there are two ways of communication: the first one is between peer and authenticator and the second one is between authenticator and the Authentication server. The first part communication in my case is managed through Wi-Fi, while the second part is controlled by RADIUS protocol.

There are dozens of protocols, which main purpose is to authenticate the established connection between the devices to communicate securely. I will introduce and explain some of them in order as follows:

- EAP
- PAP
- CHAP
- MS-CHAP
- MS-CHAPv2

These are the most common authentication protocols that have been put into use over time. Some of them are only used for educational purposes; some are used for security reasons nowadays still, so it is quite important to understand the difference between these protocols. Moreover, as long as all these protocols are PPP, the communication is established on data-link layer.

3.5.1 EAP

The abbreviation EAP stands for Extensible Authentication Protocol. EAP itself does not provide the authentication, but rather a framework for authentication protocols. This framework grants the base for a method of authentication, a method for a key exchange and a way of handling these keys between the connected nodes, and it is usually called EAP type. EAP is there to create a message format where each EAP type defines its own way of encapsulation of EAP message. The main feature of the EAP authentication is that a server is the one who initiates the session. (Aboba et al. 2004, 7.) Appendix 1 clearly shows the same as well.

The framework is widely supported by different OSs and used for point-to-point and wireless connections. WPA2 supports seven EAP methods, though the most common EAP types are: EAP-TLS, EAP-TTLSv0, PEAP (PEAPv0/EAP-MS-CHAPv2). In the practical part of the thesis I aim to use PEAP. Nowadays it has two versions: PEAPv0/EAP-MS-CHAPv2 and PEAPv1/EAP-GTC (is a Cisco proprietary protocol as an alternative to PEAPv0). However, when people talk about PEAP, they mean the EAP-MS-CHAPv2 protocol (Ou 2005). This protocol is the second most widely used after EAP-TTLSv0 (Sotillo 2007, 2).

3.5.2 PAP

PAP stands for Password Authentication Protocol. It is nowadays only used for testing purposes, because quite compatible with many OSs and it sends the credentials over the network in the plain text. The “clear” conversation opens up the possibilities for variety of attacks, such as error and playback attacks. Also, once the authentication process is successful, PAP does not talk again with the client. (Shinder 2001.)

3.5.3 CHAP

Challenge Handshake Authentication Protocol or CHAP is another authentication protocol and it does not send the shared password. However, instead of that the protocol creates a “challenge” and presents it to the client. The client on its turn hashes the challenge message and the password with MD5 function and, along with the client’s username, sends them back to the server. Server checks the hashes with its own computations and sends the verdict message to the client. CHAP can also send the challenge whenever to reauthenticate the client and to avoid the case of impersonating, meaning that CHAP eliminates most of the holes the PAP had. Although, this protocol is quite vulnerable to the remote server impersonating. (it-security.blogspot.fi 2005.)

3.5.4 MS-CHAP

MS-CHAP is a similar to CHAP protocol, but designed by the Microsoft Corporation. The main difference between them is that CHAP is required to have the clear-text version of the password on the server in order to compare the results and give response, when MS-CHAP only needs the hashed string of the password. MS-CHAP uses MD4 cryptographic hash algorithm. (Microsoft 2015a.)

3.5.5 MS-CHAPv2

MS-CHAPv2 is an upgrade version of MS-CHAP protocol. It introduces two-way authentication, where both, a server and a client, verify their identities by themselves independently. The connection is established only when both parties are satisfied with the response messages. It also uses different keys for received and transmitted messages. (Microsoft 2015a.)

3.6 Wi-Fi security standards

Wireless communication has been established for quite a while, but along with the progress, the security measures started to matter only at the edge of the 21st century. Wireless connection is by its nature very vulnerable to all kinds of interferences, and without securing the network anybody who can receive the signal can eavesdrop everything from the network. Thereby, the security standards were found to provide the system of algorithms and encapsulations for message integrity and genuineness.

3.6.1 WEP

The first of the security standards is WEP. That stands for Wired Equivalent Privacy (sometimes mistakenly called as Wireless Encryption Protocol). WEP is a security algorithm for wireless networks, which was introduced in 1999, and it consists of two parts: authenticating and encrypting. This cryptographic protocol uses RC4 as an encryption method to encapsulate both error-detecting algorithm and the text message (Shirey 2007, 336). There are two different lengths of the key, either 40 bits (WEP-40) or 104 bits (WEP-104), and the same is used to authenticate the client and to encrypt the traffic (Vibhuti 2005, 2-3). Within few years after the release it was proven that standard was easy to break, and nowadays it takes about few hours to obtain the key.

3.6.2 WPA

WPA or Wi-Fi Protected Access is considered to be a draft of the 802.11i standard, which was developed in order to replace the less secure WEP standard where vulnerabilities were quite obvious. According to the Wi-Fi Alliance (2004) as the developer, promoter and certification authority), the standard is a sum of techniques that are combined together and oriented to protect and secure the wireless network. In comparison to WEP, WPA has enhanced data security and toughened access controls to wireless networks. WPA uses TKIP (Temporal Key Integrity Protocol) which is based on the advanced RC4 encryption scheme, provides a new key for each packet and adds MIC (Message Integrity Check). There are two versions of WPA: WPA-PSK (Pre-Shared Key) and WPA Enterprise. WPA-PSK is usually used for home wireless networks, and one key is set on a wireless device for anybody who tries to gain an access from that node. It is usually either wireless access point or wireless router that works as an extension to the existing

wired network. WPA (or WPA Enterprise) introduces the EAP encapsulation which is used for remote authentication via Centralized Authentication Server (e.g. RADIUS) using certificates. (TP-LINK 2015.) Nevertheless, the standard still had some flaws what led the development to a more secure option.

3.6.3 WPA2

WPA2 (Wi-Fi Protected Access 2) is a more successful heir of WPA and an IEEE 802.11i-2004 standard, but it is backwards compatible with WPA, which made the process of switching to a new version very smooth. The main advantage of the second version is a more secure encryption protocol - CCMP, or Cipher Block Chaining Message Authentication Code (CBC-MAC) Counter Mode Protocol, of the AES (Advanced Encryption Standard) specification. CCMP uses a 128-bit key and 128-bit block size and comes as a mandatory part of WPA2, but the standard can also work with TKIP. (Wi-Fi Alliance 2004.) Also, WPA2 provides a new Pre-authentication feature, the purpose of which is to help the roaming users to receive authentication from other APs while still being connected to the previous Network Access Server (Microsoft support 2013, 893357). WPA2 is aimed more at enterprise security and provides nowadays seven different EAP types. These are: PEAPv0/EAP/MSCHAPv2, PEAPv1/EAP-GTC, EAP-TLS, EAP-TTLS/MSCHAPv2, EAP-SIM (the first 5 types implemented and supported by WPA2 in 2005), and EAP-FAST and EAP-AKA were added in 2009. (Wi-Fi Alliance 2009.) Since 2006 Wi-Fi Alliance demands for WPA2 to be implemented on the device in order to get the Wi-Fi certification label on its side.

Wi-Fi Protected Setup (WPS) is considered to be a standard, but it is more like a feature which allows a user to add new devices securely to their home wireless network. However, in 2011 it was proven that WPS feature could actuate flaws into the system by creating additional points of attack, which hackers can exploit (Viehböck 2011).

4 CREATING WINDOWS ENVIRONMENT

After the theory part of the thesis was finished, I had decided to work with additional software called TekRADIUS as a RADIUS server. Some unexpected errors have occurred during the

tryouts of the program. The program itself is not very popular and there are not that many helping guides about the problem I had faced. So, to waste no more time, I came to a decision to create a personal private network with the Windows Server as the main OS.

The installation of Windows environment that I seek to use consists of the following steps:

- Installation of the chosen OS and post-configurations,
- Installation of SQL server,
- Installation of AD DS and AD CS (along with the DNS server),
- Installation of NPS and its configuration as RADIUS server,
- Installation of DHCP on the VM using Hyper-V as a hypervisor.

The purpose of the RADIUS server is to authenticate and authorize users onto the established network which the server “solemnly swears to protect” against any unauthorized endeavor to access the network. Although, RADIUS does not provide anything else but authorizing the entries. It means that other several key services have to be set along with it. In the following sections I will explain the key steps of installations, challenges that occurred along the way and some interesting notes that I have found about particular parts of installation.

4.1 OS Installation

Before I begin, it would be good to point out that for a student of Mamk this idea will not cost one dime due to the partnership, but in a real world this might be a pricy concept. The very beginning of any machine starts with the Operating System, what can be simply described as initial software that provides communication between hardware and the rest of the applications. The choice of OS does not create much of a difference, when it comes to RADIUS server. Most of the major server aimed OSs support some type of RADIUS service or service can be installed as an application into the environment. I have decided to go with Windows Server 2012 R2, because the OS is relatively new and also the RADIUS server can be implemented as a feature there. Microsoft nowadays, due to the needs of enterprises, works very hard on server capabilities and provides really good results, no doubts, which mean that knowing the essential parts in details of such OS would be quite useful to me.

The installed version of the OS for my server is Windows Server 2012 R2 Datacenter with Graphical User Interface (GUI). The difference in the editions of Windows Server 2012 R2 is mainly about how many Virtual Machines (VMs) can be visualized. Standard edition allows only two VMs per server, Core - up to five, and Datacenter does not have any limits about this issue. After the OS has been installed, few not mandatory, but quite useful steps should be done, before installing any roles and features.

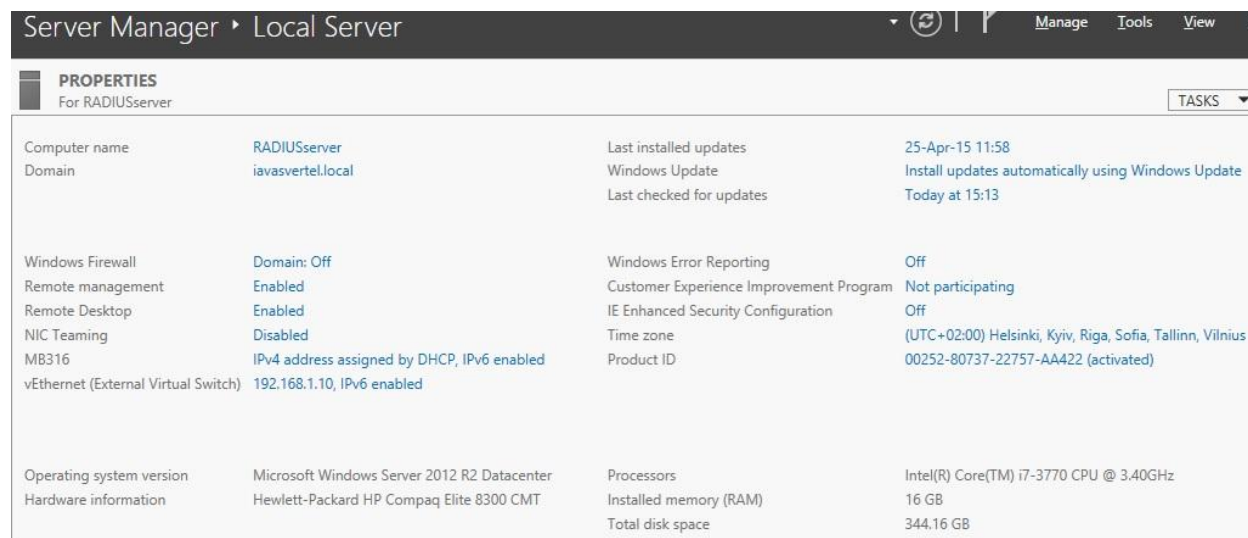


FIGURE 5. Server Manager > Local server: Final configuration

Now I will explain the handy steps for post-install stage (all of these steps are done with the help of Server Manager - Figure *). First, it would be wise to change the name of the PC, because the name that has been given during the installation is quite difficult to be managed with. Therefore, it is better to use the name which either resembles the purpose of the machine or is easy for the administrator to deal with. Secondly, the Remote Desktop feature should be enabled. Later on it is possible to configure and add users that are allowed to have the remote access to the server via Remote Desktop Connection. The third step is to provide the server with the static IP address, so that other devices know the exact location of the Authentication server or any other services that might be running on with the computer along with RADIUS. Following that, I turned off the Internet Explorer's Enhanced Security Configuration, and then I downloaded a browser just for the sake of it. At last, it is preferred to configure Windows Updates in company with time and time zone that must be correct.

With Windows Updates, I faced a challenge. When I asked it to find the updates, the process of finding anything was never-ending. After a few restarts, Windows eventually showed me an error 80070003. Microsoft has explained this error to happen due to a mess with temporary files. All I had to do was to stop the Windows Update service, to delete temporary files in folders Download and DataStore in the “C:\Windows\SoftwareDistribution” directory and finally, to restart the process in “Services”. The problem was solved after rebooting.

4.2 MS SQL server

Database server is the key point of any server-client system. Its primary aim is to perform maintenance and management of the database, which holds users' related information, and to be responsible for the integrity and security of that data. Requests are made with query language. Most of the time the SQL (Structured Query Language) is used. Also, it is a server's duty to extract needed information when a request arrives.

Therefore, the next installation was the Microsoft SQL Server 2012. I was surprised to find out that the File Explorer now can manage the ISO image files and mount them on virtual disk drive. The setup itself runs several checks during the whole installation on any possible fault and failures that may prevent from successful installation, like the need for restart for the server machine, or lack of software. That feature helps to the user to be sure that everything is alright, or, otherwise, he has to do some additional steps. In fact, as long as I just have installed server from a scratch, I have faced that problem. In order for smooth installation, I had to have Microsoft .Net framework, then Microsoft Visual C++ Redistributable, and, finally, it was important for SQL server, as it turned out during the installation, to have the NetFx3 feature of Windows Server to be enabled. Without NetFx3 being enabled, the “Database Engine Service” has failed to be installed, and that is the actual SQL server. Thus, I had to cancel the installation of SQL server, enable the required feature and redo the process again.

In the “Feature Selection” window I have checked Database Engine Services, Client Tools Connectivity, Management Tools - Basic (the “Complete” option checks automatically) and Documentation components. As it turned out later on, the “SQL Client Connectivity SDK” has been installed automatically as well. In the window of “Instance Configuration”, I have gone

with Default instance as long as I have only one aim, the RADIUS server. You can create many named instances on one machine and only one default instance per machine. On “Database Engine Configuration” screen, I have chosen “Mixed Mode”, because it allows both Windows and SQL Server Authentication.

After the installation was complete, I had to verify that the SQL server is up and running. To do so, I went to MS SQL Server 2012 Management Studio and authenticated myself as an administrator. The password for “sa” user had been set during the installation, and for the time being I was logged in as an administrator, so the system did not ask for the credentials (See Figure 6).

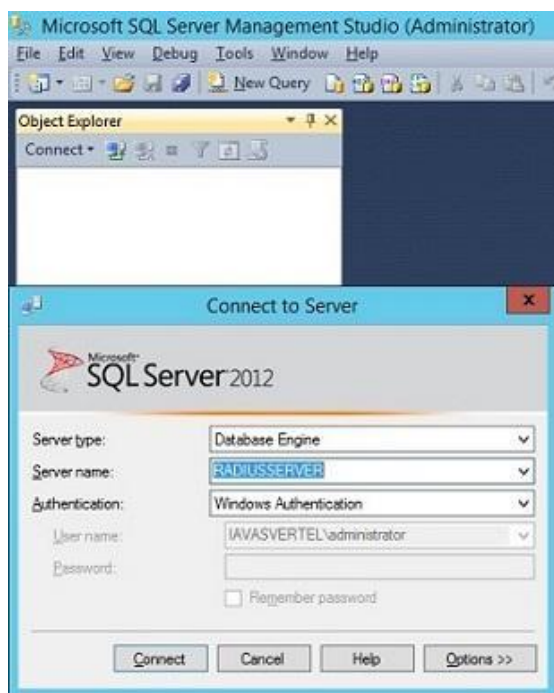


FIGURE 6. Login screen

When I was authenticated, I could see that the domain is iavasvertel and I was logged in as an administrator (See Figure 7). However, the SQL server in this study was only used for the RADIUS accounting purposes.

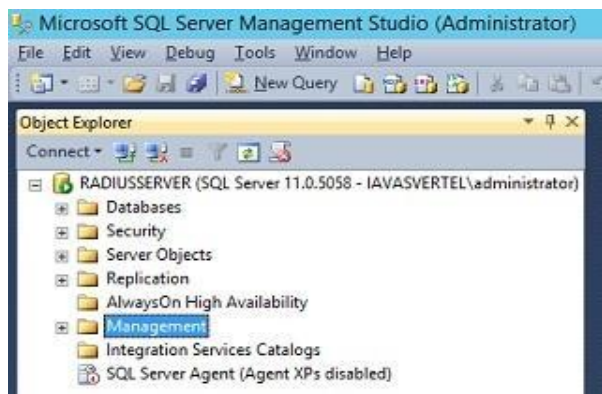


FIGURE 7. Authenticated to SQL

4.3 Active Directory implementation

At this point, I had a need for the Active Directory (AD) to create groups and users, because only few accounts are created by default. I started with AD Domain Services (AD DS), the instance that keeps database with users, groups, computers on the domain and handles users' authentication on the network and relations between users and domains. At post-installation stage, I must promote the server to be the Domain Controller (DC), because there must be at least one DC on the network in order for AD to manage users' requests. During the promotion, I have created a new forest called iavasvertel.local and set the forest and domain functional levels to be Windows Server 2012 R2. This option must be set with caution, because later on it can only be set higher, but not lower. For example, you can promote Windows Server 2008 to Windows Server 2008 R2 or Windows Server 2012, but not to Windows Server 2003. However, this option is only related to DCs. I have chosen the level to be 2012 R2, because I will not have any legacy computers on the network and that is in fact the only Windows OS I will be working with. It is still quite essential to point out that AD DS does not work without DNS, but nowadays OS takes care of that and installs DNS server along with AD DS.

Next, it is necessary to install AD Certificate Services (AD CS). This feature is a Certificate Authority and is needed for EAP connections to link the used key with the identity of the device or service. Almost everything was set by default, aside for the database and log database locations, so that they will be easier to find (C:\RootCA\DB and C:\RootCA\Logs). After the needed parts of the AD were installed, I could generate users and groups. I have created

universal security group called “Wireless Users”, then testuser account and added it to the “Wireless Users” group. The password for the user is set to “never expire” and user cannot change it. In the end, I have added user Dmitry Opikhalov with name iavasvertelADMIN and password’s setting “Password never expires” and then joined him to the “Domain Admins” group.

4.4 Establishment of Network Policy Server as RADIUS

Microsoft has developed OS’s built-in version of RADIUS server which is nowadays called Network Policy Server (NPS). It used to be called Internet Authentication Service (IAS) before Windows Server 2008. (Microsoft 2015b.) It provides AAA services for wired and wireless connections as centralized authentication, which suits the topic of my thesis ideally. Therefore, I decided to use NPS as the RADIUS server. After the installation was complete, in the NPS window I have selected “RADIUS server for 802.1x wireless or wired connections” and started to configure it. I added an AP with IP 192.168.1.51 and a shared key. Then I selected Microsoft PEAP as EAP type and the Wireless Users group that was configured previously. As a closing step, I had to register the server in AD, because NPS will not be able to authenticate users until it is registered. Then, I configured AP – WAP 121, and the configurations can be found in Appendix 2.



FIGURE 8. Properties for IaVasVerTeL

The next step was to create and configure new Wireless Network Policy (Path in “Default Domain Policy” for iavasvertel.local domain - Policies\Windows Settings\Security Setting\Wireless Network) via Group Policy Management. I created a new Infrastructure where the SSID is IaVasVerTeL, authentication is WPA2-Enterprise, encryption is AES, network authentication method is PEAP, and the authentication mode is User or Computer authentication, as shown in Figure 8. In advanced options, I have enabled the Single Sign-On feature. And finally in Public Key Policies I had to enable Auto-Enrollment for Certificate Services Client (see Figure 9) and check the Define these policy settings option for Certificate Path Validation Settings (see Figure 10).

FIGURE 9. Enabling Auto-Enrollment

With PEAP authentication, it is essential to understand what a certificate is. The certificate is a digital proof of validation that the public key in action is granted by Certificate Authority (CA) of which the user can trust. The digital certificate includes both statement of identity and public key. The idea of certificates is to prevent from impersonating. By enabling auto-enrollment, I did not have to worry anymore about certificate issuing for clients if such are needed.

Stores Trusted Publishers Network Retrieval Revocation

Specify rules for user trust of root certification authority (CA) certificates and peer trust certificates.

Define these policy settings

Per user certificate stores

Allow user trusted root CAs to be used to validate certificates (recommended)

Allow users to trust peer trust certificates (recommended) Select Certificate Purposes...

Root certificate stores

Root CAs the client computers can trust:

Third-Party Root CAs and Enterprise Root CAs (recommended)

Only Enterprise Root CAs

For certificate-based authentication of users and computers the client computers must use CAs registered in the Active Directory

CAs must also be compliant with User Principal Name constraints (not recommended)

FIGURE 10. Policy settings has been defined

Certificate path validation is a rule, when the received certificate is checked to be trusted. There are a lot of certificates in use and some CAs rely on other CAs, and therefore, it is hard to decide which certificates can be trusted. Based on that rule, only the implicitly trusted CA can be at the top of the path, according to the root CA, and the feature has to be enabled.

4.5 DHCP on Virtual Machine

By that time, I was able to authenticate the testuser, but because I had no DHCP server installed yet, the wireless user did not have an IP address. I decided to put the DHCP server onto a virtual machine. Therefore, I installed Hyper-V, created an external virtual switch and then a VM, installed Windows server 2012 R2 and added a DHCP role there, and created a scope 192.168.1.81-140 (later on was changed to 192.168.1.101 - 200). However, DHCP could not connect to the physical server on which I had the AD, DNS and RADIUS servers. Therefore, the server could not be joined to the domain.

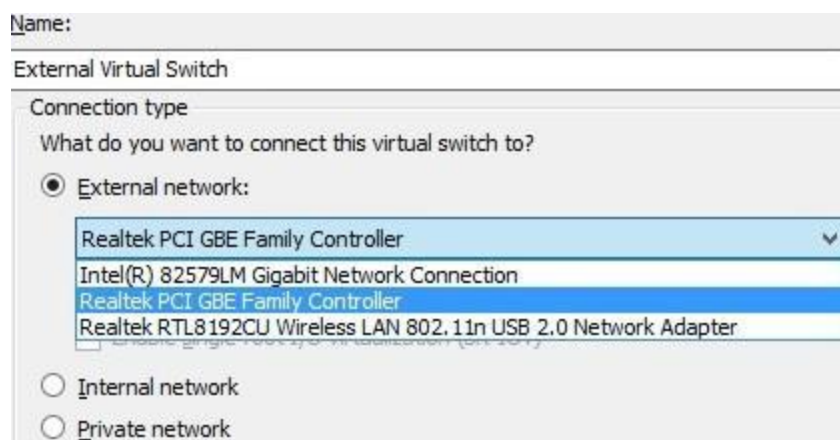


FIGURE 11. NIC selection for creating external virtual switch (Name was set by default!)

The problem was that I did not name the network adapters appropriately and mixed them up, and later I did not check the NICs' names, because when the installation was complete I was able to ping from host to the VM, but could not do it backwards. All I had to do was to rename the NICs with caution and redo the connection. As shown on the Figure 11, the Realtek PCI was that one I was supposed to configure, and before that I messed the Intel connection.

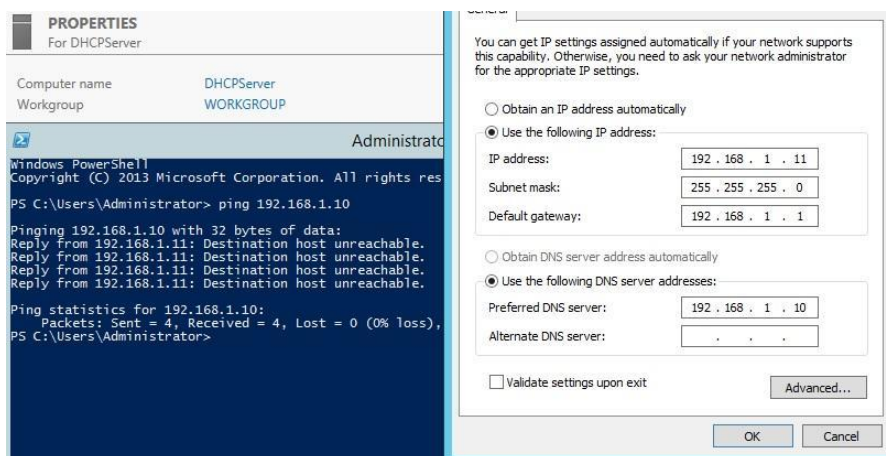


FIGURE 12. Physical NIC have to be set as the edge of the virtual network

Also I had to configure the virtual NIC's default gateway, and it was supposed to be 192.168.1.10 (Figure 12), mainly because the virtual network (visualized by the OS) must be separated from the physical one and the server's NIC is the point where it ends. After I had changed it, I was able to join to the domain iavasvertel.local successfully, and Host (A) named DHCP Server has been added to the DNS server's table (Figure 13).

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[172], radiusserver.iavasvertel.local., host...	static
(same as parent folder)	Name Server (NS)	radiusserver.iavasvertel.local.	static
(same as parent folder)	Host (A)	192.168.1.10	24-Apr-15 6:00:00 PM
DHCPserver	Host (A)	192.168.1.11	24-Apr-15 6:00:00 PM
radiusserver	Host (A)	192.168.1.10	static

FIGURE 13. DHCPserver added into the DNS table

When I had fixed the NICs' problem, I encountered the 0x8009030e error (Figure 14), while installing DHCP server role on the DHCPserver machine.



FIGURE 14. Configuration Error 0x8009030e

At the post-installation, system wizard had asked me to specify credentials of the account with privileges for authorization purposes in AD DS, because I was logged on as a local administrator. By clicking the Specify... button (Figure 15), I was prompted to input my login and password (Figure 16).

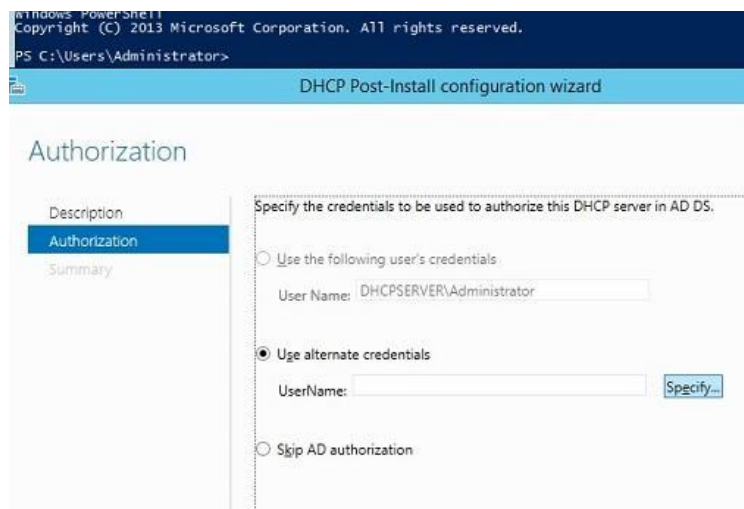


FIGURE 15. System did not recognize local administrator

I have inspected the error several times and the possible reasons that it may have happened because of, but I could not clearly say what was causing that problem. Because at the end of it all the domain administrator's credentials have solved the problem, while they were typed in in the first place.

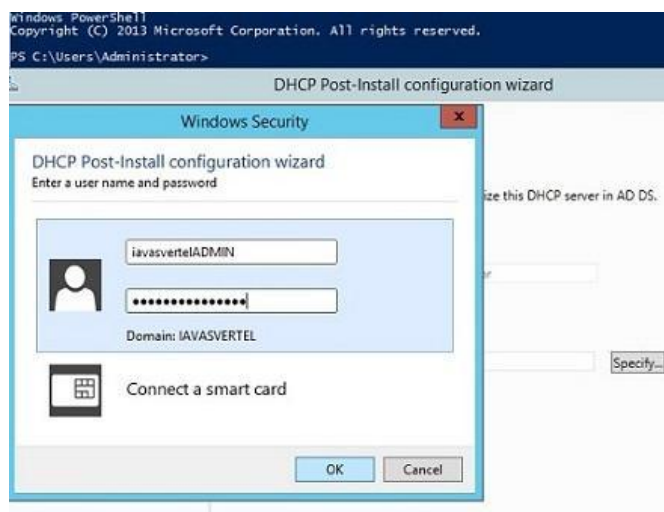


FIGURE 16. Credentials for domain administrator

After I was verified (Figure 17) and clicked Commit, the error had occurred, notifying me about my expired Kerberos session (I use Single Sign-On). I have tried it again, but the same error has occurred again.



FIGURE 17. Administrator was recognized

At that point, I was logged on as a local administrator for DHCP Server (Figures 15 and 16), and I decided to log in as a domain administrator. By doing so, the problem disappeared, and the credentials were input automatically (Figure 18), and now the server was authorized in AD DS.

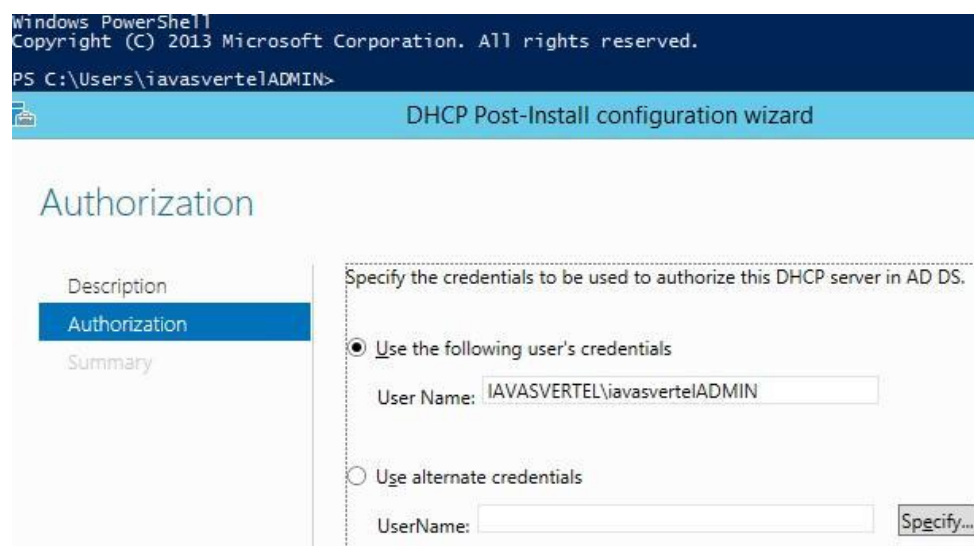


FIGURE 18. System has recognized the domain administrator

On the Figure 18 at the top left corner it is possible to see that by that time I was already logged as a domain administrator and the system has recognized me straight away. The problem has disappeared and I was able to complete the post-installation wizard.

5 IMPROVING AND TESTING

This chapter will explain some mechanisms that may improve the system's overall behavior. Some additional features will be introduced and the test of the authentication will be done with explanations. The topography of the network I partially already created is shown in Figure 19.

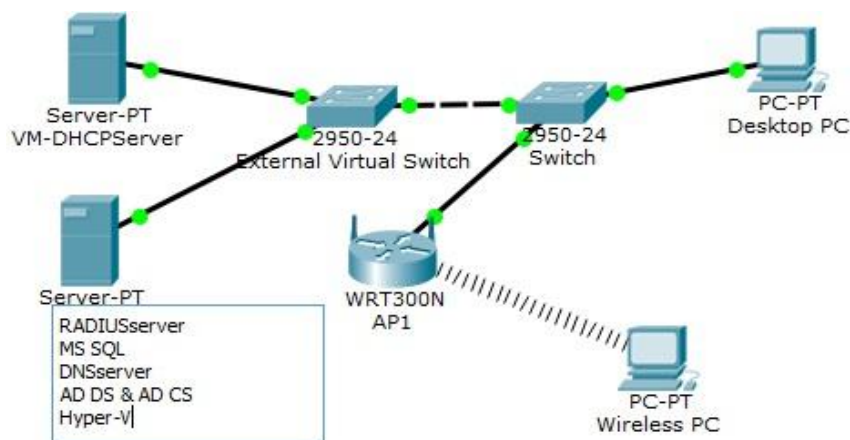


FIGURE 19. Packet Tracer Schema

5.1 Single Point Setup

The manual of Cisco's WAP-121 state that Single Point Setup feature can be enabled. This feature helps to manage several APs at once, i.e. when I will make changes to one AP, the other APs that are joined to the cluster can update the configurations automatically.

Upgrade Firmware

PID VID:	WAP121-E-K9 V01
Firmware Version:	1.0.0.3

Transfer Method: HTTP/HTTPS
 TFTP

New Firmware Image: WAP121_1.0.5.3.tar

Note: Uploading the new software may take several minutes. Please do not operation.

FIGURE 20. Firmware current version

The original firmware (version 1.0.0.3) does not support that feature, and I had to upgrade the firmware in order to use it. FAQs said that APs must run the latest firmware and be of the same model. Thus, I downloaded the version 1.0.5.3, latest at the moment, and uploaded it to the APs via HTTP (Figure 20).

The system notified me about the changes I was about to make and I should not switch the tabs of the browser. After the upgrade was completed, the browser's page was reset and it showed the logon screen. No configuration changes had been made by the system during the upgrade process. The system had just added a new option Single Point Setup. I took another AP that had default configurations, upgraded firmware there and assigned the 192.168.1.52 IP address. Next, on the AP I had configured previously, I created a cluster called LABcluster and set location as MB316. After joining the second AP to the cluster, the window froze and I was prompted by the login window. The default credentials were legit no more, because it took all the settings from the configured AP. When I got authenticated to the AP, the screen showed that second AP was successfully added to the cluster (Figure 21).

The screenshot shows the Cisco Small Business WAP121 configuration interface. The left sidebar contains navigation tabs: Getting Started, Run Setup Wizard, Status and Statistics, Administration, LAN, Wireless, System Security, Client QoS, SNMP, and Single Point Setup (selected). Under Single Point Setup, the 'Access Points' tab is active, showing a table of detected APs in the LABcluster.

Location	MAC Address	IP Address
MB316	50:57:A8:67:44:AC	192.168.1.51
MB316	50:57:A8:67:44:9C	192.168.1.52

Below the table, the configuration options for Single Point Setup are shown:

- Single Point Setup: Enabled
- Access Points detected in Cluster: LABcluster
- Location: MB316 (Range: 1-64 Characters)
- Cluster Name: LABcluster (Range: 1-64 Characters)
- Clustering IP Version: IPv6 IPv4
- Buttons: Disable Single Point Setup

On the right side, there are two status indicators: 'Clustering' (represented by a radio tower icon) and '2 Access Points' (represented by an icon of two people).

FIGURE 21. Single Point Setup: the cluster of two APs

I left the cluster afterwards, to check if the settings will remain the same. They did. Now I added new RADIUS client to the table and disconnected first AP just to check if the second operates correctly. After a while it has established the connection with the server and authenticated the wireless user (Figure 22).

The screenshot shows a web browser window with the address bar displaying '192.168.1.52/admin.cgi?action=main'. The page title is 'Business P121 Wireless-N Access Point with Single Point Setup'. A 'Log' section is visible, containing a 'Refresh' button and a 'Log Table' with the following data:

Time Stamp	Description
Dec 31 1999 22:57:46	authenticated - identity " EAP type: 25 (PEAP)
Dec 31 1999 22:57:46	The wireless client with MAC address f8:1a:67:08:bd:02 has been successfully authenticated.
Dec 31 1999 22:57:46	wlan0: WPA STA f8:1a:67:08:bd:02 pairwise key exchange completed (WPAv2)
Dec 31 1999 22:57:46	EAP authentication with the authentication server completed

FIGURE 22. Successful authentication by the second AP

The one thing that can be clearly seen from the figure is that if previously the time was configured manually, the default starting time will be set at new members of the cluster.

5.2 Sharing

The most obvious way to prove that a device has been authenticated on the network comes with the help of sharing resources. If a user is allowed to put something on the network and others can see the changes, then he was successfully authenticated and authorized. In the next sections I will prepare the environment for this task, set the privileges for users and write what exactly happened on the network and was I able to achieve the goal or not.

5.2.1 Prepare to share

To prove a point of connectivity the common folder must be created. I decided to name it as a Shared Folder (the path to the folder is shown in Figure 23) on RADIUSserver. The folder is set as a connecting point for different users.

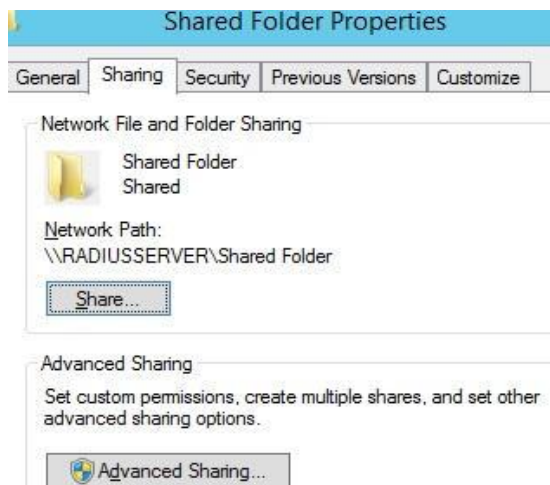


FIGURE 23. How to access the Shared Folder

Also, I have decided to share it for everyone, so that anybody could see it and do changes within the folder. Figure 24 shows who exactly is able to do the changes.

Name	Permission Level
Administrator	Read/Write ▼
Administrators	Owner
Everyone	Read/Write ▼

Everyone
Permission: Read/Write
Read/Write allows people to open, change and create files

FIGURE 24. Availability of the Shared Folder

There are two objects inside of the created folder. The first object is a picture, which is only available to the testuser (Figure 25). The second one is a folder, which is only available for user PC1 (Figure 26) in the Computer Accounts group. These objects were found during the process, because I need an evaluator to see the changes that were made, aside for administrator.

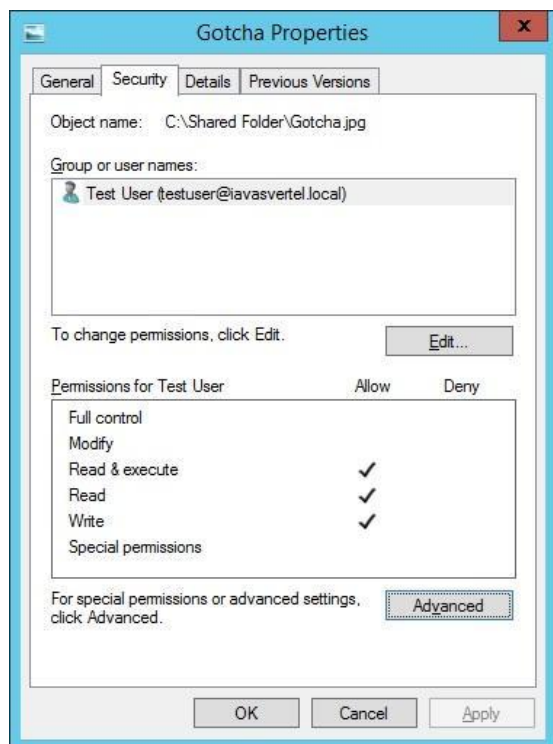


FIGURE 25. Only the testuser is allowed to modify the file

Useful note: as a system administrator you should always create a group even if there is only one user inside, because companies are tend to grow and scale very fast, therefore when times come you do not need to configure the same properties for another user, while you can simply add him to the group.

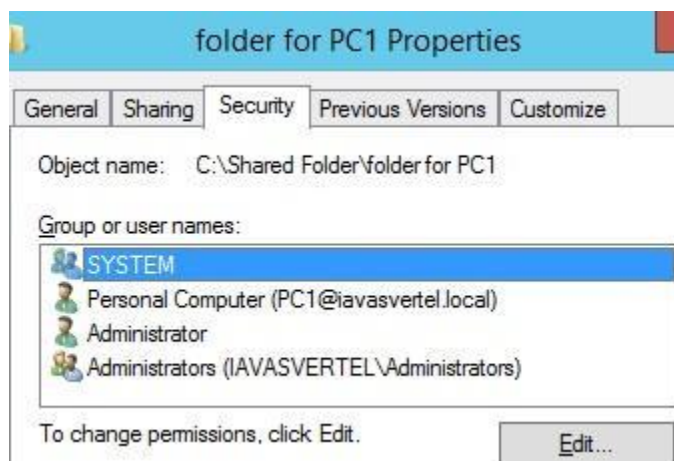


FIGURE 26. Only PC1 and administrators can access the folder

From DHCPserver I typed the “\\RADIUSserver” command into the Search field (Figure 27) and, as long as it is connected to a domain and logged on as an administrator, the search has shown me all the files that are shared.

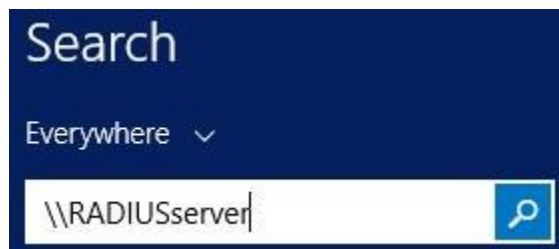


FIGURE 27. Search for RADIUSServer

Now everything should have been configured and I was able to authenticate testuser and PC1 accounts. I have connected a PC to my private network, set to obtain IP automatically, and it was welcomed by my DHCP and DNS servers (Figure 28).

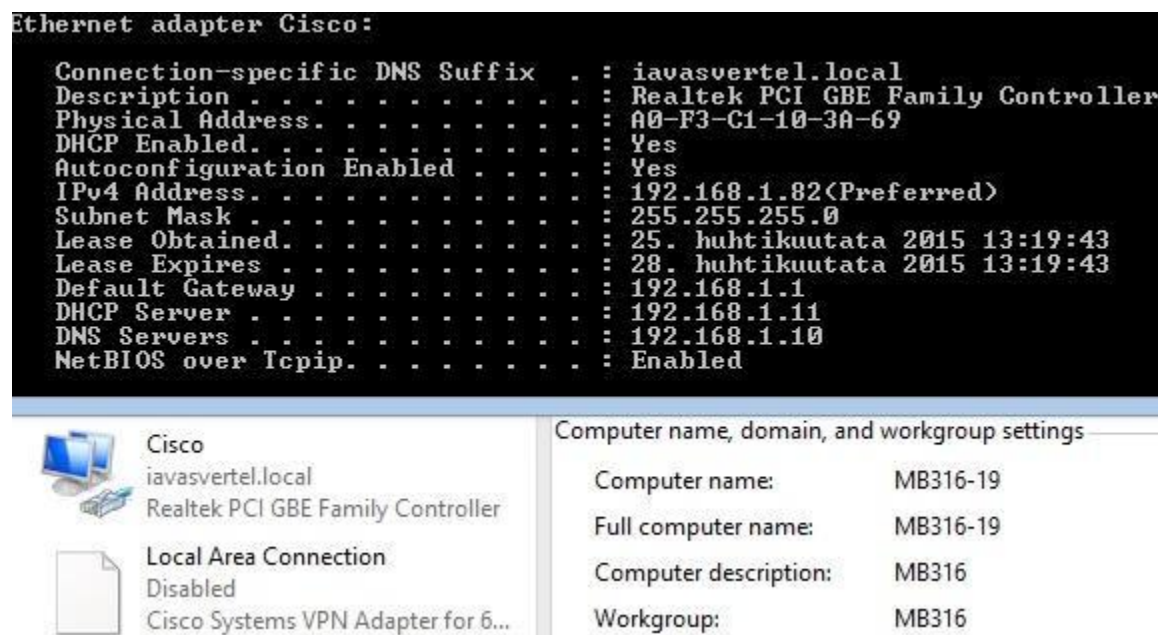


FIGURE 28. DNS and DHCP provided PC1 with their services

Nevertheless, when I typed in search the same command as I did on DHCPserver, the File Explorer froze for a minute and then asked for my credentials (see Figure 29). That proves that the PC was not yet a part of the iavasvertel.local domain and there was no point to input

credentials, because the PC was still a part of the MB316 WORKGROUP as it is stated in the Figure 28. That was my thought and I was completely wrong. When I typed in the admin credentials, I was able to see the Shared Folder and its contents.



FIGURE 29. The user is unable to connect to the server - the authentication is required

At this moment, the problem was that I did not see how to disconnect myself from the server. The solution was to type a few commands in command line. They are shown in Figure 30. Even though I typed these commands, the system still allowed connecting to the server for some time. After 15-20 minutes, I checked the connection and by that time I was asked again for credentials.

```

C:\Windows\System32>net use
New connections will not be remembered.

Status          Local          Remote          Network
-----
Disconnected P:  \\MB3\Public   Microsoft Windows Network
Disconnected Q:  \\MB3\Oppilas  Microsoft Windows Network
OK              \\RADIUSserver\IPC$  Microsoft Windows Network
The command completed successfully.

C:\Windows\System32>net use /delete \\RADIUSserver\IPC$
\\RADIUSserver\IPC$ was deleted successfully.

C:\Windows\System32>net use
New connections will not be remembered.

Status          Local          Remote          Network
-----
Disconnected P:  \\MB3\Public   Microsoft Windows Network
Disconnected Q:  \\MB3\Oppilas  Microsoft Windows Network
The command completed successfully.

```

FIGURE 30. Delete remote drive with the help of net use command

I still had to add MB316-19 to the iavasvertel.local domain. But first, I wanted to check if the PC1 credentials were worthy when joining the domain and received a message that the operation was not successful and the access was denied due to lack of authority. However, after inputting the admin credentials, I was welcomed into a domain and was asked to restart the machine so that the changes would be applied. On the login screen, I used the PC1 credentials and then I was able to see that the computer was a part of the domain (see Figure 31).

```

Computer name, domain, and workgroup settings
-----
Computer name:      MB316-19
Full computer name: MB316-19.iavasvertel.local
Computer description: MB316
Domain:             iavasvertel.local

```

FIGURE 31. The Computer Properties of PC1

AD had also added the PC1 (named “MB316-19”) to the Computers list automatically. Figure 32 shows the changes in the Active Directory Users and Computers folder.



FIGURE 32. AD has added MB316-19 to the Computers directory

The useful note here would be to check the version of the Windows OS the machine is running, because the “Home” versions of Windows cannot be connected to the domain. Luckily school’s PCs host Windows 8.1 Enterprise.

5.2.2 Share

As long as the computer now a part of the iavasvertel.local domain, the “\\RADIUSserver” path was available and I was able to browse through the Shared Folder. Figure 33 shows the search that was made from MB316-19 computer.

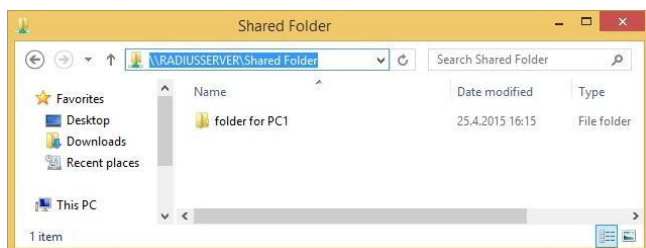


FIGURE 33. Picture is not available for PC1

However, I was not able to see the picture Gotcha. This means that I was authorized correctly. I added some picture to the Folder for PC1 (Figure 34).

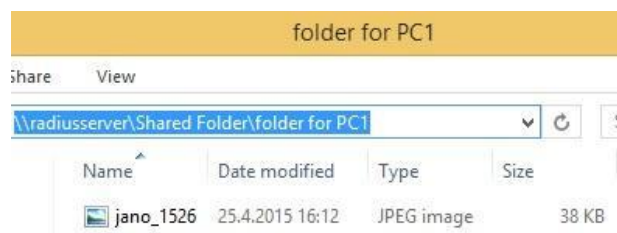


FIGURE 34. New picture was inserted

Then I tried to create “IwannaSHAREtoo” folder at PC1 and share it for Everyone with read&write rights. Nevertheless, to share something over network PC1 had to provide the administrative rights (Figure 35), which I did not have as a user. Later on, I have found out that I need the same rights also for enabling and disabling the NICs. This means that the default Domain Users group’s policies are quite limited for its users, which is very logical, so that a user would not mess the configurations.

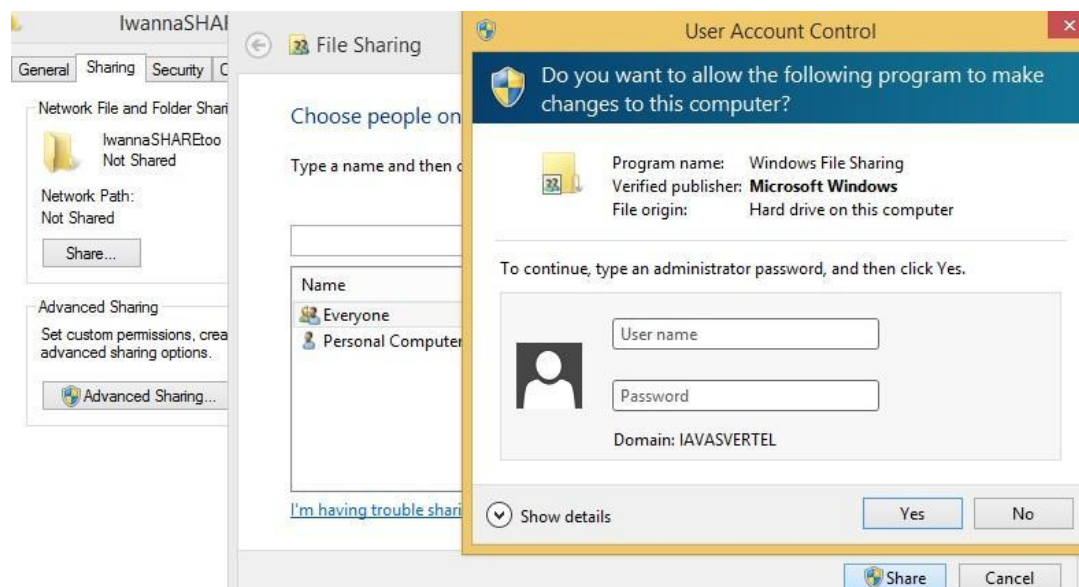


FIGURE 35. The user cannot share

When the Wi-Fi user’s turn came and I tried to connect to the \\RADIUSserver shared folders, the system asked for my login and password. And no wonder, because the user’s machine was not part of the domain, so it had to verify the claimer (Figure 36).



FIGURE 36. The system had to know who I was

I used the neighbor computer named MB316-18, and after logging in, I was able to see the Shared Folder, but there was only the Gotcha picture inside, which proved my policies to be working. Therefore, I deleted it! (Figure 37).

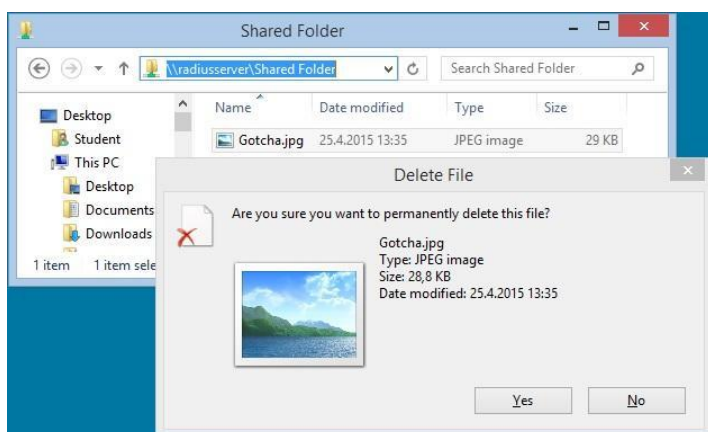


FIGURE 37. The testuser can do whatever he pleased to do with the picture

Then from the wirelessly connected computer MB316-18 I went to \\MB316-19 location and created Hi there folder. On figure 38 the path shows where the folder was created.

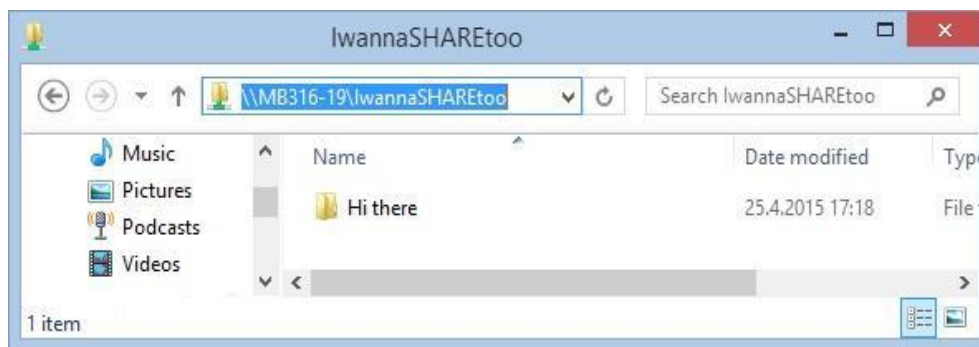


FIGURE 38. The folder was created

Finally, I had to log off from the shared network, but I learned that via net use command previously. Then I wanted to check the ownership rights on Hi there folder and was surprised that the owner is the computer on which the file is stored. On figure 39 the reader can see the C: drive, which means that the folder indeed stored on the local storage of device MB316-19.

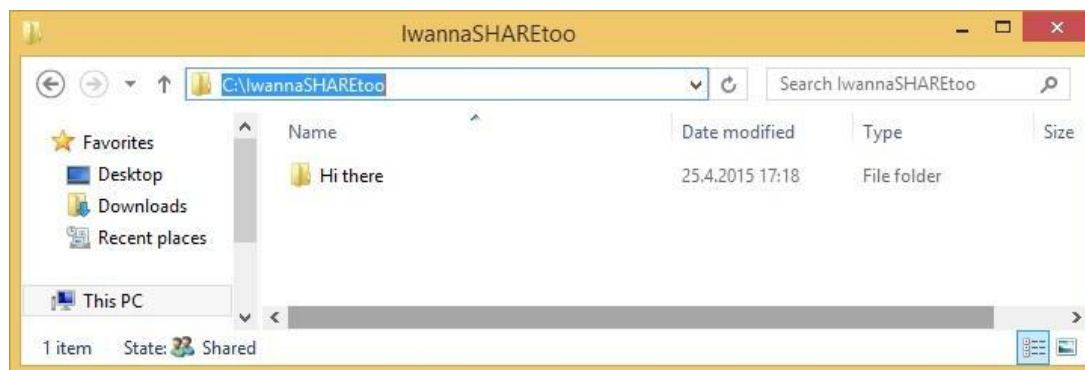


FIGURE 39. Folder was indeed added, but the ownership was MB316-19, not MB316-18

5.3 DHCP policy

As long as I know that the Wireless NICs in the MB316, lab environment where I was doing my thesis, start with F81A6708*, and I have a 100 IPs pool on the DHCP server (192.168.1.101-200), I decided to have the last 30 IPs to be associated with the beginning of their MAC address. The new feature was introduced in Windows Server 2012. In the 2012 R2 edition a new option was added for creating the policies based on the MAC address - Prefix wildcard, which is a reverse of Append option. The options for MAC address control are shown in Figure 40.

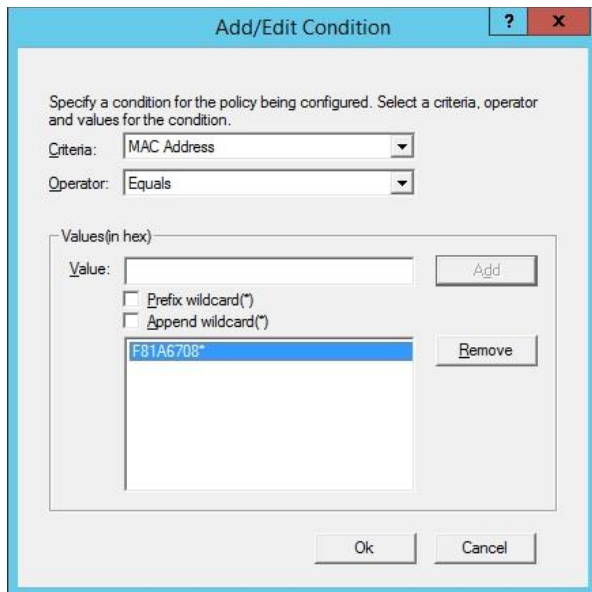


FIGURE 40. Wildcard options

Therefore, the value was “F81A6708” with Append wildcard (*) option checked for wireless users. Also I assigned first 30 IPs for stationary machines in the same classroom, because their NICs have “F81A6704*” value.

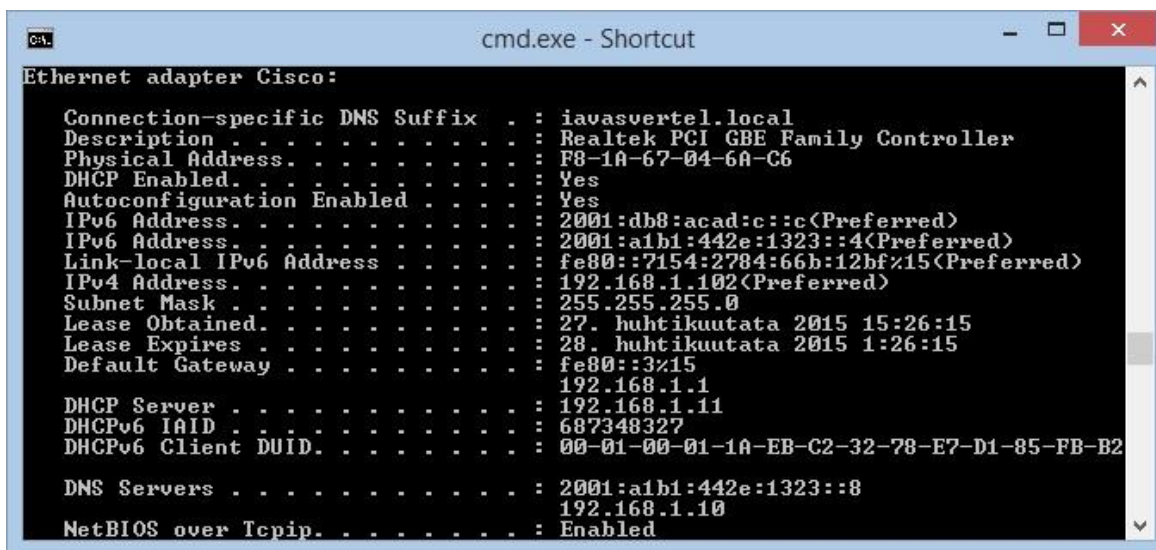
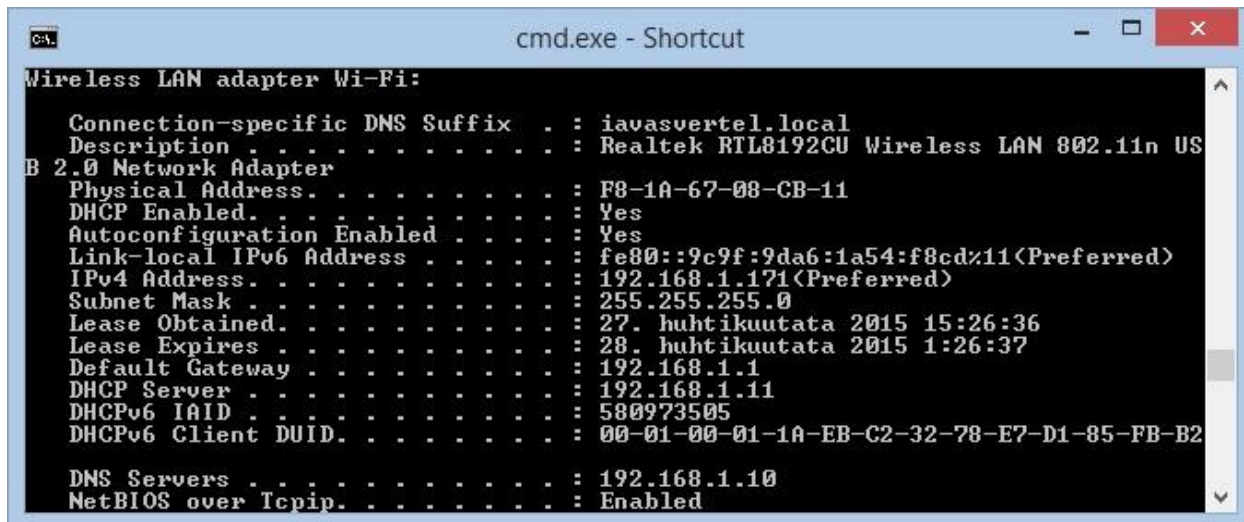


FIGURE 41. Wired user’s NIC properties

Later on the policy was changed to provide pool for wires PCs from 192.168.1.141 till 192.168.1.170. The CMD Figures 41 and 42 show the ipconfig /all command from both wired and wireless users.



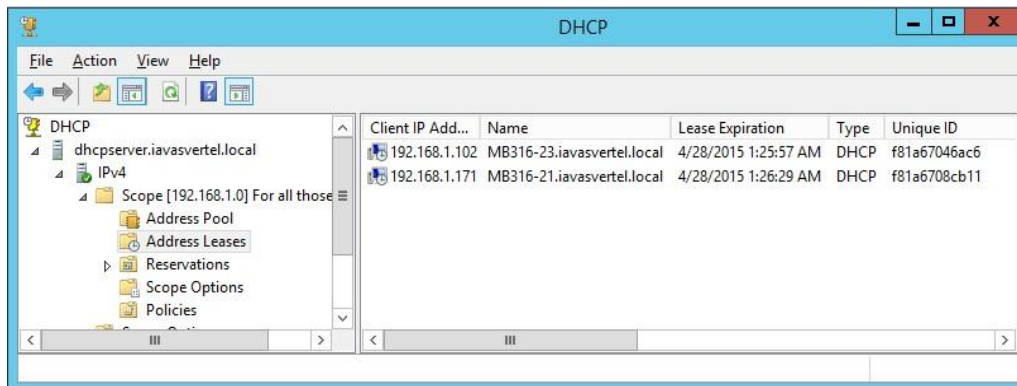
```

cmd.exe - Shortcut
Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix . : iavasvertel.local
    Description . . . . . : Realtek RTL8192CU Wireless LAN 802.11n US
B 2.0 Network Adapter
    Physical Address . . . . . : F8-1A-67-08-CB-11
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::9c9f:9da6:1a54:f8cd%11(Preferred)
    IPv4 Address. . . . . : 192.168.1.171(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : 27. huhtikuutata 2015 15:26:36
    Lease Expires . . . . . : 28. huhtikuutata 2015 1:26:37
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.11
    DHCPv6 IAID . . . . . : 580973505
    DHCPv6 Client DUID. . . . . : 00-01-00-01-1A-EB-C2-32-78-E7-D1-85-FB-B2

    DNS Servers . . . . . : 192.168.1.10
    NetBIOS over Tcpip. . . . . : Enabled
  
```

FIGURE 42. Wirelessly connected user's NIC properties

Also, the DHCP server provides the information about leases on Figure 43. There was a problem with IP address 192.168.1.101. It was always given to some unexisting device. After a small research on this topic, I have found out that because I had two NICs operating (one for the private network and one for browsing the internet), the system was creating some sort of a loop giving that address to the loop and calling it as a BAD_ADDRESS.



The screenshot shows the DHCP console window. The left pane displays the hierarchy: DHCP > dhcpserver.iavasvertel.local > IPv4 > Scope [192.168.1.0] For all those... > Address Leases. The right pane shows a table of active leases.

Client IP Addr...	Name	Lease Expiration	Type	Unique ID
192.168.1.102	MB316-23.iavasvertel.local	4/28/2015 1:25:57 AM	DHCP	f81a67046ac6
192.168.1.171	MB316-21.iavasvertel.local	4/28/2015 1:26:29 AM	DHCP	f81a6708cb11

FIGURE 43. DHCP leases for users

5.4 Accounting

Accounting is usually used for tracking a user's appearance on the network. With the help of the gathered information a system administrator can check what has happened on the network at the particular time and to use these logs to solve problems. Internet Server Providers also use that information for billing purposes or for adjusting the bandwidth allowed to a certain user. There are two ways of creating log files: SQL server logging and Local File logging.

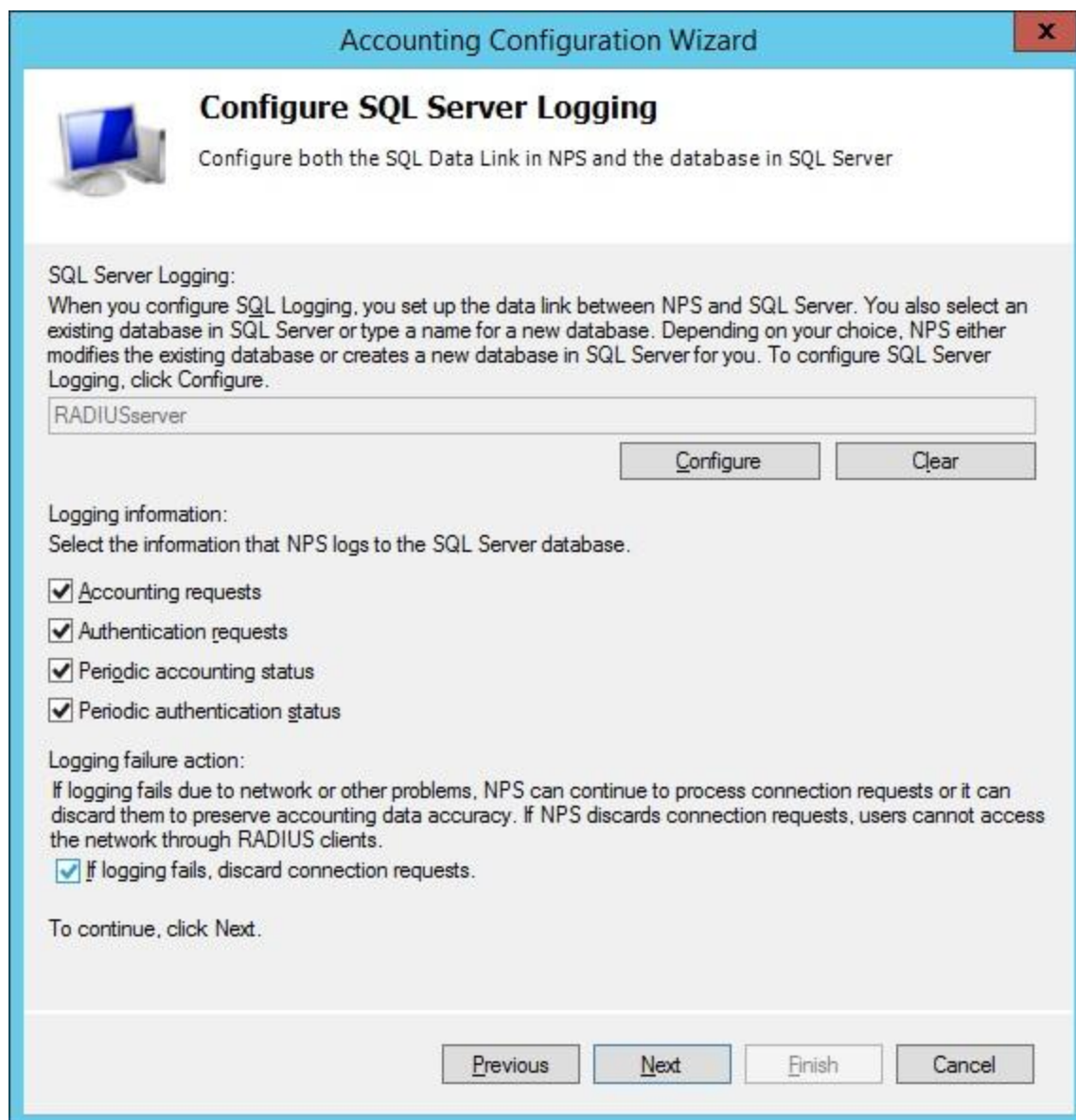


FIGURE 44. SQL server Logging configuration

I have chosen both of them (see Figure 44 for SQL server configuration and Figure 45 for Local File). If there are too many requests, it might be wise to put logs into the SQL server database and to configure Local File logging as a failover option.

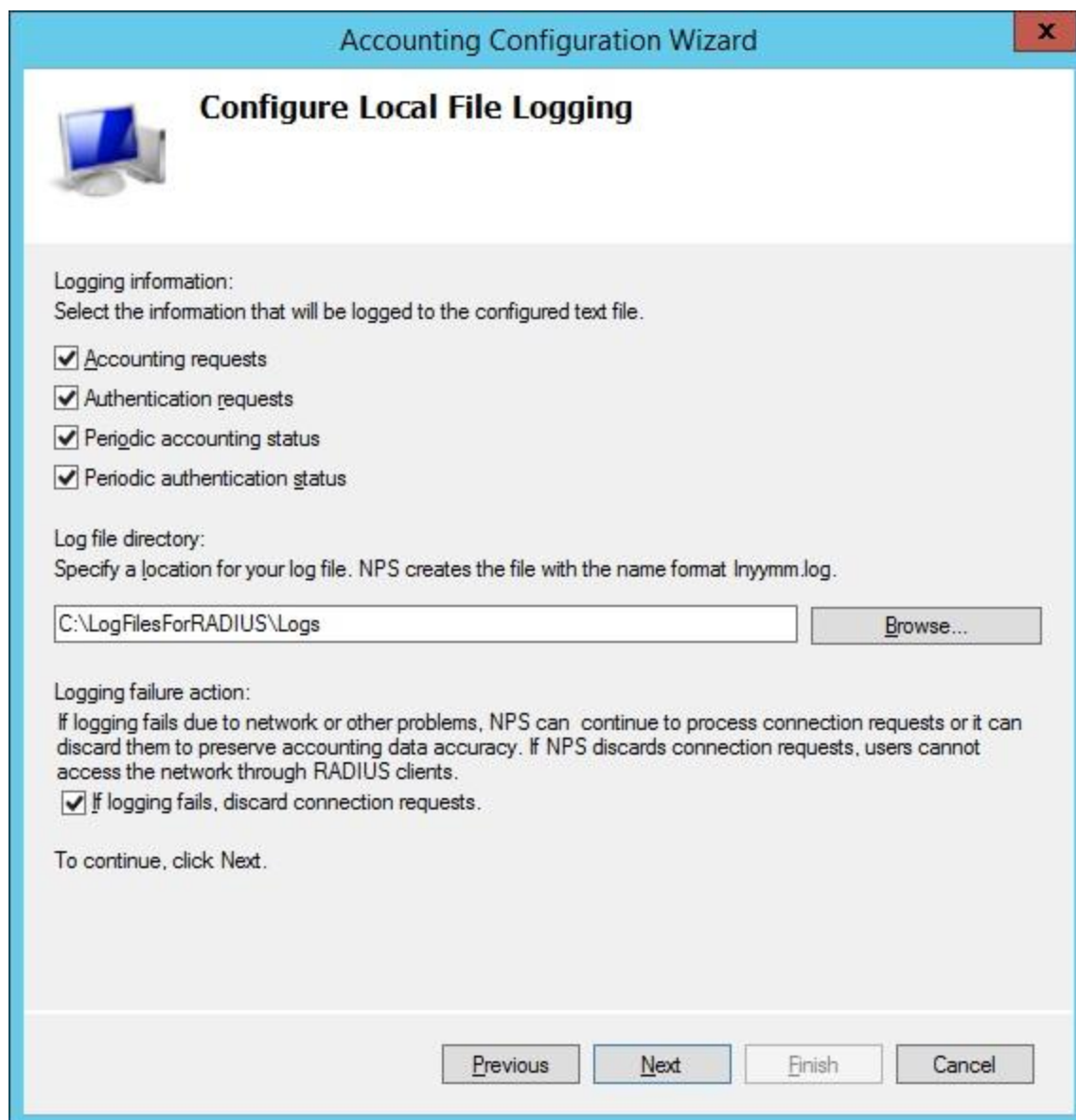


FIGURE 45. Local File Logging configuration

5.5 Final Testing

By this step, almost every feature is set up, and as the final testing, it would be essential to present what happens when a user can and cannot successfully authenticate himself into the network. Figure 46 shows the initial IP configuration for wireless device. The first attempt to authenticate the user was by using the username “intruder” with some random password.

```

cmd.exe - Shortcut
Wireless LAN adapter Wi-Fi:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Realtek RTL8192CU Wireless LAN 802.11n USB
    B 2.0 Network Adapter
    Physical Address. . . . . : F8-1A-67-08-CB-17
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes

```

FIGURE 46. Initial IP configuration of a wireless user

Logs from APs, from the Local File and SQL server can be used as a proof of an action that has taken the place. The results from the AP1 are shown in Figure 47. According to the results, “intruder” has failed the authentication on the particular AP.

Time Stamp	Severity	Service	Description
May 10 2015 19:41:43	info	hostapd[1941]	wlan0: IEEE 802.11 STA f8:1a:67:08:cb:17 disassociated from BSSID 50:57:a8:67:44:ac reason 8: Sending STA is leaving BSS
May 10 2015 19:41:43	warn	hostapd[1941]	authentication failed - identity 'intruder' EAP type: 0 (Unknown)
May 10 2015 19:41:43	info	hostapd[1941]	Station f8:1a:67:08:cb:17 had an authentication failure, reason 15
May 10 2015 19:41:43	info	hostapd[1941]	authentication server rejected EAP authentication
May 10 2015 19:40:54	info	hostapd[1941]	wlan0: IEEE 802.11 STA f8:1a:67:08:cb:17 associated with BSSID 50:57:a8:67:44:ac
May 10 2015 19:40:54	info	hostapd[1941]	wlan0: IEEE 802.11 Assoc request from f8:1a:67:08:cb:17 BSSID 50:57:a8:67:44:ac SSID IaVasVerTeL

FIGURE 47. Authentication of intruder had failed

Local log file also states that the user “intruder” had tried to authenticate from the device F8-1A-67-08-CB-17 on RADIUSserver through Network Access Server (NAS) 192.168.1.51 and at the end the “intruder” has received an Access-Reject packet with the reason code 8, which stands for no user with such a name was found in the database (Microsoft 2015c).


```
select * FROM accounting_data
```

id	timestamp	Computer_Name	Packet_Type	User_Name	Client_IP_Address	Fully_Qualified_Machine_Name	NP_Policy_Name	System
117	2015-05-10 19:41:38.743	RADIUSSERVER	1	intruder	192.168.1.51	NULL	NULL	NULL
118	2015-05-10 19:41:38.743	RADIUSSERVER	3	NULL	192.168.1.51	NULL	NULL	NULL
119	2015-05-10 20:03:04.783	RADIUSSERVER	4		192.168.1.51	NULL	NULL	NULL
120	2015-05-10 20:12:39.397	RADIUSSERVER	1	testuser	192.168.1.51	NULL	Secure Wireless Connections	NULL
121	2015-05-10 20:12:39.397	RADIUSSERVER	11	NULL	192.168.1.51	NULL	Secure Wireless Connections	NULL
122	2015-05-10 20:12:39.460	RADIUSSERVER	1	testuser	192.168.1.51	NULL	Secure Wireless Connections	NULL
123	2015-05-10 20:12:39.460	RADIUSSERVER	11	NULL	192.168.1.51	NULL	Secure Wireless Connections	NULL
124	2015-05-10 20:12:39.493	RADIUSSERVER	1	testuser	192.168.1.51	NULL	Secure Wireless Connections	NULL
125	2015-05-10 20:12:39.493	RADIUSSERVER	11	NULL	192.168.1.51	NULL	Secure Wireless Connections	NULL
126	2015-05-10 20:12:39.563	RADIUSSERVER	1	testuser	192.168.1.51	NULL	Secure Wireless Connections	NULL
127	2015-05-10 20:12:39.563	RADIUSSERVER	11	NULL	192.168.1.51	NULL	Secure Wireless Connections	NULL
128	2015-05-10 20:12:41.173	RADIUSSERVER	1	testuser	192.168.1.51	NULL	Secure Wireless Connections	NULL
129	2015-05-10 20:12:41.173	RADIUSSERVER	11	NULL	192.168.1.51	NULL	Secure Wireless Connections	NULL
130	2015-05-10 20:12:41.207	RADIUSSERVER	1	testuser	192.168.1.51	NULL	Secure Wireless Connections	NULL
131	2015-05-10 20:12:41.207	RADIUSSERVER	11	NULL	192.168.1.51	NULL	Secure Wireless Connections	NULL
132	2015-05-10 20:12:41.220	RADIUSSERVER	1	testuser	192.168.1.51	NULL	Secure Wireless Connections	NULL
133	2015-05-10 20:12:41.220	RADIUSSERVER	11	NULL	192.168.1.51	NULL	Secure Wireless Connections	NULL
134	2015-05-10 20:12:41.330	RADIUSSERVER	1	testuser	192.168.1.51	NULL	Secure Wireless Connections	NULL
135	2015-05-10 20:12:41.330	RADIUSSERVER	11	NULL	192.168.1.51	NULL	Secure Wireless Connections	NULL

Query executed successfully.

FIGURE 48. Packet_Type 11 as additional challenge sequence

After that I have tried to log in with the username that the system already knows, but I have used the wrong password. And, as the result the system started to send an additional challenge packet sequence (Figure 48).

Time Stamp	Severity	Service	Description
May 10 2015 20:23:40	info	hostapd[1941]	authenticated - identity " EAP type: 25 (PEAP)
May 10 2015 20:23:40	info	hostapd[1941]	The wireless client with MAC address f8:1a:67:08:cb:17 has been successfully authenticated.
May 10 2015 20:23:40	info	hostapd[1941]	wlan0: WPA STA f8:1a:67:08:cb:17 pairwise key exchange completed (WPAv2)
May 10 2015 20:23:40	info	hostapd[1941]	EAP authentication with the authentication server completed
May 10 2015 20:22:57	info	hostapd[1941]	wlan0: IEEE 802.11 STA f8:1a:67:08:cb:17 associated with BSSID 50:57:a8:67:44:ac
May 10 2015 20:22:57	info	hostapd[1941]	wlan0: IEEE 802.11 Assoc request from f8:1a:67:08:cb:17 BSSID 50:57:a8:67:44:ac SSID laVasVerTeL
May 10 2015 20:22:57	info	hostapd[1941]	wlan0: IEEE 802.11 STA f8:1a:67:08:cb:17 deauthenticated from BSSID 50:57:a8:67:44:ac reason 3: STA is leaving IBSS or ESS
May 10 2015 20:16:32	info	hostapd[1941]	wlan0: IEEE 802.11 STA f8:1a:67:08:cb:17 disassociated from BSSID 50:57:a8:67:44:ac reason 8: Sending STA is leaving BSS

FIGURE 49. AP1's log showed that testuser has finally was authenticated successfully

On the screen I have received the notification that the password I was typing was incorrect, and I have to try one more time, because the system knows that the username exists. After few incorrect attempts I have input the correct one and the system has successfully authenticated me (Figures 49 and 50).

```

cmd.exe - Shortcut
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : iavasvertel.local
Description . . . . . : Realtek RTL8192CU Wireless LAN 802.11n US
B 2.0 Network Adapter
Physical Address. . . . . : F8-1A-67-08-CB-17
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b59c:97e:8297:23b5%11(Preferred)
IPv4 Address. . . . . : 192.168.1.171(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 10. toukokuutata 2015 20:30:22
Lease Expires . . . . . : 11. toukokuutata 2015 0:30:22
Default Gateway . . . . . : 0.0.0.0
                                192.168.1.1
DHCP Server . . . . . : 192.168.1.11
DHCPv6 IAID . . . . . : 580973505
DHCPv6 Client DUID. . . . . : 00-01-00-01-1A-EB-C2-32-78-E7-D1-85-FB-B2

DNS Servers . . . . . : 192.168.1.10
NetBIOS over Tcpip. . . . . : Enabled

```

FIGURE 50. Testuser's IP configuration after the successful authentication

6 CONCLUSION AND FUTURE WORK

Original goal of this thesis was to create a RADIUS server with the help of third-party software, which could be used in a lab environment for educational purposes later on. However, during the process the idea evolved into a completely different goal: inspect the RADIUS protocol, implement it into the network and create an infrastructure where RADIUS server decides whether to grant the access to other resources or not.

Authenticating via RADIUS server is a quite demanding technology, because it consists of two parts. The first part is the wired part, or the server's side. In that part I have explained what the RADIUS server and RADIUS protocol are, what the alternatives can be and in what manner do they operate. The second part is related to the wireless side, or a user's side. That part was mostly concentrated on the authentication protocols and the Wi-Fi security standards.

At the beginning of the practical part of this project I have run into some problems related to insufficient support of TekRADIUS software, which has turned my goals around. By the end of it all I have created an independent network with RADIUS server as an authentication server, which is granting to authorized users additional services.

I consider this project to be successful, even though the original idea was replaced with something better. As I have already mentioned the original idea of the study was to create a RADIUS server that would be used later on for Cisco labs in classroom MB316, where users can

create automatically their accounts, modify, and delete them for study purposes. The environment that was created during this thesis also suits the original goal and it can be implemented without doubts.

One of the major limitations that I have found during the study was the inability by the devices to implement some limitations into bandwidth for particular users like most of the ISPs do in their environment. This feature is based on RADIUS server accounting and is very helpful for billing purposes.

This thesis still can be improved in several ways. First of all, it is a private network and has no access to the internet. Therefore, the first improvement could be done by implementing the firewall as a default gateway. Firewall will provide the protection of the traffic and will allow to the inside users to access the internet. If firewall will operate successfully, as an addition, there can be possibility of remote access via VPN tunnel with port forwarding or configuring public HTTP server for future testing and development.

Secondly, RADIUS server is a very sensitive service, which must be available whenever. Stating that I would point out that it is very essential to implement the second RADIUS backup/failover or load-balancing server. This feature will ensure the constant presence of the service on the network. And as the final addition I would set the SNMP authentication traps. These traps will inform the administrator if someone is testing the system, so that the needed actions for protecting the system will be taken in time.

BIBLIOGRAPHY

Aboba et al. 2004. RFC 3748: Extensible Authentication Protocol (EAP).

Andress, Jason 2011. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Book. Referred 30.3.2015.

Ballad, Bill & Ballad, Tricia & Banks, Erin 2010. Access Control, Authentication, And Public Key Infrastructure (Information Systems Security & Assurance). Book. Referred 13.4.2015.

Bartik, Christopher 2014. Industry News, report. WWW article.

<http://www.cloudentr.com/latest-resources/industry-news/2014/1/10/3-different-types-of-user-authentication>. Updated 10.1.2014. Referred 30.3.2015.

Calhoun et al. 2003. RFC 3588: Diameter Base Protocol.

Cao, Kai 2014. Federated Single-Sign On (SSO) Approach for Enterprise System. Aalto University. Department of Computer Science and Engineering. Master's Thesis. PDF document. https://into.aalto.fi/download/attachments/14189248/Thesis_CaoKai.pdf?version=1&modificationDate=1415088430202&api=v2. Referred 5.4.2015.

Child, Evan Paul 2004. TRUST NEGOTIATION USING HIDDEN CREDENTIALS. Brigham Young University. Department of Computer Science. Master's Thesis. PDF document. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.7787&rep=rep1&type=pdf>. Referred 30.3.2015.

Cisco 2006. Document ID: 12433. How Does RADIUS Work? WWW document.

<http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html>. Updated 19.1.2006. Referred 30.3.2015.

Cisco 2008. Document ID: 13838. TACACS+ and RADIUS Comparison. WWW document.

<http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#comparing>. Updated 14.1.2008. Referred 30.3.2015.

De Clercq, Jan 2004. Windows Server 2003 Security Infrastructures: Core Security Features. Book. Referred 13.4.2015.

Finseth 1993. RFC 1492: An Access Control Protocol, Sometimes Called TACACS.

Goswami, Subrata 2003. Internet Protocols: Advances, Technologies and Applications. Book. Referred 13.4.2015.

It-security.blogspot.fi 2005. PAP, CHAP, MS-CHAP, EAP, PPP. WWW article. <http://it-security.blogspot.fi/2005/02/pap-chap-ms-chap-eap-ppp.html>. Referred 4.5.2015.

Jia, Zhou 2008. Adding bandwidth specification to a AAA Server. Sweden Royal Institute of Technology. Department of Communication Systems. Master's Thesis. PDF document. <http://www.diva-portal.org/smash/get/diva2:511017/-FULLTEXT01.pdf>. Referred 30.3.2015.

Král, Tomáš 2011. Advanced authentication in Java applications using Kerberos protocol. Masaryk University of Brno. Department of Informatics. Master's Thesis. PDF document. http://is.muni.cz/th/173010/fi_m/masters-thesis.pdf. Referred 30.3.2015.

Larsson, Anton 2002. Authentication, Authorization and Accounting within an Access Network using Mobile IPv6 and Diameter. University of Luleå. Department of Computer Science and Electrical Engineering. Master's Thesis. PDF document. <http://pure.ltu.se/portal/files/30900919/LTU-EX-03029-SE.pdf>. Referred 30.3.2015.

Messer, James 2014a. Authorization and Access Control - CompTIA Security+ SY0-301: 5.2. Video. <https://www.youtube.com/watch?v=6aXMuJPkuiU>

Messer, James 2014b. Overview of Kerberos - CompTIA Security+ SY0-301: 5.1. Video. <https://www.youtube.com/watch?v=VpBCJ8vS7T0>

Microsoft 2015a. Authentication Methods. WWW article. <https://technet.microsoft.com/en-us/library/-cc958013.aspx>. Referred 4.5.2015.

Microsoft 2015b. Internet Authentication Service and Network Policy Server. WWW article. [https://msdn.microsoft.com/en-us/library/bb892033\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/bb892033(v=vs.85).aspx). Referred 4.5.2015.

Microsoft 2015c. Interpret NPS Database Format Log Files. WWW article. <https://technet.microsoft.com/en-us/library/cc771748%28v=ws.10%29.aspx>. Referred 4.5.2015.

Microsoft support, 2013. Article ID: 893357. WPA2 for Windows XP is available. WWW article. <https://support.microsoft.com/en-us/kb/893357?wa=wsignin1.0>. Referred 4.5.2015.

Monrose, Fabian & Rubin, Aviel D. 2000. Elsevier Science B.V. Journal: Future Generation Computer Systems 351–359, Volume 16, Issue 4. Keystroke dynamics as a biometric for authentication. PDF document.

<http://www.cs.columbia.edu/4180/hw/keystroke.pdf>. Updated Feb. 2000. Referred 30.3.2015.

Neuman et al. 2005. RFC 4120: The Kerberos Network Authentication Service (V5).

Niemi, Aki 2002. Authentication, Authorization and Accounting in Session Initiation Protocol Networks. Helsinki University of Technology. Department of Electrical and Communications Engineering. Master's Thesis. PDF document.
<http://www.tml.tkk.fi/Publications/Thesis/niemi.pdf>. Referred 30.3.2015.

Ou, George 2005. Understanding the updated WPA and WPA2 standards. WWW article.
<http://www.zdnet.com/article/understanding-the-updated-wpa-and-wpa2-standards/>. Referred 4.5.2015.

Pasupathinathan, Vijaykrishnan 2009. Hardware-based Identification and Authentication Systems. University of Macquarie. Department of Computing. Thesis the degree of Doctor of Philosophy. PDF document.
http://web.science.mq.edu.au/~josef/CONTENTS/PHD_THESES/Vijay_Pasupathinathan_thesis.pdf. Referred 30.3.2015.

Purser, Jimmy Ray 2013. Networking 101: RADIUS Vs TACACS+. Cisco. Video.

Rigney et al. 2000. RFC 2865: Remote Authentication Dial In User Service (RADIUS).

Salazar, Alex 2014. SSO vs. Centralized Authentication. WWW document. <https://stormpath.com/blog/sso-vs-centralized-auth/> Updated 8.8.2014. Referred 5.4.2015.

Shinder, Debra 2001. Understanding and selecting authentication methods. WWW article. <http://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/>. Referred 4.5.2015.

Shirey 2000. RFC 2828: Internet Security Glossary.

Shirey 2007. RFC 4949: Internet Security Glossary, Version 2.

Sotillo, Samuel 2007. Extensible Authentication Protocol (EAP) Security Issues. PDF-document. http://www.infosecwriters.com/text_resources/pdf/SSotillo_EAP.pdf. Referred 4.5.2015.

TACACS.net, 2011. The Advantages of TACACS+ for Administrator Authentication. PDF document. http://www.tacacs.net/docs/TACACS_Advantages.pdf. Updated Apr. 2011. Referred 30.3.2015.

TANAMA 2015. Different Types Of Network Topologies That You Can Use. WWW article. <http://tanama.net/different-types-of-network-topologies-that-you-can-use/> Referred 8.4.2015.

Team Rivan, 2013. Windows 2012 Domain Controller 802.1x Authentication Radius Cisco Part 2. Video. <https://www.youtube.com/watch?v=jkvayOyoX-E> Referred 13.4.2015.

Todorov, Dobromir 2007. Mechanics of User Identification and Authentication: Fundamentals of Identity Management. Book. Referred 13.4.2015.

TP-LINK Technologies Co. 2015. The differences between WPA-Personal and WPA-Enterprise. WWW article. <http://www.tp-link.fi/article/?faqid=500>. Referred 4.5.2015.

Tuomimäki, Jaakko 2003. Seminar on Internetworking. Overview, details and analysis of Radius protocol. Helsinki University of Technology. PDF document. <http://www.tml.tkk.fi/Studies/T-110.551/2003/papers/12.pdf>. Referred 8.4.2015.

Ventura, Håkan 2002. Diameter next generation's AAA protocol. University of Linköping. Department of Information technology. Master's Thesis. PDF document. <http://www.diva-portal.org/smash/get/diva2:18347/FULLTEXT01.pdf>. Referred 30.3.2015.

Vibhuti, Shivaputrappa 2005. IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability. PDF document. <http://www.cs.sjsu.edu/~stamp/CS265/projects/Spr05/papers/WEP.pdf>. Referred 4.5.2015.

Viehböck, Stefan 2011. Brute forcing Wi-Fi Protected Setup. PDF document. https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf. Referred 4.5.2015.

Wi-Fi Alliance 2004. Wi-Fi Alliance Introduces Next Generation of Wi-Fi Security. WWW article. <http://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-next-generation-of-wi-fi-security>. Referred 4.5.2015.

Wi-Fi Alliance 2009. Wi-Fi CERTIFIED™ expanded to support EAP-AKA and EAP-FAST authentication mechanisms. WWW article. <http://www.wi-fi.org/news-events/newsroom/-wi-fi-certified-expanded-to-support-eap-aka-and-eap-fast-authentication>. Referred 4.5.2015.

Woland, Aaron 2014. Network World. RADIUS versus TACACS+. WWW document.

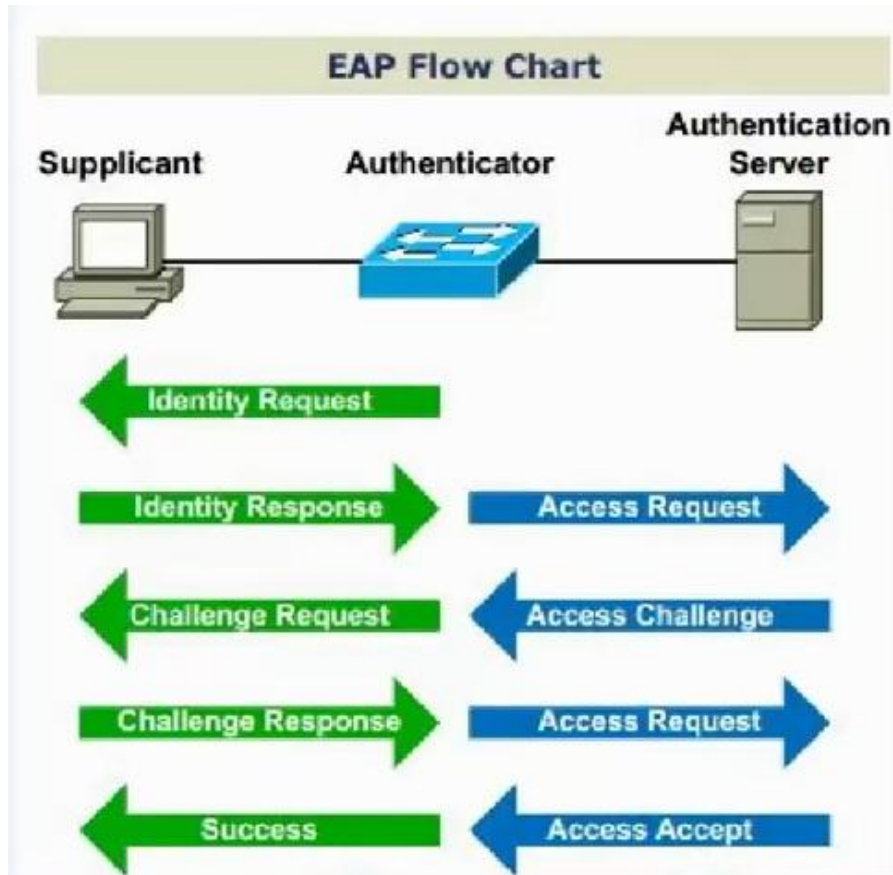
<http://www.networkworld.com/article/2838882/radius-versus-tacacs.html>. Updated 26.10.2014.
Referred 30.3.2015.

Yan, Jing 2008. Continuous Authentication Based on Computer Security. University of Luleå. Department of Business Administration and Social Sciences. Master's Thesis. PDF document.
<http://epubl.ltu.se/1653-0187/2009/005/LTU-PB-EX-09005-SE.pdf>. Referred 30.3.2015.

Zadjmool. <http://blog.tevora.com/authentication/radius-vs-tacacs-2/>. Referred 30.3.2015.

APPENDICES

APPENDIX 1. EAP FLOW CHART (Team Rivan, 2013)



APPENDIX 2. Client's configuration

192.168.1.51/admin.cgi?action=main

Apps Google Bookmark

Small Business
cisco WAP121 Wireless-N Access Point with Power Over Ethernet

Getting Started
 Run Setup Wizard
 ▶ Status and Statistics
 ▶ Administration
 ▶ LAN
 ▶ **Wireless**
 Radio
 Rogue AP Detection
Networks
 Scheduler
 Scheduler Association
 Bandwidth Utilization
 MAC Filtering
 WDS Bridge
 Work Group Bridge
 QoS
 WPS Setup
 WPS Process
 ▶ System Security
 ▶ Client QoS
 ▶ SNMP

Networks

Virtual Access Points (SSIDs)						
	VAP No.	Enable	VLAN ID	SSID Name	Security	MAC Filter
<input checked="" type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	laVasVerTeL	WPA Enterprise ▼	Disabled ▼

WPA Versions: WPA WPA2
 Enable pre-authentication

Cipher Suites: TKIP CCMP (AES)

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 2-64 Characters)
 Key-2: (Range: 2-64 Characters)
 Key-3: (Range: 2-64 Characters)
 Key-4: (Range: 2-64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: (Range: 0-86400)
 Session Key Refresh Rate: (Range: 0-86400)