


Petras Kasiulynas

Radius Authentication in wireless lab environment

Bachelor's Thesis
Information Technology

May 2016

DESCRIPTION

		Date of the bachelor's thesis 30.05.2016
Author(s) Petras Kasiulynas	Degree programme and option Information Technology	
Name of the bachelor's thesis RADIUS Authentication in wireless lab environment		
Abstract <p>The aim of the thesis was to learn and research the development of the Wi-Fi access control methods. This topic will be covered in a chronological order starting from old open-access networks ending to modern methods used today. The practical aim of the study is to implement network access control with an external RADIUS server and to create a RADIUS lab for students. This method has two main advantages. The use of the external server provides a possibility to use one database for many devices like access points and routers. Resources used for this thesis are MB316 classroom access points, hubs, computers and virtual machines of Mikkeli University of Applied Sciences.</p> <p>In the beginning of the study, the theoretical foundation for the study is created with a literature review on authentication, authorization and accounting in Wireless Local Area Networks (WLANs). In the practical part of the study, I implement three different forms of wireless centralized authentication. These forms were autonomous access point RADIUS, Medium business RADIUS setup in Windows server environment and Enterprise RADIUS setup in Windows server environment</p> <p>The findings of the study suggest that autonomous access point solution is no longer a valid method even in small environments because it is not supported in Windows 10 operating system. The server-based solutions either implemented with one or multiple servers are the best for centralized user authentication management and access control.</p>		
Subject headings, (keywords) Network Policy Server, Windows Server 2012R2, Wireless RADIUS authentication		
Pages 38 p. +5 p. appendix	Language English	URN
Remarks, notes on appendices		
Tutor Matti Koivisto	Employer of the bachelor's thesis Mikkeli University of Applied Sciences	

LIST OF ABBREVIATIONS

802.1x – Wireless LANs

AAA - Authentication Authorization Accounting

AD CS – Active Directory Certificate Services

AD DS – Active Directory Domain Services

AP – Access Point

ATM - Automatic Teller Machine

BSS - Basic Service Set

BYOD – Bring Your Own Device

CLI – Command Line Interface

DNS – Domain Name System

DoS – Denial of Service

DSL - Domain-Specific Language

DSSS - Direct Sequence Spread Spectrum

FHSS - Frequency Hopping Spread Spectrum

GHz – Gigahertz

GUI – Graphical User Interface

IEEE - Institute of Electric and Electronic Engineers

IoT – Internet of Things

IP – Internet Protocol

IPS - Intrusion Prevention System

IV - Initialization Vector

LAN – Local Area Network

MAMK - Mikkeli University of Applied Sciences

MIMO – Multiple Input Multiple Output

MU-MIMO – Multi user MIMO

NAC – Media Access Control

NAP – Network Access Protocol

NAS – Network Access Server

NIC – Network Interface Card

NPS – Network Policy Server

OFDM – Orthogonal Frequency-Division Multiplexing

OS – Operating System

Pre shared key – password-based authentication set on AP

RADIUS – Remote Authentication Dial-in User Service

RC4 – Rivest Cipher 4

RF - Radio Frequency

SG – Study Group

SSID – Service Set Identifier

TACACS – Terminal Access Controller Access System

TG – Task Group

VLAN – Virtual Local Area Network

VPN - Virtual Private Network

WEP – Wired Equivalent Privacy

WLAN – Wireless Local Area Network

WPA – Wireless Protected Access

CONTENTS

LIST OF ABBREVIATIONS	1
1 INTRODUCTION	4
2 AUTHENTICATION AUTHORIZATION ACCOUNTING.....	5
2.1 Authentication	5
2.2 Authorization.....	7
2.3 Accounting	7
2.4 Network Access Control (NAC)	8
3 WIRELESS LOCAL AREA NETWORK AND AUTHENTICATION.....	9
3.1 WLAN standards	9
3.2 Wi-fi Alliance.....	11
3.3 WLAN authentication and encryption	11
3.4 Network Access Server Methods	16
4 PRACTICAL PART	16
4.1 Autonomous AP RADIUS	17
4.2 Medium Business Radius server	20
4.3 Enterprise Radius	26
5 CONCLUSIONS	32
BIBLIOGRAPHY	33
APPENDICES.....	37

1 INTRODUCTION

With ever more developing new technologies and the rapid growth of wireless networks access became easier in the beginning of the 20th century. This provided users with more convenient connection to the internet, but also along with it arose many security problems. The biggest security issue is managing personal and enterprise wireless environments that only approved users are granted access to the networks. The authentication systems had to be centralized and secured.

The security policy mechanism methods as a network access control defined essential authentication rules and has played a big role the growth and protection of networks. Some organizations chose modern network-layer protection in the past, and relied on Windows authentication as their means for controlling network access. The limited network access controls were effective in the early 2000s, but soon after that they became unreliable with evermore expanding the variety of network devices and wireless networks.

The local area networks (LAN) are physical devices and wires that make closed and secure environment while the wireless local area network (WLAN) is based and works on the same principle. Yet, it is exposed to external factors. Wireless access points work as small radio transmitters and receivers with specific frequency and range. This allows devices in the range of the wireless access point to monitor wireless data traffic, even if the device is not connected to an access point or LAN. Based on this issue I decided to research it and find out the security methods practiced in personal and enterprise environments.

The theoretical aim of the study is to learn and research the development of the Wi-Fi access control methods. This topic will be covered in a chronological order starting from old open-access networks ending to modern methods used today. The practical aim of the study is to implement network access control with an external RADIUS server and to create a RADIUS lab for students. This method has two main advantages. The use of the external server provides a possibility to use one database for many devices like access points and routers. Resources used for this thesis are MB316 classroom access points, hubs, computers and virtual machines of Mikkeli University of Applied Sciences.

The structure of the study is as follows: The second chapter introduces authentication, authorization and accounting as well as network access control. In Chapter 3 the focus of the study moves to Wireless Local Area Network (WLANs) and their authentication methods. In Chapter 4 I focus on the practical implementation of the RADIUS server WLAN in the lab environment. Final conclusions of the study are then made in Chapter 5.

2 AUTHENTICATION AUTHORIZATION ACCOUNTING

AAA is a key security concept known as authentication, authorization, accounting and it defines network resource protection. It is a widely used model in the industry. However, there are other protocols and methods that can satisfy similar requirements. Earlier different machines used different authentication protocols, user profiles or small databases. For small networks using products from one manufacturer authentication worked well. But, when adding different equipment to the network with different authentication methods it created a big problem. According to Hassell (2002, 1-2), Internet Research Task Force (IRTF) formed an AAA workgroup to address system limitations at that time. Remote access services continually need standards to be improved to effectively verify and monitor users throughout the network.

There are three independent functions of AAA framework. Briefly, authentication is the verification of who the users are, authorization refers to what you are able to do and accounting to what the users did, when logged in. In the following sections they are described in more detail.

2.1 Authentication

The authentication process verifies a machine's or person's submitted identity. It allows to form a trust relationship between two points: the client and the service. Trust functionality allows granting access in the name of submitted identity in the following way: AAA spans over a network, for example in a proxy server. Authentication can work as a separate process or in a combination with authorization and accounting.

The everyday example is an ATM (Automatic Teller Machine). Before a user can withdraw money or do something else, he goes through two steps of authentication: First, the credit card is recognized, and second, the pin is checked.

The example above highlights that authentication can be based on multiple factors. The three main factors typically used are:

- Something users has (card, key)
- Something users features (biometrics as eye, fingerprint scan)
- Something users know (password or other relevant information)

When more than one factor is used, the system is called a multifactor authentication system. Some of the most popular authentication methods are described below.

Password is the most popular authentication method. This method is simple and fast requiring low processing power. In modern systems passwords are encrypted and big corporations as Google and Microsoft store them in separate databases. Service providers do not know what users password is. Some of the password method vulnerabilities are: simple and easy to guess, writing the password down, social engineering and eavesdropping (physically or in a network with the “man in the middle”).

One time passwords were developed to solve the password reuse problem. This method is further grouped into two types: a password list and a challenge response. The password list means that after a password has been used it is no longer valid. It provides a user within one-time temporary access to the system.

Challenged response password in this model when connection is requested a user receives challenge value based on it he needs to provide a matching response value that can be based on a table or an electronic device. Similar authentication is used when connecting to an online bank account.

In password based methods the connecting client is authenticated, but there is no authorization of the accessed system. Therefore, these methods are vulnerable to the man in the middle attacks and the spoofing.

2.2 Authorization

When a client is authenticated, authorization determines what the user is allowed to do in a system. This involves a set of templates and rules. For example, the system administrator determines rules according to which the client connects to the service and he can access only the services which are defined by the created rules. An example of authorization is a user of the ATM. With the use of multifactor authentication, a credit card is something user has and pin is something user knows. The user wants to withdraw money from the account with a balance of EUR 200. If he tries to withdraw EUR 100, he will get the money. But, if he tries to withdraw EUR 10 000, authorization checks that this amount exceeds the maximum withdraw limit and request is denied.

2.3 Accounting

The accounting system plays a huge role in the AAA framework. Implemented accounting systems track the number of users, login and log out time, session status, what data was sent what data was received, network load etc. Accounting helps an administrator to analyze and evaluate resources, capacity, the loads of the network and access request rules of the users, their actions which are permitted or denied. The system monitoring available tracks usage and how much it costs for a specific user group or individual users. Clearly, accounting uses spans more than just in the system administration. It helps to predict costs of services and much more. It is a very useful versatile system. In the ATM example accounting keeps a list of all the clients actions like withdrawals and deposits. Yet, in the computer environment accounting requiring generated reports, weekly or monthly, by the administrators to check that everything is in order. For critical services that might require daily observation.

2.4 Network Access Control (NAC)

Network access control or network admission control is a concept closely related to AAA. It has been used for many years as a part of Intrusion Prevention Systems (IPS) which come integrated into various products.

In the NAC-enabled networks a health check is performed on the connecting device before a new device is to the network. It is called posture assessment. Based on created authentication policies it checks if the devices are trusted, what anti-virus software it is using what applications are installed, if the device is mobile, and if the disk is encrypted and what OS the device uses. When the device does not meet the criteria, it can be quarantined, blocked, connected to a separate VLAN or given enough access for fixing the issue.

According to Margaret (2016) the implemented NAC method increases and reinforces security, restricting network resources, availability to endpoint devices. Usually when the NAS network access server authorizes and authenticates users, NAC adds the following functionality:

- Regulating user data access
- Regulating and restricting user's actions individually when he connects companies resources
- Implementing anti-threat application: firewalls, antivirus software and spyware-detection programs

In the physical network NAC is great at detecting and protecting LAN from rogue devices such as computer or access points. However, a wireless network has a huge number of devices and the variety of these devices requires a specific authentication approach. This creates a phenomenon known as (BYOD) Bring your own device.

Bring your own device presents challenge of control to smartphones, tablets and other appliances. To handle devices authentication correctly NAC vendors, cooperate with MDM mobile device management providers to ensure the compatibility and security.

3 WIRELESS LOCAL AREA NETWORK AND AUTHENTICATION

There are many wireless internet standards developed by IEEE. These standards specify many different dimensions of the WLANs including transmission speeds, frequencies and their use, encryption and authentication methods etc. In the following section these issues are discussed in more detail.

3.1 WLAN standards

Institute of Electric and Electronic Engineers (IEEES) creates and develops LAN standards. Based on Hucaby (2016, 76-78) the project 802 is considered as a family further divided into work groups and each of them has a different index number assigned. Wireless LAN or the 802.11 workgroup was established in 1980. This was the beginning of the WLAN standard development. Later on the standards developed by the working groups have been used by wireless vendors to design wireless equipment.

Technology is constantly evolving, and for existing standards to meet new technological demands they are consistently improved. IEEE Study Group (SG) researches standards and if they need to be improved or updated to meet the latest technological needs. If yes, then a Task Group (TG) is formed for developing and improving the standard. Every new TG by alphabetical order is assigned a letter thru the standard the same process is repeated with a standard that already has a letter assigned and the second alphabetical letter is added: for example, already patented standard 802.11a requires further development and new TG is formed 802.11aa. As standard development takes a long time and is a continuous process IEEE keeps a document database of each standard. This allows vendors to use existing documentation for developing up to date appliances.

In 1997 IEEE published the original 802.11 standard also known as legacy. It was based on a single band steam of 2.4 GHz with 2.0 Mbps maximum theoretical bandwidth. RF (radio frequency) modulation used FHSS (Frequency Hopping Spread Spectrum) transmitted radio signals among different frequencies and DSSS (Direct Sequence Spread Spectrum). In 1997, 802.11 was the first of its kind and placed strong a foundation for wireless technology.

In 1999 IEEE published the 802.11a and 802.11b standards. 802.11a was a single band stream of 5 GHz with the maximum theoretical bandwidth of 54 Mbps. A range of 5 GHz provided less interference and high bandwidth, but drawbacks were high cost and low range (It cannot penetrate walls well.). The 802.11b standard a was single band stream of 2.4 GHz with the maximum theoretical 11Mbps bandwidth. Its advantages were good range (works through walls), but disadvantages were interference with devices on similar a frequency, and slow transmission speed.

In 2003 IEEE published the 802.11g standard. It was a single 2.4 GHz band with the maximum theoretical throughput of 54Mbps. It's advantages included good bandwidth and range disadvantages instead were interference with some RF devices such as microwaves. Compatibility with 802.11b allowed migration from one standard to the other and vice versa.

In 2009 IEEE published the 802.11n standard. It was a dual band using 2.4 and 5 GHz combination. By adding the MIMO technology it reached the maximum theoretical bandwidth of 600 Mbps. It's advantages were fast bandwidth with less interference in 5GHz and good range in 2.4GHz. This standard was designed with the OFDM backwards compatibility to 802.11a and 802.11g.

In 2013 IEEE published the 802.11ac standard. Works as 5GHz technology. The advantages of this technology is fast bandwidth with less interference. With improved MU-MIMO combined with OFDM maximum theoretical throughput is 1.3 Gbps. Table 1 below summarizes the development of the WLAN standards.

TABLE 1. Wireless standard table (Hucaby 2016, 76-78)

Year	Standard	Transmission type	GHz	Theoretical Bandwidth
1997	802.11	FHSS DSSS	2.4	1 - 2Mbps
1999	802.11a	OFDM	5	6 - 54Mbps
	802.11b	DSSS	2.4	5.5- 11Mbps
2003	802.11g	ERP-OFDM	2.4	6- 54Mbps
2009	802.11n	OFDM MIMO	2.4&5	150- 600Mbps
2013	802.11ac	OFDM MIMO MU-MIMO	5	450Mbps- 1.3Gbps

Wireless throughput relies on the enabled transmission type and the RF modulations as additionally accounting distance from the AP. It is Important to know that speed and modulation/ transmission type change accordingly, depending on the distance from AP.

3.2 Wi-fi Alliance

The Wi-fi Alliance was formed in 1999. This nonprofit organization makes sure that multiple standards meet today's requirements and that vendors comply with the standards Wi-fi Alliance test and certify various vendor device's that work with wireless technology. This certification is rigorous and done in authorized laboratories, and if some weakness / bugs are found the vendor can correct them to avoid bugs in mass production. After the certification the right to place a logo on the appliance and a certificate are received. Primarily the Wi-fi Alliance logo represents reliability that the product meets industry standards and it guarantees the interoperability between different manufacturer's devices. The Wi-fi Alliance certification is not mandatory, yet it unifies the quality of service.

According to Beal (2010) Wi-Fi does not mean "wireless fidelity". It is rather a trademark for Wi-fi Alliances that stands for the WLAN wireless local area network of IEEE 802.11x standards. As a term it was used only with the 802.11b standard, yet it got stuck ever since.

3.3 WLAN authentication and encryption

This chapter researches WLAN authentication frameworks that consists of the following: null authentication, MAC, WEP, WPA, WPA2, PSK, server based, 802.1x. The parts of this framework ensure security by authenticating and encoding information for wireless connection.

3.3.1 MAC Authentication

The MAC-Based Authentication method uses MAC physical (media access control) address to authenticate devices. Adding a layer of security and control in device authentication regarding various wireless devices as phones. MAC authentication efficiency is dependent on the number of clients, if it is used as the main authentication method.

More clients meant less efficiency. Therefore, this method is used in small scale environments that do not require high security. The working principle is a list of devices that are authenticated and granted the access while the rest, not listed devices, are denied. Additionally, this method be implemented alongside existing authentication structure. As the MAC list of denied or permitted devices, thus adding extra security (H3C, 2016).

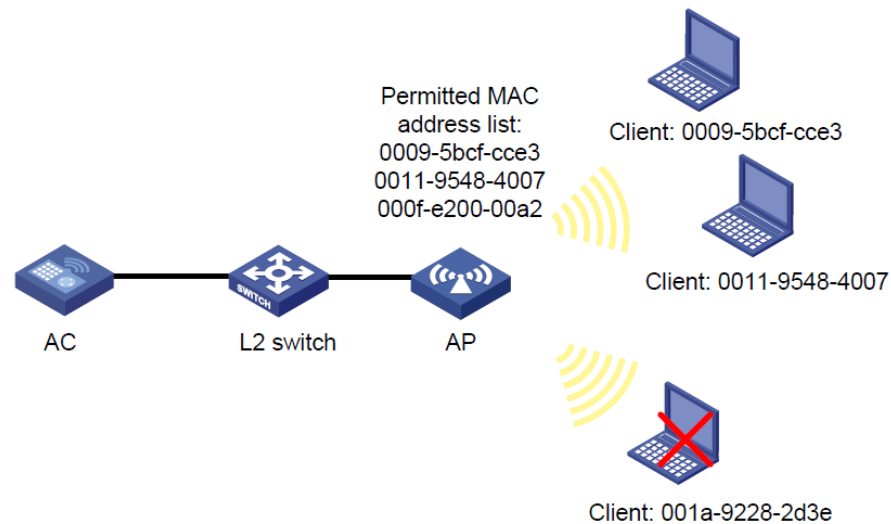


FIGURE 1. Local MAC authentication (H3C, 2016)

Furthermore, this method has two modes: Local MAC authentication and RADIUS based MAC authentication. In the case of local MAC authentication, the MAC address list of permitted devices is configured. Devices that are not on the list will not be authenticated and will not connect to the network, as Figure 1 shows.

The RADIUS-based MAC authentication works by the same principle as described previously. The difference is that authentication is now performed by a RADIUS server. On WLAN, the AP takes care of the client's association requests and forwards them to the RADIUS server as shown in Figure 2. Both the local MAC and RADIUS based MAC authentication have security flaws. When the authentication is based on MAC addresses the attacker can use a spoofed address on its own device and this way gain the access to the network.

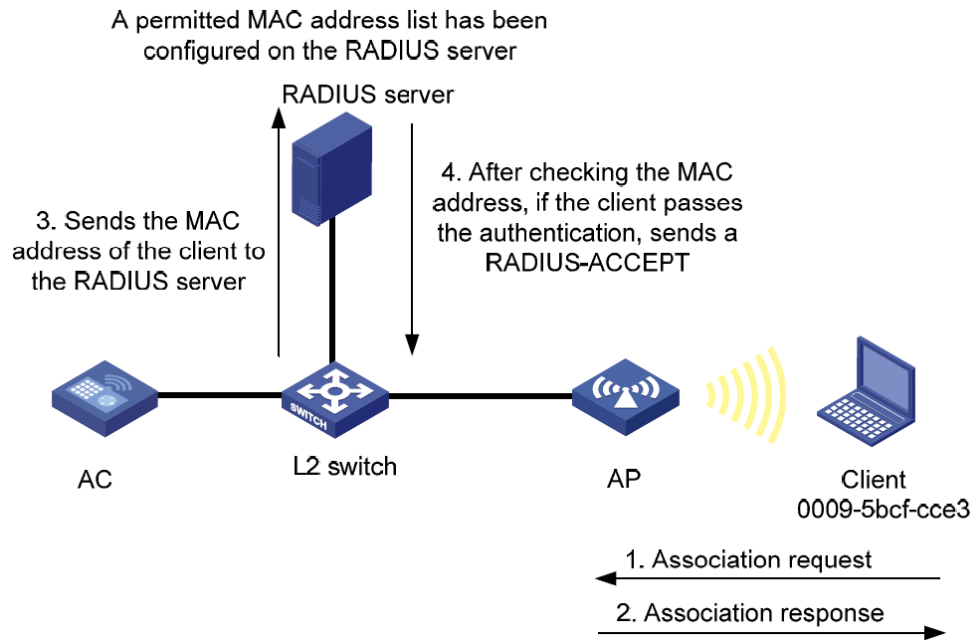


FIGURE 2. RADIUS-based MAC authentication (H3C, 2016)

3.3.2 Open authentication (null)

Also known as the open system authentication the null authentication method is used to verify that a wireless device uses 802.11 before it is permitted to join a BSS basic service set. It is required that a client device use the 802.11 standard. The open authentication carries out validation and as a result device hardware and protocols are authenticated to confirm that the device uses 802.11 standards. As shown in Figure 3, it is a two-step, simple algorithm process: First the client requests authentication, and second, the AP returns an authentication response. This is just device authentication. If a user authentication is needed, it must be handled in a different way (H3C, 2016).

With some public WLAN locations web authentication is used to agree to the terms of public AP and OS usually flagging and warns the client of unsecured connection. Another security disadvantage of open networks is that no encryption is used. Thus, all the data can be monitored and exploited.

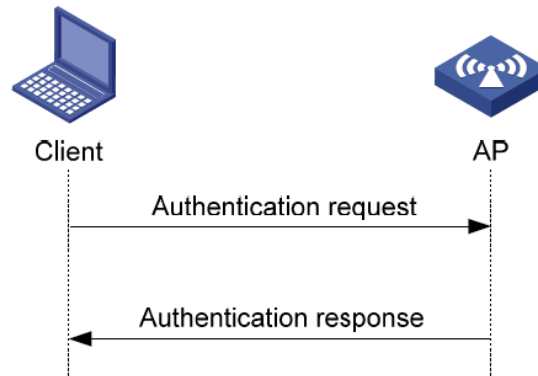


FIGURE 3. Open authentication (H3C, 2016)

3.3.3 WEP

In 1999 IEEE 802.11 defined the WEP (Wired Equivalent Privacy) standard. This method uses encryption and authentication and requires APs and clients to use WEP keys. Used in WLAN, a WEP can have up to four pre-shared keys configured, but only one of them can be active at the time. The wireless frame includes the key number with the sender and the receiver knows what key is used. For encryption the RC4 cipher algorithm is used. It uses WEP keys that consist of 40 or 104 bits which make up a string. Also the receiver and sender operate with the same key that encrypts and decrypts the data (Hucaby 2016, 360-361).

According to Wong (2003), in 2001 the major vulnerability of WEP was discovered and exposed. It makes it possible to recover a WEP key by monitoring for reused IVs. This made the standard no longer safe. In 2004, 802.11i was released to fill in security the gaps of WEP.

Due to backwards compatibility it is still used by many clients and can be found on many APs. WEP keys can be easily recovered with publicly available software e.g. *AirSnort*, *Aircrack*, *WireShark*, and there is a lot of documentation thus implementing an attack. The main problem is the encryption type RC4 cipher. Encryption keys can be recovered from network monitoring. With the security gaps filled this standard is widely used in publicly available WLANs and in homes providing unsecured network access. WEP is not used wireless networks that require security.

3.3.4 WPA/WPA2

According to Coleman & Westcott (2014, 481-483) WPA Wi-Fi Protected Access is upgraded version of WEP but instead of RC4 cipher this standard uses TKIP Temporal Key Integrity Protocol that adds 20 additional bits in data frame. Furthermore, TKIP as data confidentiality protocol is compatible with WEP reinforcing existing RC4 exploit.

WPA2 Wi-Fi Protected Access 2 uses stronger encryption to guarantee data security. CCMP Counter Mode with Cipher Block Chaining Authentication Code data confidentiality protocol and AES advanced encryption standard. The example is shown in Table 2. WPA2 does not use TKIP due to deprecation, which is why it is recommended to use WPA2 instead of WPA and WEP.

Based on Hucaby (2016, 365) WPA/WPA2 have two authentication modes that depends on deployment scale personal mode and enterprise mode. Personal mode authenticates clients by pre shared key, on WLAN environment APs have identical pre shared key configured. Personal mode works without server. Thus PSK is vulnerable to social engineering and dictionary attacks. Enterprise mode uses dedicated server (NAS) to authenticate users, this mode also might be known as 802.1x, and this allows centralized client and device management and control. EAP RADIUS or other authentication method must be used to authenticate clients. Table 2 summarizes the characteristics of WPA and WPA2.

	WPA	WPA2
Authentication	Pre-shared key or 802.1x	Pre-shared key or 802.1x
Encryption and MIC	TKIP or AES (CCMP)	AES (CCMP)
Key management	Dynamic key management	Dynamic key management

Table 2. WPA and WPA2 Comparison (Hucaby 2016, 365)

3.4 Network Access Server Methods

As mentioned earlier one the essential part of modern WLAN networks is authentication. The focus of the study is in Radius based authentication. This implementation uses centralized server to authenticate and authorize users. Alternative names are RADIUS, 802.1X, NAS. All of these methods follow the logic show in Figure 4.

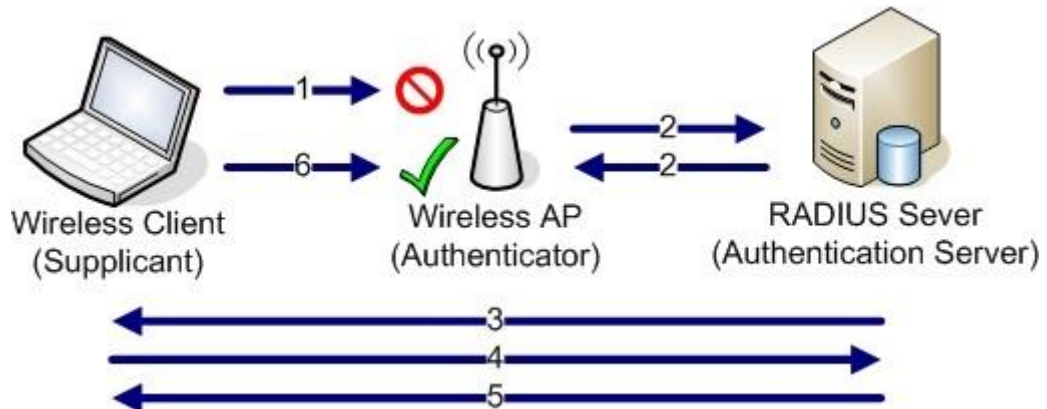


Figure 4. Principle of server based authentication (jakehe.blogspot.fi, 2016).

The authentication takes place in following steps. First, the client associates with the access point which denies communication, second an AP completes a handshake with the authentication server, third the authentication server sends a challenge to the supplicant, fourth the supplicant responds to the challenge using the specified authentication method. In step five the authentication server provides a session key for the supplicant and with a sixth step a supplicant is now synced with the authentication server and AP can now communicate on the wireless network. Based on (jakehe.blogspot.fi, 2016).

4 PRACTICAL PART

In the practical part, I will implement wireless centralized RADIUS authentication in three different ways. As shown in Table 3, the first method is based only on the access point, as the two other methods utilizes a separate authentication server. The second solution suits for medium-sized businesses with one virtual server and the third implementation is for enterprise setup with two virtual servers. All of the implementations are done in MAMK MB316 classroom.

Table 3. Three methods implemented in the thesis

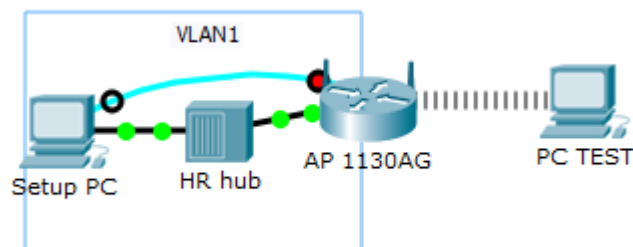
Method 1	Autonomous access point RADIUS
Method 2	Medium business RADIUS setup in Windows server environment
Method 3	Enterprise RADIUS setup in Windows server environment

The presentation below is divided in to three parts, practice 4.1, 4.2 4.3. Then each part is grouped by the steps taken, which are represented step by step.

Each practical part requires the same amount of equipment that are the following: One physical computer, one hub and one access point (Aironet 1130AG or Aironet 1200). Software used for each practical implementations is specified in following chapters. The server based solutions use the latest available stable Windows server (Windows 2012R2) along with an available free Windows NAP role which functions as network access server.

4.1 Autonomous AP RADIUS

The following setup represents personal or small business AP autonomous authentication implementation. We will be working with two computers, one Hewlett Packard hub and AP Aironet 1130AG for RADIUS authentication configuration. The required software is Tera Term Web and a web browser. The logical scheme of setup is shown in Figure 5 and the IP settings follow the data provided in Table 4.

**Figure 5. AP logical scheme**

VLAN1		
	Setup PC	AP 1130AG
NIC	Cisco	BVI1
IP	10.0.0.2	10.0.0.1
Mask	255.255.255.0	255.255.255.0
Gateway	10.0.0.1	--
DNS	--	--

Table 4. IP Table

4.1.1 Environment setup

Firstly, before the start I have to reset factory default on AP, due to the previous configuration could compromise further work. According to following (Cisco, 2013) instructions resetting AP to default configuration. Then, based on the selected computer I refer to (Appendix 2), to connect the devices together with Ethernet and CLI. Note: On the computer I have to disable all NIC except for the cisco NIC because it connects hub to physical computer. After successful connection cisco NIC state should change to up Figure 6. And configure the ipv4 address 10.0.0.2, with a mask 255.255.255.0 and the gateway 10.0.0.1.

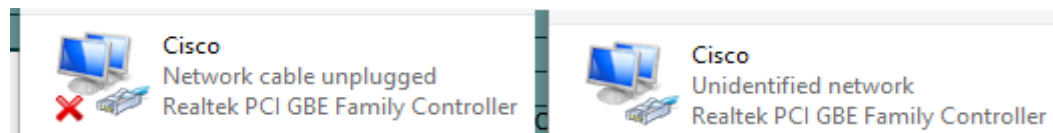


Figure 6. NIC states

4.1.2 AP configuration

I start the configuration of the AP with *Tera Term Web* in order to configure the AP with the CLI. First, I have to check the running configuration to confirm successful reset, disable DHCP services and set an IP address to *BVII* interface, thus allowing to access AP GUI with web browser. After these basic configurations, I test the connectivity with ping from *setup pc* to AP to ensure that connection is working.

AP GUI was accessed by entering preconfigured IP address of AP to browser. Password and user name are *Cisco* with capital c. Then, following instructions of a Surendra

(2013) and a Sharma (2012) the autonomous RADIUS server was configured. Firstly, I go to *Security > Server Manager* and set AP IP address along with shared secret and the authentication, authorization ports. Second, I navigate to *Local RADIUS server > General's setup*, where we enter the same IP address and shared secret thus enabling NAS. Furthermore, in here the users with password are created and stored. Third Authentication methods are selected and applied on NAS server. Fourth I assign a name to the SSID so it would be broadcasted from AP. Fifth step I turn on radio interfaces because due to the reset they are disabled by default.

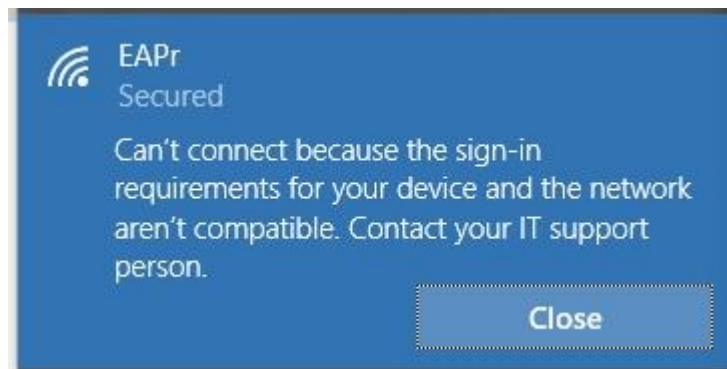


Figure 7. AP user failed authentication

When attempting to connect and enter the created user credentials I receive following message shown in Figure 7. And in event log and Tera Term Web of AP it is possible to view notification of failed authentication shown in Appendix 1. According to support.microsoft.com, (2014) eap-fast and TKIP is no longer supported in Windows 10 OS. When attempted to create new wireless network on *setup pc* the TKIP option was hidden, and all available security types had only the default option available - the AES encryption. Despite attempting various ciphers from AP Figure 8 the outcome was the same and all attempts were unsuccessful.

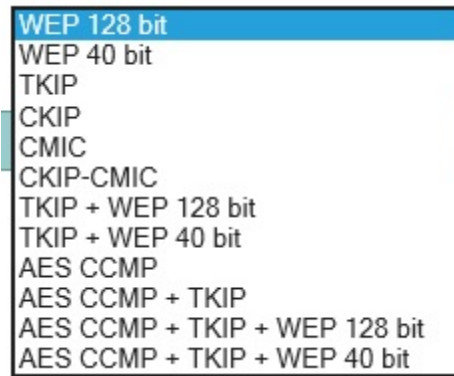


Figure 8. AP encryption modes ciphers

For older operating systems this method can still be used, but as it is not supported in a Windows 8.1 and the latest Windows 10 thus this solution has lost its meaning.

4.2 Medium Business Radius server

In the second implementation, I demonstrate Radius server configuration in Windows environment suitable for medium-sized organizations. Installation and configuration process is based on msdn.microsoft.com (2012) and Ethical Hacker (2013).

For RADIUS server I use existing Windows default role NPS (Network Policy Server) also known as NAS (Network Access Server). As an operating system I use *Windows server 2012r2 datacenter evaluation GUI* installed on virtual machine. Other devices include *Hewlett Packard* hub and *Cisco Aironet 1130AG* access point. Like in first set up I use *Tera Term web* to access the AP through CLI command-line interface.

The logical scheme of setup is shown in Figure 9 and the IP settings follow the data provided in Table 5.

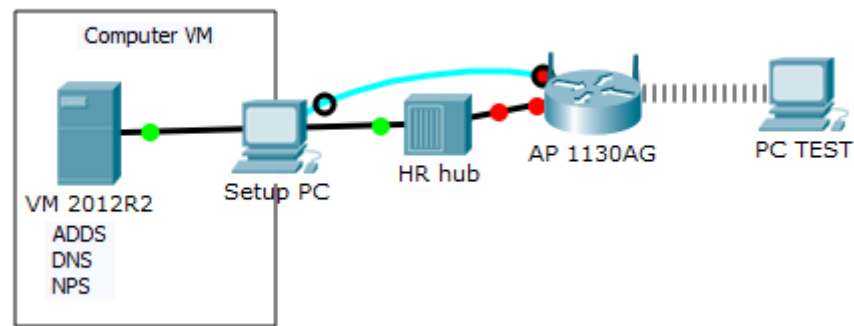


Figure 9. Logical scheme

Virtual environment		VLAN1	
	VM 2012R2	Setup PC	AP 1130AG
NIC	VM Bridge	Cisco	BVI1
IP	192.168.101.9	192.168.101.5	192.168.101.3
Mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	--	192.168.101.9	--
DNS	192.168.101.9	--	--

Table 5. IP table

4.2.1 Settings and configurations

Using VMware I created VM and mounted 2012R2 iso file to start installation. The selected edition is Datacenter GUI. After finishing installation work the environment was connected (as shown in picture above) in preparation for configuration.

On physical computer *Setup Pc* I open *Cisco* NIC and configure IPv4 as shown in Table 5 above. Note that on local computer I leave only *Cisco* and *MB316* interfaces enabled.

To setup and connect NIC of VM *Server2012r2* first I navigate to *Virtual Machine Settings* > click on existing NIC then in network connection select *bridged* and *Replicate physical connection* > in *configure adapters* I select only NIC that represent *Cisco* NIC on physical computer (this step connects virtual NIC to desired physical NIC in computer). After completing this action I apply settings and configure IPv4 of VM NIC according to Table 5 above. Figure 10 below shows the required settings of the virtual machine.

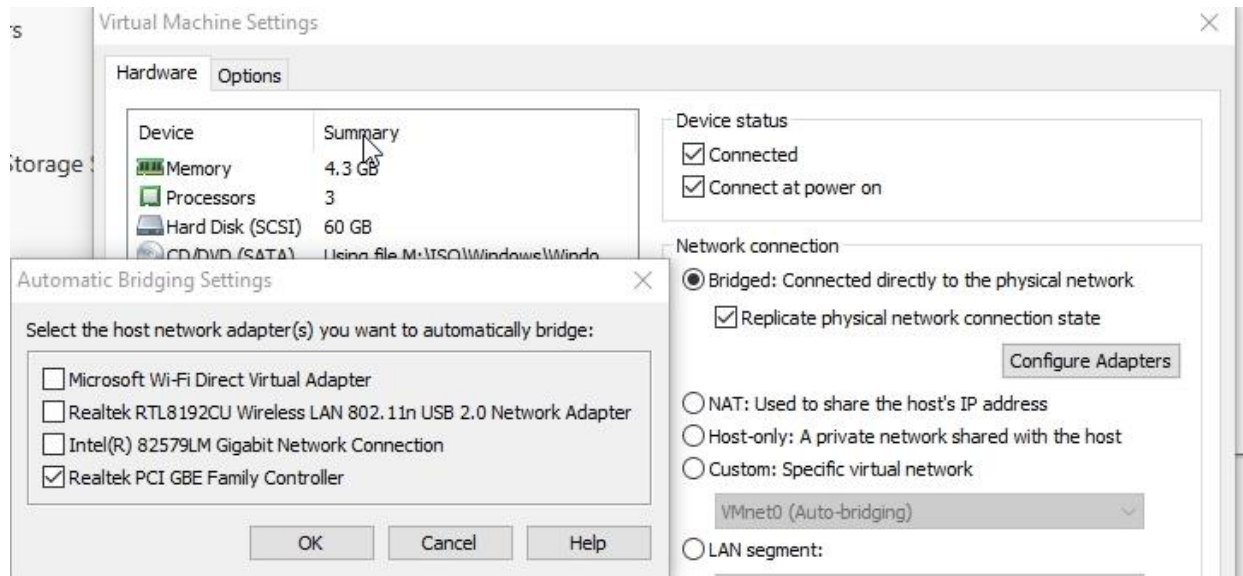


Figure 10. NIC setup

Before AP configurations can be started I had to reset AP as previously mentioned in part 4.1.1. To setup right IP address for AP use Tera Term as described in previous section. After configuring the IP address, I was again able to access from *setup PC* to the AP Figure 11 via browser using Aps IP address.



Figure 11. APs connection

The next step is to install and configure server roles. It is done as follows. To start using authentication I need install following roles to the server ADDS (Active Directory Domain Services), DNS (Domain Name System) and NPS. It is worth pointing out that just ADDS and NPS installation is needed because DNS is a requirement for ADDS and it will be automatically promoted to be configured after ADDS installation. Figure 12 below shows the properties for ADDS and configured domain *pkdomain.local*.

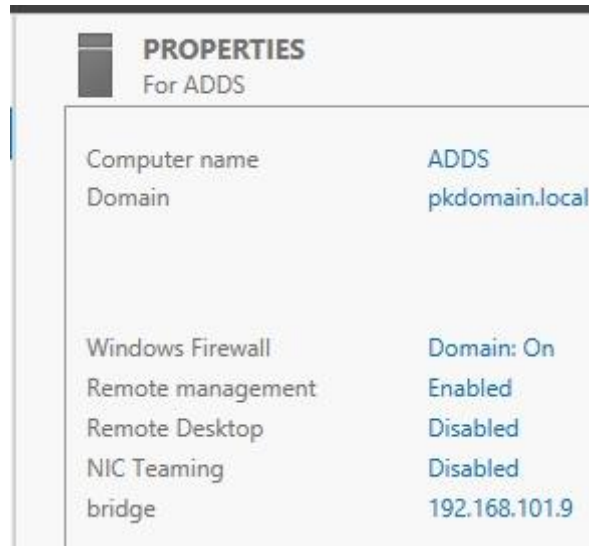


Figure 12. Domain configuration

When ADDS is configured the next step is to create dedicated user group which is used in wireless authentication. To do that I navigate to server manager *server manager* > tab *Tools* > *Active Directory Users and Computers*, select created domain and in user folder create *WIFIusers* group. The following user is created user:cisco, password: Passw0rd with capital p and 0 for o, and user:test the same password as user cisco, then added to user group *WIFIusers* as shown in Figure 13. When creating users it is important to uncheck *User must change password at next login* to not interfere with authentication process.



Figure 13. User group

According to Shinder (2013), for NPS to be installed correctly I need to disable IPv6 on NICs. First to install NPS role, from *Sever Manager* I add new role and follow an installation guidelines, according to Shinder (2013) documentation. Second NPS service are started and then registered in active directory, navigating to *Tools* > *Network*

Policy Server > Action tab > Start NPS service in the same *action* tab select the *Register server in Active Directory* a pop up message confirms successful registration.

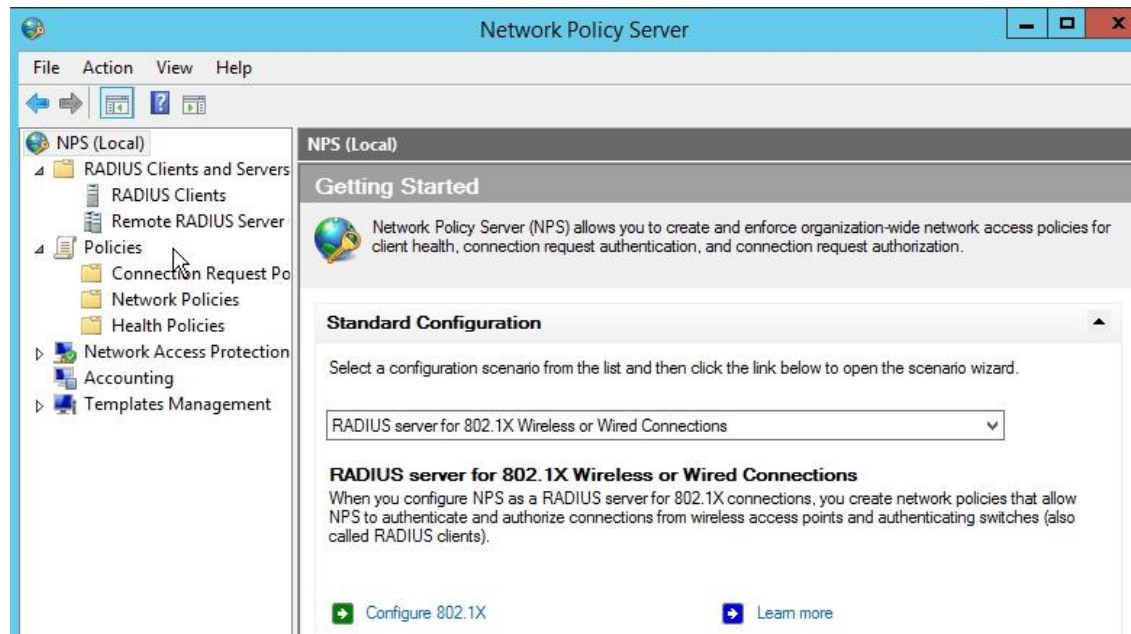


Figure 14. NPS scenario wizard

Third I configure RADIUS using scenario wizard shown in Figure 14. By selecting wireless connections and writing policy name, then adding AP with information and generating shared secret that will be used in further access point configuration, then adding created user group WiFiusers that are used for authentication and lastly authentication method EAP-MSCHAPv2. According to Ethical Hacker (2013) PEAP authentication method needs to be added newly created policy, which is done by navigating to *network policies* shown in Figure 14 selecting created policy and in tab *constraints > authentication* methods PEAP is added. With server configuration finished, lastly I need to configure AP with shared secret, servers IP address and generated shared secret.

Fourth step, according to Coldiron (2014) AP configuration using browser I navigate to *Express Security Set-Up* and configure SSID *WiFi33*, enable broadcasting, then select EAP Authentication thus allowing to input server IP address and shared secret as shown in Figure 15. As mentioned in previous AP configuration 4.1.2 radio interfaces are manually turned on.

Express Security Set-Up

SSID Configuration

1. SSID [Broadcast SSID in Beacon](#)

2. VLAN

No VLAN Enable VLAN ID: (1-4094) Native VLAN

3. Security

[No Security](#)

[Static WEP Key](#)

Key 1 128 bit

[EAP Authentication](#)

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

WPA

Figure 15. AP configuration

4.2.1 Testing and troubleshooting

Using one of MB316 classroom computer I disable all NIC leaving wireless NIC enabled for testing. When connecting to *WiFi33* SSID none with both users I received message *cant connect to this network*. Then using server *event viewer > custom view > Network Policy and Access Service* I was able to determine that access request message is recived from AP but is not validated (event id 18) as shown in Appendix 3. According to documentation.meraki.com (2016) this event id shows problem with shared secret. As a solution I changed shared secret in AP and server to manual, after this correction users successfully authenticated as shown in Figure 16. Additionally users can be authenticated in three methods first with user name second specifying domain name and third using domain email, also shown in Figure 16. Successful user authentication is also confirmed in event viewer of server (note it is important to refresh event log after user authenticates to view changes). Additionally users that are not in *WiFiUsers* group have been tested and their access is denies event viewer logs information what user attempted authentication as shown in Appendix 4.

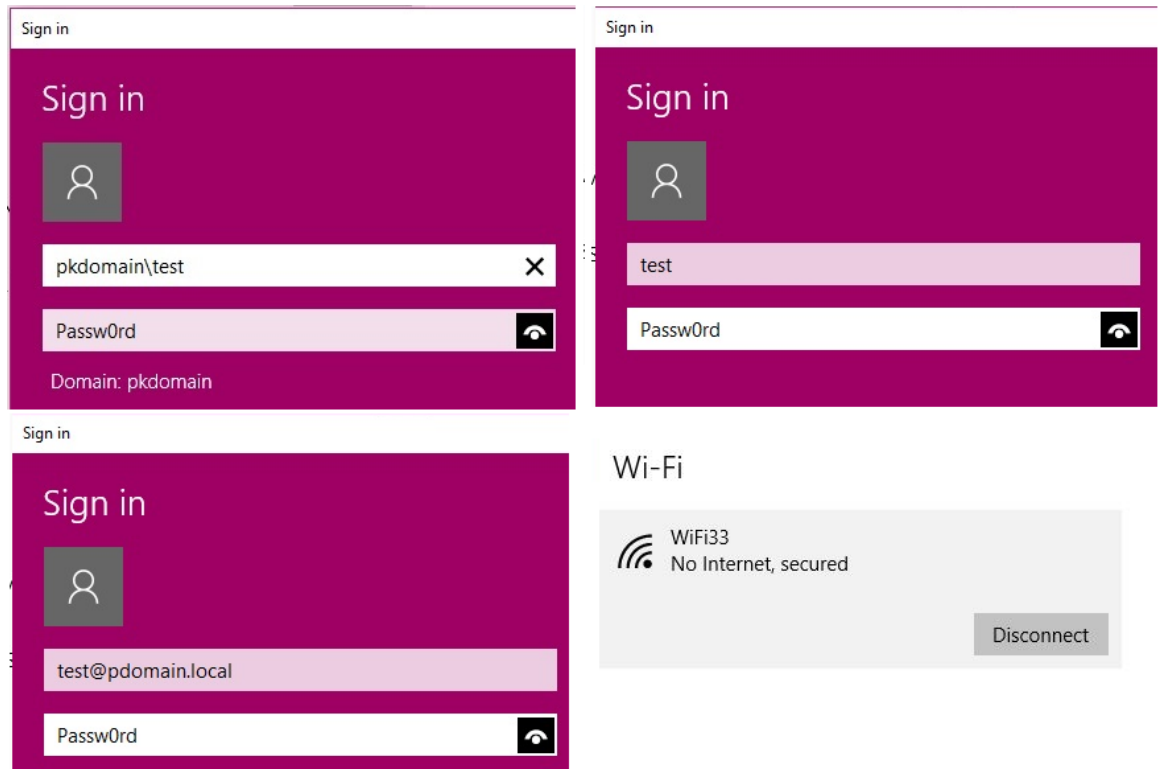


Figure 16. Connecting users

Conclusions technet.microsoft.com, (2013). ADDS and DNS are not recommended to be installed in any other roles additionally in to VM these 3 server roles requires powerful machine if following Microsoft recommendations but for company up to 100 people this is an optional solution. NPS provides control over users and devices connected to RADIUS server, furthermore it additional features can be added as allowed authentication time, device health test, multiple SSID authentication these are just few examples of many available features. NPS can work as standalone RADIUS server not connected to the domain thus providing more security to existing network setup.

4.3 Enterprise Radius

The third implementation is ment for multiple servers and targeted for larger organization. The logical scheme of setup is shown in Figure 17 and the IP settings follow the data provided in Table 6.

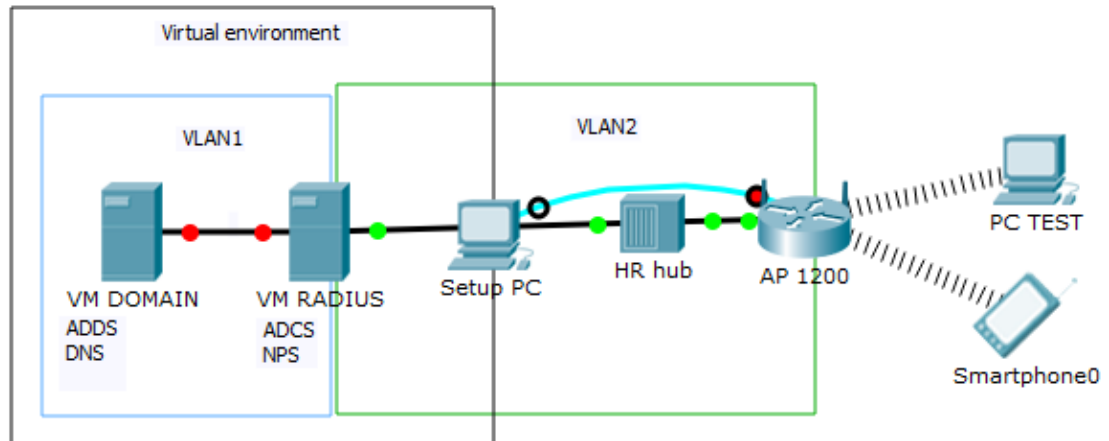


Figure 17. Logical scheme

	Virtual environment				
	VLAN1			VLAN2	
	VM Domain	VM Radius		Setup PC	AP 1200
NIC	VM Host	VM Host	VM Bridge	Cisco	BVI1
IP	192.168.11.10	192.168.11.9	192.168.50.9	192.168.50.5	192.168.50.3
Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	---	192.168.11.10	192.168.50.5	192.168.50.9	--
DNS	192.168.11.10	192.168.11.10	--	--	--

Table 6. IP table

4.3.1 Setup and configuration

Firstly I have created two virtual machines as shown in Figure 17, VM DOMAIN and VMRADIUS both are connected with host only virtual network adapters. For VM RADIUS additional network interface is added in bridge mode thus enabling it to connect to physical cisco NIC setup process is the same as in 4.2 chapter. After renaming and configuring virtual machines NICs as shown in Table 6 I tested ping command and virtual machines can't ping each other as shown in Figure 18, according to (technet.microsoft.com, 2012. Nobody Can Ping My Computer) on firewall incoming icmp request is disabled, I also used provided instruction to allow incoming icmpv4 communication in both virtual machines and thus ping being able to ping.

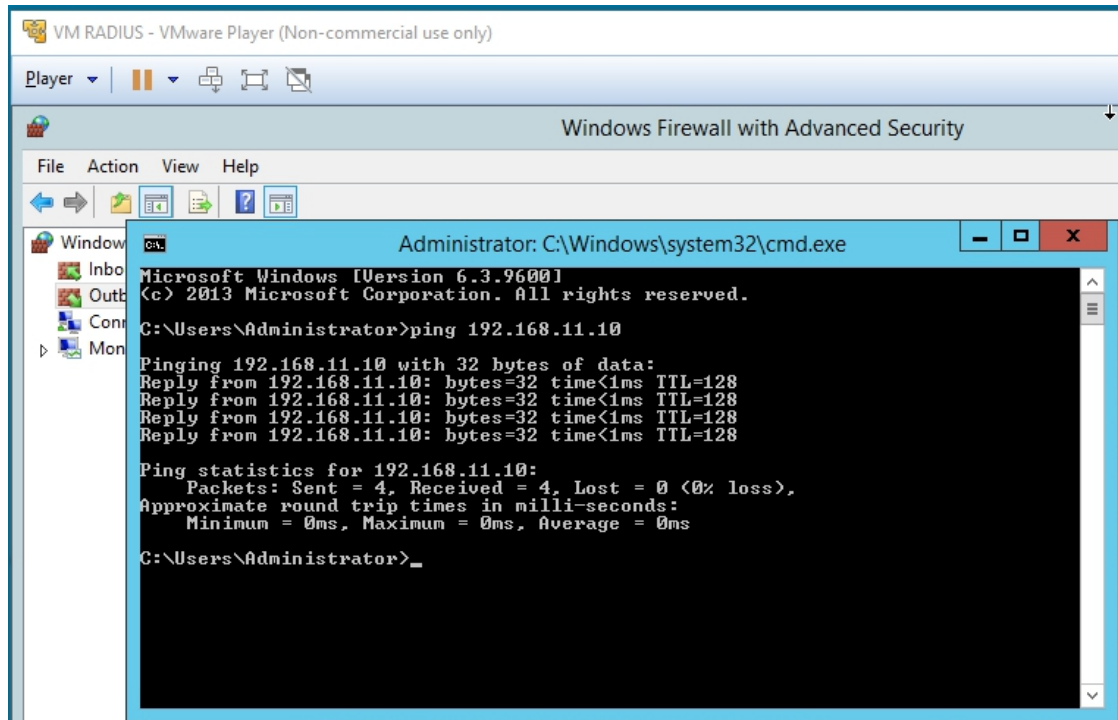


Figure 18. VM RADIUS ping VM DOMAIN

Secondly I connected AP Aironet 1200 as shown in Figure 17 and restored default configuration of AP, IP address were configured from Table 6 the same way as mentioned in practical part 2. SSID used was *APradius*.

Third in VM DOMAIN I install ADDS DNS thus creating *mamkradius.com* domain as shown in Figure 19.



Figure 19. VM DOMAIN configured ADDS



Figure 20. User group WIFusers

Fourth step is to create user and user group in VM DOMAIN the process is the same as in 4.2 chapter the created user:user1, password:Passw0rd with capital p and 0 for o, and user:user2 passwords are the same for both users, then they are added to user group *WIFusers* as shown in Figure 20.

Fifth step is VM RADIUS virtual machine is connect to domain MAMKRADIUS. And I login with VM DOMAIN administrator to install and configure NPS. The NPS is installed, registered, started and configured in the same way as 4.2 chapter but this time I use manual shared secret, AP is configured in the same way as well using IP addresses from Table 6. I have encountered a problem when adding PEAP authentication method in *network policies* I received the following error message shown in Figure 21. Along with this protocol comes certificate required for successful communication between domain and NPS servers.

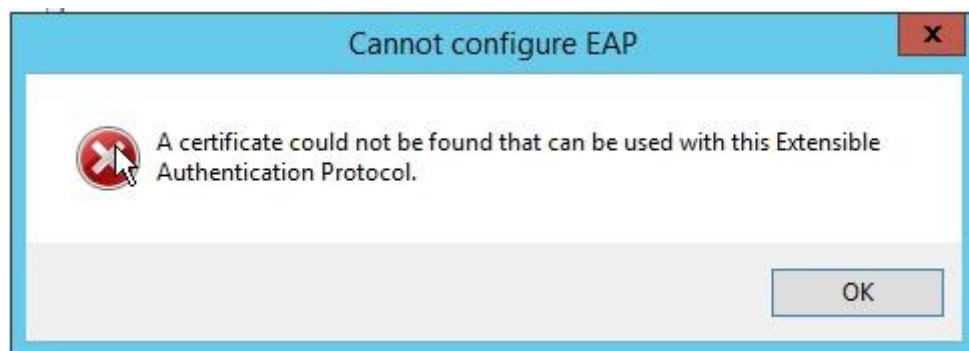


Figure 21. EAP certificate not found

4.3.2 Testing and troubleshooting

According to msdn.microsoft.com, Certificate Requirements (2012) ADCS is required in NPS server, because PEAP protocol does not have certificate associated with domain according to msdn.microsoft.com, Deploying Certificates for PEAP and EAP (2012) there are 3 ways to add certificate to NPS server: first *Deploy Client Computer Certificates*, second *Deploy User Certificates*, third *Deploy a CA and NPS Server Certificate*. In my case I have selected *Deploy a CA and NPS Server Certificate* because it is a simple few step process that requires installing ADCS in VM RADIUS server.

The ADCS role was installed to VM RADIUS based on instruction from msdn.microsoft.com (, 2012. NPS Server Certificate: CA Installation). After installation I navigated to NPS network policy and in the created policy > tab constraints > authentication method added PEAP as shown in Figure 22.

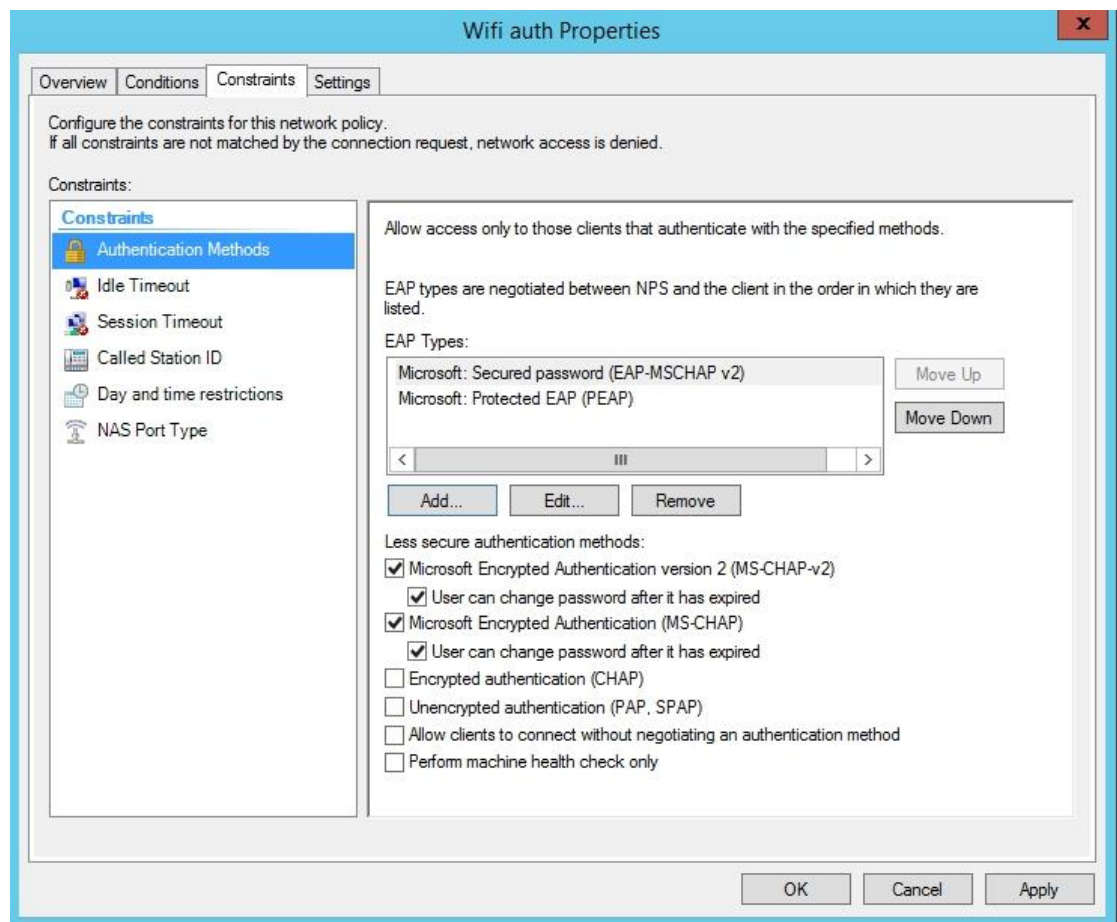


Figure 22. Authentication method PEAP

After successful configuration and troubleshooting I again prepared one of the MB316 classroom computers and tested user authentication that the created users are able to authenticate and the successful authentication process is tracked on VM RADIUS virtual machine event viewer logs as mentioned above in 4.2.1 chapter. Users are able to login using same three methods as mentioned in previous chapter 4.2.1 as shown in Figure 23. Also user not belonging to domain has been tested and failed authentication as shown in Appendix 5.

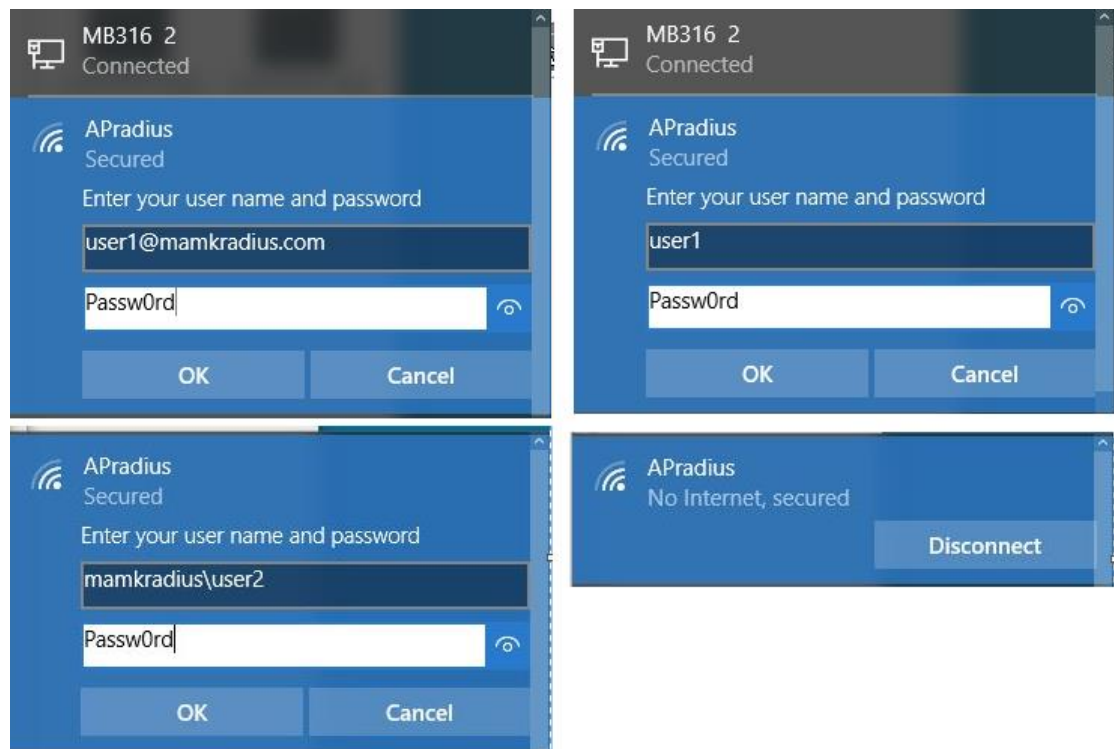


Figure 23. WiFiusers authentication

This enterprise solution uses dedicated RADIUS server for the authentication thus allowing more features to be used based on server or computer performance. Additionally in second and third practical part the users are able to use single sign-on this allows easier management for domain administrators. More over dedicated RADIUS server can be configured as VPN, posture assessment feature can be added or day and time restrictions.

5 CONCLUSIONS

The aim of the study was to learn and research the development of the Wi-Fi access control methods. This topic was covered in a chronological order starting from old and ending at modern secure methods used today. The practical aim of the study was to implement network access control with an external RADIUS server and create a RADIUS lab for students. And that the created external server would provide a possibility to use one database for multiple devices management as access points and routers. The implementation was done on existing MAMK MB316 classroom equipment.

The theory part of the study introduced different authentication methods used in WLANs. In the practical part of the study the focus was on Radius based methods and I implemented three different Radius authentication solutions. The first method was based on autonomous RADIUS authentication. The results of the study clearly point out that this method is no longer valid as current operating systems do not support it anymore. The remaining two implementation methods are server based RADIUS that centralizes the services, device and users management in to one or several servers, virtual or physical. Windows server are limited by the amount of roles installed per server, due to roles requiring high amount computing power and network throughput thus creating delays and service issues. As in the second practical implementation part, active directory domain service should not be installed along with NPS.

For the future studies the created virtual environment can be used to design lab assignments for students or further developed by using available NAS features and policies. Authentication currently works with all windows based devices the android and ios require additional policy configuration. DHCP role could be added. Over all original goal of the thesis was fulfilled.

BIBLIOGRAPHY

Cisco, 2013. Quick Start Guide Cisco Aironet 1130AG Access Point - Resetting to Default Configuration. http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1130/quick/guide/ap1130qs.html#wp30482. Updated on 29.02.2007. Referred 20.04.2016.

Coldiron, Larry, 2014. Configure WPA on CISCO Aironet 1200. Type of document video. <https://www.youtube.com/watch?v=RwlFfVWxrWc> . Updated 28.11.2014. Referred 20.04.2016.

Coleman David D. & Westcott David, 2014. CWNA Certified Wireless Network Administrator Official Study Guide Fourth Edition. City of publisher: Indianapolis.

documentation.meraki.com, 2016. Common Wireless RADIUS Configuration Issues . https://documentation.meraki.com/MR/Encryption_and_Authentication/Common_Wireless_RADIUS_Configuration_Issues No update information. Referred 20.04.2016

Ethical, Hacker, 2013. 802.1x WiFi Radius server in Server 2012 Part-2. Type of document video. <https://www.youtube.com/watch?v=lWUs9pwUcuc>. Updated on 18.07.2013. Referred 04.05.2016

Ethical, Hacker, 2013. 802.1x WiFi Radius server in Server 2012 Part-1. Type of document video. <https://www.youtube.com/watch?v=wliUq5KxOHA>. Updated on 15.07.2013. Referred 04.05.2016

H3C, 2016, WLAN Security Introduction. http://www.h3c.com.hk/Products___Technology/Technology/WLAN/Technology_Introduction/200812/624019_57_0.htm. No update information. Referred 15.03.2016.

Hassell, Jonathan 2003. Radius 1st edition by Hassell, Type of document, ebook. <https://books.google.cz/books?id=o5xQNbuvJ7QC&printsec=frontcover&hl=cs&sour>

ce=gbs_ge_summary_r&cad=0#v=onepage&q&f=true. City of publisher: Sebastopol.
Referred 20.04.2016.

Hucaby, David 2016. CCNA Wireless 200-355 Official Cert Guide (Certification Guide). City of publisher: Indianapolis.

jakehe.blogspot.fi, 2016. 802.1X/EAP User Authentication. <http://jakehe.blogspot.fi/2014/07/8021x-user-authentication.html>. No update information. Referred 25.05.2016

Margaret, Rouse, 2016. NAC network access control. <http://searchnetworking.techtarget.com/definition/network-access-control>. No update information. Referred 15.03.2016.

msdn.microsoft.com, 2012. Certificate Requirements for PEAP and EAP. [https://msdn.microsoft.com/en-us/library/cc731363\(v=ws.11\).aspx](https://msdn.microsoft.com/en-us/library/cc731363(v=ws.11).aspx). Updated on 29.03.2012. Referred 2016.

msdn.microsoft.com, 2012. Checklist: Configure NPS for Secure Wireless Access. [https://msdn.microsoft.com/en-us/library/cc771696\(v=ws.11\).aspx](https://msdn.microsoft.com/en-us/library/cc771696(v=ws.11).aspx). Updated on 29.03.2013. Referred 20.04.2016

msdn.microsoft.com, 2012. Deploying Certificates for PEAP and EAP [https://msdn.microsoft.com/en-us/library/cc754367\(v=ws.11\).aspx](https://msdn.microsoft.com/en-us/library/cc754367(v=ws.11).aspx). Updated on 29.03.2012. Referred 2016.

msdn.microsoft.com, 2012. NPS Server Certificate: CA Installation. [https://msdn.microsoft.com/en-us/library/cc771431\(v=ws.11\).aspx](https://msdn.microsoft.com/en-us/library/cc771431(v=ws.11).aspx). Updated on 29.03.2012. Referred on 20.04.2016.

Sharma, Vinay, 2012. Configuring Autonomous AP for Local RADIUS Authentication. <https://supportforums.cisco.com/document/101121/configuring-autonomous-ap-local-radius-authentication>. Updated on 28.05.2012. Referred 20.05.2016.

Shinder, Deb, 2013. Understanding and Configuring Network Policy and Access Services in Server 2012 (Part 3). http://www.windowsecurity.com/articles-tutorials/Windows_Server_2012_Security/understanding-configuring-network-policy-access-services-server-2012-part2.html. Updated on 27.03.2013. Referred 20.04.2016

Stanley, Wong, 2003. The evolution of wireless security in 802.11. Type of document, PDF. <https://www.sans.org/reading-room/whitepapers/wireless/evolution-wireless-security-80211-networks-wep-wpa-80211-standards-1109> Updated on 20.05.2003, viewed 20.04.2016.

support.microsoft.com, 2014. Windows 10 devices can't connect to an 802.1X environment. <https://support.microsoft.com/en-us/kb/3121002>. Updated on 12.07.2015. Referred 20.04.2016

Surendra, BG, 2013. EAP-FAST with the Internal RADIUS Server on the Autonomous Access Point Configuration Example. <http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116580-configure-eapfast00.html#anc7>. Updated on 10.10.2013. Referred 20.05.2016.

technet.microsoft.com, 2012. Nobody Can Ping My Computer. [https://technet.microsoft.com/en-us/library/cc749323\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc749323(v=ws.10).aspx). Updated on 18.02.2012. Referred 20.04.2016.

technet.microsoft.com, 2013. Active Directory Domain Services Overview. [https://technet.microsoft.com/en-us/library/hh831484\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh831484(v=ws.11).aspx). Updated on 22.08.2013. Referred 23.05.2016

technet.microsoft.com, 2013. Network Policy and Access Services Overview. [https://technet.microsoft.com/en-us/library/hh831683\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh831683(v=ws.11).aspx). Updated on 07.11.2013. Referred 23.05.2016

Vangie, Beal 2010. Wi-Fi, Definition is Not Wireless Fidelity. http://www.webopedia.com/DidYouKnow/Computer_Science/wifi_explained.asp. Updated on 14.08.2010. Referred 04.04.2016

Wi-Fi Alliance, 2016. Alliance information. <http://www.wi-fi.org/who-we-are> No update information. Referred 04.04.2016

Zhangh, Mervyn, 2011. completely reinstall NPS with original settings. <https://social.technet.microsoft.com/Forums/windowsserver/en-US/337d0ce8-1f0a-4b25-92fc-5c7384e5c378/completely-reinstall-nps-with-original-settings?forum=winserverNAP>. Updated on 11.11.2009. Referred 04.05.2016

APPENDICES

Appendix 1. Authentication failure

The screenshot shows the Cisco Aironet 1130AG Series Access Point configuration page. The browser address bar shows 'http://10.0.0.1/'. The page title is 'Cisco Aironet 1130AG Series Access Point'. The hostname is 'ap' and the uptime is '12 minutes'. The left sidebar contains navigation options: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is divided into sections: Home: Summary Status, Association, Network Identity, Network Interfaces, and Event Log. A terminal window titled 'Tera Term Web 3.1 - COM1 VT' is overlaid on the Network Interfaces section, displaying the error message: '*Apr 17 05:59:13.411: %DOT11-7-AUTH_FAILED: Station f81a.6708.b d1f Authentication failed'. The Event Log table below shows a list of events with columns for Time, Severity, and Description. The most recent event is an authentication failure at 05:59:13.411.

Hostname ap ap uptime is 12 minutes

Home: Summary Status

Association

Clients: 0 Infrastructure clients: 0

Network Identity

IP Address: 10.0.0.1

MAC Address: 0015.c6ff.35ee

Network Interfaces

Interface

- FastEthernet
- Radio0-802.11G
- Radio1-802.11A

Event Log

Time	Severity	Description
Apr 17 05:59:13.411	◆Debugging	Station f81a.6708.bd1f Authentication failed
Apr 17 05:57:41.016	◆Debugging	Station f81a.6708.bd1f Authentication failed
Apr 17 05:52:49.798	◆Information	DFS scan complete on frequency 5320 MHz
Apr 17 05:52:09.305	◆Notification	Line protocol on Interface Dot11Radio0, changed state to up
Apr 17 05:52:08.305	◆Error	Interface Dot11Radio0, changed state to up
Apr 17 05:52:08.304	◆Information	Interface Dot11Radio0, frequency 2422 selected
Apr 17 05:52:03.129	◆Notification	Configured from console by console
Apr 17 05:51:50.796	◆Notification	Line protocol on Interface Dot11Radio1, changed state to up
Apr 17 05:51:49.796	◆Error	Interface Dot11Radio1, changed state to up
Apr 17 05:51:49.795	◆Information	Interface Dot11Radio1, frequency 5320 selected

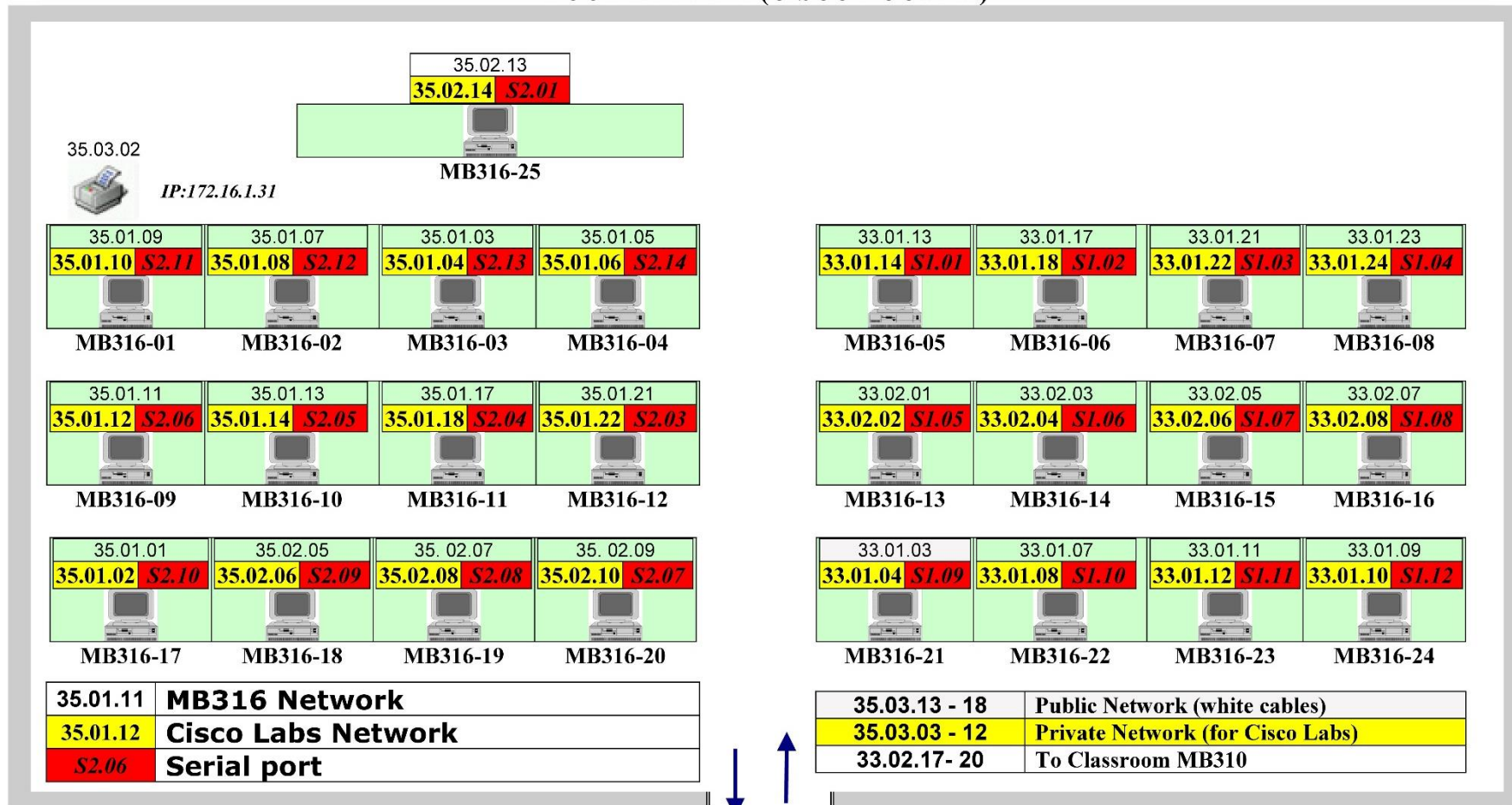
Refresh

Close Window Copyright (c) 1992-2009 by Cisco Systems, Inc.

Appendix 2. MAMK MB316 classroom wire scheme

 MAMK University of Applied Sciences				Mikkelin ammattikorkeakoulu Tarkk'ampujankuja 1 PL181; 50101 Mikkeli http://www.mamk.fi	4.3.2015
---	---	--	---	---	----------

LUOKKA MB316 (CISCO-LUOKKA)



Appendix 3. Not validated access request

NPS THESIS Windows Server 2012 - VMware Player (Non-commercial use only)

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
 - Server Roles
 - Network Policy and Access Services
 - Remote Desktop Services
 - Administrative Events
 - Windows Logs
 - Applications and Services Logs
 - Subscriptions

Network Policy and Access Services Number of events: 123

Number of events: 123

Level	Date and Time	Source	Event ID	Task Category
Error	5/13/2016 3:42:36 AM	NPS	18	None
Error	5/13/2016 3:42:31 AM	NPS	18	None
Error	5/13/2016 3:42:26 AM	NPS	18	None
Error	5/13/2016 3:42:21 AM	NPS	18	None

Event 18, NPS

General Details

An Access-Request message was received from RADIUS client 192.168.101.3 with a Message-Authenticator attribute that is not valid.

Log Name: System
 Source: NPS
 Event ID: 18
 Level: Error
 User: N/A
 OpCode:

Logged: 5/13/2016 3:42:36 AM
 Task Category: None
 Keywords: Classic
 Computer: PKserver.pkdomain.local

More Information: [Event Log Online Help](#)

Appendix 4. Unauthorized user authentication pkdomain

Network Policy and Access Services Number of events: 21

Number of events: 21

Level	Date and Time	Source	Event ID	Task Categ...
Information	5/15/2016 7:42:40 AM	Microsoft ...	6273	Network Po...
Information	5/15/2016 7:42:06 AM	Microsoft ...	6273	Network Po...

Event 6273, Microsoft Windows security auditing.

General Details

Network Policy Server denied access to a user.
Contact the Network Policy Server administrator for more information.

User:

Security ID:	NULL SID
Account Name:	notworking
Account Domain:	PKDOMAIN
Fully Qualified Account Name:	PKDOMAIN\notworking

Client Machine:

Security ID:	NULL SID
Account Name:	-
Fully Qualified Account Name:	-
OS-Version:	-
Called Station Identifier:	0015.2c4a.2960
Calling Station Identifier:	a0f3.c129.5bec

NAS:

NAS IPv4 Address:	192.168.101.3
NAS IPv6 Address:	-
NAS Identifier:	ap
NAS Port-Type:	Wireless - IEEE 802.11
NAS Port:	276

RADIUS Client:

Client Friendly Name:	Wifi33Radius
-----------------------	--------------

Log Name: Security

Source: Microsoft Windows security Logged: 5/15/2016 7:42:06 AM

Event ID: 6273 Task Category: Network Policy Server

Level: Information Keywords: Audit Failure

User: N/A Computer: ADDS.pkdomain.local

OpCode: Info

More Information: [Event Log Online Help](#)

Appendix 5. Unauthorized user authentication mamkradius

Event 6273, Microsoft Windows security auditing.

General Details

Network Policy Server denied access to a user.
Contact the Network Policy Server administrator for more information.

User:

Security ID:	NULL SID
Account Name:	baduser
Account Domain:	MAMKRADIUS
Fully Qualified Account Name:	MAMKRADIUS\baduser

Client Machine:

Security ID:	NULL SID
Account Name:	-
Fully Qualified Account Name:	-
OS-Version:	-
Called Station Identifier:	0016.46f8.4ee0
Calling Station Identifier:	f81a.6708.b4fd

NAS:

NAS IPv4 Address:	192.168.50.3
-------------------	--------------

Log Name: Security

Source:	Microsoft Windows security	Logged:	5/21/2016 12:35:18 PM
Event ID:	6273	Task Category:	Network Policy Server
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	WINNPS.mamkradius.com
OpCode:	Info		

More Information: [Event Log Online Help](#)