

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

FACULTY OF ECONOMICS AND MANAGEMENT

DEPARTMENT OF INFORMATION TECHNOLOGIES



DIPLOMA THESIS

Multiple SSIDs Wi-Fi Networks for Heavy Loads

Author: B.Sc. Seyed Ali SadatMousavi

Supervisor: Ing. Tomas Vokoun

© 2020 CULS Prague

DIPLOMA THESIS ASSIGNMENT

B.Sc. Seyed Ali SadatMousavi

Systems Engineering and Informatics
Informatics

Thesis title

Multiple SSIDs WiFi Networks For Heavy Loads

Objectives of thesis

Make a plan to redesign a new network topology by making hardware and configuration upgrades to the current design.

Focus on current hardware and the choice between the best needed devices based on the required performance and optimization of signals for clients.

Finally, consideration of cost optimization will be included in the new implementation of the network. In this way, the Security will be the most important part while considering maximum benefits of connectivity speeds with the lowest possible budget.

Methodology

This diploma thesis is divided to 3 categories:

First one is the introduction of the current situation and consist of different literature review in order to implement a solution and a vision of external technical persons.

Second part is the main focus of the author for this thesis which consist of actual implementation of Multiple SSIDs WiFi networks for heavy loads, including installation of new HW, redesign of the topology and a configuration of both old and new devices on the network.

Thirdly, it consists of the conclusion part which will describe the overall implementation, observation and testing of the new redesigned network to measure a success factor by taking the feedback from the "WiNG management system" and internal employees.

The proposed extent of the thesis

50-60

Keywords

SSIDs, Network Topology, WiFi, Security

Recommended information sources

GEURTS, J. et al. Transparent handover using WiFi network prediction for mobile video streaming. [s.l.] : Springer Verlag, [s.d.]. v. 353
How Wi-Fi Works Gintzler, A. S. Cavendish Square Publishing LLC 2018
HUTCHISON, D. et al. Implementation of 802.21 for Seamless Handover Across Heterogeneous Networks. In: Managing Next Generation Networks & Services
WiFi, WiMAX and LTE Multi-Hop Mesh Networks : Basic Communication Protocols and Application Areas Wei, Hung-Yu; Rykowski, Jaroqnew; John Wiley & Sons, Incorporated

Expected date of thesis defence

2019/20 SS – FEM

The Diploma Thesis Supervisor

Ing. Tomáš Vokoun

Supervising department

Department of Information Technologies

Electronic approval: 11. 10. 2019

Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 14. 10. 2019

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 11. 02. 2020

DECLARATION

I declare that I have worked on my diploma thesis titled " Multiple SSIDs Wi-Fi Networks for Heavy Loads " by myself and I have used only the sources mentioned at the end of the thesis. As the author of the Diploma thesis, I declare that the thesis does not break the copyrights of any third person.

Prague, March 2020

ACKNOWLEDGMENT

I would like to thank my Diploma Thesis supervisor Ing. Tomas Vokoun, my managers Mr. Petr Kraus, Mr. Martin Bambas and especially the main member of the network team Mr. B.Sc. Vit Peterek Expert Network Engineer at SPORTISIMO and also Mr. Matousek Network Expert of EXTREME company for their advice and support during my work on this thesis. This thesis work is dedicated to my parents, who have always loved me unconditionally and whose good examples have taught me to work hard for the things that I aspire to achieve.

Multiple SSIDs Wi-Fi Networks for Heavy Loads

Abstract

With the improvement of technologies, its wide range of usability expose like an epidemic in our world, the needs of a network have been felt more and more in our routine life that makes connectivity between clients, devices, servers and provide internet service for some of them which are essential. In this way, lots of job position has been created to handle and run this network for a variety of users from companies, shops, universities, hotels, local area network users and any other systematic collection which needs to make fast connectivity for cooperating of their clients.

In this thesis, we have thousands of clients in Sportisimo who need non-stop connectivity with the highest possible speed. In this step, the Sportisimo Network Team must find the problems, decide the best solutions and do troubleshooting or maintenance of the network after the redesign by new solutions.

In Sportisimo, clients are connected to the main network but in different buildings with several devices that provide internet connectivity, accessibility of relevant applications for warehouses, stores, and ServiceDesk service for employees' tasks.

Non-stable connectivity and areas that are not covered by Wi-Fi, bad communication and transformation data between the Access Points and the Network Controllers, low-security level to compare with number and volume of clients and networks, etc. According to the above problems, it encourages Sportisimo managers to set up a semi-huge upgrade to the whole of Sportisimo network topologies.

These upgradings contain upgrading of access points and controller firmware, resorting the network sites categories into the management application to have easier accessibility, the increase of security level, solve the connectivities issues, need to have a main Wi-Fi SSID for all users and clients instead of several numbers of SSIDs for connections of each devices group and one Wi-Fi SSID for guests who come to any Sportisimo building and want to have an internet connection for a short period of time.

Keywords: SSIDs, Network Topology, Wi-Fi, Security

Abstraktní

Se zlepšením technologií se jejich široká škála použitelnosti projevuje jako epidemie v našem světě. Proto se v naší každodenní rutině stále více a více pocítuje potřeba sítě, která umožňuje propojení mezi klienty, zařízeními, servery a někdy všemi z těchto prvků k internetu. Je to život. Tímto způsobem bylo vytvořeno mnoho pracovních pozic, aby bylo možné tuto síť udržovat a provozovat pro různé uživatele, od společností, přes obchody, univerzity, hotely, uživatele místní sítě až po jakékoli jiné systematické prvky, která musí zajistit rychlé připojení pro spolupráci svých klientů.

Tato práce je zaměřena na tisíce klientů ve společnosti SPORTISIMO, kteří potřebují nepřetržité připojení s nejvyšší možnou rychlostí. V tomto kroku musí tým spravující vnitřní síť SPORTISIMO najít problémy, rozhodnout se o nejlepších řešeních a řešení problémů / údržbě sítě po přepracování na nová řešení.

Ve SPORTISIMO jsou klienti připojeni k hlavní síti, to jest činěno v několika různých budovách s mnoha zařízeními, která zajišťují připojení k internetu, dostupnost příslušných aplikací pro sklady, obchody a službu ServiceDesk pro úkoly zaměstnanců.

Podle nestabilní konektivity a někde nekryté oblasti Wi-Fi, též ale i tak dobrých komunikačních a transformačních dat mezi přístupovými body a síťovými radiči, nízkou úrovní zabezpečení pro porovnání s počtem a objemem klientů a sítí atd., povzbuzujte manažery SPORTISIMO, aby vytvořili dostatečně velký upgrade celé topologie sítí SPORTISIMO.

Tyto upgrady obsahují upgrade přístupových bodů a firmwaru radičů, třídění kategorií síťových serverů v aplikacích pro správu za účelem snazší přístupnosti, zvýšení úrovně zabezpečení, řešení problémů s připojením, potřebu hlavního Wi-Fi SSID pro všechny uživatele a klienty namísto několik čísel SSID pro připojení každé skupiny zařízení a jeden Wi-Fi SSID pro hosty, kteří přicházejí do jakékoli budovy Sportisimo a chtějí mít připojení k internetu na krátkou dobu.

Klíčová slova: SSIDs, Network Topology, Wi-Fi, Security

Table of Contents

1. INTRODUCTION.....	14
2. OBJECTIVES & METHODOLOGY	15
2.1.Objectives.....	15
2.2.Methodology	15
3. LITERATURE REVIEW.....	16
3.1.Introduction Of Wireless & Wired Networks	17
3.2.Wireless Network Principles.....	17
3.3.Types Of Wireless Networks	18
3.3.1. Wireless Local Area Networks (WLAN).....	18
3.3.2. Wireless Personal Area Networks (WPAN)	18
3.3.3. Wireless Metropolitan Area Networks (WMAN).....	18
3.3.4. Wireless Wide Area Networks (WWANS).....	18
3.4.Wireless Networks, Usage, Benefits, Dimensions.....	19
3.4.1. Indoor Wireless Network	20
3.4.2. Outdoor Wireless Network	21
3.4.3. Access Point Output Power.....	21
3.4.4. Access Point Output Sensitivity.....	21
3.4.5. Antenna Power	22
3.5.ACTIVE ELEMENTS OF WIRELESS LAN	22
3.5.1. Wireless station	22
3.5.2. Access Points	22
3.6.RANGE & COVERED AREA	22
3.7.Wi-Fi.....	23
3.8.IEEE STANDARDS	25

3.9. Wireless Network Security	25
3.9.1. What is Encryption?	26
3.9.2. Wired Equivalent Privacy (WEP)	26
3.9.3. Wi-Fi Protected Access (WPA)	27
3.9.4. The difference between TKIP & AES	27
3.9.5. Wi-Fi Protected Access II (WPA2).....	28
3.9.6. WPA Personal & WPA Enterprise Difference.....	28
3.9.7. Wi-Fi Protected Access III (WPA3)	28
3.9.8. IEEE 802.1x	30
3.10. Service Set Identifier (SSID)	33
3.10.1. Definition of SSID.....	34
3.10.2. SSID Usage	34
3.11. Multiple SSIDs By Multiple APs	34
3.12. RADIUS Server	36
3.12.1. AAA	36
3.12.2. Network Policy Server (NPS)	38
3.12.3. NPS As A RADIUS Server	38
3.12.4. RADIUS Proxy.....	38
3.12.5. RADIUS Accounting.....	39
4. Practical Part.....	40
4.1. Sportisimo Wireless Network Overview	41
4.2. Problem Statement	43
4.3. Localization Re-Sorting	44
4.4. Access Points Firmware Update	46
4.5. Implementation of a RADIUS Server	47
4.6. Create a New Single WLAN SSID for Radius Server.....	54

5.	Results and Discussion.....	58
6.	Conclusion.....	59
7.	Recommendation.....	60
8.	References	61

Table of Figures

Figure 1 - Types of Network usage at Different Distance	19
Figure 2 - IEEE Standards	25
Figure 3 - Process of Encryption of Plain Text to Crypted One	26
Figure 4 - Wireless Network Security Protocols	29
Figure 5 - Network Client Filtering by IEEE 802.1x.....	30
Figure 6 - User Authorization by IEEE 802.1x	31
Figure 7 - ESS Access Points & BSS Cells	35
Figure 8 - RADIUS Server (Radius Server, n.d.)	37
Figure 9 - Typical Windows Server NPS.....	39
Figure 10 - Pie Chart of Devices Activity Situation	41
Figure 11 - Wireless Network Device Types.....	42
Figure 12 - Mix localization organize.....	44
Figure 13 - New Locally Re-Sorted Network Sites of Sportisimo	45
Figure 14 - Access Points Firmware Update	46
Figure 15 - Microsoft Windows Server 2016	47
Figure 16 - Radius Configuration in NPS Setup.....	48
Figure 17 – Connection of Access Points to Radius Client	48
Figure 18 - Network Policies PEAP Certificate.....	49
Figure 19 - Access Point Setting in Radius Server-Side.....	49
Figure 20 - Sportisimo Certificate	50
Figure 21 - Sportisimo Active Directory	51
Figure 22 - Network Policies Overview	51
Figure 23 - Network Policies Conditions.....	52
Figure 24 - Network Policies PEAP	52
Figure 25 - Network Policies Overview	53
Figure 26 - Devices of Hala C Office	54
Figure 27 - WLAN Management Page in Wing App	55
Figure 28 - Setup New WLAN in Wing App	55
Figure 29 - Security Adjustment of New WLAN in Wing App	56
Figure 30 - AAA Policy setting and Joined of the NPS.....	56
Figure 31 - Authentication Server Registration in Wing App	57

1. INTRODUCTION

Sportisimo is a premium retailer of sporting goods and has been established in 1999 at Brno, Czech Republic. Sportisimo provides everything for athletic & leisure time activities in almost 200 stores + e-shop in the Czech Republic, Slovakia, Poland, Hungary, and Romania with more than 6 warehouses.

The company must be eligible to provide a central network which connects the whole of the company departments, partitions, sections, and groups to run their task. This network needs also to be stable, without any disconnectivity and the highest possible security level and speed.

In this thesis, decided the network must be redesigned and changes to have a better performance, connectivity, security level, and an easier way to troubleshoot more than 5000 devices which are located in stores, warehouses and official buildings. This responsibility is one of the duties of the IT Department and the network department of Sportisimo.

Sportisimo is using Extreme Development Network Software Management which is named “Extreme Wireless WiNG Software Environment” and for network infrastructure devices. They are mostly equipped with Extreme access points and controllers and Unifi switches and routers. It is also good to mention that the company is using Microsoft services for operating systems and servers.

Most types of connectivities are supplied by **11** SSIDs of wireless connections which a management technique must run to reduce this number of SSIDs to increase the main network performance and also make it easier to be supported by the IT department.

These objects of the network must be provided or corrected by mixed methods of network sciences and experiences that will be explained in the following part of the thesis.

2. OBJECTIVES & METHODOLOGY

2.1. Objectives

Make a plan to redesign a new network topology by making hardware and configuration upgrades to the current design.

Focus on current hardware and the choice between the best-needed devices based on the required performance and optimization of signals for clients.

Finally, consideration of cost optimization will be included in the new implementation of the network. In this way, the security will be the most important part while considering the maximum benefits of connectivity speeds with the lowest possible budget.

2.2. Methodology

First, the introduction of the current situation and it is consisting of different literature reviews to implement a solution and a vision of external technical persons.

The second part is the main focus of the author for this thesis which consists of an actual implementation of Multiple SSIDs Wi-Fi networks for heavy loads, including installation of new HW, redesign of the topology and a configuration of both old and new devices on the network.

Thirdly, it consists of the conclusion part which will describe the overall implementation, observation, and testing of the newly redesigned network to measure a success factor by taking the feedback from the "WiNG management system" and internal employees.

3. LITERATURE REVIEW

3.1. Introduction Of Wireless & Wired Networks

Local area networks (LAN) for home and workplace can be designed in either wired or wireless form. At first, these networks were designed with cable and using Ethernet technology, but now we are experiencing an increasing trend in the usage of wireless networks with Wi-Fi technology.

Cable networks (which are now mostly used the Star topology) must be independently wired from each workstation to the distribution unit like hub or switch. (the CAT5 cable length must not exceed 100 meters. Otherwise, optical fiber is used). Used equipment has two categories, passive devices such as cable, outlet, duct, patch panel, etc. and active devices such as hubs, switches, routers, network cards, and so on. The IEEE Institute of Engineering has set 802.3u standards for Fast Ethernet, 802.3ab and 802.3z for Gigabit Ethernet (for electric and optic cables).

Both cable and wireless networks claim superiority over the other, but the right choice depends on network demands. The following capabilities can be considered for comparing wireless and cable networks:

- Installation and commissioning
- Cost
- Reliability
- Efficiency
- Security

3.2. Wireless Network Principles

Wireless networks are one of the fascinating technologies that have attracted a lot of attention. Offering Wireless service and internet, known as Wi-Fi is being performed today in many parts of the world to attract customers and serve as a new service to enhance the organization in a competitive marketplace. Also, to numerous locations such as hotels, exhibitions, sports gyms, conference halls, and airports, wireless internet services are provided at home and work, providing customer and passenger satisfaction, especially for foreign customers and travelers.

Wi-Fi provides access to the Internet without any need for cables or wires for devices such as laptops, PDAs, mobile phones and more. This allows the user to easily access the

Internet at the hotel or workplace without having to connect their devices to the telephone line or their room network.

3.3. Types Of Wireless Networks

Let us take a look at the main types of wireless networks that are usually used to implement a different variety of targets.

3.3.1. Wireless Local Area Networks (WLAN)

This type of network is useful for local users such as campuses or laboratories that need to use the Internet. In this case, if the number of users is limited, the connection can be made without the use of an Access Point. Otherwise, the usage of an Access Point is necessary.

3.3.2. Wireless Personal Area Networks (WPAN)

The two technologies used for these networks are IR (Infra-Red) and Bluetooth (IEEE 802.15) that allow communication in an area of about 90 meters, although IR requires direct communication and distance limitation.

3.3.3. Wireless Metropolitan Area Networks (WMAN)

This technology enables the communication between multiple networks or buildings in one city. As a backup, they can use optical fiber or copper cables.

3.3.4. Wireless Wide Area Networks (WWANS)

This type of network is used for long-distance networks, such as between cities or countries. The connection is provided via wireless antennas or satellites.

The following figure shows the different types of wireless networks at different distances:

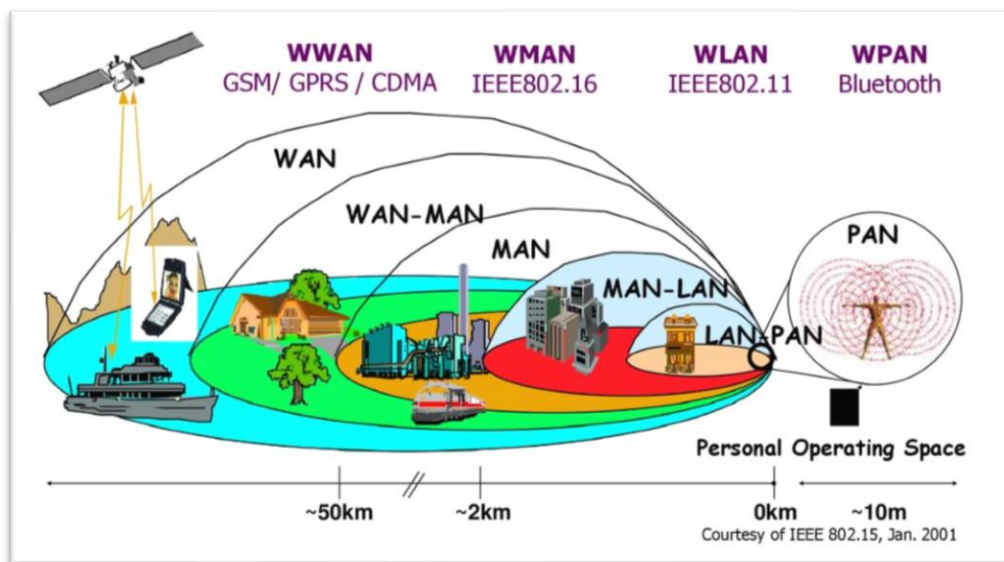


Figure 1 - Types of Network usage at Different Distance (1)

3.4. Wireless Networks, Usage, Benefits, Dimensions

Wireless networking technology, using data transmitted by radio waves, allows hardware devices to communicate with another one without the use of physical platforms such as wires and cables. Wireless networks cover a wide range of applications, from complex structures such as cellular wireless networks - often used for cell phones - and wireless LANs (WLANs) to simple types such as wireless headphones.

On the other hand, including infrared waves, all equipment that uses infrared waves, such as keyboards, mice and some cell phones, falls into this category. The most natural advantage of using these networks is the need to have no physical structure and the ability to move equipment connected to such networks, as well as to make changes to their virtual structure. In terms of structure, wireless networks are divided into three categories: WWAN, WLAN, and WPAN.

WWAN, which stands for Wireless WAN, is a network with high wireless coverage. An example of these networks is the cellular wireless structure used in mobile networks. A WLAN provides more limited coverage in a building or organization, and the small dimensions of a hall or several rooms. WPAN or Wireless Personal Area Network is for home use. Communications such as Bluetooth and infrared fall into this category.

WPAN networks, on the other hand, fall into the category of Ad-Hoc networks. In Ad-Hoc networks, the hardware is dynamically added to the network as it enters the space covered. An example of such networks is Bluetooth. In this type, various equipment, such as a keyboard, mouse, printer, laptop or pocket PC, and even a mobile phone, will be able to access the network if they are in a covered environment and they will be able to exchange data with other network-connected equipment. The difference between Ad-Hoc networks and WLANs is their virtual structure. In other words, the virtual structure of wireless LANs is based on a static design, while Ad-Hoc networks are dynamic in every aspect. It is natural that along with the benefits that this dynamic provides to users, maintaining the security of such networks also has many problems. However, one of the solutions available to enhance security on these networks, especially in the case of Bluetooth, is to reduce the coverage radius of the network signals. Even though Bluetooth performance is based on low power transceivers and this advantage is significant in pocket PCs, the relative amount of hardware involved is due to the limited coverage area that is considered a security consideration. In other words, this advantage, along with the use of not-so-sophisticated passwords, are the only security concerns for these networks. (2)

Wireless computer equipment and networks are manufactured and used on either Indoor or Outdoor.

3.4.1. Indoor Wireless Network

The organizations and companies need to have a secure network and limitations in cabling have encouraged professionals to find alternatives to a computer network. Indoor networks are those that are created inside the building. These networks are designed in two types. Ad-Hoc networks and Infrastructure networks. Ad-Hoc networks do not have a centralized device and computers have wireless network cards. The Ad-Hoc strategy applies to small networks with limited workstations. The second strategy of implementing the wireless network standard is the Infrastructure Network. In this method, one or more centralized devices called Access Point are responsible for communicating.

3.4.2. Outdoor Wireless Network

Outdoor Wireless Communication is known as Outdoor Wireless. In this method, having Line of Sight, two-point height and distance are the criteria for selecting the type of Access Point and antenna.

The Outdoor Wireless Network can be implemented with three types: Point To Point, Point To Multipoint and Mesh topologies.

- **Point to Point**

In this method, two points of contact are considered. In each part antenna and Access Point are installed and the two parts are connected.

- **Point to Multi-Point**

In this method, one point is considered as the center of the network and the other points are connected to this point.

- **Mesh**

Wireless connectivity of several points is referred to as Mesh topology. In this method, there may be several central points that are interconnected.

Wireless communication between two points depends on two factors, Access Point Output Power (Upload Data) and Access Point Sensitivity (Download Data).

3.4.3. Access Point Output Power

One of the features of the design of wireless communication systems is the access point output. More power provides a stronger and longer range of the signal.

3.4.4. Access Point Output Sensitivity

One of the key determinants in the reception quality of the waves produced by Access Point is the access point sensitivity. By increasing the amount of this sensitivity, the

probability of no signal delivery will decrease, and this will ensure reliable and effective communication.

3.4.5. Antenna Power

For each antenna, the output power and angle of coverage or propagation are important. In this regard, varieties of antennas with different characteristics of power and angle of propagation have been created, such as Omni, Sectoral, Parabolic, Panel, Solied.

3.5. ACTIVE ELEMENTS OF WIRELESS LAN

There are usually two types of active elements in wireless LANs:

3.5.1. Wireless station

A wireless station or station is typically a laptop or stationary workstation that connects to a local area network using a wireless network card. It can also be a pocket PC or even a barcode scanner. In some applications, the use of cables at computer terminals can be a hassle for the designer and conductor, and these terminals, usually housed inside kiosks, use wireless connectivity to the local area network.

3.5.2. Access Points

Access points in wireless networks, as discussed earlier, are active hardware that plays the role of a switch in wireless networks and can also connect to wired networks. In practice, the network's main platform structure is generally wired and is connected to the main wired network by these access points, meadows, and wireless stations.

3.6. RANGE & COVERED AREA

The wireless coverage measure based on the IEEE standard 802.11, depends on many factors which are as follows:

- Bandwidth used

- Sources of transmitted waves and the location of transmitters and receivers
- Wireless network installation and installation specifications
- Waves Power
- Antenna type and model

The coverage measure varies from 29 meters (for indoor spaces) and 485 meters (for open spaces) to 802.11b. However, these values are moderate and depend on the measure of powerful receivers and transmitters currently work, it is possible to use this protocol and its receivers and transmitters for up to several kilometers.

However, the overall measure mentioned for using this protocol (802.11b) is anything between 50 and 100 meters. This measure is a function and it is valid for closed spaces and buildings. The following figure shows a comparison between sample boards in different applications of 802.11b wireless networks:

One of the functions of access points as wireless switches is to operate between wireless areas. In other words, using several wireless switches can achieve the same function as a Bridge for wireless networks. The connection between the access points can be point to point to create a connection between two subnets or can be point to multi-point or opposite to create a connection between different subnets simultaneously.

Access points that are used as a bridge between local networks together use very high power to send data, which means a higher area coverage. This hardware is usually used to make connections between points and buildings that are 1 to 5 kilometers apart. It should be noted, however, this is an average distance based on the 802.11b protocol. Additional protocols such as 802.11a can be extended further.

The following figure shows an example of point-to-point communication using appropriate access points:

3.7. Wi-Fi

About 15 years ago, Wi-Fi technology turned from a slow, unreliable connection to a strong, all-encompassing connection. Wi-Fi plays a vital role in our lives today. Researchers are still working to increase the quality of this technology and introduce a variety of Wi-Fi

standards. The higher-speed and longer-range are two factors that customers and manufacturing companies are looking for.

Wi-Fi technology, as a popular option for wireless Internet access, has met various standards. Routers available to use this technology also have different types.

Smartphones these days have become multifunctional electronic gadgets that provide a wide range of services to their owners. In the meantime, connecting to the Internet is a key feature that provides a better and more diverse service. Although smartphones allow the use of the cellular network to access the Internet, various reasons encourage the user to use Wi-Fi. Among these reasons may be the greater stability of Wi-Fi networks or higher speeds. With these interpretations, familiarity with Wi-Fi network standards will be of particular importance for achieving the best user experience. (3)

- **Wi-Fi Demands**

Today's workforce, equipped with digital personal assistants (PDAs), laptops, smartphones, and other mobile devices, demands Wi-Fi access to your network from anywhere, without the hassle of a fixed network. Your business allows you to operate a network faster, at a lower cost, and with greater flexibility than a wired system. The benefits of Wi-Fi are also increasing, since employees can be connected to a network for a longer time, and will be able to work with their colleagues when and where needed. (3)

Wi-Fi networks are smoother than wired networks. Another network is no longer a fixed thing, networks can be created or opened in the afternoon instead of days or weeks requiring a structured cable network. These networks can have home, office, or industrial applications, examples of which are:

- Internet distribution networks in public places (HotSpot)
- Wireless LANs in Companies and Offices for Data Transfer
- Wireless Local Area Networks (VOIP)
- Wireless Local Area Networks for Video Transfer (CCTV, Video Conference)
- Wireless LANs for Security Systems

3.8. IEEE STANDARDS

Personal and business users have different arrays when shopping for network equipment. However, the compatibility of smartphones or other electronic devices with these standards is just as important. The Institute of Electrical and Electronics Engineers (IEEE) has been exposing some standards such as 802.11a, 802.11b / g / n, or 802.11ac for a wide range of products with Wi-Fi technology. (4)

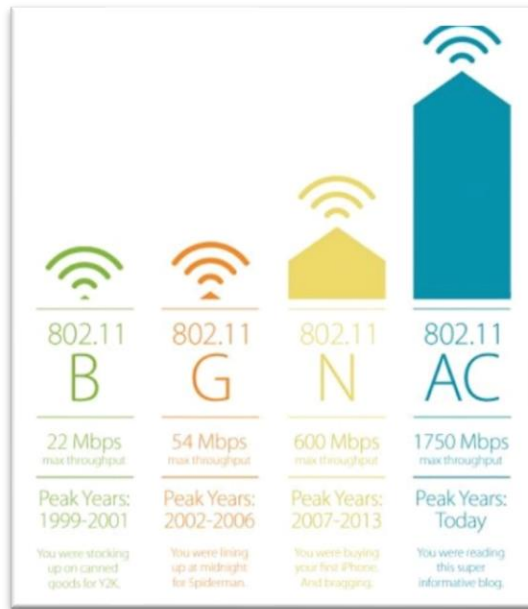


Figure 2 - IEEE Standards (5)

3.9. Wireless Network Security

Wi-Fi networks have very powerful security features that prevent unauthorized access to these networks. (6) Among these standards are:

- WEP - Wired Equivalent Privacy
- WPA - Wi-Fi Protected Access I
- TKIP/AES
- WPA2 - Wi-Fi Protected Access II
- WPA3 - Wi-Fi Protected Access III
- IEEE 802.1x

Wireless network security and encryption protocols have become one of the hottest topics among technology audiences today. The range of audiences is propagated from computer engineers and IT to every regular home internet user.

Due to the increasing number of attacks on wireless networks in recent years, new methods and technologies have been developed using various algorithms and encryption to increase the security of these networks more than ever before. Let us describe existing protocols and standards to make these networks more secure and prevent attacks below. (3)

3.9.1. What is Encryption?

Cryptography is one of the fundamental keys to wireless network security. Encryption is an operation that converts comprehensible text to encrypted text using encryption techniques that make it impossible to access primary information and text that can only be accessed through the key or key Access.

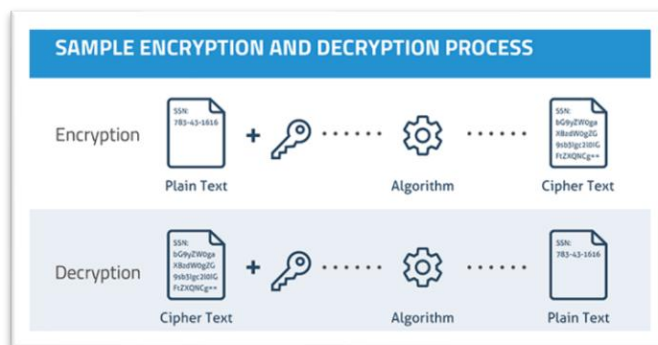


Figure 3 - Process of Encryption of Plain Text to Crypted One (7)

Now for the best choice of security level, we need to have more knowledge about Wireless Network Security Protocols.

3.9.2. Wired Equivalent Privacy (WEP)

WEP is one of the first protocols in wireless network security, as defined in Wireless 802.11b standard, which is part of the IEEE 802.11 standards.

WEP uses a 64-bit RC cipher or a 128-bit encryption key to encrypt data in the second network layer. This WEP key contains a user-defined key that is either 40-bit or 104-bit,

and one of the two key models combines with a 24-bit primary carrier and the WEP key is either 64-bit or 128-bit. The WEP standard is no longer a safe and secure way of identifying wireless devices. Attackers analyze the sum of data seizures and crack WEP keys using tools such as AirSnort, WEPCrack, and deputies. (2)

3.9.3. Wi-Fi Protected Access (WPA)

Protected access to Wi-Fi, or WPA, was provided one year before WEP retirement and came to replace it. The most widely used WPA structure can be called WPA-PSK, which can encode between 8 and 63 ASCII characters. The keys used by WPA are 256 bits, which is a significant improvement over the 64 and 128 bit WEP modes. Some of the most important changes made by the WPA include message integrity checking to determine whether an attacker has been able to capture the packets exchanged between the access point and the client and the Temporary Key Integration Protocol (TKIP). Later, TKIP was replaced with the Advanced Encryption Standard or AES. Although WPA was designed to make it easier for users to get rid of the WEP, because it was provided by firmware updates on WEP-enabled devices, it had to modify certain elements of it, which ultimately made it vulnerable. After a while, WPA suffered the fate of the WEP, and a public demonstration was made to prove its vulnerability.

3.9.4. The difference between TKIP & AES

TKIP and AES are two different encryption methods that can be used by a Wi-Fi network. TKIP is a step-by-step encryption protocol introduced by the WPA to replace highly secure encryption with the WEP network. TKIP is almost similar to WEP encryption. TKIP is no longer safe and generally outdated. You should not use this encryption method either.

AES is a much more secure encryption protocol introduced with WPA2. AES is not another weak cryptographic standard designed for Wi-Fi networks. This encryption protocol is a very serious standard of encryption that has been endorsed and even adopted by the US government. For example, when you encrypt a hard drive, your cryptographic software may use the AES protocol to do.

3.9.5. Wi-Fi Protected Access II (WPA2)

It was in 2006 that WPA was replaced with WPA2. One of the biggest changes to this replacement was the forced use of AES algorithms as well as the introduction of CCMP (Anti-Code Mode with Blockchain Message Validation Protocol) as a replacement for TKIP. The use of WPA2 for home users is currently virtually without a major disadvantage, with major concerns about business security. Unfortunately, the biggest concerns in WPA are still in WPA2, and although breaking the wall created by WPA2 requires between 2 and 12 hours of continuous work on a PC, there is still the need to review and resolve security gaps.

3.9.6. WPA Personal & WPA Enterprise Difference

- **Personal**

Both the WPA and WPA2 protocols, when combined with your network, includes a small office or home network with no server for authentication. It uses an access point with a 2-bit key. This is also called WPA-PSK.

- **Enterprise**

Both WPA and WPA2, when combined with the word Enterprise means that you have a huge network, so it requires a **RADIUS server** to authenticate users. This needs a more complex implementation but protects better against attacks like dictionary attacks. This is known as WAP-**802.11X** and sometimes also known as WAP.

3.9.7. Wi-Fi Protected Access III (WPA3)

After the problems reported for WPA2, the Wi-Fi union introduced the new WPA3 standard. The first actual draft of this protocol is not yet available, but the Wi-Fi union has announced several features as follows:

- Change Wi-Fi public network data to secure encrypted mode

- Protection against Brute-force attacks by blocking the detection process after multiple failed login attempts
- Ability to make security adjustments on phones and tablets on non-display devices. This will provide greater security for the Internet of Things (IoT) gadgets and other devices where it is difficult to make security adjustments.
- 4-bit security suite to protect networks such as government and industrial sites, etc. that need more security.

After the standard is fully introduced by the Wi-Fi Union, it is time for companies to add WPA3 support to modem routers, computers, phones, tablets and devices equipped with the Internet of Things. Therefore, we are still a few years away from the popularity of WPA3. In the current situation, the best you can do is make sure your devices receive the latest security updates. If you have a device that is old enough to not receive an update, you may want to consider a newer alternative.

There are a few years remains until WPA3 implementation, easy connection protocols, and optimum open time. Public use of WPA3 occurs when existing routers are upgraded or replaced with new routers. However, if you are concerned about the security of a home network, you can replace your existing router with a WPA3-Certified router, as the companies will release them in the upcoming months.

	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

Figure 4 - Wireless Network Security Protocols (7)

As a result, WPA2-PSK AES is currently the safest option to choose from. Use the latest Wi-Fi encryption standard along with the latest modern encryption method, AES. We recommend using this option. For routers whose graphical interfaces are a bit confusing, this is probably the case with titles such as WPA2 or WPA2-PSK that most likely use AES encryption (as this is the most logical case).

3.9.8. IEEE 802.1x

The IEEE 802.1X standard is a standard for PNAC - port-based Network Access Control and forms part of the IEEE 802.1 standard protocol, which is a network protocol that aims to improve network security and its core is to identify users who want to connect to LANs such as LAN Local Area Network and WLAN Wireless Local Area Network. (8)

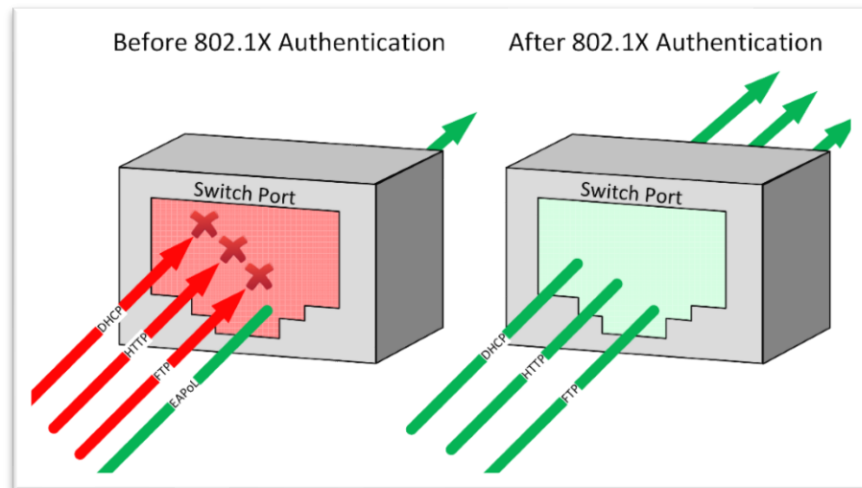


Figure 5 - Network Client Filtering by IEEE 802.1x (8)

The use of LAN networks and their security vulnerability to various attacks, in the second Layer, led the IEEE to consider developing several security protocols and standards to secure this layer. Although using MAC Address Filtering and ACL access control list can be effective, these solutions are almost impossible for large networks with a large number of users and even smartphones or laptops on wireless networks that are extremely difficult to control. The IEEE 802.1X standard identifies users based on connected ports to the network presented by using Authentication servers such as:

- CISCO ACS (Cisco Secure Access Control Server)
- NAC (Network Access Control)
- RADIUS (Remote Authentication Dial-in User Service)
- **Users Identification by 802.1x**

Imagine a user logs into our organization and wants to connect to the network as soon as the user connects his connection cable to the network socket. Let us take a look at what is going on. (8)

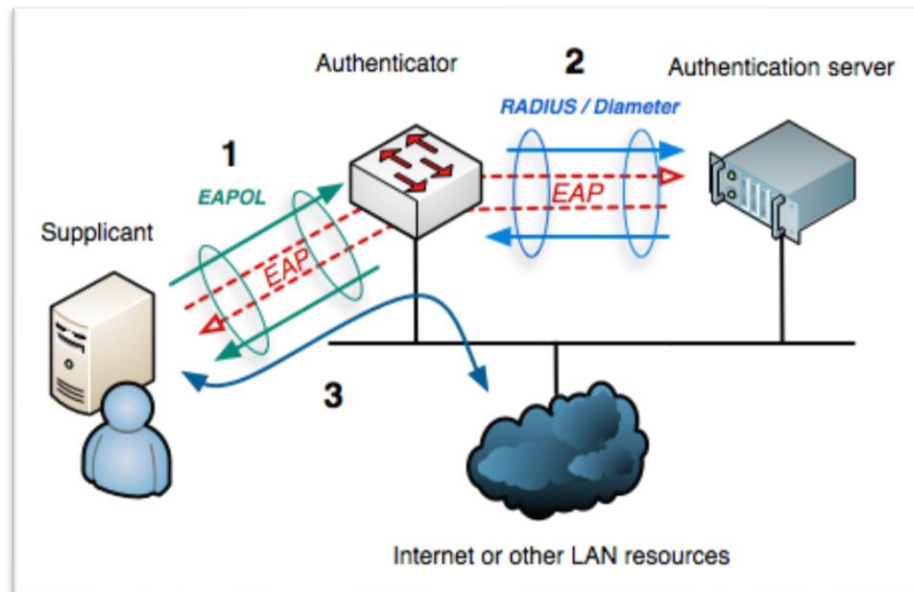


Figure 6 - User Authorization by IEEE 802.1x (8)

- a) Once a new user is detected on the switch port before the computer can connect to the network, the user authentication mode is activated and the port is set to Unauthorized, preventing public traffic such as DHCP, DNS, etc. It only permits pass-through protocols that work for authentication, such as the Extensible Authentication Protocol EAP, but this EAP protocol alone cannot be used as an authentication protocol. EAP has many different types of security features and different encryption capabilities in each of these methods, enabling network administrators to use the appropriate method for their application as needed. The most common types of protocols are:

- EAP-PEAP
- EAP-TTLS
- EAP-TLS
- EAP-MD5
- LEAP
- EAPOL (Extensible Authentication Protocol over LAN)

It should be noted that the Cisco switches also include Spanning tree protocol STP and Cisco discovery protocol CDP.

- b) After the port is unauthorized, an EAPOL request containing the Username / Password content is sent by the Authenticator, which is our switch or access point to the network, to perform authentication. Meanwhile, one of the main tasks of the Authenticator is to encapsulate the EAP frame.
- c) The user sends the response as a response to the Authenticator connected to itself, at which time the Authenticator receives the EAP frame, sends the received response to the respective Authentication server.
- d) If the Authentication server finds the computer username and passwords valid in your DataBase, the port will be set to Authorized mode by other network services so that the user can use their network resources. The important point here is that if the network is different from different VLANs and we want each user to access a specific VLAN according to the level of access specified, we can use Authenticator servers such as CISCO ACS to enable Mobile Users without any physical limitations. NAC Server can also be used to enhance security during user authentication, for example: Check that the user system must have Antivirus should be specific or it must have been updated by the date of that day or even one Rey's security policies, for example, include removing the RUN option from the connected system so that it can connect to the network, and will automatically be directed to the specified file server if it does not have an anti-virus on the system, for example. To install the program and then log on to the desired network.
- e) Finally, when the user logs off an EAP-Logoff message is automatically sent to the connected Authenticator to return the desired Authenticator to the unauthorized port and all traffic other than EAP, EAPOL STP and CDP are blocked.

- **MAC Authentication by IEEE 802.1x**

As the title implies, the MAC Address is used to identify the devices instead of the Username/Password. The explanation for this is that when the device is connected to the network port, the client sends its MAC Address as the passport to the Authenticator instead of the username and password, and the Authenticator sends it to its Authentication Server, If the MAC Address sent to the Data Base of the Authentication Server device was present, then the device could eventually be connected to the network and forget that this setting must be applied to the corresponding port. Such settings are also used for network peripherals such as a printer. (8)

- **Web Authentication 802.1x**

Web authentication is a mode in which users use web pages to authenticate. This is usually the case when the system does not support this standard and can support up to eight users simultaneously on one port.

3.10. Service Set Identifier (SSID)

SSID (Service Set Identifier) is the primary name associated with a wireless 802.11 (WLAN) local area network (home networks and public hotspots) which appear by access points and routers. Client devices use this name to identify and join the network.

For example, suppose you want to connect to a wireless network at a school or workplace called the guest network, but you will find several other networks that have completely different names. All the names you see are SSIDs of those networks.

On home Wi-Fi networks, a broadband router or broadband modem stores the SSID but allows management to change it. Routers can allow wireless applicants to find the network by transmitting this name.

3.10.1. Definition of SSID

SSID is an uppercase and lowercase case sensitive text string that can be up to 32 characters long, including alphabets or numbers. With these rules, SSID can be anything.

Router manufacturers consider a default SSID for a Wi-Fi unit, such as Linksys, NETGEAR or default. However, since the SSID can be changed, not all wireless networks have the same names.

3.10.2. SSID Usage

Wireless devices like smartphones and laptops scan nearby areas for networks that broadcast their SSIDs and display a list of names. The user can start connecting to that network by selecting a name from this list.

In addition to obtaining a network name, Wi-Fi scanning determines whether each network has active security options. In most cases, the device identifies a secure network with a lock icon next to the SSID.

Most wireless devices record different networks to which the user has joined, along with their connection settings. In particular, the user can set up a device to automatically connect to the network by storing the settings of certain SSIDs in their profile.

3.11. Multiple SSIDs By Multiple APs

When a wireless network is created, the problem is that wireless devices can be assigned to a WLAN. This is done using the Service Set Identifier (SSID).

As mentioned, the SSID can contain a maximum of 32 characters. The SSID is used to specify which device to connect wireless devices too. In general, SSID is a feature that is defined in devices that play the role of access points so that other devices can see it and connect to the device.

Now, if a network has too many clients of its wireless networks, which they use one or multiple SSIDs to connect, Network Services Sharing must be changed and infrastructure

devices must be provided as well with different settings. In the following, the types of connections of access points and their settings are discussed.

There is another form in installing WLAN networks to provide a wireless network for heavy usage of multi-client in free places or huge buildings. Although the Ad-hoc layout is suitable for small wireless networks, larger wireless networks require a device to control communication, and today as mentioned before, this role is played by a device called an access point. In this type of network, wireless clients cannot communicate directly with each other, and this is done through access points. For this purpose, each device must receive an access point from the access point. The range covered by this type of network is known as the Basic Service Set (BSS).

The space that an access point can cover is limited. To expand this space, several BSSs must be used, this is called the Extended Service Set (ESS). The ESS wireless network uses multiple access points and covers a wider range. It should be noted that each access point here is a BSS. (9)

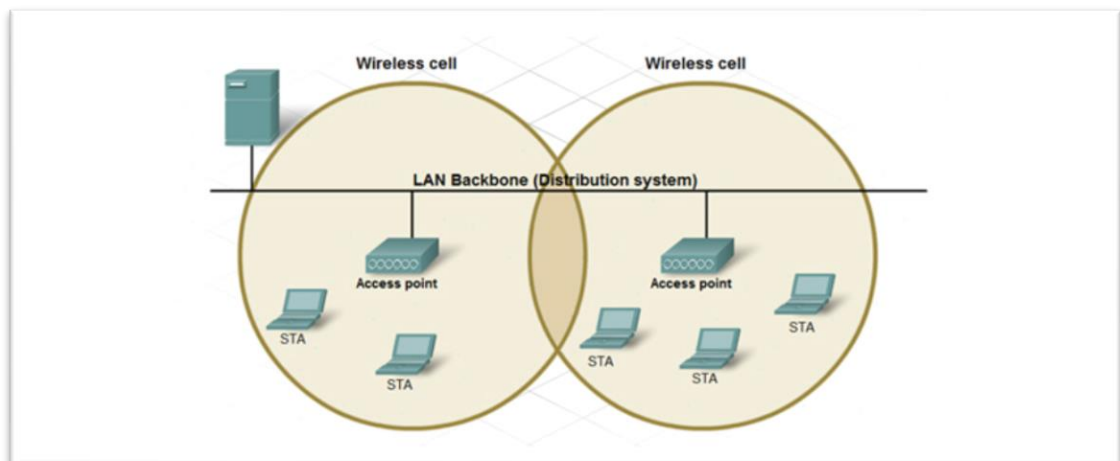


Figure 7 - ESS Access Points & BSS Cells (9)

A wireless network can also be set up using Access Point. In this type of network, the access point acts as a hub and creates a wireless connection for the computers defined in its system. Access points can connect a wireless LAN to a cable LAN; in this case, wireless computers can access cable network resources such as server files or Internet connections. Software Access Points (SAP): Ability to connect to a cable network They run on devices

that work with a wireless network card. Hardware Access Points (HAP): Supports most wireless capabilities. With network software support, users can easily share each other's wireless LANs and cable LANs. (10)

Another type of connection consists of wireless systems that are connected wirelessly by multiple access points. If a large environment is not covered by an access point, the solution that will be considered for it is to use multiple access points. When using multiple access points, each of them must overlap with the surrounding access points to some extent. Have. This allows users to move access points seamlessly and seamlessly within the overlap and antenna coverage area. This feature is known as "Roaming". (10)

3.12. RADIUS Server

The RADIUS is the abbreviation of the "Remote Authentication Dial-In User Service" and supported by IEEE 802.1x. is a protocol for centralizing the three tasks of Authentication, Authorization, Accounting. (11)

3.12.1. AAA

In computer security systems, AAA stands for "Authentication, Authorization, and Accounting" which is used on networks.

- **Authentication**

AAA means, during the process and operations, the identification of the client will be checked as verified or denied. for example, when a client wants to connect to a server, the person's ID (for example, username and password) will be sent to the server where the server matches this information with the available information and will enter the next step if this information is correct.

- **Authentication**

This part of these three steps looks at user permissions and login credentials. This part and the above (authentication) usually are not in a very different format

and most likely would be used together. Determines the access and amount of user access and determines to what extent the user has the right to use resources. This may include items such as the ability to use one person at a time, or the ability to enter the user with IP numbers or properties, or at specified times, etc.

- **Accounting**

At this point, the accounting program will tell the user about the number of resources used or the purchase of proprietary rights.

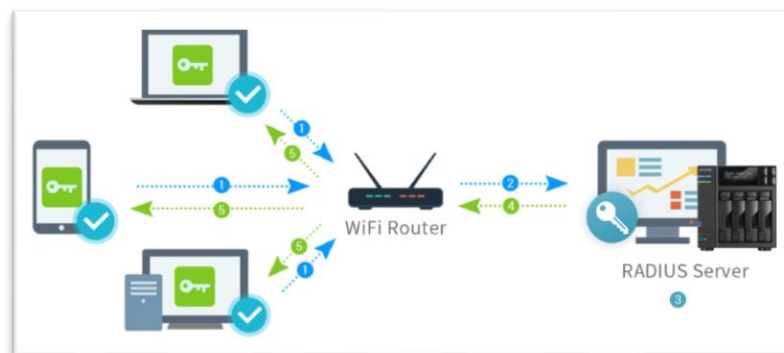


Figure 8 - RADIUS Server (11)

AAA protocol includes Radius, Diameters, Tacacs, Tacacs + and other protocols that use: PPP, EAP, HIP, PEAP, LEAP, LDAP.

On the below figure, as it showed, Clients will ask the server (RADIUS) for data via a Wi-Fi Router. The Radius server will check the client's accessibility by the AAA protocol and then send back the needed data to the client.

Radius is a client/server protocol that transmits information using the UDP protocol and it is one of the most widely AAA protocols used supported by a wide range of devices. This protocol is currently used in a wide variety of cases, for example in accessibility management of the Internet, wireless networks and in all cases accessing and using DSL, Access point, VPN, web servers, etc can be used.

This protocol is implemented by many methods around the world, one of the most popular being the Microsoft Radius Server, which has been running Radius Server on Windows servers for the last 7 years. In Microsoft Windows Servers, there is a role as

Network Policy Services or NPS, which allows you to configure Radius settings. This service can also be implemented in Macrotics.

3.12.2. Network Policy Server (NPS)

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication and authorization.

It is possible also to configure NPS as a Remote Authentication Dial-In User Service (RADIUS) proxy to forward connection requests to a remote NPS or other RADIUS servers so that you can load balance connection requests and forward them to the correct domain for authentication and authorization. (12)

NPS allows you to centrally configure and manage network access authentication, authorization, and accounting with the following features:

3.12.3. NPS As A RADIUS Server

NPS performs centralized authentication, authorization, and accounting for wireless, authenticating switch, remote access dial-up and virtual private network (VPN) connections. When you use NPS as a RADIUS server, you configure network access servers, such as wireless access points and VPN servers, as RADIUS clients in NPS. You also configure network policies that NPS uses to authorize connection requests, and you can configure RADIUS accounting so that NPS logs accounting information to log files on the local hard disk or in a Microsoft SQL Server database.

3.12.4. RADIUS Proxy

When you use NPS as a RADIUS proxy, you configure connection request policies that tell the NPS which connection requests to forward to other RADIUS servers and to which RADIUS servers you want to forward connection requests. You can also configure NPS to forward accounting data to be logged by one or more computers in a remote RADIUS server group. To configure NPS as a RADIUS proxy server.

3.12.5. RADIUS Accounting

You can configure NPS to log events to a local log file or a local or remote instance of Microsoft SQL Server.

A typical Windows Server NPS-based configuration is shown below:

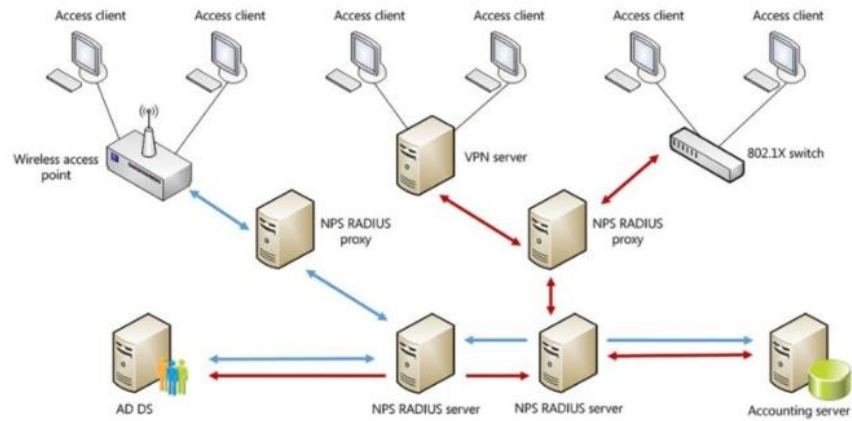


Figure 9 - Typical Windows Server NPS (13)

4. Practical Part

4.1. Sportisimo Wireless Network Overview

Sportisimo's wireless network is provided by different types of connectivity by more than 5000 devices by 818 access points and 4 controllers.

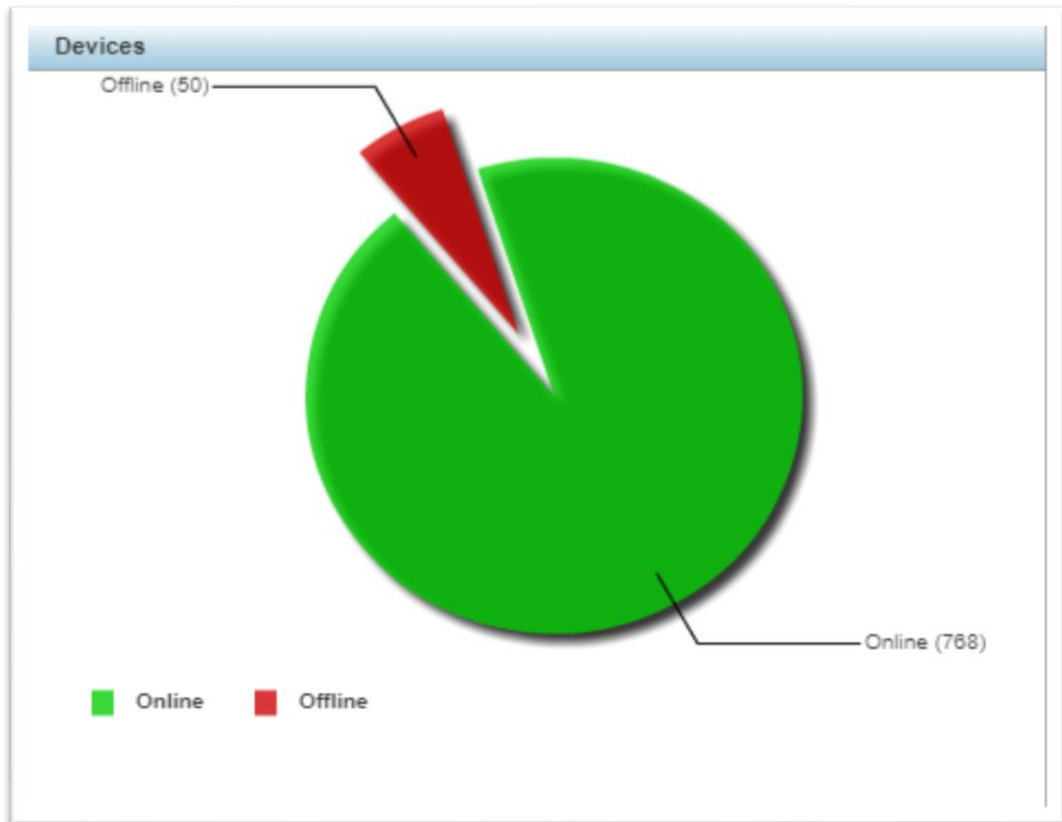


Figure 10 - Pie Chart of Devices Activity Situation

These 818 access points have been distributed throughout the warehouses, stores, and offices. There are 11 Wi-Fi SSIDs, which are:

- ❖ Simo-Frima & Simo-Frima-5G for
- ❖ Simo-Prodejna & Simo-Prodejna-5G for Stores
- ❖ Simo-Host
- ❖ Simo-Kiosk
- ❖ Simo-Private
- ❖ Simo-Sklad-A & Simo-Sklad-B & Simo-Sklad-C for warehouses
- ❖ Simo-IT for setting up the new devices









Device Types			
Device Type		Online	Offline
 AP6521		148	5
 AP7522		6	0
 AP7532		506	25
 AP7622		3	1
 AP7632		101	18
 NX5500		2	1
 RFS6000		1	0
 VX9000		1	0

Figure 11 - Wireless Network Device Types

4.2. Problem Statement

One of the biggest issues in Sportisimo is the problem of the non-integrated network. Because it has expanded in different time-periods and they only were able to add new settings in several years with opening new stores in a different country and just apply the same previous setting to keep the network useable. It created an issue for the IT department to use the highest possible performance of devices and networks.

On the other hand, management of the network with controllers also has been affected, because of non-sorted sites based in various cities and countries. Also, The relation between the different Access Points was not set up correctly. Their relation with the controller is just in a single mode. Because of this when the network administrator wants to change or apply any setting it takes a long time for this command to be received by the access points.

The other issues which Sportisimo wants to solve are unstable connectivity with some devices at warehouses or stores and some in offices that use 5GHz channel. Behind this, the current security level of Wi-Fi networks is WPA, which is not suitable in this volume and needs to be improved.

The whole of the Sportisimo network and especially the wireless devices are affected by all of these issues which forced the Sportisimo management to request the network team for a revision on the selected targets. The project targets which the thesis author needs to work on are summarized by:

- Re-sorting all sites based on locations to make the management more comfortable
- Update the firmware of the points to make better communication with controllers
- Network integration and increase the security level
- Allow the company to reduce the number of SSIDs by covering the variety of different types of user's accessibilities

4.3. Localization Re-Sorting

The site organization was mixed and in case we would find a specific site somewhere, we must spend several minutes instead of only 3 clicks to see that. The previous organization is visible on the figure below:

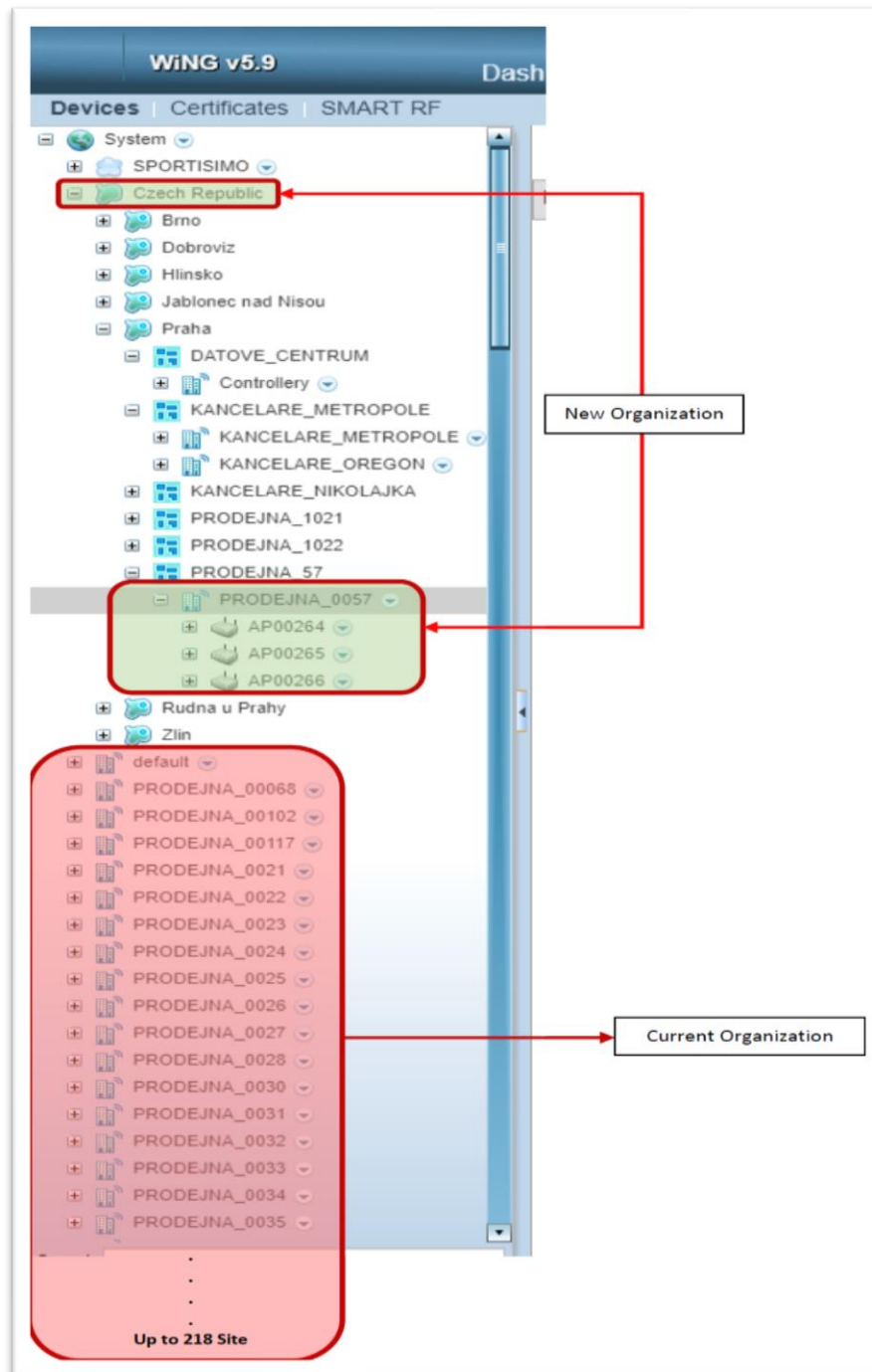


Figure 12 - Mix localization organize

As the categories of sites have been modified and by adding main groups for each country, all official buildings, warehouses, and stores located in a city or country have been added as subcategories that include all devices in that city or country. Current mode is visible in the following figure

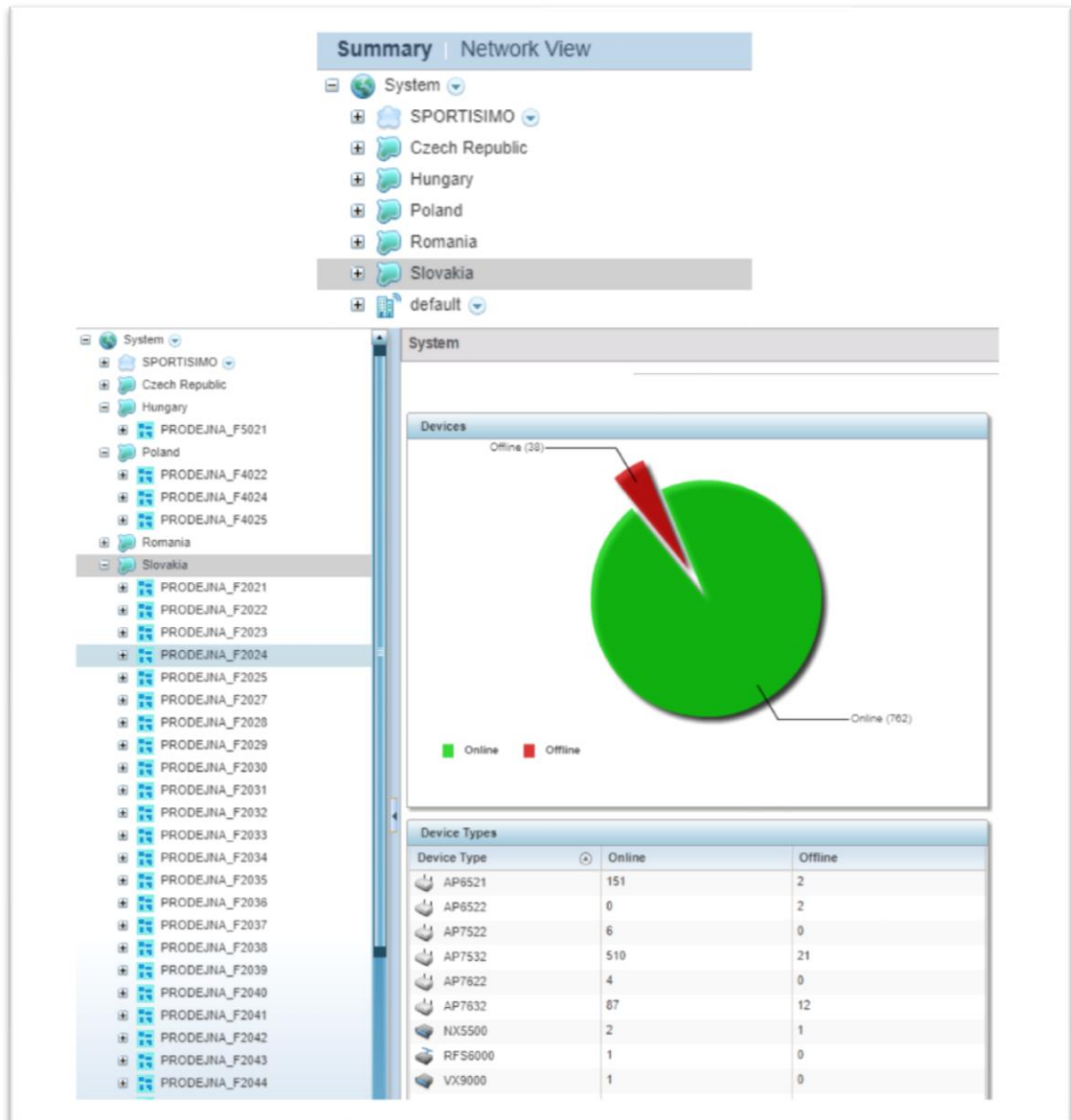


Figure 13 - New Locally Re-Sorted Network Sites of Sportisimo

4.4. Access Points Firmware Update

In the new version of access points firmware, the controller sets an access point as a supervisor for other ones in a single site. It helps the network controller communicate with only one access point for each site at the same time. Despite setting the supervisor AP, the unavailability probability has been assumed which works when the supervisor AP has stopped working for any reason, the next AP will take the supervisor's responsibility to receive any setting from the main network controller.

We have ordered the firmware update to update one by one by the Wing application to avoid any disconnections inside of the sites. Firstly, the new firmware is uploaded to a server with a specific IP address and then set the Wing application by the server and firmware details to download and install the firmware on each AP individually. With a low volume of images, we can upload directly to the Wing application but in this case, we chose FTP (File Transport Protocol) which is doable for images more than 25MB.

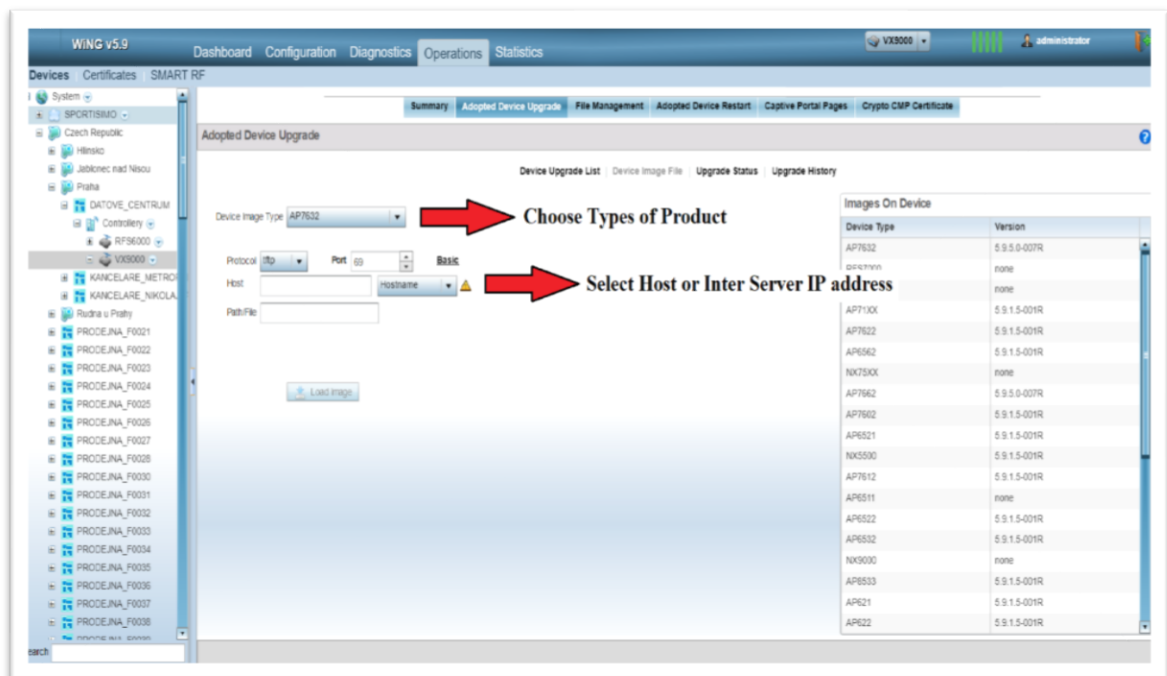


Figure 14 - Access Points Firmware Update

4.5. Implementation of a RADIUS Server

To solve the security issue and also reduce the number of SSIDs, the network team decided to implement the Radius Server to have only one single SSID for all clients and devices. For those clients who have Sportismo email and password, it only needs to connect Sportismo Active Directory (which included the database of all Sportismo groups and clients sorted by their department and permission) to the Radius Server. By this action, the network makes an opportunity to let users log into the Sportismo network only if they have the right permission. In this way, we need essential certificates to provide the Radius server for authorization and authentication.

After the basic setup of Microsoft Windows Server 2016, we needed to run Network Policy Server service in the windows server.

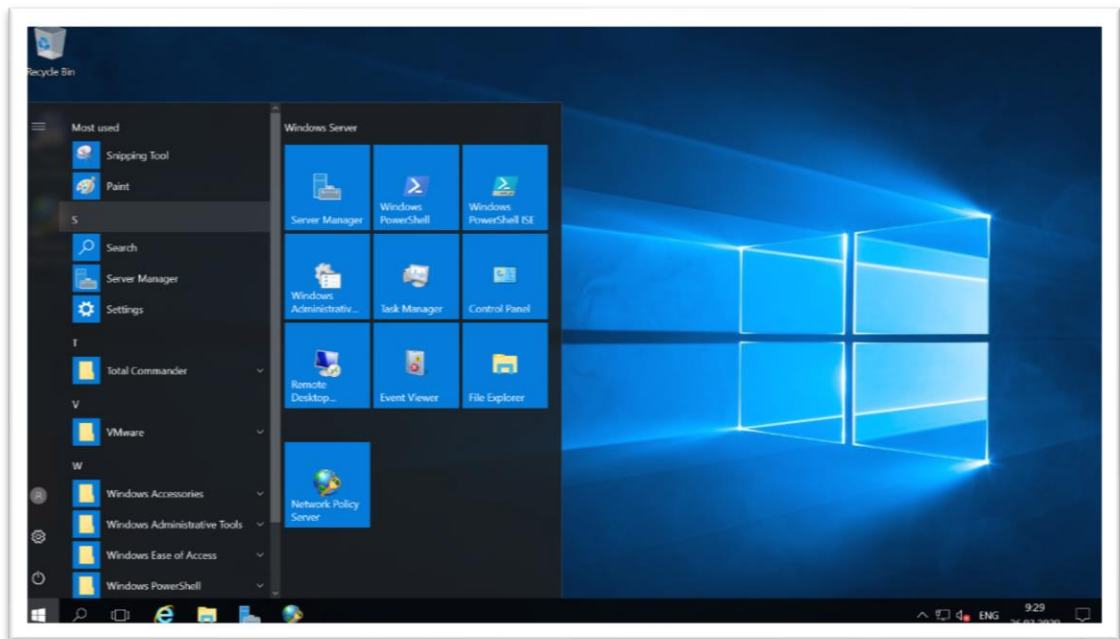


Figure 15 - Microsoft Windows Server 2016

Network Policy & Access Services must be added as a role in Server Manager. Then NPS is required to be selected in role services as well as Remote access, Services, Routing.

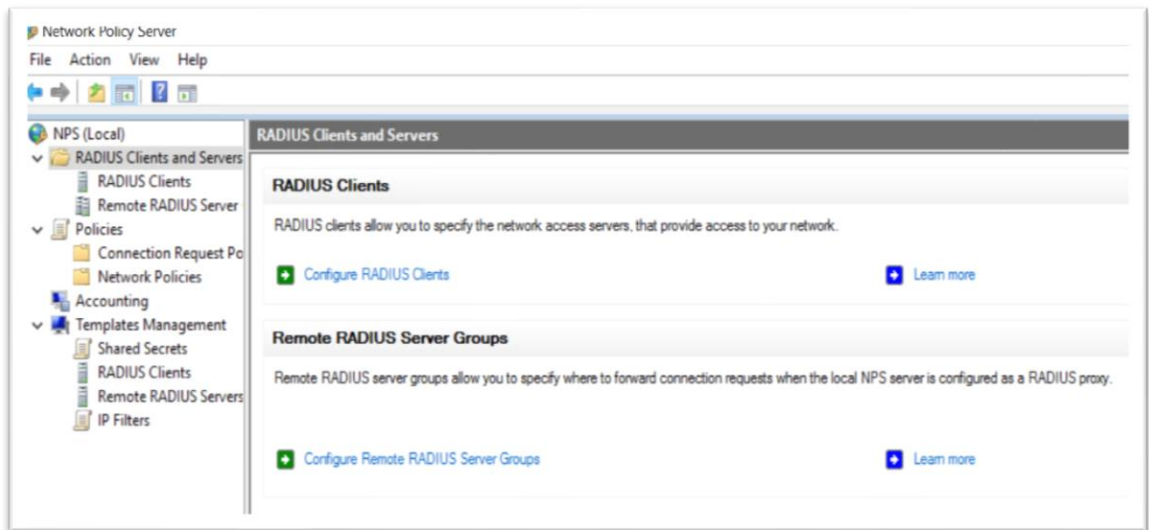


Figure 16 - Radius Configuration in NPS Setup

In the following steps, the access point details and a password and also authentication method must be specified. In this way, firstly, for testing purposes, we only added an access point for an office and then after evaluating and solving the bugs, if everything works correctly, we will expand it to the other access points.

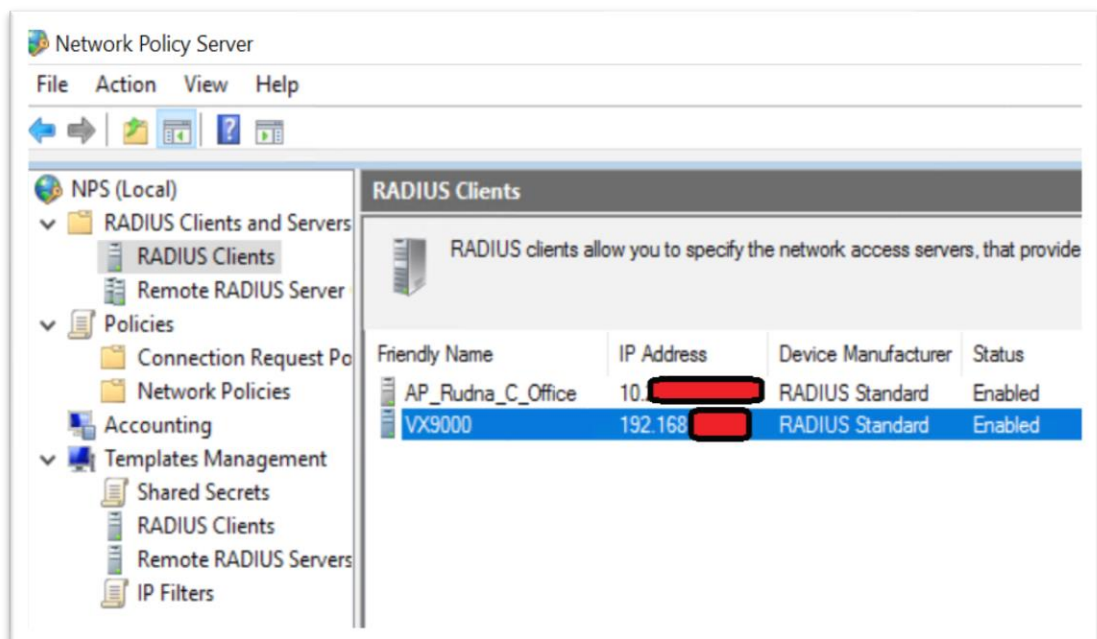


Figure 17 – Connection of Access Points to Radius Client

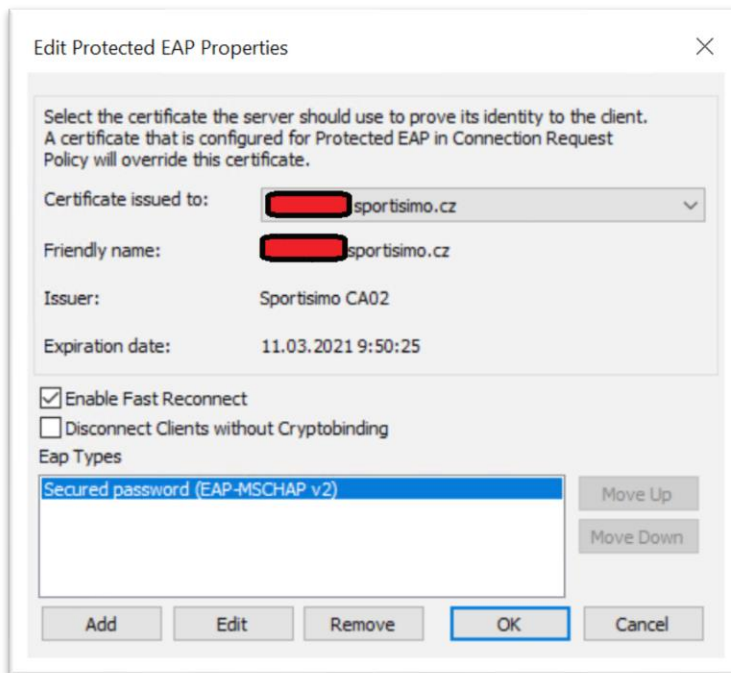


Figure 18 - Network Policies PEAP Certificate

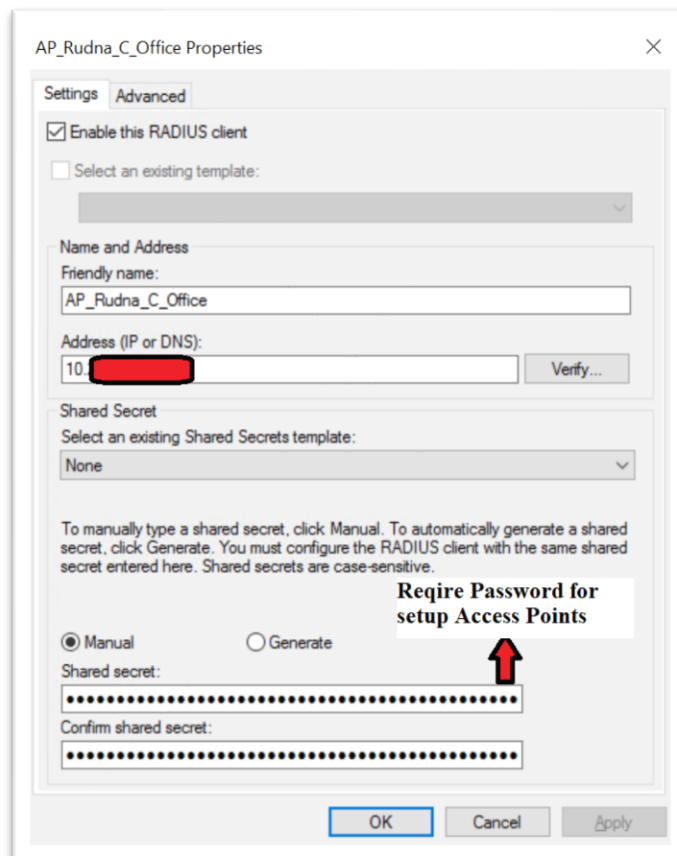


Figure 19 - Access Point Setting in Radius Server-Side

Now, the server and access point steps are configured and clients need to install a certificate created by the CA to access the wireless network. This allows clients to authenticate to the server before authentication. If you are on the domain and have Active Directory, you need to apply the certificate created by Group Policy to all clients. Otherwise, it must be installed manually on the clients.

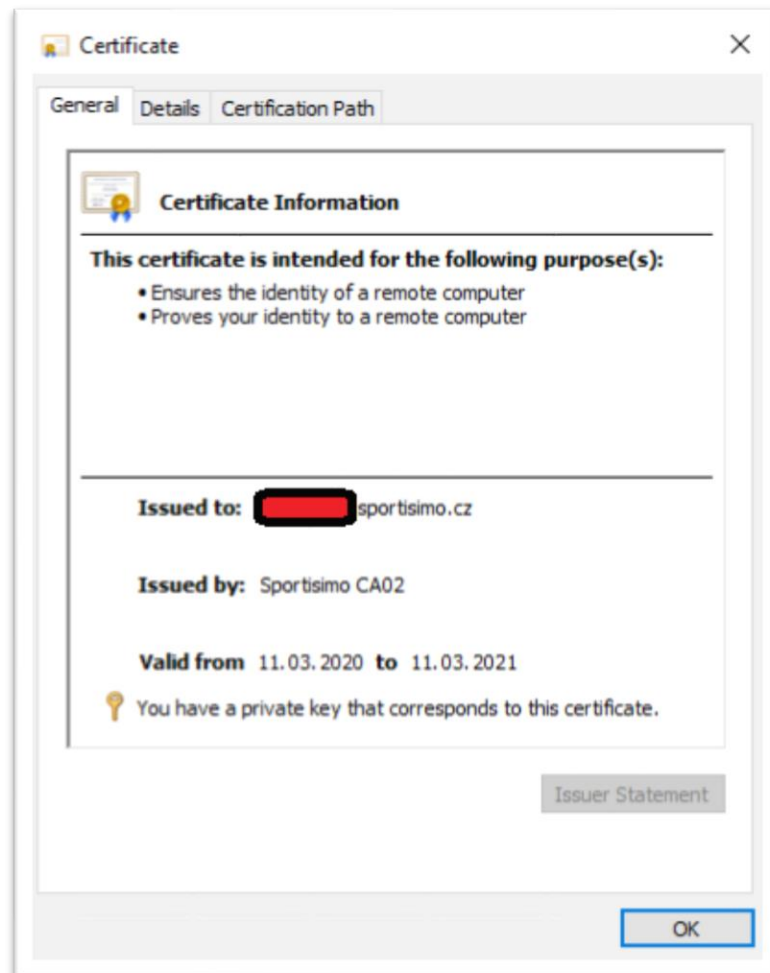


Figure 20 - Sportisimo Certificate

In the next step, NPS must be registered in the Sportisimo Active Directory which includes all details of Sportisimo users, groups, departments, etc. Obviously, in this thesis, the author is not allowed to show any secret details. For this reason, only the title of Active Directory is visible in the figures below.

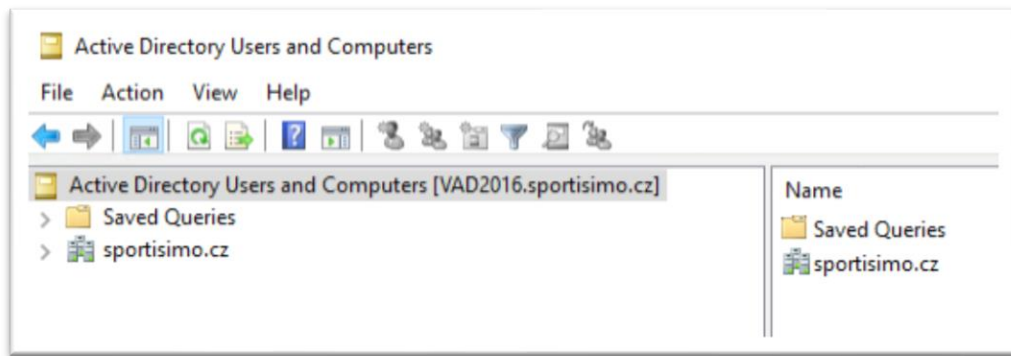


Figure 21 - Sportisimo Active Directory

Now, it is time to configure the client network settings. Like certificate installation, these settings can be applied through a group policy or installed manually.

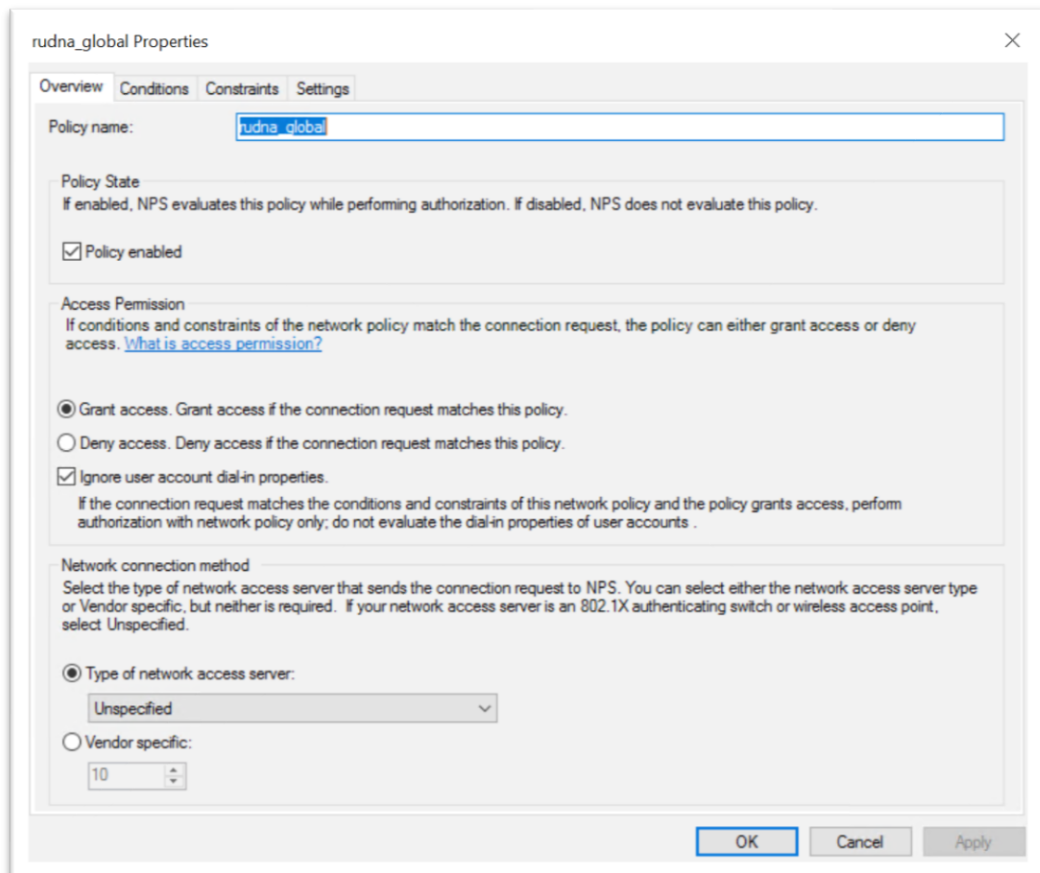


Figure 22 - Network Policies Overview

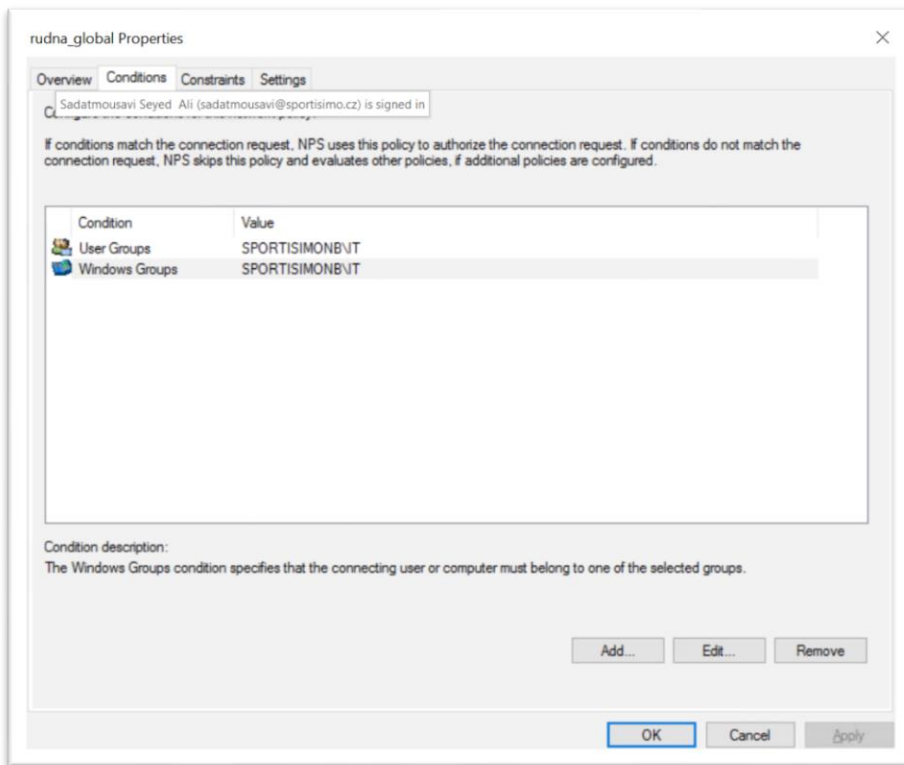


Figure 23 - Network Policies Conditions

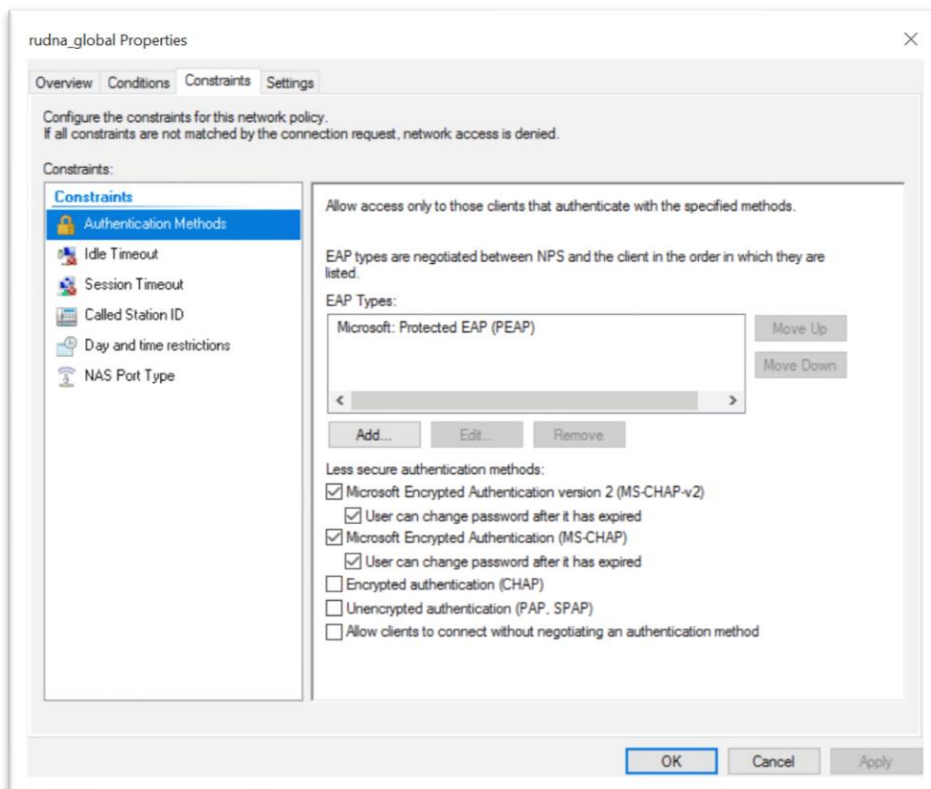


Figure 24 - Network Policies PEAP

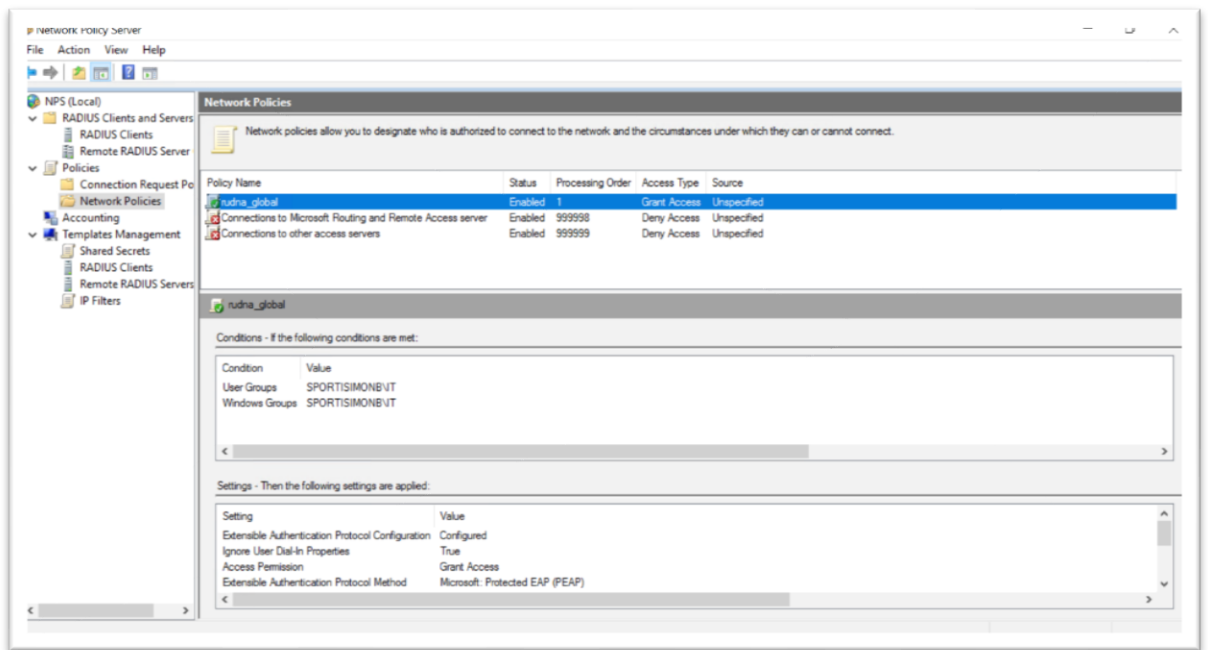


Figure 25 - Network Policies Overview

4.6. Create a New Single WLAN SSID for Radius Server

Now, to complete and activate the NPS (RADIUS Server), it requires applying the settings on the Wing application. After inserting the NPS details, we made a single SSID to test the settings and configuration which is set on the NPS.

As it's visible on the below figure, on the left side, in the devices section, we have the Hala C office where we put the access point during the testing period.

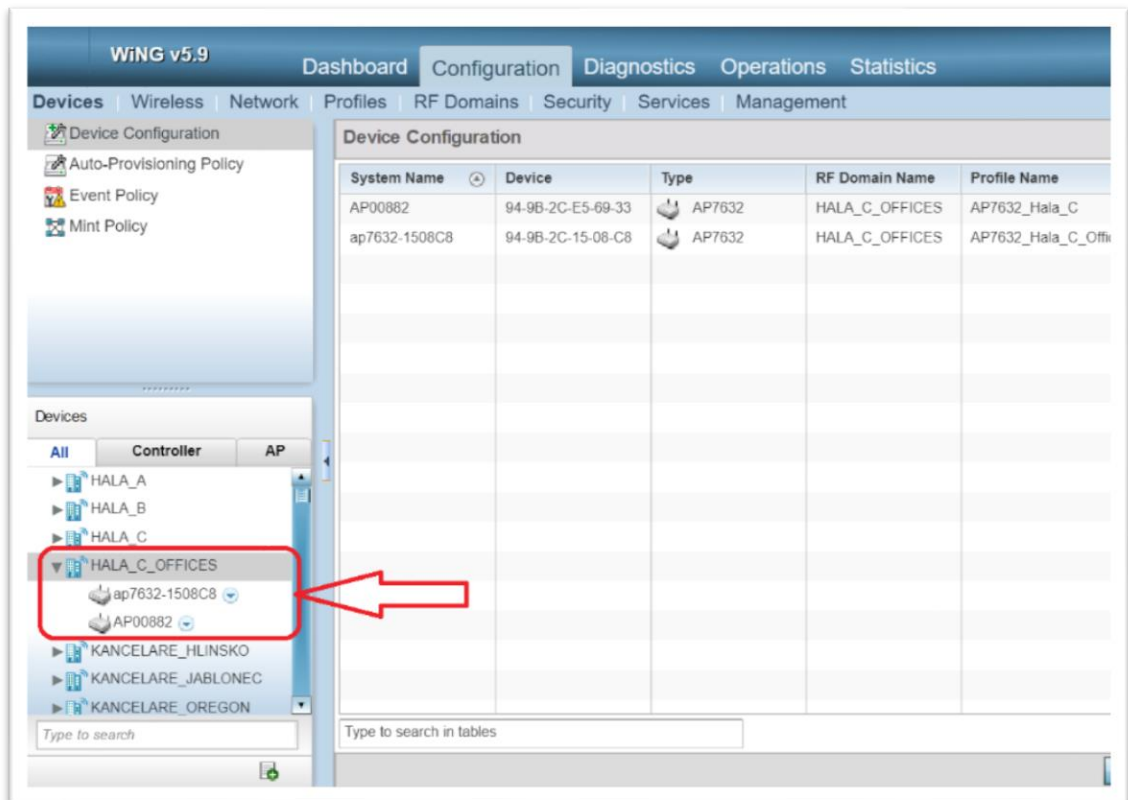


Figure 26 - Devices of Hala C Office

We needed to create a new WLAN and by our detail from NPS, connect it to the Radius server.

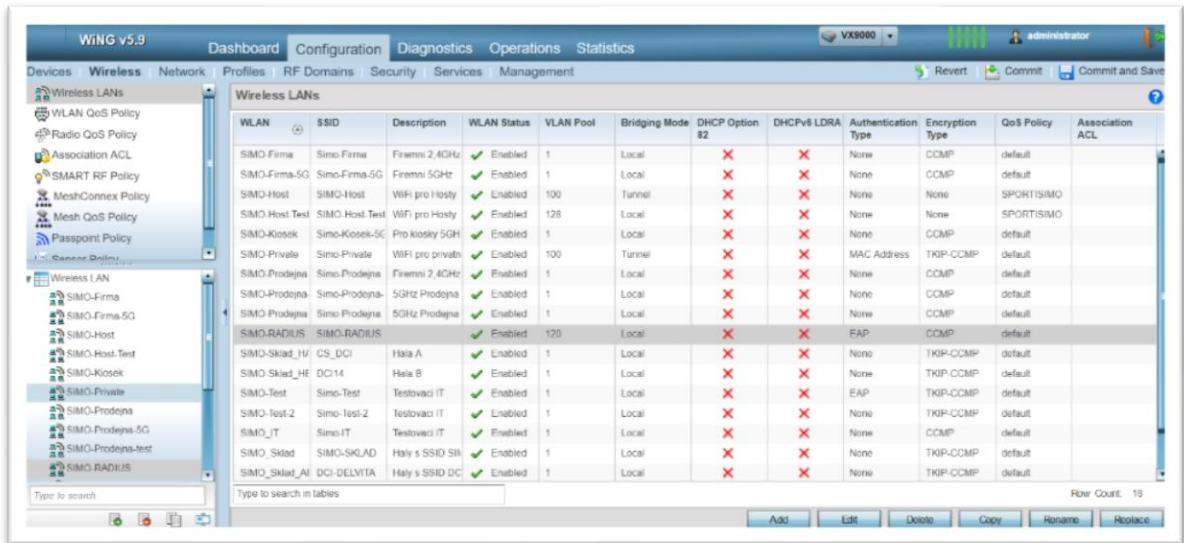


Figure 27 - WLAN Management Page in Wing App

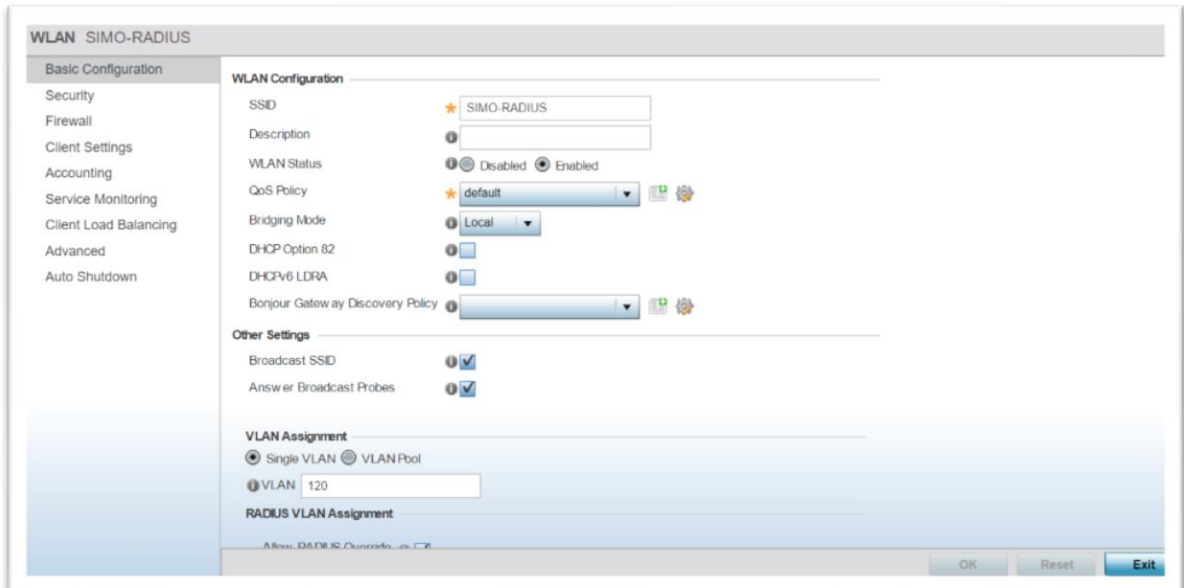


Figure 28 - Setup New WLAN in Wing App

In the Security section, we must choose the EAP protocol as we set in the Radius Server and then select the NPS server for AAA policy.

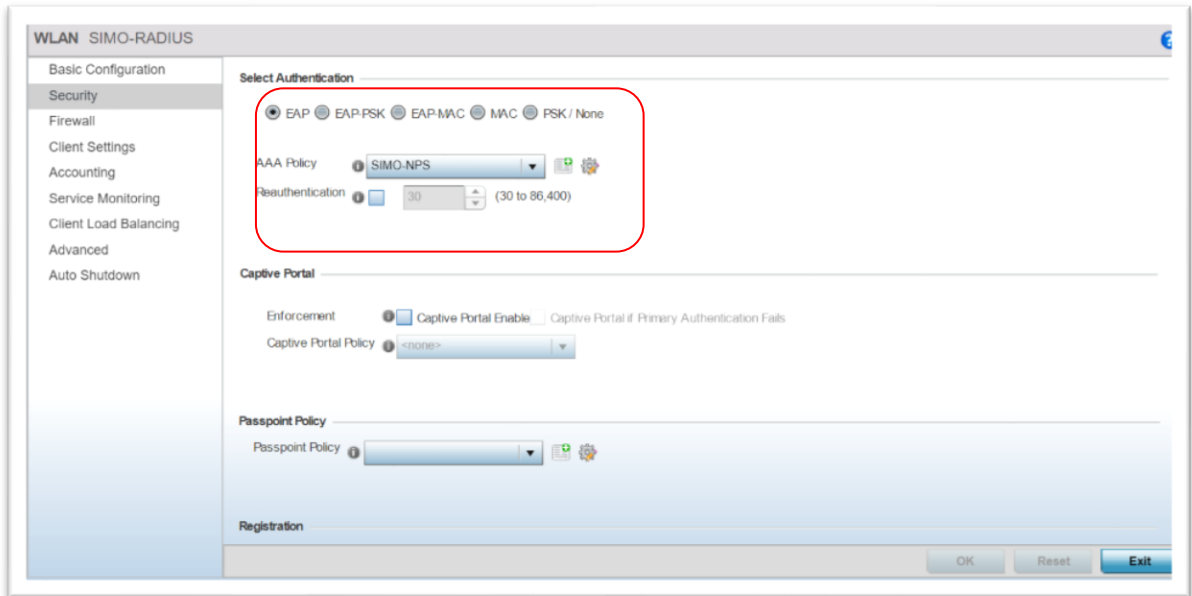


Figure 29 - Security Adjustment of New WLAN in Wing App

Now, by clicking on the setting icon on the right of the AAA policy part, adjustment of server information in the Wing application will be open. After selecting the edit button, a page will appear to insert server details, IP address, and password.

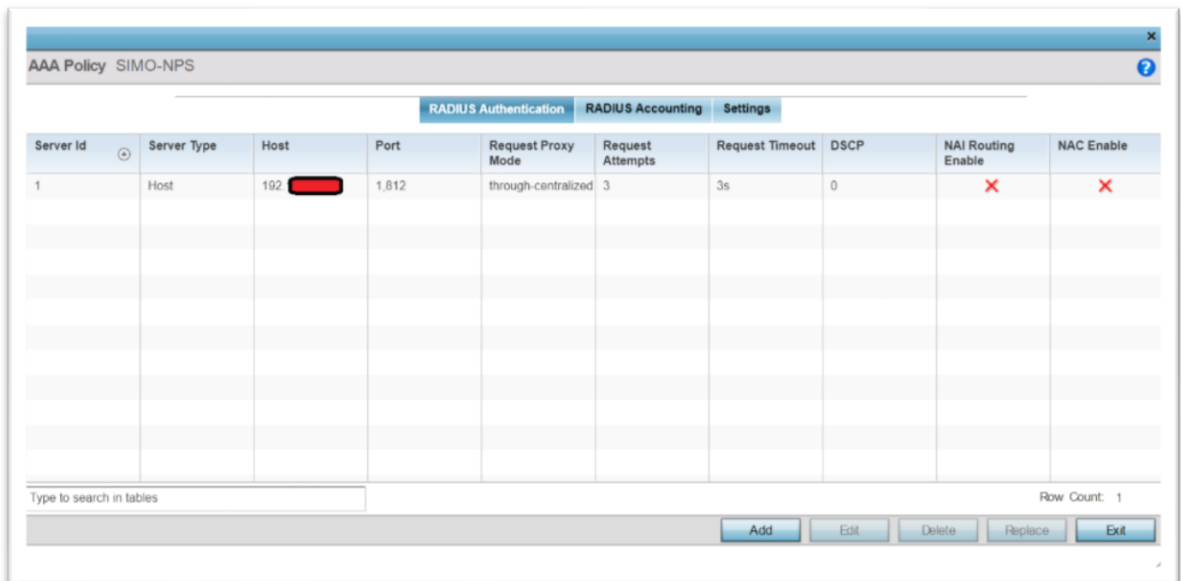


Figure 30 - AAA Policy setting and Joined of the NPS

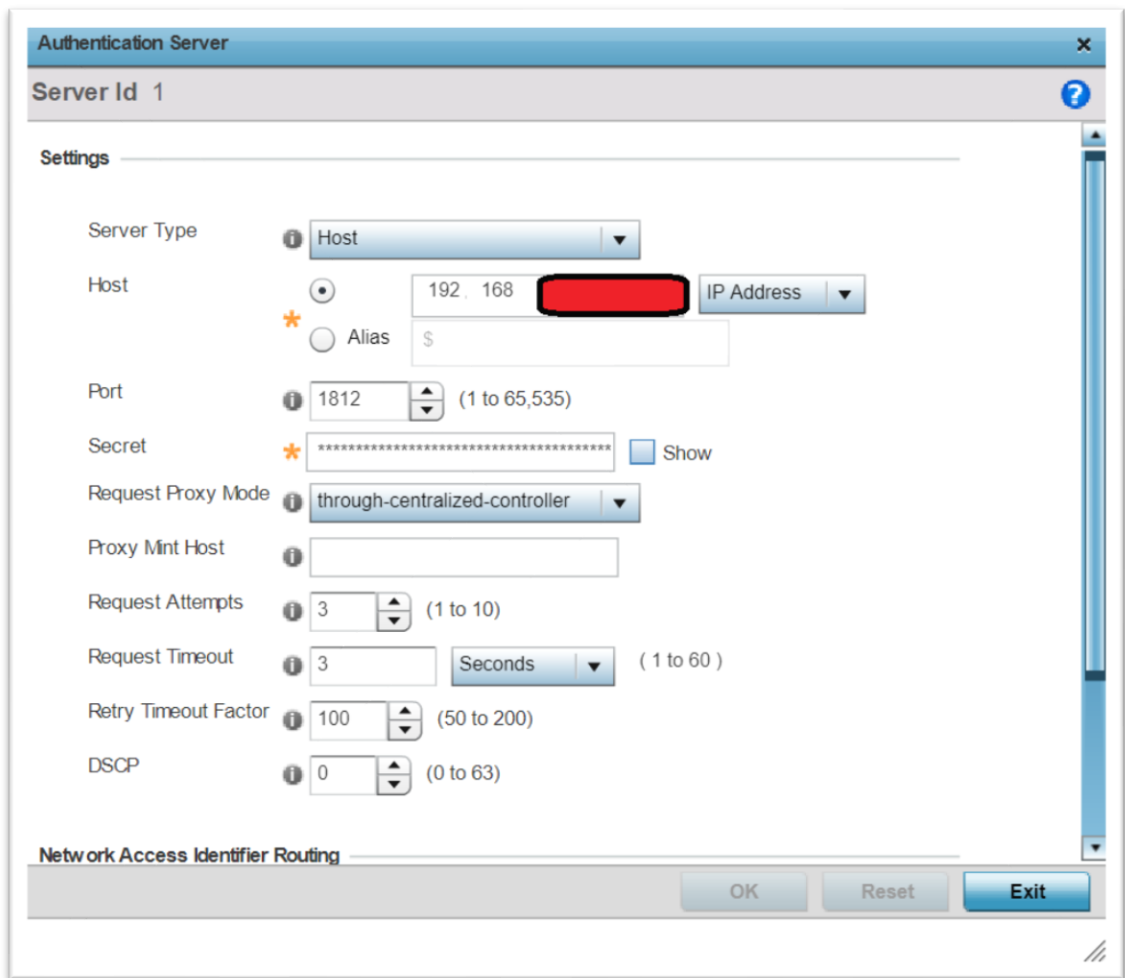


Figure 31 - Authentication Server Registration in Wing App

5. Results and Discussion

As the targets that the company had to solve them before, which were:

- Re-sorting all sites based on locations to make the management more comfortable
- Update the firmware of the points to make better communication with controllers
- Network integration and increase the security level
- Allow the company to reduce the number of SSIDs by covering the variety of different types of user's accessibilities

By the implementation of this process, if there would not be any problem during the testing period time, we will achieve 100% of our goals. As a result, by the changes what we performed, we are experiencing:

- ✓ More comfortable accessibility to the sites by the new organization
- ✓ Better faster Communication between access point and controllers
- ✓ Radius Server has been implemented and providing us a higher level of security for windows group employees or allows access to the devices by known Mac address
- ✓ Instead of the 11 WLAN SSIDs, the company used for a variety of devices, now only one single SSID remains that is more powerful and provides the network with a better speed and range coverage

6. Conclusion

So far, we have added a new single WLAN SSID which is supported by the NPS server. For a few months, Sportisimo Network Team has planned to add some departments with their staff's step by step and one by one to test and check the network.

The next step the network team would like to do to finish this project is to create another policy based on MAC address for only the devices which are not working with any company email and use this as a way to login to the network it for log-in to the network. As mentioned, Sportisimo has more than 5000 devices and during purchasing, they recorded MAC addresses except for 1300 PDAs. On the other hand, during the last 10 months, the company uses device management that provides the MAC address of the whole of PDAs in a list. So the last step should be only to connect the remaining devices to the single new WLAN SSID to be integrated the Sportisimo network. After a while and when we finished the testing period of the client's accessibility to the network, the main single SSID for the whole of our devices and clients will be added.

To conclude the project, Sportisimo has been decided to change the whole of previous network topologies for the above-mentioned reasons and those were that worth to spend lots of time and also money to have better performance, higher speed, higher security and set a main understandable and logical structure for the whole of the company network.

7. Recommendation

Sportisimo still has another problem with the Guest's Network. Of course, our helpdesk employees do not like to ask their second level colleagues every time to add the Identification factor of a guest to the radius server whenever a new guest comes to Sportisimo. There are several numbers of meetings with external guests per week and this would increase the workload of the ServiceDesk to much. So my high recommendation for second and probably last phase of the Sportisimo WI-Fi projects is to prepare a Guest WLAN SSID by a quick registration with phone number and email address of the guest when he\she visit open page "Sportisimo Guest Internet Connection" on their smartphone and then receive a username and password to login for a "limited time and consumption of internet connection".

Seyed Ali SadatMousavi

March 2020

Prague

8. References

1. [Online] <https://slideplayer.com/>.
2. BRISBIN, Shelly. *Build your own Wi-Fi network*. Prague : Neocortex, 2003.
3. Gintzler. *How Wi-Fi Works*. s.l. : A. S. Cavendish Square, 2018.
4. Kapp, Steve. *802.11a: More Bandwidth without the Wire*. 2002.
5. *shahrsakhtafzar*. [Online] www.shahrsakhtafzar.com.
6. BARKEN, Lee. *How to secure your wireless network*. Brno : Computer Press, 2004.
7. [Online] <http://wirelessman.ir/>.
8. IEEE 802.1X. *Geekboy*. [Online] <https://www.geekboy.pro/>.
9. SSID Definition in Wireless Networks. *networkuser*. [Online] <http://www.networkuser.ir/>.
10. Tetz, Edward. *Cisco Networking All-in-One For Dummies*.
11. Radius Server. *hushplus*. [Online] <https://hushplus.ir>.
12. Microsoft. Network Policy Server. [Online] docs.microsoft.com.
13. Plan NPS as a RADIUS server. *Microsoft Doc*. [Online] <https://docs.microsoft.com/>.