

UNIVERZA V LJUBLJANI
FAKULTETA ZA ELEKTROTEHNIKO

Bojan Pekevski

Nadzor in upravljanje omrežij Wi-Fi

MAGISTRSKO DELO

MENTOR: prof. dr. Andrej Kos

Ljubljana, 2016

UNIVERSITY OF LJUBLJANA
FACULTY OF ELECTRICAL ENGINEERING

Bojan Pekevski

**Control and management of Wi-Fi
networks**

MASTERS THESIS

MENTOR: prof. dr. Andrej Kos

Ljubljana, 2016

COPYRIGHT. The results of this Masters Thesis are the intellectual property of the author and the Faculty of Electrical Engineering, University of Ljubljana. For the publication or exploitation of the Masters Thesis results, a written consent of the author, the Faculty of Electrical Engineering, and the supervisor is necessary.

©2016 BOJAN PEKEVSKI

DECLARATION OF MASTERS THESIS AUTHORSHIP

I, the undersigned Bojan Pekevski am the author of the Master Thesis entitled:

Control and management of Wi-Fi networks

With my signature, I declare that:

- the submitted Thesis is my own unaided work under the supervision of prof. dr. Andrej Kos
- all electronic forms of the Masters Thesis, title (Slovenian, English), abstract (Slovenian, English) and keywords (Slovenian, English) are identical to the printed form of the Masters Thesis,
- I agree with the university right of saving and reproduction of the copyrighted work in electronic form and the right of enabling public access and download of the copyrighted work online via the "Repository of University of Ljubljana".

In Ljubljana, January 2016

Author's signature:

ACKNOWLEDGMENTS

I would like to thank my mentor prof. dr. Andrej Kos and the researchers at Laboratory for Telecommunications at the Faculty of Electrical Engineering, University of Ljubljana, for their guidance and helpful suggestions throughout the process of writing this thesis. I would also like to thank my parents, my sister, my girlfriend and my close friends, for their unconditional love and support.

Bojan Pekevski, 2016

Contents

Povzetek	i
Abstract	iii
1 Introduction	1
2 IEEE 802.11 WLAN networks	3
2.1 Introduction to wireless technologies	3
2.2 Wireless LAN overview	4
2.3 Wireless LAN standards	5
2.4 WLAN components and topologies	6
2.5 Management operations	10
3 Planning and designing a WLAN network	15
3.1 Access networks architectures	18
3.1.1 Autonomous access point architecture	18
3.1.2 Controller-based access point architecture	20
3.1.3 Ad hoc architecture	21
3.1.4 Mesh network architecture	21
4 Controller-based wireless architecture and introduction to Wireless LAN Controller	23
4.1 Different solutions for WLAN management	26
4.2 Controller-Based WLAN Functional and Elemental Architecture	27
4.3 Architecture solutions	30

CONTENTS

4.3.1	Controller-based Management Only	30
4.3.2	Controller-based with Traffic Tunneling	31
4.3.3	Controller-based with Split Traffic	32
5	Commercial and open-source platforms for control and management of wireless network	35
5.1	Cisco	35
5.2	Ubiquity Networks	38
5.2.1	Demo test of the UniFi Controller	39
5.3	Meraki	42
5.3.1	Demo test of the Cisco Meraki cloud management platform	43
5.4	OpenWISP	47
5.4.1	OpenWISP sample architectures	48
5.4.2	OpenWISP Manager and OpenWISP Firmware	49
5.4.3	Installation of OpenWISP Manager and its prerequisites	50
5.4.4	Compiling and installing OpenWISP Firmware	55
	The overlay configuration file and its structure	57
	Hands-on experience with the OWF instalation	59
5.4.5	Demo test of OpenWISP manager	60
6	Conclusion	63

List of Figures

2.1	Wireless network categories [1]	4
2.2	802.11 data link and physical layers [4]	5
2.3	Components of 802.11 networks [4]	7
2.4	Independent BSS, [4]	8
2.5	Infrastructure BSS [4]	8
2.6	Access point, IP router and DSL modem in a single device [7]	9
2.7	Extended service set [4]	10
2.8	Graphical representation of 2.4 GHz band channels overlapping [5]	11
2.9	Authentication and association of a client device with an access point [7]	12
3.1	Autonomous access points offer distributed management and control [9]	19
3.2	Simple small office/home network [9]	19
3.3	Controller-based access points provide centralized management and control [9]	20
3.4	Ad hoc network architecture [9]	21
3.5	Mesh network architecture [9]	22
4.1	Functional elements in a WLAN [11]	24
4.2	Elements for controller-based WLAN [11]	27
4.3	Functional implementation for an autonomous WLAN and in a controller-based CUWN [11]	28

LIST OF FIGURES

4.4	CAPWAP architecture [11]	28
4.5	Management architecture for multiple WCS deployments with WCS navigator [11]	30
4.6	Controller-based management only system [13]	31
4.7	Controller-based system with traffic tunneling [13]	32
4.8	Controller-based system with split traffic [13]	33
5.1	Typical AP receiver and Unifi AP with multi-lane RF [17] . .	39
5.2	UniFi controller dashboard [18]	40
5.3	UniFi site map [19]	40
5.4	UniFi APs and users lists [19]	41
5.5	UniFi statistics preview [19]	41
5.6	Meraki's out of band management architecture [20]	43
5.7	Meraki cloud management platform, multi-site deployment map representation of the available demo networks	44
5.8	Meraki cloud management platform, network management screen	44
5.9	Meraki cloud management platform, network-wide tab and it's options	45
5.10	Meraki cloud management platform, list of user clients	45
5.11	Meraki cloud management platform, summary reports	46
5.12	Meraki cloud management platform, "wireless" tab	46
5.13	Meraki cloud management platform, "organization" tab	46
5.14	Typical OpenWISP installation: behind a firewall with NAT [23]	49
5.15	WPA/WPA2 Enterprise (802.1x) [23]	50
5.16	The edited file database.yml	51
5.17	gmaps_api_key.yml	53
5.18	OWM log in page	55
5.19	OWM home screen	60
5.20	OWM, APs list and management	61
5.21	OWM, editing configuration of AP	61
5.22	OWM, traffic shapping options	62

LIST OF FIGURES

5.23 OWM, editing operator's rules 62

List of Tables

2.1	Different amendments of the 802.11 standard [5], [6]	6
2.2	Encryption methods in 802.11 WLANs [2]	13
5.1	Summerized information about Cisco controllers [16]	36

Acronyms

ACL Access Control List.

AES Advanced Encryption System.

AP Access Point.

BSS Basic Service Set.

CAPWAP Control and Provisioning of Wireless Access Points.

CUWN Cisco Unified Wireless Network.

DHCP Dynamic Host Configuration Protocol.

DNS Domain Name System.

EAP Extensible Authentication Protocol.

ESS Extended Service Set.

FTP File Transfer Protocol.

GRE Generic Routing Encapsulation.

HREAP Hybrid Remote Edge Access Point.

IEEE-SA Institute of Electrical and Electronics Engineers Standards Association.

IETF Internet Engineering Task Force.

LWAPP Lightweight Access Point Protocol.

MAC Media Access Control.

MSE Mobility Services Engine.

OEAP Office Extend Access Point.

OSI Open Systems Interconnection.

OWF OpenWISP Firmware.

OWM OpenWISP Manager.

Acronyms

PSK Pre-Shared Key.

QoS Quality of Service.

RADIUS Remote Authentication Dial In User Service.

RF Radio Frequency.

RFC Request for Comments.

SSID Service Set Identity.

TKIP Temporary Key Integrity Protocol.

VLAN Virtual LAN.

VPN Virtual Private Network.

WAN Wide Area Network.

WCS Wireless Control System.

WEP Wired Equivalent Privacy.

WISP Wireless Internet Service Provider.

WLAN Wireless Local Area Network.

WLC Wireless LAN Controller.

WPA Wi-Fi Protected Access.

WPA2 Wi-Fi Protected Access, version 2.

Povzetek

Iz današnje perspektive Wi-Fi dostop je zelo pomemben za vsakogar. Uporaba interneta je ogromna in velik del uporabnikov dostopa preko 802.11 WLAN (Wi-Fi) omrežjih. Taka omrežja so preprosta za namestitev in so primerna tako za domače uporabnike, kot tudi za velika podjetja. Možnost uvedbe stabilnih omrežjih v krajih, kjer je žična rešitev težja za izvajanje ali pa ni tako stroškovno učinkovita, je samo eden izmed razlogov za široko uporabo WLAN-a.

Današnja WLAN omrežja postajajo vse bolj zapletena ter njihovo upravljanje in nadzor je vse težje. Večja podjetniška omrežja so dolžna imeti centralizirano upravljanje za lažje in hitrejše opravljanje svojih nalog. Element, ki zagotavlja to vrstno funkcijo je Wireless LAN Controller (WLC), ki predstavlja namen pričujoče magistrske naloge. Wireless LAN Controller se lahko uvede v WLAN omrežjih na različne načine in v disertaciji so proučene in obravnavane možne rešitve. Podan je pregled obstoječih arhitektur, ki vsebujejo tovrsten krmilnik, podane so tudi različne rešitve in platforme, ki se uporabljajo za nadzor in upravljanje takšnih arhitektur kot tudi naše praktične izkušnje z nekaterimi od njih. Na podlagi njihovih značilnosti in lastnosti, lahko poudarimo v katerih primerih so najbolj primerni.

Lahko sklepamo, da je WLC s svojimi značilnostmi neizogiben element pri oblikovanju sodobnih WLAN omrežjih. Evolucija in razvoj programskih platform bosta povzročila bolj kakovostne rešitve brez fizičnega krmilnika in bosta postala alternativa za manjše organizacije ali podružnice, medtem ko pa za večje organizacije fizični krmilnik bo še vedno potreben element.

Ključne besede

IEEE 802.11 WLAN, Wi-Fi, Dostopna točka, Brezžični LAN krmilnik, Upravljanje WLAN omrežij, Krmilno zasnovano centralizirano upravljanje

Abstract

From today's perspective Wi-Fi access is very important for everyone. The usage of the Internet is enormous and a huge portion of the users are accessing through 802.11 Wireless Local Area Network (WLAN). These networks are easy to install and are not only suitable for home users but also for big enterprises. The possibility for deployment a stable network in places where wired solutions are difficult for implementation or not so cost-efficient, is one of the reasons for the wide usage of WLAN.

Today's WLANs are becoming more and more complex and their management and control is getting harder. Bigger enterprise networks are obligated to have centralized management in order to make that management easier and less time-consuming. The element which provides these features is the Wireless LAN Controller (WLC) and the focus of this thesis is mostly on it. The Wireless LAN Controller can be implemented in WLANs on various ways and the possible solutions are examined and discussed in this thesis. We give an overview of existing controller-based architectures, different solutions and platforms used for the control and management of such architectures and our hands-on experience with some of them. Based on their characteristics and features we can point out in which cases they are most suitable.

We can conclude that the WLC with its features is an inevitable element in the design of a modern WLAN. The evolution and development of the software platforms will cause quality solutions without physical controller to become the alternative for smaller or branch organizations, but for bigger enterprises the physical controller will still be a needed element.

Keywords

IEEE 802.11 WLAN, Wi-Fi, Access point, Wireless LAN Controller, WLAN management, Controller-based centralized management

Chapter 1

Introduction

Over the years 802.11 WLAN(or Wi-Fi as usually called) technology became widely spread and is one of the leading wireless technologies used. It is incorporated in our daily routines whether we use such networks in our working environment or in our home. Especially in complex enterprise environment the need for stability of WLANs is a crucial challenge for their administrators. The evolution of these networks and its growth brought the necessity of centralized management and monitoring. The main element responsible for that task is the Wireless LAN Controller (WLC). WLC is a part of the controller-based WLAN architecture and the point from which the centralized management is done. It can perform various tasks that guarantee the stability, security and performance of the network.

The solutions for controller-based networks implementing WLC are widely spread on the telecommunication market. Vendors of network equipment are providing solutions from classic hardware on-site solutions to completely cloud-based solutions. Depending on the needs or the size of the planned network every user can choose its suitable configuration. For bigger enterprises the classic hardware solution doesn't take a big part of the overall cost of their network, but for smaller or midsize organizations that could be expensive and the cloud solution could be a better choice.

The quality and robustness of the classic hardware are guaranteeing high

performance and because of that this solution will still hold the market of large enterprises. For smaller or branch enterprises there are software solutions that can be alternative for the physical controller, which over the years became more reliable and are getting close to the physical controllers in terms of providing similar features.

We take a look on the possible architectures for deploying such controller-based networks and also examples of some solutions and platforms available on today's market. With the pallet of controllers that Cisco offers we gave overview on the solution with physical controller included. Software solutions without physical controller were presented through the Ubiquity-UniFi controller and the Meraki cloud platform for management. We also analyzed the open-source solution OpenWISP which is a software solution for providing Wi-Fi services. The applications from the OpenWISP suite are used for building a Wireless Internet Service Provider (WISP) and through their features they provide centralized management, geographic monitoring of the deployed network, etc. For each solution we output the benefits of using and the situations in which they are most suitable.

The undoubting development of the software solutions is just showing us the way things will evolve and it is inevitable that the future architectures will go towards elimination of the hardware controller or integrating it in other parts of the network.

Chapter 2

IEEE 802.11 WLAN networks

2.1 Introduction to wireless technologies

The enormous growth of the Internet usage and our need for mobility and communication resulted in enormous improvement of the wireless networks in the last decade. Also it resulted in enormous growth and development of the electronic industry which provided new devices that improve our user experience and are capable to be connected on various wireless networks. The biggest advantage of a wireless network is that it allows mobility of its users and that is maybe the most significant reason for its success. Also the smaller infrastructure cost for the providers in comparison with wired networks is another significant reason for the worldwide expansion of the wireless networks. With performance improvement offering similar capabilities as wired networks, wireless networks became a serious alternative even in some cases better communication solution.

All that fast development brought the need for standardization and regulation of the new technologies and the equipment using them. The organization “Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA)” within the IEEE is one of the responsible organizations for setting up the rules and providing the standards. This organization develops the standards for many industries including telecommunication industry. The

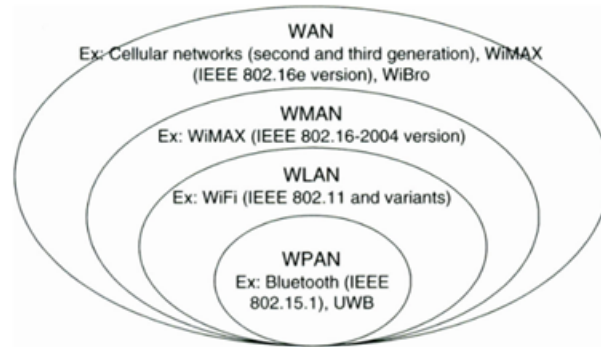


Figure 2.1: Wireless network categories [1]

IEEE 802 family of standards includes standards for local area networks and metropolitan area networks. On Figure 2.1 we can see the wireless representatives from the IEEE 802 family of standards and together with the most famous technologies for each type of network [1].

2.2 Wireless LAN overview

The IEEE 802.11 standard was published in 1997 and got its name Wireless LAN (WLAN) from the similarity with the already existing 802.X LAN standards (802.3), known also as Ethernet. It is defining the radio waves instead of wires as its medium for communication and transmission of the data. WLANs have the ability to switch dynamically between data rates when transmitting and receiving [2]. They have the ability to step down to a lower rate when facing poor transmission conditions and back up when the conditions are improved. When the conditions are poor due to low signal strength they can dynamically impose their fragmentation, reducing packet size to reduce data loss. This brings big flexibility for these systems, but also a cost in network complexity and security challenges as the radio medium is less reliable and less secure than a wired network.

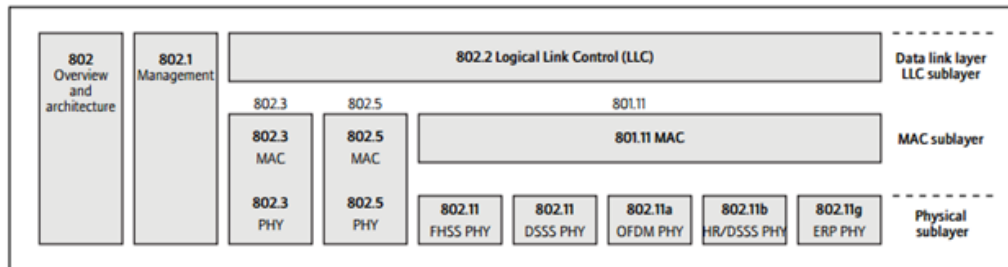


Figure 2.2: 802.11 data link and physical layers [4]

2.3 Wireless LAN standards

The IEEE 802 standards are defining the lowest two levels (Data Link and Physical) of the Open Systems Interconnection (OSI) model. For the 802.11 standard the crucial difference from its ancestors, the use of radio waves as medium for data transfer, is defined exactly in the specifications for the physical layer. The physical layer defines the data transmission for the WLAN, using various modulation schemes. Different amendments to 802.11 define specific physical (PHY) layers, such as 802.11b, 802.11g or 802.11a.

The frequency bands dedicated for industrial, scientific and medical purposes, shortly called ISM frequency bands are generally license-free because of the low-power devices (up to 100 mW). For the 802.11 mostly used ISM bands are 2.4 GHz and 5 GHz bands.

In Table 2.1 we can see the different amendments of the 802.11 standard through the years, with their working frequency, data rates and approximate ranges.

802.11 Protocol	Release date	Frequency (GHz)	Bandwidth (MHz)	Stream data rate (Mbit/s)	Approximate range	
					indoor (m)	outdoor (m)
802.11-1997	Jun 1997	2.4	22	1,2	20	100
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	35	120
		3.7				5000
b	Sep 1999	2.4	22	1, 2, 5.5, 11	35	140
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	38	140
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	70	250
			40	15, 30, 45, 60, 90, 120, 135, 150	70	250
ac	Dec 2013	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3	35	
			40	15, 30, 45, 60, 90, 120, 135, 150, 180, 200	35	
			80	32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3	35	
			160	65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7	35	
ad	Dec 2012	60	2160	Up to 6912 (6.75 Gbit/s)	60	100
af	Feb 2014	54MHz-790MHz	6,7	Up to 26.7	up to few 100 m	up to few km
			8	Up to 35.6		
ah	2016	0.9	1	150Kb/s– 4Mb/s	~100m	up to 1 km
			2	650Kb/s – 7.8Mb/s		
			4	1.35 – 18		
			8	2.9– 39		
			16	5.8– 78		
ay	2017	60	8000	Up to 100 Gbit/s	60	1000

Table 2.1: Different amendments of the 802.11 standard [5], [6]

2.4 WLAN components and topologies

The four main components of an 802.11 network are [4]:

- **Distribution system:** The logical component of 802.11 used to forward frames to their destination. In most commercial products, the distribution system is implemented as a combination of a bridging en-

gine and a distribution system medium, which is the backbone network used to relay frames between access points, often called simply the backbone network. In nearly all commercially successful products, Ethernet is used as the backbone network technology.

- **Access points:** The middle node devices between the stations and the network called Access Points (APs) perform the wireless-to-wired bridging function. (Access points perform a number of other functions, but bridging is by far the most important).
- **Wireless medium:** The radio frequency bands where the data transmission is performed.
- **Stations:** Mobile or stationary users (PCs, laptops, tablets, smartphones, etc.) connected to the network.

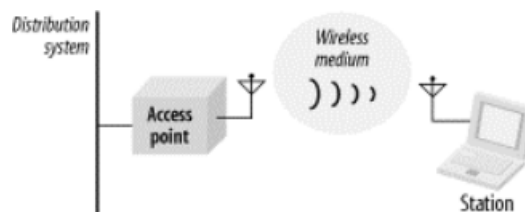


Figure 2.3: Components of 802.11 networks [4]

The area in which these stations communicate with each other on the same transmission channel, forming the basic block in 802.11 networks, is called **Basic Service Set (BSS)**. There are two types of BSS arrangements. The first type is the **independent BSS** (Figure 2.4), also known as ad-hoc, where the stations communicate directly between each other. Because they use the same transport medium, all of the stations receive the sent packages and every station except the intended recipient discard the incoming packages.

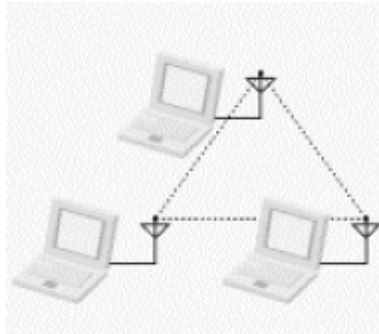


Figure 2.4: Independent BSS, [4]

The second type of BSS is the **infrastructure BSS** (Figure 2.5). Here the communication between two stations is relayed by the AP. The AP is also the gateway for the stations from the wireless network to the wired network and the Internet. Here the packets from one station A intended for station B are first sent from station A to the AP, then the AP resends to station B. This is suitable in situations when stations A and B are too far to reach each other but they are both close enough to the AP which will forward the sent packets.

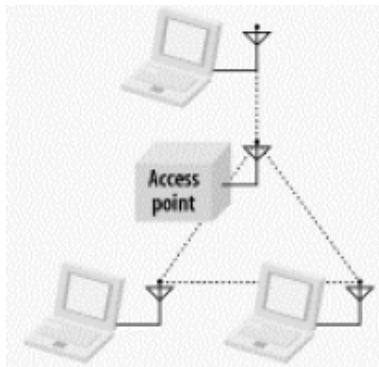


Figure 2.5: Infrastructure BSS [4]

Nowadays APs are able to fulfill many additional tasks [7] (Figure 2.6):

- They have integrated 10/100/1000 Mbit/s ports for wireline Ethernet devices and can also act as a layer 2 switch.

- They include integrated IP router to the Internet that can be connected via Ethernet to a DSL or cable modem.
- They also have integrated DHCP (Dynamic Host Configuration Protocol) server to configure devices automatically. It returns all necessary configuration information like the IP address for the device, the IP address of the DNS server and the IP address of the Internet gateway.

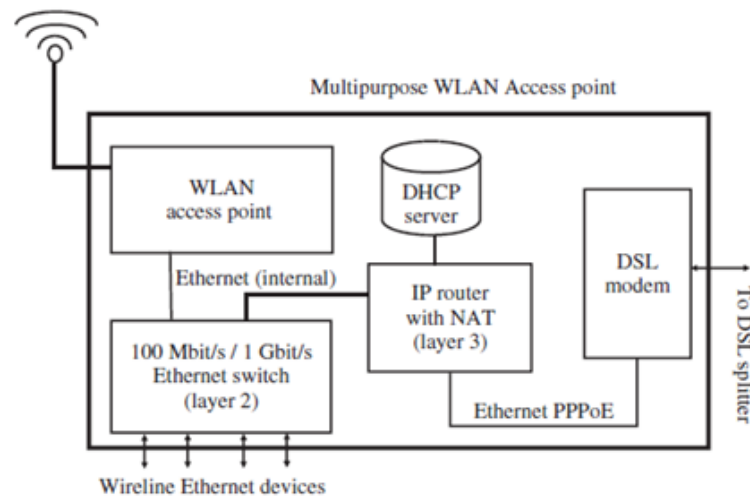


Figure 2.6: Access point, IP router and DSL modem in a single device [7]

One BSS can cover a small area and for the purpose of increasing the coverage area several BSSs can cooperate and link with each other creating configuration called **Extended Service Set (ESS)**. They are connected to the same wired network and this gives the possibility of forwarding the traffic from one BSS to another using the wired network they are both connected to. This allows roaming of a mobile station from one BSS to another in the same ESS without losing the connection to the network.

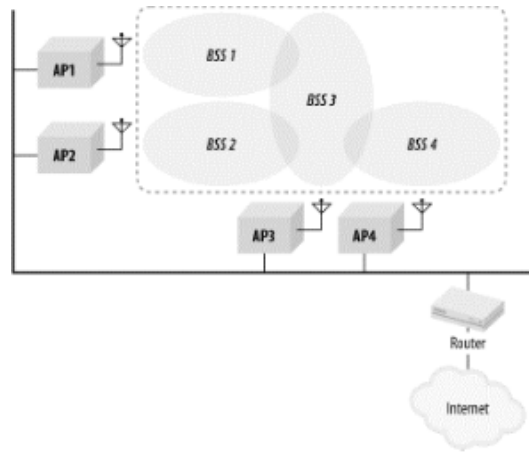


Figure 2.7: Extended service set [4]

2.5 Management operations

Every AP needs to have several parameters set for proper functioning. Two basic parameters for an AP are: the **Service Set Identity (SSID)** and the frequency or the channel number [7]. The SSID is basically the name of the network and it is incorporated in the beacon frames that are sent from the AP over the covered area. The potential users of the network can register this beacon messages and depending on SSID they decide if they will connect to that network. Depending on the standard, frequencies are set in the ISM bands ranges of 2.4 GHz (802.11b,g) or 5 GHz (802.11a,n). In the 2.4 GHz range, frequencies are set from 2.4 GHz to 2.5 GHz and divided in 11(US), 13(Europe) or 14(Japan) channels, each of them 22 MHz wide. Their centers of adjacent are 5 MHz apart and they overlap one another. Because the required channel bandwidth for WLAN is 25 MHz, APs at close range should be separated by at least five channels, (for e.g. if we use 3 AP, they should use channels 1, 6 and 11).

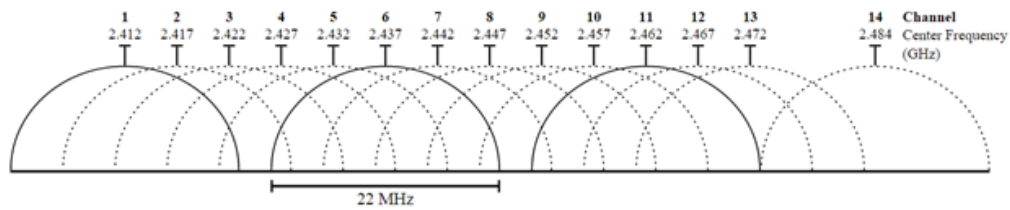


Figure 2.8: Graphical representation of 2.4 GHz band channels overlapping [5]

For the 5 GHz range (802.11a/n) frequencies are set from 5.150-5.350 GHz and 5.470-5.725 GHz. Here is a 455 MHz available bandwidth where 18 different non-overlapping channels can exist.

Joining a network is simpler for a client device. The device automatically searches for available APs on all possible frequencies. The user can choose from the discovered SSIDs of the networks which one he wants to join. In case of more SSIDs with the same name, the device assumes that they are part of the same ESS and connects to the AP from which it gets beacons with highest signal strength.

In the process of establishing a connection there are three functions that the standard guarantees: authentication, association and confidentiality [2].

Authentication is the process where nodes ensure that everyone is who and what they claim to be. There are two forms of authentication: open and shared key. The open key allows any user to authenticate to the AP, while with shared key only the client that have the shared key can connect with the access point.

After the authentication, association must be done in order to exchange data traffic. Figure 2.9 graphically shows the process of authentication and association with the sent messages. For insuring confidentiality in the network and preventing it from unauthorized access a few techniques can be applied. **MAC filtering** is one way to prevent unauthorized access by adding to the AP a list of MAC addresses of user devices allowed or forbidden to connect to its network. With a big amount of users and APs this method can be very time-consuming and difficult to manage but for small networks or short

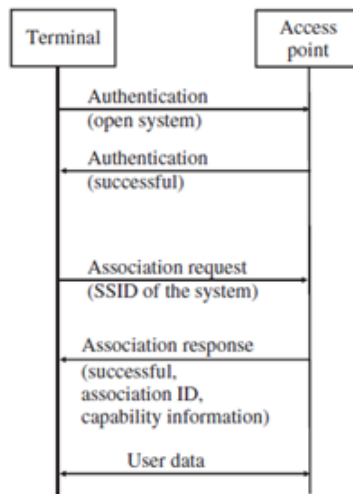


Figure 2.9: Authentication and association of a client device with an access point [7]

term limitations of misbehaving users, it can be useful. Another way to do authorization is by making a “closed network”, where the SSID is not broadcasted by the APs and the potential users must know it if they want to associate. This prevents from unwanted users but with the disadvantage that new nearby networks, without knowing, could set on the same channel as the closed network and cause interference. The most reliable authentication method for identifying wireless users is **encryption**. There are three encryption methods for WLAN:

- **Wired Equivalent Privacy (WEP):** It is the first encryption method for WLAN networks. It is supported by 802.11a/b/g equipment and uses shared 40-bit key to encrypt the data between AP and client, which is added on each of the networks APs and every client has to use it to associate. Because all users share the same key, it is not the strongest method for encryption in case one of the users reveals the key to someone. Then the compromised key needs to be changed on each AP and each client.
- **Wi-Fi Protected Access (WPA):** It was the next established en-

Wi-Fi name	Authentication	Key distribution	Encryption	Algorithm
(none)	open	none	none	none
WEP	open or shared key (WEP)	out of band	WEP	RC4
WPA – Personal	open, followed by shared secret = PSK	out of band (PSK=PMK)	TKIP	RC4
WPA – Enterprise	open, followed by 802.1x, in which shared secret = certificate or other token	PMK from Authentication Server	TKIP	RC4
WPA2 – Personal	open, followed by shared secret = PSK	out of band (PSK=PMK)	CCMP	AES
WPA2 – Enterprise	open, followed by 802.1x, in which shared secret = certificate or other token	PMK from Authentication Server	CCMP	AES

Table 2.2: Encryption methods in 802.11 WLANs [2]

encryption method by the 802.11i working group. It was a temporary solution for dealing with the vulnerabilities of WEP, covering the existing equipment, while the full standard 802.11i (WPA2) was developed [3]. WPA has two configurations WPA-PSK (WPA-Personal) and WPA-Enterprise. WPA-PSK is suitable for homes or small organizations, uses pre-shared key and doesn't require authentication server. WPA Enterprise is suitable for larger enterprise networks and it requires a Remote Authentication Dial In User Service (RADIUS) authentication server. WPA provides better authentication than WEP, using the Temporary Key Integrity Protocol (TKIP). As opposed to WEP and its fixed key, TKIP employs a per-packet key system which is generating a 128-bit key for each packet. But as well as WEP, WPA also showed vulnerabilities and was later replaced by Wi-Fi Protected Access, version 2 (WPA2).

- **802.11i/WPA2:** The next generation of encryption was the full standard 802.11i or WPA2. The main difference from WPA is the use of the Advanced Encryption System (AES) instead of TKIP. Opposed to the WPA2-Personal mode where Pre-Shared Key (PSK) is used, for company or campus deployments using a larger number of APs,

the WPA2-Enterprise mode exists. In this mode the APs support the 802.1X standard where an additional authentication RADIUS server is added which authenticates the client (supplicant) and sends information about that to the authenticator (AP). This is done by the Extensible Authentication Protocol (EAP).

Chapter 3

Planning and designing a WLAN network

A good planning and design process of a new WLAN network is crucial for its quality functioning and meeting user's requirements. In order to provide that, this process has to be done carefully and few steps have to be covered [8]:

- **Planning:** The initial plan is the first step that is taken. Here we decide about the bandwidth, working frequencies, protocols, etc., all dependent on the user's requirements.
- **Design:** The next step is designing the layout of APs in the area of coverage. From the types of antennas, to their placement, cells size, etc., all of that needs to be determined. A site survey could be helpful for easier decision.
- **Implementation:** In this phase the decided deployment is installed, then tested and tuned for proper functioning.
- **Optimization and operation:** Monitoring and making reports for the working network are essential for keeping track of the occurring problems because it helps in the process of necessary adjustments and improving performances.

At the beginning, depending on the applications that will be used on the network and estimated number of users, the designer can calculate the bandwidth requirements and make deployment decisions. Some typical applications have these bandwidth requirements [3]:

- Web surfing 500-1000 kb/s
- Audio 100-1000 kb/s
- Streaming video 1-4 Mb/s
- Printing 1 Mb/s
- File sharing 1-8 Mb/s
- Device backup 10-50 Mb/s

In usual office environments there are 20-30 users per cell and one AP is installed per 250-500 m², but in dense environments that may be insufficient. That's why it is best to be calculated and, for example if we have 10 users in a 100 m² area, where 8 are surfing the web and 2 are watching online videos, we will need:

$$8 * 1000 \text{ kb/s} + 2 * 4000 \text{ kb/s} = 16\,000 \text{ kb/s},$$

for the area of a 100 m² or 160 kb/s per m².

When it comes to frequency bands we can choose (or depending on the available equipment) either the 2.4 GHz or the 5 GHz band. The 2.4 GHz band is supported in most of the devices and has better range (in theory, not in every case) than the 5 GHz, but there are only 3 available non-overlapping channels. This limits the number of APs that can be placed in a certain area, as performance degrades with overlapping channels due to co-channel interference. On the other hand, in the 5 GHz band there are 18 non-overlapping channels and despite the shorter range, deployment without interference in this band is much easier. This band is a better choice for high performance in high density networks. The Wi-Fi standard that will be used needs to be chosen considering the average throughput in Mb/s it will need. For the most common technologies the average throughputs are:

- 802.11b: 7.2 Mb/s
- 802.11g: 25 Mb/s
- 802.11a: 25 Mb/s
- 802.11n: 25-160 Mb/s

When devices using 802.11b and 802.11g are served by the same AP, the performance drops and the AP shifts down to lower speeds.

Also as a part of the planning all the architectural elements should be taken in consideration from the type of the access network (architecture, APs, mesh nodes, controllers), to the distribution system (wired switches and routers), Voice over WLAN (VoWLAN) system that enables the use of wireless IP phones (if needed), etc. Here we focus on the wireless access network, as it is the part where the components controlled and managed by the administrators are installed (WLAN controllers, APs, etc.).

In the initial face of the designing of new network gathering as much information as possible about the deployment area is crucial for the later success. All kinds of requirements need to be taken into consideration: coverage area, throughput, mobility, density of users, security, applications, etc.

After considering the user's requirements a preliminary plan for the network layout is done. The potential architecture elements (hardware) and their placement are decided with the intention for high performance and low interference.

The next step in the deployment is the **site survey** which will help in acknowledging whether the preliminary plan and requirements are possible and acceptable. During the site survey we test our preliminary design using various experiment tools and combinations of solutions which can give us information how to finally adjust it and make it most efficient. With the performed tests we gather the following information [4]:

- The actual coverage of the APs and their optimal location.
- Actual bit rates and error rates in different locations, especially locations with large number of users.

- The right number of APs needed (more or less than the initial plan may be required)
- The performance of some applications on the WLAN

With all the gathered information conducted into site survey report containing the final network design and all its elements, we can proceed to the installation of the network. During the installation it is important to check if the installed APs are working as planned and defined in the design, and if needed to do adjustments. By measuring throughput and signal strength after the installation, we can make sure that everything works as expected. After the installation, we need constant monitoring of the installed system, support and troubleshoot in order to keep up with the user's requirements.

3.1 Access networks architectures

The first part in creating the architecture is the wireless access network. There are few primary access networks architectures:

- Autonomous access point architecture
- Controller-based access point architecture
- Ad hoc architecture
- Mesh network architecture

3.1.1 Autonomous access point architecture

Figure 3.1 shows the architecture with autonomous access points that form a WLAN. These APs are relatively intelligent, can interconnect with other APs via Ethernet switches and can operate independently from each other [9]. Because of the possibility of independent functioning they are very suitable for smaller networks that don't need controller. They can directly connect to wired switch and this is making them less expensive as less hardware is

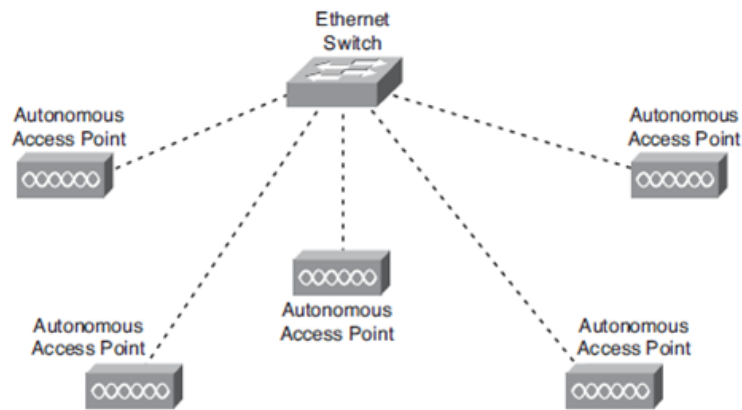


Figure 3.1: Autonomous access points offer distributed management and control [9]

needed. For example, for a small office or home, we can create a network using one AP with built in router functions for connecting several devices with each other and to the Internet.

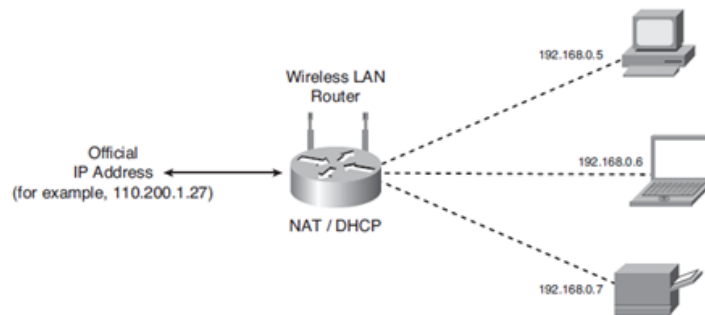


Figure 3.2: Simple small office/home network [9]

There are also disadvantages of this architecture as every AP needs to be configured manually during installation and after that every AP separately managed when changing configuration settings (SSID, etc.). This can be very time-consuming for bigger network with more than 10 APs.

3.1.2 Controller-based access point architecture

In this architecture we can see that Lightweight Access Points are implemented. The lightweight access points are an alternative to the traditional intelligent access points and they only implement the basic 802.11 functions. They connect to a WLAN controller, which provides centralized management, security and performance functions.

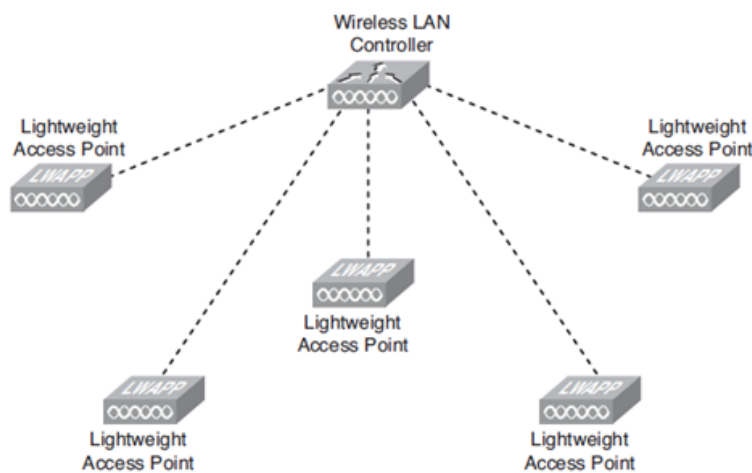


Figure 3.3: Controller-based access points provide centralized management and control [9]

Advantages that this architecture brings are:

- **Easy installation:** Each AP is automatically configured by the controller, which reduces the time needed for installation of the AP in comparison with autonomous APs.
- **Robust security:** Every AP must conform to a specific security configuration to be part of the network.
- **Effective mobility:** Users are tracked by the controllers and the roaming functions are centrally handled, without the need for re-authentication when roaming from one AP to another.
- **Simple expanding:** New AP can be easily added with very little configuration changes, as the controller automatically configures them and

connects to the wired network.

Disadvantage in this case is the need of more hardware installation which can bring more costs which is not suitable for organizations with smaller networks. That is why this architecture is appropriate for networks with more than 10 APs.

3.1.3 Ad hoc architecture

In this architecture there are no access points nor controllers and client devices that communicate directly with each other.

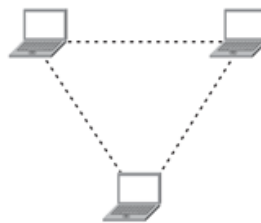


Figure 3.4: Ad hoc network architecture [9]

Advantages of the architecture are the low cost, easy and fast setup, and possible higher performance between users.

Disadvantages are: limited connection to wired networks, difficult for managing because the absence of connection to wired network, and the high security risk of outside attack. Because of these disadvantages it is mostly recommendable not to use this architecture for enterprise deployments, or maybe even using it at all.

3.1.4 Mesh network architecture

This architecture is consisted of mesh nodes that are actually APs that are capable to communicate wirelessly instead via Ethernet as the standard APs.

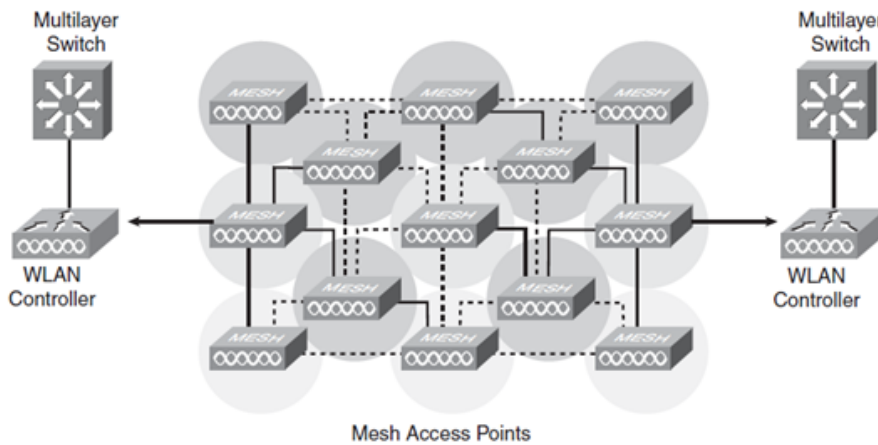


Figure 3.5: Mesh network architecture [9]

Advantages of this architecture are:

- No need for connection of the mesh nodes to wired network, so no cables are used which reduces the installation time and the expenses.
- Easily expandable with new nodes since they automatically mesh with the network and configure themselves on a centralized configuration profile.

Disadvantages that come with this architecture are:

- Reduced performance due to slower communication between the mesh nodes in comparison with traditional APs.
- The need of electrical power to operate, which is not always available.
- Difficult maintenance. If the node does not mesh to the network it cannot be accessed remotely and it must be fixed on the location where it is installed.

It is advisable that some of the mesh nodes in larger networks are designated as gateways, which interface the mesh network to the wired network. This architecture is suitable mostly for outdoor and citywide network deployments where wired cabling is not feasible.

Chapter 4

Controller-based wireless architecture and introduction to Wireless LAN Controller

At the beginning WLAN networks were imagined and deployed with simple architecture and standalone APs, which will link the Radio Frequency (RF) media with the Ethernet media. With the quick evolution of Wi-Fi devices and used applications, additional functions become needed, such as: centralized management, increased security, application services, etc. Enterprise networks became more and more complex, with large number of APs which made them difficult to manage with the existing autonomous AP architecture. The inability of the autonomous APs to communicate with each other caused problems like power adjustment, co-channel interference and client roaming. So instead of the time-consuming management of each AP separately, the idea of centralized approach for maintenance and optimization quickly evolved in main architecture for enterprise WLANs. Wireless switches, later referred as **wireless LAN controllers (WLC)** were implemented in the network architecture, as the elements which will provide the centralized network operation. The first WLAN switching technology was introduced by Symbol (later acquired by Motorola) in 2001 and became in-

teresting and more known on the market by the year 2003 [10]. But mostly responsible for the wide implementation of the controller-based wireless architecture was Cisco, with their *Cisco Unified Wireless Network (CUWN)* solution. The majority of Cisco WLANs have transitioned to a controller-based architecture by the year 2006, because it addresses a wide array of issues identified through the evolution of 802.11 WLAN usages [11]. Previously in 2004, Airespace published the Lightweight Access Point Protocol (LWAPP) standard as an Request for Comments (RFC) based on the Internet Engineering Task Force (IETF)'s Control and Provisioning of Wireless Access Points (CAPWAP) standard and in 2005 Cisco acquired Airespace. By 2006, the majority of large new Cisco-based WLANs were deployed using wireless LAN controllers.

The many issues in the WLANs evolution were the reason to use WLCs for providing WLAN to multiple locations or deploying WLAN to a large number of APs. Many organizations like hospitals, educational institutions, large companies, etc. have networks with maybe few hundreds of APs. The operational and managing costs for these kinds of networks were the biggest reason for the implementation of WLCs. Some principles from the cellular phone network deployment were adopted, learning how to build large wireless networks without enormous costs. They used the principle of separating the access control and the traffic-forwarding (transport) functions in order to scale and control operational costs. Figure 4.1 shows the major functions of wireless LAN.

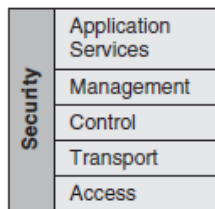


Figure 4.1: Functional elements in a WLAN [11]

In order to meet the demands of an enterprise network with centralized administration, WLCs were developed to have many capabilities and fea-

tures. Some of the main capabilities and features that a WLC should deliver are [14]:

- **AP discovery and provisioning:** Using discovery protocols like CAPWAP to allow APs to find nearby controllers and automatically join a WLAN.
- **Radio resource management:** Statically or dynamically assigning of channels to APs to prevent co-channel and RF interference, adjustment of transmit power and optimizing cell size.
- **Authentication:** Support of different authentication methods (Media Access Control (MAC) Access Control Lists (ACLs), captive portal login, PSK, 802.1x).
- **Encryption and Roaming:** Allowing clients to roam faster between APs that use the same controller by using pairwise master key caching or opportunistic key caching in 802.11i, support for layer 3 mobility of clients across subnets without session disruption.
- **Firewall and Virtual LAN (VLAN):** Traffic control between WLAN segments and core network, traffic inspection and reporting as well as capability of mapping WLAN traffic through VLAN trunks.
- **Quality of Service (QoS):** Traffic shaping, application-aware QoS capabilities, such as proprietary voice prioritization protocols or multicast optimizations for video, bandwidth management, etc.
- **Surveillance:** Control of the operational status of APs, detection and report of a rogue AP.
- **Built-in network services:** Built-in services like Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), File Transfer Protocol (FTP), or Virtual Private Network (VPN), to host higher-level services like locationing.
- **Integrated network hardware:** Incorporated wired or wireless network devices, like Ethernet switches, 3G/4G Wide Area Network (WAN)

cards, 802.11n APs. 3G/4G may be used in case of a failure of the LAN to WAN uplink.

4.1 Different solutions for WLAN management

With the evolution of the WLAN technology over the years and the expansion of the market players in this segment, numerous solutions are offered and users can choose from a wide pallet of products. The combinations and the chosen solutions will vary from the needs of the enterprise users and its configuration of the network. The basic difference in the deployed architectures including WLC is whether the network is **locally** or **cloud-managed**. Locally managed networks usually include locally installed hardware and they are entirely located and managed on the premises of the enterprise. With the cloud solutions the managing operations are shifted to the cloud. Here we find two different solutions: “**cloud-controlled**” WLAN and “**cloud-managed**” WLAN [12]. In the “cloud-controlled” WLAN the controller is placed in the cloud and the entire control and management is done from there, only the APs are locally placed, whereas in “cloud-managed” WLAN the control and the management are locally placed in WLC or controller-less APs and only the monitoring part is cloud-based.

Each of these solutions comes with its advantages and also disadvantages and the right solution depends from the specific environment of their implementation. The locally managed WLAN comes with robust and finely adjust hardware capable of more specific settings which some cloud solutions can't offer. But its high quality performance comes with big expense and it is suitable only for large enterprise networks with big campus facilities that can afford it. Cloud-controlled WLANs are suitable for deployment with a lot of branches where the management of each branch is easily done from one centralized point on the cloud. There is no need for having a controller on each branch site and also many vendors offer zero-touch APs that

can be configured before installation and only connected on-site without the need of reconfiguration. Also the expenses are lot smaller with this kind of solutions which makes them suitable for smaller or midsize organizations. But the cloud-controlled solution comes also with the disadvantage in case of internet connectivity failure because all the operations are depending on it. There are solutions that offer functioning in the “last known state” if it comes to short outages, but this can be only implemented in environments that are not 100% dependent (healthcare institutions...) and are tolerant to interruptions.

4.2 Controller-Based WLAN Functional and Elemental Architecture

Being the biggest market player Cisco has defined the basic rules and architecture configurations for the centralized controller-based networks. We will take Cisco’s architecture (*Cisco Unified Wireless Network (CUWN)*) as a basic example of controller-based WLAN to discover its structure. In this architecture the mandatory elements are the AP and the WLC [11]. Some optional elements might be needed if we want to provide some additional services or lower the operating costs.

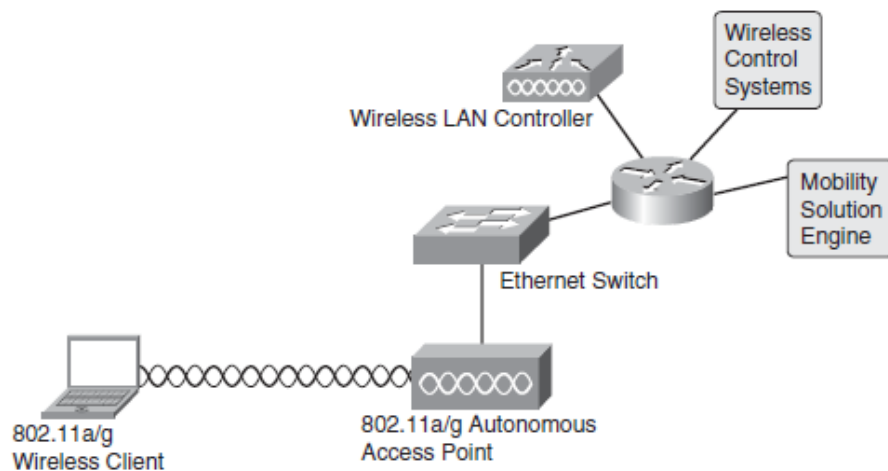


Figure 4.2: Elements for controller-based WLAN [11]

The AP can be either autonomous or lightweight. The autonomous AP is mostly used in networks without WLC and the lightweight AP is always associated with the WLC. In the WLC architecture we have separation of the WLAN functions in comparison to the autonomous architecture.

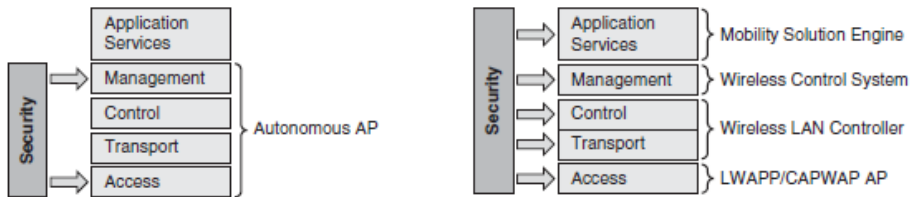


Figure 4.3: Functional implementation for an autonomous WLAN and in a controller-based CUWN [11]

This separation is the reason for increasing the functionality, scalability and security, as well as decreasing the operational costs.

The protocol that is used for the communication between the AP and the WLC is CAPWAP. The CAPWAP protocol is defined by IETF in their RFC 5415. CAPWAP centralizes WLAN configuration and control into a device called an access controller (AC). In CUWN, the WLC serves as the access controller.

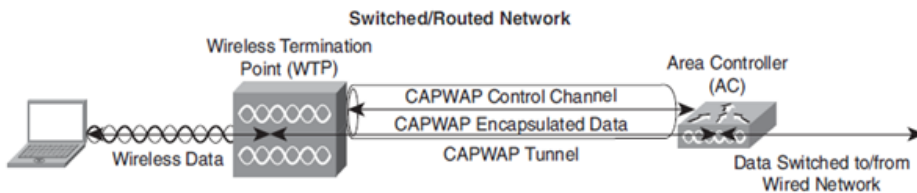


Figure 4.4: CAPWAP architecture [11]

APs can communicate with WLCs through the CAPWAP protocol, which defines both a control-messaging protocol and format and a data path component and supports both a distributed and centralized data path. There can be different reasons for exchanging CAPWAP control messages between the WLC and the APs, such as: AP configuration and firmware push from the controller, messages used in process of controller discovery and join, authentication, mobility, etc. CAPWAP control messages are secured in a Datagram

Transport Layer Security (DTLS) tunnel and CAPWAP is transported in UDP datagrams over the network.

When the centralized data path is used, all client packets are encapsulated in CAPWAP when send between the AP and the WLC. The AP is responsible for adding a CAPWAP header to the client packet, and the controller is responsible for removing the CAPWAP header and switching the packet onto a VLAN in the switching infrastructure. For the backward packets, from the wired network to the AP, the procedure is the same. Now the WLC encapsulates the packet with CAPWAP header, forwards to the AP, where it is removed by the AP and bridged to the RF medium.

In some networks there is a different deployment and distributed data path is used. CAPWAP can bridge data frames to the wired network at the AP. In the CUWN architecture this distributed data path is known as *Hybrid Remote Edge Access Point (HREAP)* and its secured version is known as *Office Extend Access Point (OEAP)*. Here, not all traffic is encapsulated in CAPWAP and delivered to the controller. Instead, some data traffic is bridged to the Ethernet LAN at the AP and MAC processing is pushed to the AP at the network edge.

From Figure 4.5 we can see that the Wireless Control System (WCS) is above the WLC, providing additional managing services beyond what is provided in the WLC. It is also used for managing other devices that are part of the architecture, like the Mobility Services Engine (MSE). The MSE is responsible for separating the application resources from the data transport on the WLCs, preventing applications from interfering with some time-sensitive operations on the WLC. In very large WLANs there can even be a manager of the managers, referred as WCS Navigator, which is capable of monitoring multiple WCSs.

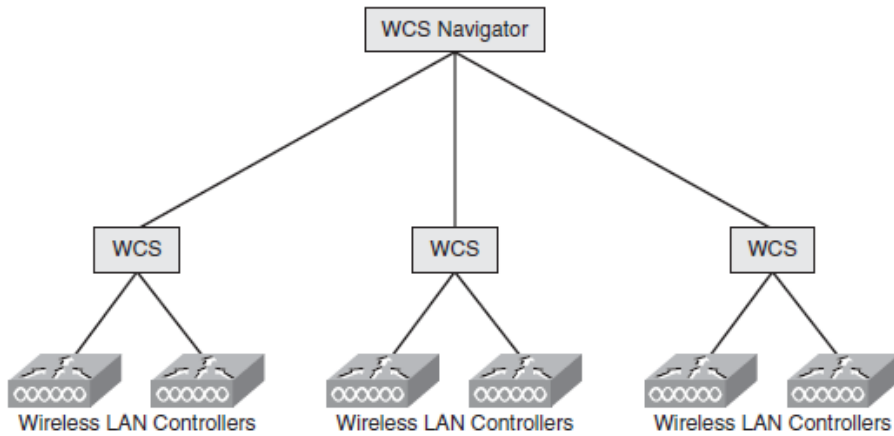


Figure 4.5: Management architecture for multiple WCS deployments with WCS navigator [11]

4.3 Architecture solutions

The controller-based architecture systems can be deployed in various network solutions and combinations depending on the user's requirements. Here we will outline the basic system architectures from which all kinds of variations can be developed [13].

4.3.1 Controller-based Management Only

In this architecture “heavy” APs are used with a central management software or hardware, offering central monitoring and managing what would be otherwise done by the autonomous AP. It helps with firmware updates to APs, pushing security settings, pushing wireless networks and SSIDs, etc. But, basically it is just a management system that can modify configurations of individual AP.

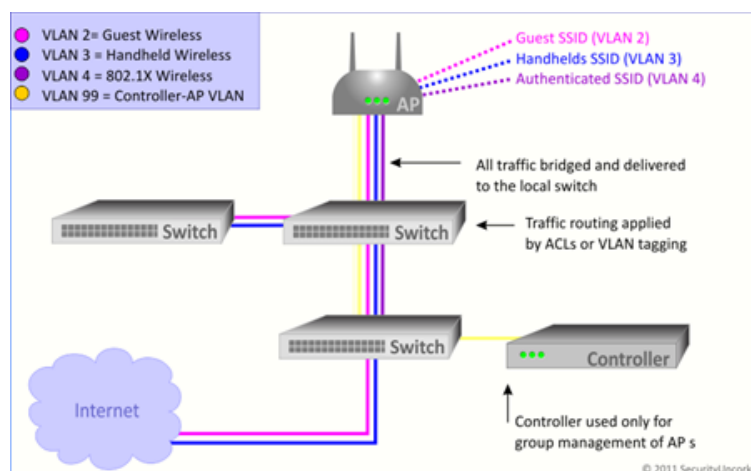


Figure 4.6: Controller-based management only system [13]

As advantage of this system we can point the low price for a much more manageable wireless solution than autonomous APs. It could be solved with a virtual appliance or even as a cloud-based hosted service, which are very popular options in organizations with small resources for a complex wireless systems.

Disadvantages come from the fact that the AP is still autonomous and the need to be configured as such. Also there is a need to extend wireless VLANs through the network and out to the port the AP is attached to. For example, in case of 3 wireless networks on 3 different VLANs, each VLAN needs to be delivered to each AP port. For additional need of a new wireless network the procedure needs to be done again. When 802.1X is used for authentication, we need registration of each AP as RADIUS client on the RADIUS server and configuration with the shared secret on both sides. When using the cloud-based management solutions, the changes that are made to the system can become more time-consuming because all configurations are pushed from the Internet based server through a WAN link down to the APs.

4.3.2 Controller-based with Traffic Tunneling

This solution uses light or semi-light APs with almost no intelligence, where all wireless traffic is tunneled to the controller. The traffic through the tunnel

can be encrypted or can be a simple Generic Routing Encapsulation (GRE) tunnel. When the traffic arrives at the controller it can be either filtered, firewalled, routed or just dropped further on the network.

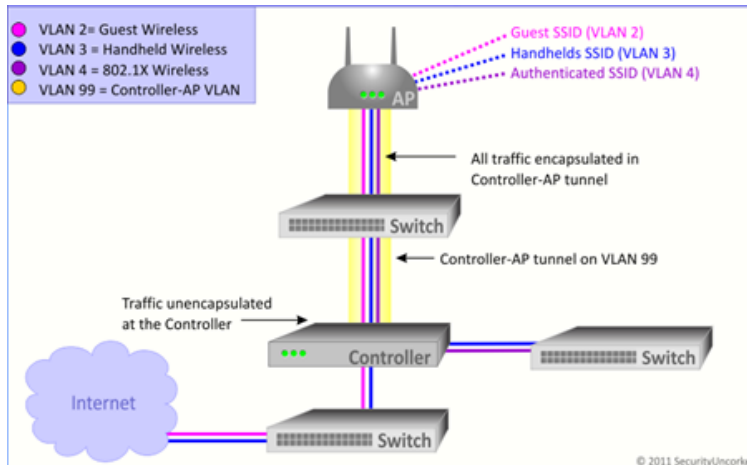


Figure 4.7: Controller-based system with traffic tunneling [13]

The lower price of the less-intelligent APs used with these systems is the first advantage they offer. The tunneled traffic is another advantage, assuring security for the wireless traffic protecting it from rouge route or misconfiguration on the wired side. Also comparing to the previous solution, we have simplified monitoring and more advanced RF management and troubleshooting.

The fully tunneled traffic sometimes can become a disadvantage too, because all traffic is send back to the controller and there is no option to bridge or drop it locally on a switch. This is maybe not the best solution when a large amount of files are sent through the network or there are distant branches.

4.3.3 Controller-based with Split Traffic

The most flexible solution by far is the one with split traffic design, where the AP can be configured to either tunnel traffic back to a controller or to bridge and drop it on the switch it is directly attached to. This is mostly used when we what to separate the authenticated wireless traffic from the

guest traffic, meaning that authenticated traffic will be sent to the wired network and the guest traffic will be tunneled to the controller and directed out to the Internet. With the encryption all the way to the controller, the protection of the data is guaranteed and that is why it is appropriate for secure transport from one protected resource in the network to another.

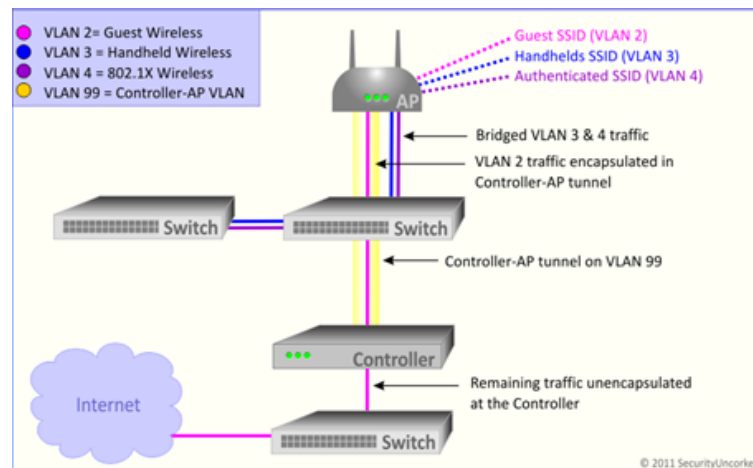


Figure 4.8: Controller-based system with split traffic [13]

The advantage of this system is that it is the most flexible solution offered and it can support various user requirements. It offers many monitoring and managing tools, option for extended encryption all the way to the controller, and advanced troubleshooting and reporting.

As disadvantage we can address the bigger price of this system and its complexity. For not so experienced wireless managers the extended array of options can bring some difficulty while implementing, but the fact that these systems are covering the problems that may occur with the previous types of systems makes this disadvantage minimal.

Chapter 5

Commercial and open-source platforms for control and management of wireless network

5.1 Cisco

Cisco is the market leader in the networking industry with 85% of the Internet traffic traveling through Cisco's systems. They offer a wide spectrum of products that can provide end-to-end network solutions for different users. They have mostly on-premises WLAN controllers and large family of APs compatible with them. Using the CAPWAP protocol they are also compatible with other vendor APs that support CAPWAP.

CHAPTER 5. COMMERCIAL AND OPEN-SOURCE PLATFORMS
36 FOR CONTROL AND MANAGEMENT OF WIRELESS NETWORK

	Virtual Controller	Controller for ISR G2	2500 Series	3650	5500 Series	5760	3850	WISM2	Flex 7500 Series	8500 Series
Product Image										
Target Deployments	Small or Mid-sized Business Branch	Small or Mid-sized Business Branch	Small or Mid-sized Business Branch	Small or Mid-sized Business Branch	Mid-sized to Large Enterprise	Mid-sized to Large Enterprise	Small to Large Enterprise	Mid-sized to Large Enterprise	Large Number of Branches	Large Enterprise and Service Provider
Form Factor	Virtual Machine Software	ISR-G2-UCS-E	Desktop	1RU Switch	1RU Appliance	1RU Appliance	1RU Switch	Catalyst 6500 Module	1RU Appliance	1RU Appliance
Deployment Modes										
FlexConnect	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes	Yes
Central Mode (Formerly Local Mode)	-	Yes	Yes	-	Yes	-	-	Yes	-	Yes
Mesh	No	No	Yes	No	Yes	No	No	Yes	No	Yes
OfficeExtend	Yes	-	Yes	-	Yes	-	-	Yes	Yes	Yes
FlexConnect + Mesh	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes	Yes
Scale										
Min Access Points	5	5	5	1	12	25	1	100	300	300
Max Access Points	200	200	75	25	500	1,000	50	1,000	6,000	6,000
Max Client Support	6,000	6,000	1,000	1,000	7,000	12,000	2,000	15,000	64,000	64,000
Max RF Tag Support	3,000	500	500	1,000	5,000	10,000	1,000	5,000	50,000	50,000
Max Throughput	500 Mbps	500 Mbps	1 Gbps	20 Gbps and 40 Gbps	8 Gbps	60 Gbps	20 Gbps and 40 Gbps	20 Gbps	1 Gbps	10 Gbps
Max Number of Access Point Groups	200	200	30	25	500	1,000	50	1000	6,000	6,000
Max Number of Flex Groups	100	100	30	-	100	-	-	100	2,000	2,000
Max Access Points per Group	100	100	25	25	25	25	25	25	100	100
Max WLANs	512	512	16	64	512	512	64	512	512	512
Max VLANs	512	512	16	4,000	512	4,000	4,000	512	4,096	4,096
Platform Details										
Interfaces or Network I/O	2 vNICs	ISR G2 Backplane	Four 1GbE	4 * 1G/10G Uplink 2 * 1G/10G Uplink 4 * 1G Uplink 24 and 48 * 10/100/1000 Mbps Data/ POE+	Eight 1GbE	6 * 1/10 GbE	4 * 1G/10G Uplink 2 * 1G/10G Uplink 4 * 1G Uplink 24 and 48 * 10/100/1000 Mbps Data/ POE+	Catalyst 6500 Backplane	Two 10GbE	Two 10GbE
Redundant Power	NA	Yes (Option)	No	Yes (option)	Yes (Option)	Yes (Option)	Yes (Option)	Yes	Yes (Installed)	Yes (Installed)
Redundant Fans	NA	Yes	Built-in Fan	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Max Power Consumption	-	Refer to UCS-E	80W	350W	125W	350W	350W	220W	675W	675W
Standard Hardware Warranty	NA	90 Days	90 Days	E-LLW	90 Days	90 Days	E-LLW	90 Days	90 Days	90 Days
Standard Software Warranty	90 Days	90 Days	90 Days	90 Days	90 Days	90 Days	90 Days	90 Days	90 Days	90 Days
Feature Support										
Workgroup Bridge	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Link Aggregation Group (LAG)	-	Yes	Yes	Yes	Yes	Yes	Yes	-	Yes	Yes
Radio Resource Management (RRM)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Datagram Transfer Layer Security (DTLS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco Compatible Extensions Call Admission Control (CAC)/ Wi-Fi Multimedia (WMM)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco VideoStream	Yes	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Guest Services (Wireless)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Guest Services (Wired)	-	-	Yes	Yes	Yes	Yes	Yes	Yes	-	-
Guest Anchor	-	-	Yes	-	Yes	Yes	-	Yes	-	Yes
Access Control Lists (ACLs)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HA with AP SSO	NO - vMotion Base HA	No - vMotion Base HA	No - Only N+1 HA	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HA with Client SSO	vMotion HA	vMotion HA	No	No	Yes	No	No	Yes	Yes	Yes
Integrated Wireless Policy Engine	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes	Yes
Application Visibility & Control (AVC)	-	-	Yes**	Yes	Yes**	Yes	Yes	Yes**	Yes**	Yes**
Bonjour Gateway	Yes**	Yes**	Yes**	Yes	Yes**	Yes	Yes	Yes**	Yes**	Yes**
Mobility	L2	L2	L2 & L3	L2 & L3	L2 & L3	L2 & L3	L2 & L3	L2 & L3	L2	L2 & L3
QoS	Yes	Yes	Yes	Yes (MOC based)	Yes	Yes (MOC based)	Yes (MOC based)	Yes	Yes	Yes
Bi-Directional Rate Limiting	Yes	Yes	No	No	Yes	No	No	Yes	Yes	Yes
Government Certifications										
FIPS	In Plan	In Plan	In Plan	In Plan	Certified	In Plan	In Plan	Certified	In Plan	In Plan
Common Criteria	In Plan	In Plan	In Plan	In Plan	Certified	In Plan	In Plan	Certified	In Plan	In Plan
DISA UCAPL	In Plan	In Plan	In Plan	In Plan	Certified	In Plan	In Plan	Certified	In Plan	In Plan
DISA UCAPL	In Plan	In Plan	In Plan	In Plan	Certified	In Plan	In Plan	Certified	In Plan	In Plan

Table 5.1: Summarized information about Cisco controllers [16]

Here we will make a quick overview of the WLAN controller lines that are offered [15]:

- **2500 Series**

The Cisco 2500 Series wireless LAN controller appliance is suitable for smaller organizations and branch offices that require on-site controller capabilities. It has maximum throughput of 1 Gb/s, it can manage from 5 up to 75 APs with maximum client support of 1000 users.

- **5500 Series**

The 5500 Series WLC appliance is suitable for medium to large organizations. It can manage from 12 up to 500 APs with maximum client support of 7000 users. The maximum throughput is 8 Gb/s.

- **5700 Series**

The 5700 Series is different from all other Cisco WLCs because it uses the *Internetwork Operating System (IOS)* that Cisco routers and switches run on. This feature is extremely efficient and fast and gives the 5700 Series the highest throughput of 60 Gb/s, compared to all other Cisco's controllers. The number of APs that can be managed is 25-1000 and the maximum client support is 12000 users. That is why it is most suitable for environments with very large amounts of data throughput over wireless.

- **8500 Series**

The 8500 Series is the most powerful Cisco WLC, managing from 300 to 6000 APs, with maximum throughput of 10 Gb/s and client support of maximum 64000 users. This is why it is ideal for large organizations or campuses with large number of APs and wireless devices.

- **Cisco Virtual Wireless Controller**

Besides high-end hardware solutions Cisco also offers Virtual Wireless Controller which is suitable for medium-sized organizations or branch offices that have on-premises virtual server. It can manage from 5 to 200 APs, with maximum throughput of 500 Mb/s and client support

of maximum 6000 users.

- **Integrated controllers**

Besides the previously mention standalone controllers there are also integrated controllers like the ones found in the **Catalyst 3650** and **3850** switches. These are used for branch offices. They are using the *FlexConnect* technology for managing the APs and offloading data remotely, as opposed to having it tunnel back to a Cisco WLC across a wide area network. They can manage up to 50 APs, support up to 2000 user, with maximum throughput of 40 Gb/s (depending on the model in use).

5.2 Ubiquity Networks

Ubiquity networks are another vendor on the networking market with high-performance technology for enterprises and service providers. They offer wide pallet of products from Wi-Fi equipment, routing and switching, video surveillance, VoIP products, to broadband wireless technology. As we are interested in the Wi-Fi enterprise solutions control and management we took a look of what Ubiquity Networks offer.

Their Wi-Fi system is called **UniFi** and within they offer hardware equipment (APs) for indoor and outdoor use and also software controller for device management. From functioning point, they highlight the zero handoff roaming and their Multi-Lane RF Technology [17].

Zero handoff roaming means that in a system with multiple APs, they will act as a cluster and appear as one AP, regarding the size of the network. The client maintains the connection to the nearest AP as it moves, without the need to renegotiate. As all the negotiation is offloaded to the APs, they decide which AP will provide the connection when the client starts moving based on the signal strength. This is ideal for mobile users preventing from any packet loss or latency.

The Multi-Lane RF technology is using specialized circuitry: the High-

Selectivity receiver, which helps in isolating the signals on the operating channel and rejecting the interference. In theory channels 1, 6 and 11 of the 2.4 GHz band should not overlap, but in high density environments there is a cross-channel interference, which affects the receiver performance.

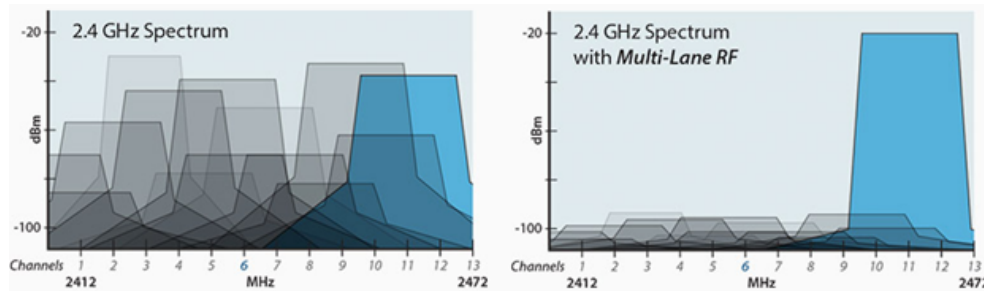


Figure 5.1: Typical AP receiver and UniFi AP with multi-lane RF [17]

The typical AP receiver operating on channel 6 can hear RF from channels 1 and 11 because it has generic filter for eliminating non-2.4 GHz interference and allowing all 2.4 GHz frequencies. The UniFi AP-Outdoor+ with its Multi-Lane RF technology, eliminates the interfering frequencies from channels different from the one it is operating on.

5.2.1 Demo test of the UniFi Controller

The UniFi Controller is a software solution controller for management of UniFi Wi-Fi networks. When installed it is accessible from any device using a web browser [18]. The APs running on the same subnet as the controller are automatically recognized and can be adopted by the controller for further configuration and management. The user interface gives a graphical representation of the network status with all its components.



Figure 5.2: UniFi controller dashboard [18]

The administrator can choose from the options in the side menu what to configure (dashboard, map, devices, clients, statistics, insights). All APs connected to the controller are available for configuration and remote firmware upgrade if needed. There is a possibility for uploading your site map or using Google maps for graphical representation of your network coverage (Figure 5.3). The coverage area is only estimated by the characteristics of the placed APs and it is not considering the indoor interference of the wall materials. Because of that, it can not be taken as totally true but only as a useful information.

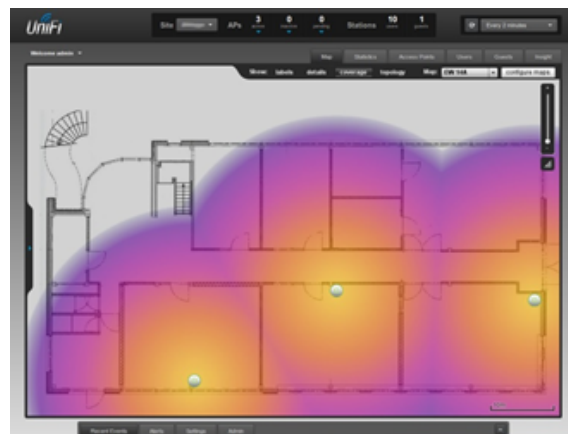
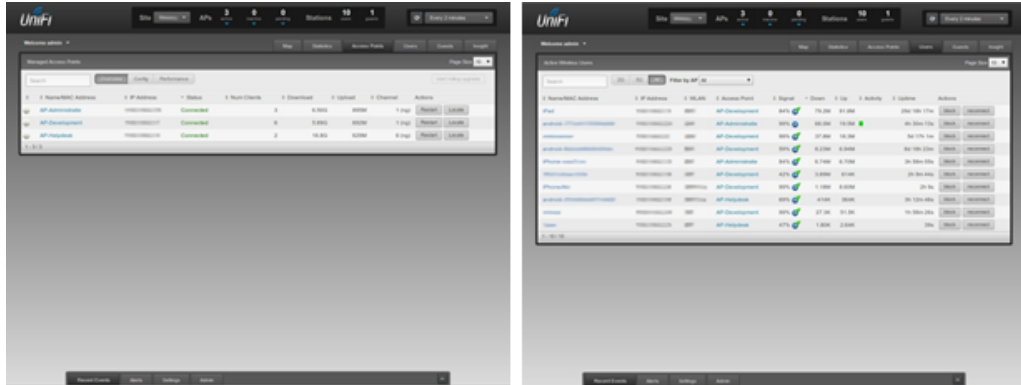


Figure 5.3: UniFi site map [19]

The administrator has the ability to control and edit all devices, control the access of every user or guest on the network by setting authentication rules, etc.(Figure 5.4)



The figure shows two screenshots of the UniFi web interface. The left screenshot displays a table of APs (Access Points) with columns for Name, Address, Status, Num Clients, Download, Upload, Channel, and Action. The right screenshot displays a table of users with columns for Name, Address, AP, Signal, Chan, Activity, and Action.

Figure 5.4: UniFi APs and users lists [19]

Also there are real-time statistics for the current state of the network, traffic, number of clients, etc.(Figure 5.5) which can be used for network analyzing, troubleshoot and improving the overall performance. There is a possibility for setting email notifications and alerts for different events and keeping track of what is happening on your network(s).



Figure 5.5: UniFi statistics preview [19]

With the guest portal and hotspot support, there is an option for separating private user networks from guests and applying different network bandwidth rates for them, limiting usage etc.

5.3 Meraki

Meraki was started by three MIT students (Sanjit Biswas, John Bicket, Hans Robertson) who worked on the MIT *Roofnet* project where they were focusing on creating self-configuring wireless network using Wi-Fi radios and routing software. Founded in 2006, Meraki managed to practically invent the cloud networking segment and by the year 2012 it was acquired by Cisco for \$1.2 billion. Now as Cisco's "Cloud Networking Group" is one of their most successful units.

They produce powerful wireless APs, Ethernet switches and security appliances that could be part of their cloud networking architecture and easily deployed and managed from one centralized point on the cloud.

Meraki uses an out of band management architecture [16], which means that they are separating only the management data to flow through their cloud infrastructure and the user's data doesn't. The management data (configuration, monitoring, statistics, etc.) flows to the Cisco Meraki cloud over a secure Internet connection and the user data (web browsing, applications, etc.) is directly flowing to its destination on the LAN or across the WAN.

This brings advantages in scalability, reliability and security. The scalability is improved because there are no centralized controller bottlenecks, which gives unlimited throughput and also there is no need for MPLS tunnels for newly added devices or sites. The reliability comes from the redundant cloud service and the provided network functions even with management traffic interrupted. The fact that no user traffic flows over Cisco Meraki's cloud, is improving the security. The only disadvantage is if due some reason the Cisco Meraki cloud is unreachable, then management, monitoring and hosted services are unavailable. This does not affect most end users because established configurations are still in force, for example: access of the local network is available (printers, file shares. . .), access to Internet if WAN connectivity is available, all network policies (QoS, firewall) are still in force, user authentication via 802.1x/RADIUS, roaming between APs is available, VPN tunnels continue to work, local configuration tools (IP configuration)

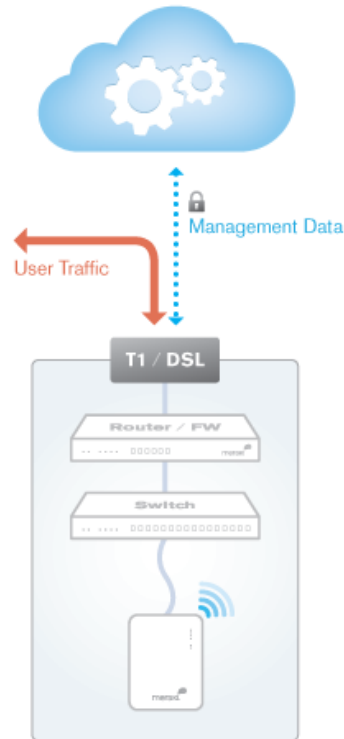


Figure 5.6: Meraki's out of band management architecture [20]

are available. During the interruption all usage statistics are stored locally and pushed to the cloud when the connection is re-established.

5.3.1 Demo test of the Cisco Meraki cloud management platform

Meraki even offers 3 ways for new potential users to get free trial hands-on experience with their products. There is a possibility to request any Cisco Meraki product to test it on your network and return if not satisfied, possibility to receive a free 802.11n AP by attending one of their Webinars and third option to start a demo use of their cloud management platform on your browser. We took a closer look on this option. With a quick registration on their web site, you get the opportunity to explore the possibilities their cloud platform offers. It has already made demo networks you can choose from or make your own one. The platform gives an opportunity for multi-site

management with choosing from your deployed networks (Figure 5.7).

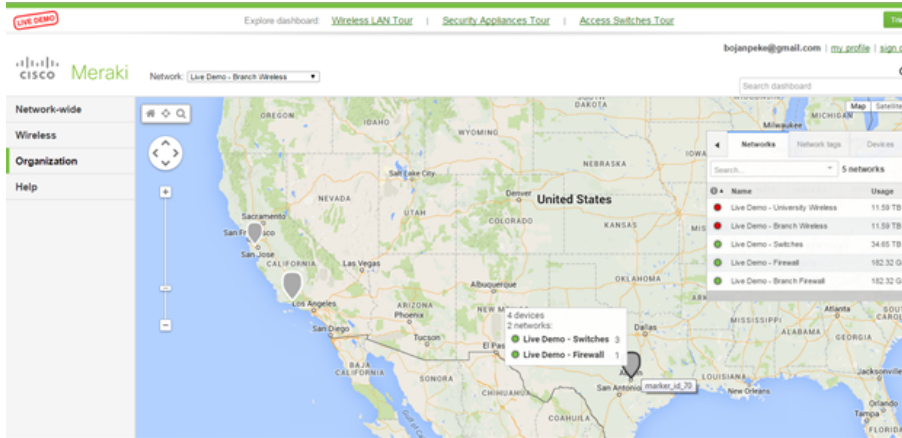


Figure 5.7: Meraki cloud management platform, multi-site deployment map representation of the available demo networks

The available demo university wireless network was the example we took a closer look because it was the most complex with most deployed APs. From Figure 5.8 we can see that the platform firstly offers a graphical presentation of the network traffic, a map of the APs deployed in the network and a side menu for all the management options. It is easy for use and well organized. From the side menu there are options for monitoring and managing depending on your needs.

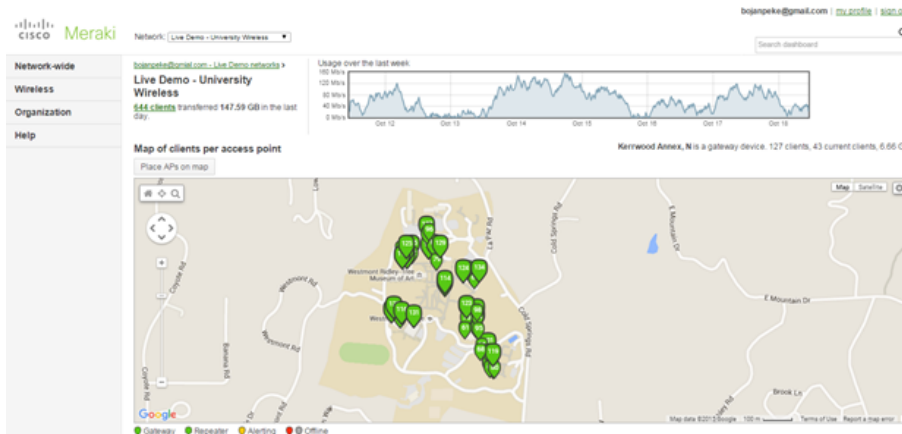


Figure 5.8: Meraki cloud management platform, network management screen
In the “Network-wide” tab there are options to monitor and configure

as we can see on Figure 5.9. There are options to get a list of all clients using the network, we can capture specific packages on the network or AP, get event log for the network or specific AP, get summary report, configure general rules, add group policies, configure users and devices, etc.

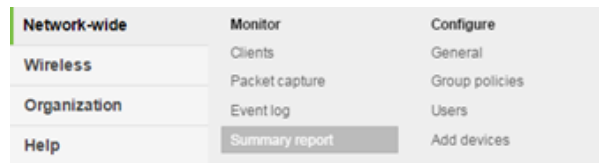


Figure 5.9: Meraki cloud management platform, network-wide tab and its' options

For each client attached to the network we can get a graphical explanation of its traffic, used applications and event log with alerts and previous conditions.

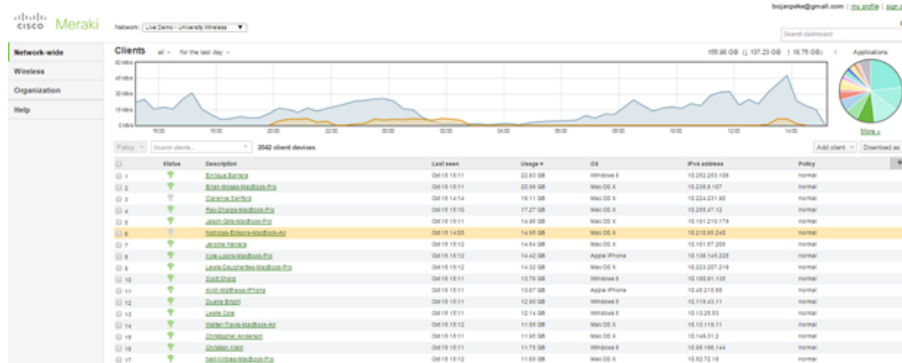


Figure 5.10: Meraki cloud management platform, list of user clients

With the summary report we get statistics and graphical presentation of usage of the network, lists for top usage by APs, by SSIDs, by clients, by applications, by device manufacturer and by operating system. That gives us total overview about the traffic on the network and it can help us with further configuration and optimization depending on the needs of the users. These are just few examples of the possibilities that this platform offers.

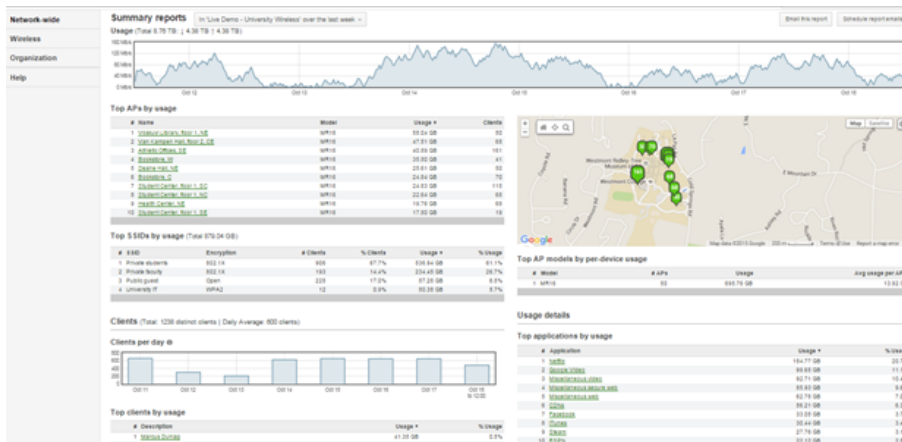


Figure 5.11: Meraki cloud management platform, summary reports

In the “Wireless” tab there are options to monitor and configure settings for every aspect of the wireless network as we can see on Figure 5.12.

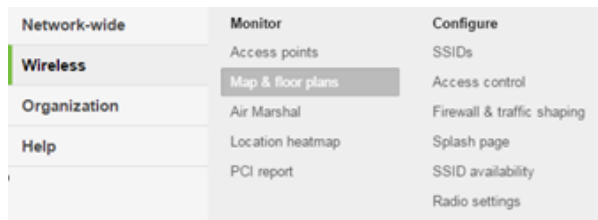


Figure 5.12: Meraki cloud management platform, “wireless” tab

From the “Organization” tab we arrange all the settings for the user account currently logged in on the platform and control the functioning of every network available for managing from that user account.

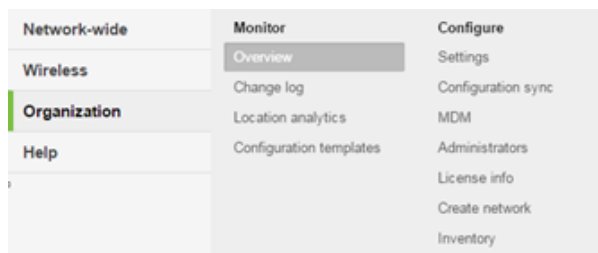


Figure 5.13: Meraki cloud management platform, “organization” tab

All the above mentioned features and the cost advantages, make this platform a really good solution for a centralized cloud management suitable for small and medium-sized, but also for large enterprises.

5.4 OpenWISP

OpenWISP (Open Wireless Internet Service Provider) is an open-source software platform that provides implementation of a complete Wi-Fi service [21]. It is a software suite that includes five applications that can be used for implementing Wi-Fi services. As an open-source project available on GitHub it is completely free of charge and it can be used by anyone, also it is open for anyone who wants to work on improvement of the applications code.

The OpenWISP project was made by the university consortium CASPUR for the purposes of Province of Rome and their plan to start a free public Wi-Fi network over its territory, including Rome and 120 other cities [22].

With its methodology for distribution of networks (more precisely Virtual LANs used for Wi-Fi connectivity) between geographically distant sites, the project made possible to host public connectivity services on non-dedicated network infrastructure (e.g.: private xDSL). Also it was allowed for anyone to add and host an AP and contribute for the network growth. Just two months from its start, in December 2008, there were 50 hotspots dislocated in the Province of Rome. The quick expansion of the network was the reason for development of the software responsible for management and control of the network, and also responsible for the enormous future growth of the network (March 2012, 1000 hotspots).

The 5 main applications that are used for building a Wi-Fi service:

- **OpenWISP Manager (OWM) and OpenWISP Firmware (OWF):** OWM is a Ruby on Rails application, web GUI for centralized management of APs. OWF is customized firmware for the devices which will be part of the OpenWISP service, in order for them to be compatible for managing and monitoring from the other applications that are part of the OpenWISP suite.
- **OpenWISP User System Management (OWUMS):** The OWUSM is an application responsible for the management of the OpenWISP user base.

- **OpenWISP Geographic Monitoring (OWGM):** The OWGM is an application that provides geographic monitoring of the APs, showing their current status and providing statistics and graphs.
- **OpenWISP Captive Portal Manager (OWCPM):** The OWCPM is captive portal (login page shown as a startup page when browser is open, where the user needs to sign up in order to use the public-access network), based on Linux's netfilters.
- **OpenWISP MiddleWare (OWMW):** OWMW is a Sinatra application that helps for connection between all OpenWISP applications via RESTful API.

Features that can be outlined are the centralized management of the APs and user's connectivity, the users self-signup, the possibility for multiple SSIDs with different security (e.g. a public network with captive portal-based access control and a service network protected with 802.1x), etc. As a result of the VPN configuration, these networks can be multiplexed in a single VPN, or multiple VPNs can be used for distribution to different destinations.

5.4.1 OpenWISP sample architectures

There are two OpenWISP sample architectures that are outlined [23]:

- **Typical OpenWISP installation, behind a firewall with NAT, (Figure 5.14):** When booting every AP with OWF, creates a setup VPN (openVPN) with the OWM server [23]. Then the AP requests and downloads its configuration through the established setup VPN. After the new configuration is deployed, for instance another VPN is created where the Wi-Fi user's traffic is encapsulated, the set up VPN remains up, and AP monitoring and administration is available (even if it is behind a firewall/NAT). The AP is set to periodically check the OWM server for new/changed configuration and, if so, it restarts and updates.

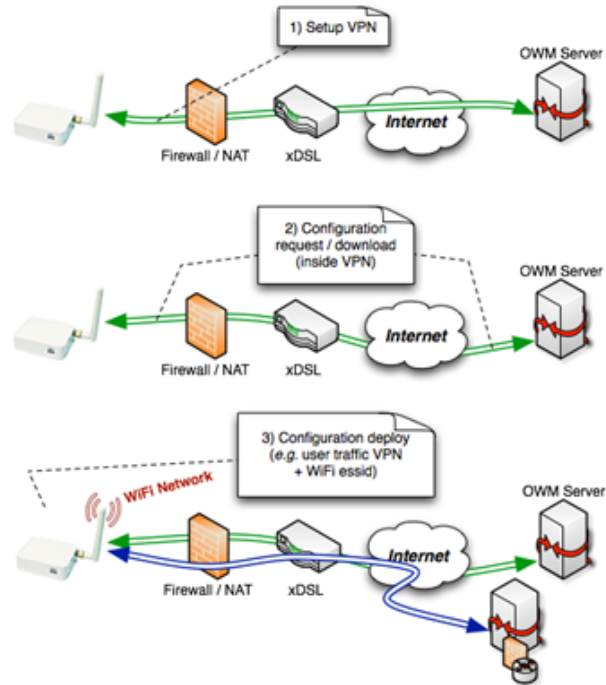


Figure 5.14: Typical OpenWISP installation: behind a firewall with NAT [23]

- **WPA/WPA2 Enterprise (802.1x), (Figure 5.15):** Here, we have two 802.1Q VLANs encapsulated in a single (layer2) openVPN tunnel. One is used for authenticated user traffic and the other is used for the RADIUS traffic between the authentication server and the authenticator. In these kind of VPN connections we can encapsulate multiple networks that have different policies, dependent on our needs. For example, in the OWF we can define 802.1X network and open Wi-Fi network to be broadcasted simultaneously.

5.4.2 OpenWISP Manager and OpenWISP Firmware

OWM is a Ruby on Rails application which is used for configuring networks with OpenWISP firmware-based APs. The OWF is a customized version (with OWF package included) of the OpenWRT firmware which is also open-source, and it can be deployed on devices with Atheros Wi-Fi card supported by OpenWRT.

Since OWM is a RoR (Ruby on Rails) application we need to set that on our system. We did that with the following commands entered through terminal:

```
sudo apt-get install ruby 1.8
sudo apt-get install ruby1.8-dev
sudo apt-get install rubygems
sudo gem install rails
sudo gem install activerecord
```

Next we set mysql, create empty database (in our case named "owm") and set up the `/var/www/config/database.yml` file to match our credentials:

```
sudo apt-get install mysql-server mysql-client
sudo gem install mysql
```

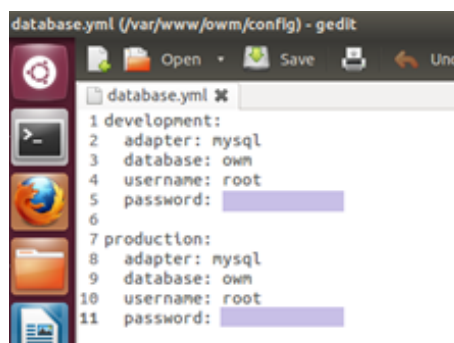


Figure 5.16: The edited file database.yml

Also we needed to set up web server (Apache) and application (Phusion Passenger) to power our RoR application.

```
sudo apt-get install apache2
sudo apt-get install passenger
```

After Passenger is compiled, it is installed into Apache as a module with the following command:

```
passenger-install-apache2-module
```

When using Apache and Passenger, the instructions stated that our virtual host configuration needs to be updated. For that purpose configuration file (`owm.conf`) was created in the folder `/etc/apache2/sites-available` and the following snippet was added into the content of the file:

```
Alias <RAILS BASE URI> "<RAILS BASE PATH>/owm/public/"
<Directory <RAILS BASE PATH>/owm/public>
Options ExecCGI FollowSymLinks
AllowOverride all
Order allow,deny
Allow from all
RailsEnv production
RailsBaseURI "<RAILS BASE URI>"
</Directory>

# We need a rewrite rule here because by default the OWF will use http://<
  server IP>/get_config/<MAC ADDRESS>[.md5]
# to download the access point configuration.
RewriteEngine on
RewriteRule ^/get_config(.+)/$ <RAILS BASE URI>/get_config$1 [L]

<Location "/get_config">
Order Deny,Allow
Deny from all
Allow from <your access point setup network (setup VPN)>
</Location>

<Location "<RAILS BASE URI>/get_config">
Order Deny,Allow
Deny from all
Allow from <your access point setup network (setup VPN)>
</Location>
```

We enable the site with: `a2ensite owm.conf`, and we can see that a symlink to the configuration file is added also to `/etc/apache2/sites-enabled`. Also the following line needs to be added into the content of the file `/etc/apache2/mods-available/passenger.conf`:

```
PassengerDefaultUser www-data
```

To apply all the changes we also need to restart Apache:

```
service apache2 restart
```

For using Google Maps in the application, GMAPS API Key is needed. We created the file `gmaps_api_key.yml` (using the file "gmaps_api_key.yml.example" as an example) into the folder `var/www/owm/config` and we included our own key there:

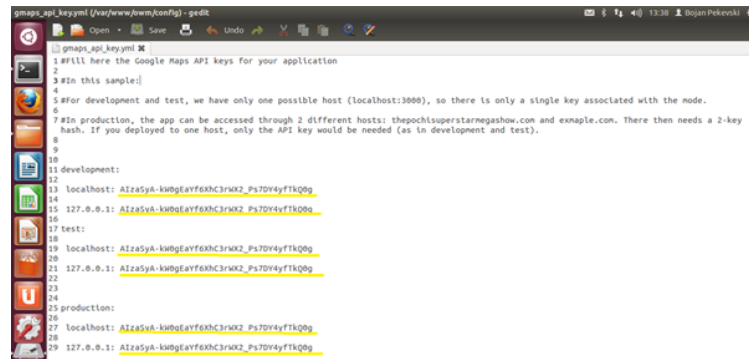


Figure 5.17: gmaps_api_key.yml

The key was created from the Google Developers Console which guides how to do that (<https://developers.google.com/maps/documentation/javascript/get-api-key>).

As stated in the instructions [24], we create startup script (named "owm-daemons") into the folder /etc/init.d:

```

#!/bin/sh
### BEGIN INIT INFO
# Provides:          owm-daemons
# Required-Start:    $local_fs $network
# Required-Stop:     $local_fs $network
# Default-Start:    2 3 4 5
# Default-Stop:     0 1 6
# Short-Description: Starting owm-daemons
# Description:      Starting owm-daemons
### END INIT INFO#

##### Variables for openwisp-daemons #####

# The directory in which all the various OpenWisp
# applications are deployed. Generally it's /var/www
# or /var/rails
OPENWISP_BASE_PATH="/var/rails"

# The daemon you wish to start with this script
# (it must have already been deployed of course).
OPENWISP_APP="owm"

# The Rails environment in which the script must be run.
# It will almost always be set to production.
RAILS_ENV="production"

#####

export PATH RAILS_ENV

# Define LSB log_* functions.
# Depend on lsb-base (>= 3.0-6) to ensure that this file is present.
. /lib/lsb/init-functions

bundle_exec() {
cd $1 && bundle exec $2
return $?
}

```

```
openwisp_daemons_start() {
bundle_exec $OPENWISP_BASE_PATH/$OPENWISP_APP 'rake daemons:start'
}

openwisp_daemons_stop() {
bundle_exec $OPENWISP_BASE_PATH/$OPENWISP_APP 'rake daemons:stop'
}

openwisp_daemons_restart() {
bundle_exec $OPENWISP_BASE_PATH/$OPENWISP_APP 'rake daemons:restart'
}

openwisp_daemons_status() {
bundle_exec $OPENWISP_BASE_PATH/$OPENWISP_APP 'rake daemons:status'
}

case "$1" in
start)
log_daemon_msg "Starting OpenWISP daemon" "$NAME"
openwisp_daemons_start
RET="$?"
log_end_msg $RET
return $RET
;;
stop)
log_daemon_msg "Stopping OpenWISP daemon" "$NAME"
openwisp_daemons_stop
RET="$?"
log_end_msg $RET
return $RET
;;
restart)
log_daemon_msg "Restarting OpenWISP daemon" "$NAME"
openwisp_daemons_restart
RET="$?"
log_end_msg $RET
return $RET
;;
status)
openwisp_daemons_status
RET="$?"
return $RET
;;
*)
echo "Usage: /etc/init.d/$NAME {start|stop|restart|status}" >&2
exit 1
;;
esac

exit 0
```

In order to check if the right gems are installed on our system we enter the following commands into the terminal:

```
gem install bundler
bundle install --deployment
```

Once all the required gems and software is installed as stated in the instructions, we run: `rake db:migrate` to create an empty database and `rake db:seed` to populate the database with default data. After all of these

steps you should have a working OpenWISP Manager. For starting the application we need to start the server first with the following commands:

```
cd /var/www/owm
script/server
```

Then the startup script needs to be run with the following commands:

```
chmod +x owm-daemons
/etc/init.d/owm-daemons start
```

Once both the server and the startup script are started and running we can open our browser and visit localhost:3000 and see the working OWM with its log in page :

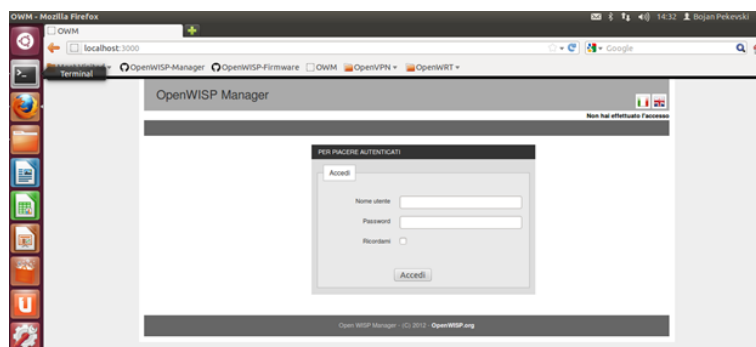


Figure 5.18: OWM log in page

5.4.4 Compiling and installing OpenWISP Firmware

The devices (APs) that we want to manage and control with OpenWISP manager or some other application from the OpenWISP suite, must have installed OpenWISP Firmware on them. OWF is a package included in OpenWRT firmware and in order to work properly we need to compile it ourselves [25]. The OWF package supports an *overlay configuration file*, provided when compiling, in which custom configuration is included. (This file and its structure will be explained further in this chapter).

The procedure for making an installable OpenWRT firmware image, explained on their wiki page [26], is:

- Updating OpenWRT sources.
- Updating and installation of package feeds.
- Configuration of the firmware image we need.
- Building of the custom firmware image. This will automatically compile toolchain, cross-compile sources, package packages, and finally generate an image ready to be flashed.
- Installing the built image to the devices.

In our case we first updated OpenWRT sources:

```
sudo apt-get update
sudo apt-get install build-essential subversion git-core
libncurses5-dev zlib1g-dev gawk flex quilt libssl-dev xsftproc
libxml-parser-perl mercurial bzip2 ecj cvs unzip
```

The last line makes **package installations for Ubuntu 12.04**, installs **git** which is used for downloading of the OpenWRT source code and **build tools** used later for the cross-compilation process. Then the OpenWRT bleeding edge (trunk Version) is downloaded:

```
git clone git://git.openwrt.org/openwrt.git
```

This creates a directory "openwrt" on our system, which is the OpenWRT build system build-directory.

When we have properly configured machine with the prerequisites that OpenWRT needs, we continue as the instructions from OWF suggested [25]. We apply the following steps inside the OpenWRT root directory:

```
cp feeds.conf.default feeds.conf
echo "src-git openwisp https://github.com/openwisp/OpenWISP-
Firmware.git" $>>$ feeds.conf
./scripts/feeds update
./scripts/feeds install openwisp-fw
```

A “feed” represents a collection of packages which share a common location and the following commands check our system for missing packages:

```
make defconfig
make prereq
make menuconfig
```

In this step we choose the wanted configuration for compiling (the right architecture for a certain device) and we also include the OWF package. With the next command we provide the overlay configuration file, and it must be provided with the variable “OPENWISP_CONF”. The file can be local tar.gz file, an url address where the file is located and available for download or a local directory. In our case we stored the file on a Dropbox account and proceeded the link in the following as shown below:

```
export OPENWISP\_CONF="https://www.dropbox.com/s/9gvbs50fwb3hzbq/
etc.tar.gz?dl=0"
```

The structure of this overlay configuration file is explained later in the thesis.

After this we can proceed to the last command for building the firmware image:

```
make
```

The overlay configuration file and its structure

The overlay configuration file has the following structure:

```
etc
├── config
│   └── owispmanager
├── openvpn
│   ├── ca.crt
│   ├── client.crt
│   └── ta.key
└── shadow
```

The content of the file etc/config/owispmanager looks like this:

```
config 'server' 'home'
option 'address' 'my_OWM_server'
option 'port' ''
option 'status' 'configured'
option 'inner_server' ''
option 'inner_server_port' ''

config 'server' 'local'
option 'hide_server_page' '1'
option 'setup_wpa_psk' 'owf_safemode_wpakey'
option 'setup_wifi_dev' ''
option 'setup_httpd_port' ''
option 'setup_ssid' ''
option 'setup_ip' ''
option 'setup_netmask' ''
option 'setup_range_ip_start' ''
option 'setup_range_ip_end' ''
option 'hide_ums_page' '1'
option 'hide_mesh_page' '1'
option 'hide_ethernet_page' '0'
```

The `etc/openvpn/` directory contains the RSA certificates necessary for establishing a successful connection with our own openvpn server. The `etc/shadow` provides a default password for the root user.

The RSA certificates/keys are created during the openvpn installation [27]. First openvpn is installed, then the folder `etc/openvpn/easy-rsa` is created and all needed certificates are created in it [28]:

```
sudo apt-get install openvpn
sudo mkdir /etc/openvpn/easy-rsa/
sudo cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/
openvpn/easy-rsa
```

The server keys are generated next:

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server
cd keys
openvpn --genkey --secret ta.key
```

Some of the keys are copied `/openvpn` directory:


```
cp server.crt server.key ca.crt dh1024.pem ta.key /etc/openvpn/
```

Then the client keys are created:

```
cd /etc/openvpn/easy-rsa/  
source vars  
./pkitool client
```

This creates `client.key` and `client.crt` into the folder `/easy-rsa/keys`. We used the created `ca.crt`, `client.crt` and `ta.key` and copied them into the overlay configuration file which was used for the OWF build.

After the overlay configuration file was provided, as explained earlier, the last task was the making of the firmware image. It was triggered by the command `make`, where the building started and lasted for a quite long time (few hours).

Hands-on experience with the OWF instalation

At the end of the firmware making process we got successfully built image ready for installation. We used TP-LINK AC1750 (Archer C7 architecture) router as the device we would flash with new firmware. Through the web GUI, reachable on 192.168.0.1, we installed the new firmware, but after the reboot the device was unreachable, neither to the supposed new IP address 192.168.1.1 stated in OpenWRT instructions as a default for OpenWRT firmware devices, neither to the old 192.168.0.1 the router had before the firmware flash. After numerous unsuccessful attempts and techniques tried to connect to the router's GUI (other possible IP addresses, Wireshark sniffing, etc.), we concluded that something in the `/etc/config/owispmanager` file, provided through the overlay configuration file, was set wrong and caused the change of the router's default IP address. We have decided to not attempt the same procedure of firmware flash to another device with the same firmware image in order not to get another bricked device. Instead of building an OpenWISP network and managing it with the OpenWISP Manager we decided to analyze the features of previously installed and working

OpenWISP Manager. The construction of an OpenWISP network was left for future work until the problem with the OpenWISP Firmware is resolved.

5.4.5 Demo test of OpenWISP manager

The OpenWISP Manager is suitable for centralized configuration of network with large number of APs. It allows the administrator of the network to create new or easily modify the characteristics of existing WISPs and WISP Servers.

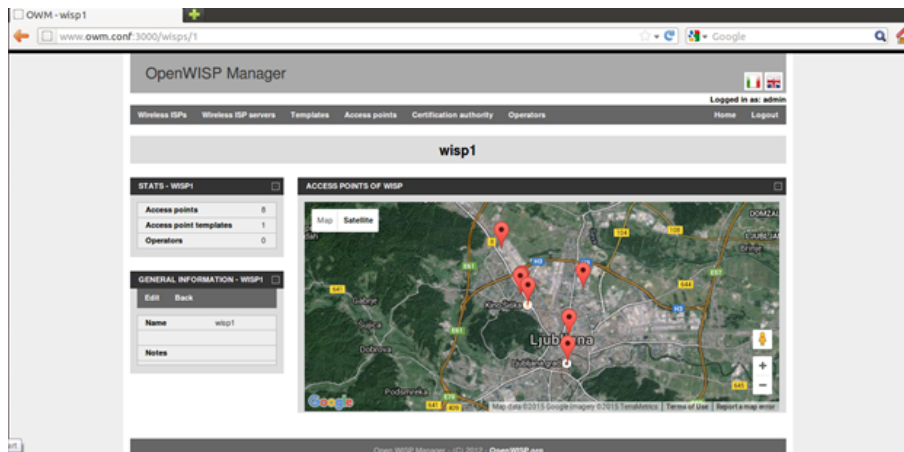


Figure 5.19: OWM home screen

In the created WISP it is possible to create new or adjust existing APs, creating templates of APs for future APs to be labeled, creating different SSIDs on same AP, defining the authentication methods for each SSID, etc.

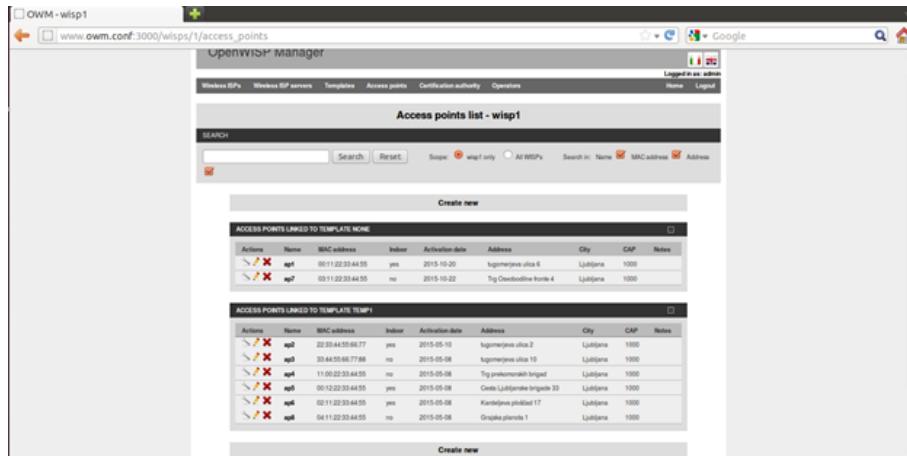


Figure 5.20: OWM, APs list and management

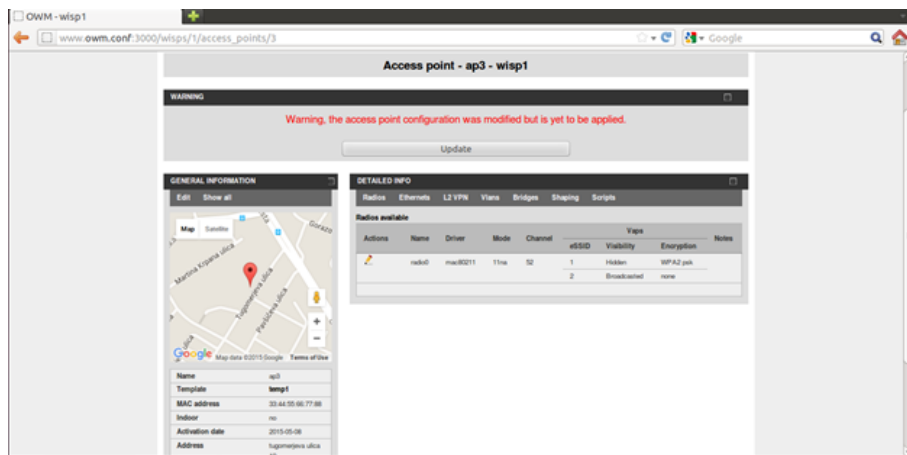


Figure 5.21: OWM, editing configuration of AP

Traffic shaping is also available option that can be defined for each SSID on a certain AP and bandwidth limitations can be set (Figure 5.22).

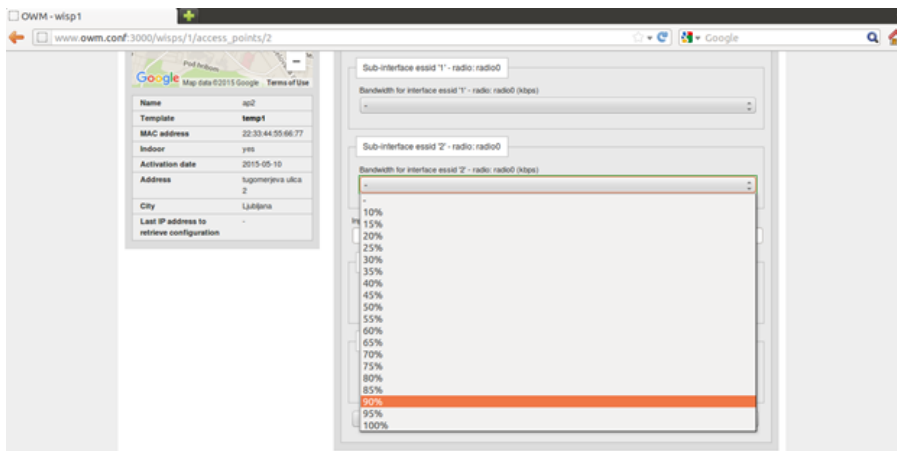


Figure 5.22: OWM, traffic shapping options

Also there are possibilities for defining operators that will be able to enter the application and defining what privileges for modifying they will have.

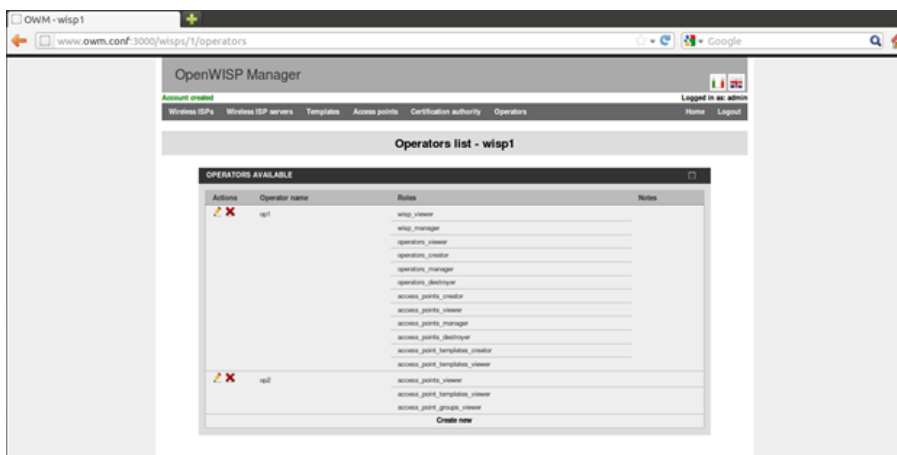


Figure 5.23: OWM, editing operator's rules

The OpenWISP Manager along with its features is a good open-source tool for deploying a WISP and configuring its APs. In combination with all of the other applications that are part of the OpenWISP suite they become a complete solution for deploying, configuring and monitoring of wireless services.

Chapter 6

Conclusion

The importance of the WLAN networks for providing Internet access is enormous and their complexity will continue to grow. That is why it is most important to have quality tools for design and further control and management of such networks.

Through the overview of WLAN architectures and the process of designing a WLAN network we point out the main principles and challenges that should be taken into consideration. Then we analyzed the use of controlled-based architecture for WLAN networks with its main element, the Wireless LAN Controller (WLC). As a standard part of enterprise networks we saw the benefits of using WLC and its variations on the market. Each of the analyzed solutions that we presented has its own benefits and depending on the user's needs and resources can be deployed as an efficient solution. The best performances would come out of the classical hardware solution, but also it will cost much more. The software alternatives can also bring quality performances for lower cost and in some cases they are even better choice. The open-source solution OpenWIPS is not bringing any costs for the user but as any open-source software it can be a little bit more complicated for setup and it is not the best choice for unexperienced users. From what we had chance to see and test, with the proper setup it can be a solid tool for implementing Wi-Fi services.

All in all, the main conclusion is that the WLC will remain to be an important element in WLAN networks and the market demand will just give the direction in which it will evolve and improve.

Bibliography

- [1] Loutfi Nuaymi, “Introduction to Broadband Wireless Access”, *WiMAX-Technology for Broadband Wireless Access*, UK: John Wiley & Sons, 2007
- [2] WildPackets, Inc., “Guide to Wireless LAN Analysis”, *Emerging Technologies in Wireless LANs-Theory, Design, and Deployment*, Cambridge: Cambridge University Press, 2008, pp. 13-38
- [3] The WNDW Authors, *Wireless Networking in the Developing World*, 3rd ed., Feb. 2013
- [4] Matthew Gast, *802.11 Wireless Networks: The Definitive Guide*, Apr. 2002
- [5] Wikipedia, *IEEE 802.11* [Online], Available: https://en.wikipedia.org/wiki/IEEE_802.11, Accessed: 24.10.2015
- [6] Weiping Sun, Munhwan Choi, and Sunghyun Choi, *IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz* [Online], Available: <http://www.mwnl.snu.ac.kr/~schoi/publication/Journals/13-ICT-SUN-rev.pdf>, Accessed: 24.12.2015
- [7] Martin Sauter, *From GSM to LTE: An introduction to mobile networks and mobile broadband*, UK: John Wiley & Sons, 2011
- [8] Jim Florwick, Jim Whiteaker, Alan Cuellar Amrod and Jake Woodhams, *Wireless LAN Design Guide for High Density Client Environments in*

- Higher Education- Design Guide*, Cisco Systems, Inc., San Jose, CA, Nov. 2013
- [9] Jim Geier, *Designing and Deploying 802.11n Wireless Networks*, Cisco Systems, Inc., Indianapolis, USA: Cisco Press, 2010
- [10] Microwave Journal (June, 2005), *WLAN Switch... or Just "Switch"?* [Online], Available: <http://www.microwavejournal.com/articles/828-wlan-switch-or-just-switch>, Accessed: 24.12.2015
- [11] Jeff Smith, Jake Woodhams, Robert Marg, *Controller-Based Wireless LAN Fundamentals*, Cisco Systems, Inc., Indianapolis, USA: Cisco Press, 2011
- [12] Michael McNamee, *Cloud controlled wireless vs. cloud managed WiFi* [Online], Available: <http://www.securedgenetworks.com/blog/Cloud-Controlled-Wireless-VS-Cloud-Managed-Wifi>, Accessed: 06.08.2015
- [13] Jennifer Jabbusch (Jan. 2012), *The 4 Wireless Controller Architectures You Need to Know* [Online], Available: <http://securityuncorked.com/2011/11/the-4-wireless-controller-architectures-you-need-to-know/>, Accessed: 09.08.2015
- [14] Lisa Phifer (Feb. 2011), *Buyer's Guide to Enterprise WLAN Controllers* [Online], Available: <http://www.enterprisenetworkingplanet.com/netsysm/article.php/3924291/Buyers-Guide-to-Enterprise-WLAN-Controllers.htm>, Accessed: 08.10.2015
- [15] Andrew Froehlich, *Cisco wireless controllers: Product overview* [Online], Available: <http://searchnetworking.techtarget.com/feature/Cisco-wireless-controllers-Product-overview>, Accessed: 14.10.2015
- [16] Cisco and/or its affiliates (2014), *Cisco Wireless Controllers At-A-Glance* [Online], Available: http://www.cisco.com/c/dam/en/us/products/collateral/interfaces-modules/services-modules/at_a_glance_c45-652653.pdf, Accessed: 13.10.2015

-
- [17] Ubiquiti Networks, Inc. (2015), *Enterprise technology* [Online], Available: <https://www.ubnt.com/enterprise/technology/>, Accessed: 04.11.2015
- [18] Ubiquiti Networks, Inc. (2015), *Enterprise software* [Online], Available: <https://www.ubnt.com/enterprise/software/>, Accessed: 04.11.2015
- [19] 1A First Alternative, *Revolutionary WiFi with Unifi Ubiquity* [Online], Available: <http://nl.1a-first-alternative.com/revolutionaire-wifi-met-unifi-van-ubiquity.html>, Accessed: 04.11.2015
- [20] Cisco Systems, Inc. (2015), *Out of Band Control Plane* [Online], Available: <https://meraki.cisco.com/trust/#oob>, Accessed: 18.10.2015
- [21] openWISP.org (2012-2015), *What is OpenWISP?* [Online], Available: <http://openwisp.org/whatis.html>, Accessed: 05.05.2015
- [22] openWISP.org (2012-2015), *OpenWISP History* [Online], Available: <http://openwisp.org/history.html>, Accessed: 05.05.2015
- [23] openWISP.org (2012-2015), *OpenWISP Sample architectures* [Online], Available: <http://openwisp.org/architectures.html>, Accessed: 05.05.2015
- [24] openWISP.org (2012-2015), *OpenWISP Manager Installation instructions*, openwisp/OpenWISP-Manager Github Repository [Online], Available: <https://github.com/openwisp/OpenWISP-Manager>, Accessed: 05.05.2015
- [25] openWISP.org (2012-2015), *OpenWISP Firmware*, openwisp/OpenWISP-Firmware Github Repository [Online], Available: <https://github.com/openwisp/OpenWISP-Firmware>, Accessed: 25.05.2015
- [26] OpenWRT, *OpenWrt build system - Usage* [Online], Available: <http://wiki.openwrt.org/doc/howto/build>, Accessed: 05.06.2015

- [27] OpenVPN Technologies, Inc. (2002-2015), *HOWTO* [Online], Available: <https://openvpn.net/index.php/open-source/documentation/howto.html>, Accessed: 05.06.2015
- [28] Super Library of Solutions, *Installing OpenVPN on Ubuntu Server 12.04 or 14.04 using TAP* [Online], Available: <http://www.slsmk.com/getting-started-with-openvpn/installing-openvpn-on-ubuntu-server-12-04-or-14-04-using-tap/>, Accessed: 05.06.2015