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

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

4.3.1 Controller-based Management Only 30
4.3.2 Controller-based with Tra c Tunneling 31
4.3.3 Controller-based with Split TTra c 30

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 o er distributed management and control [9] 19
3.2 Simple small o ce/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

4.4 CAPWAP architecture [11] 28

List of Tables

2.1 Di erent amendments of the 802.11 standard [5], [6]
LANs [2]

Acronyms

ACL Access Control List.

AES Advanced Encryption System.

AP Access Point.

BSS Basic Service Set.

CAPWAP

Povzetek

Iz današnje perspektive Wi-Fi dostop je zelo pomemben za vsakogar. Upo-

Abstract

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 io.0 0992(wth.001(i)5.9b356gh0.998(en)4.001(of)-3

pen34whi5.996(suc)27.0998(34362.997998(34c360.998(en)ral-27.996(t)]ize)1.078ise)-managem

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 o ers we gave

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 signi cant reason for its success. Also the smaller infrastructure cost for the providers in comparison with wired networks is another signi cant reason for the worldwide expansion of the wireless networks. With performance improvement o ering 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

gine and a distribution system medium, which is the backbone network used to relay frames between access points, often called simply the back-

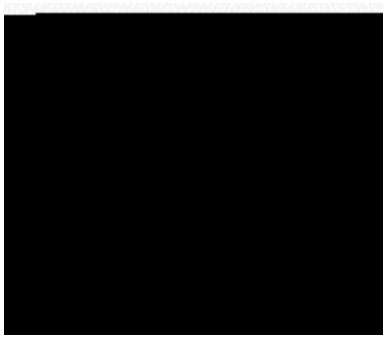

Figure 2.7: Extended service set [4]

2.5 Management operations

Every AP needs to have several parameters set for proper functioning. Two

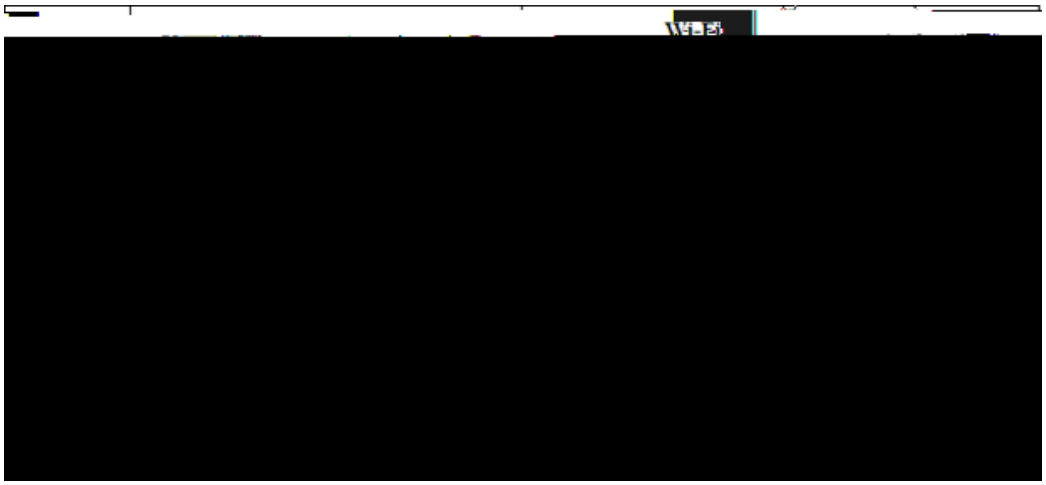

Table 2.2: Encryption methods in 802.11 WLANs [2]

cryption method by the 802.11i working group. It was a temporary solutionfordealingwiththe vulnerabilitiesofWEP,coveringtheexisting equipment, whilethefull standard 802.11i (WPA2) was developed[3]. WPA has two con gurations WPA-PSK (WPA-Personal) and WPA-

Chapter 3

Planning and designing a WLAN network

The right number of APs needed (more or less than the initial plan may be required)

The performance of some applications on the WLAN

634Wrst[(634)-26part[(634)-26in05(64e(n7(cre02fr7)T(634)-26tTd[(634)-26arc)997(n)2hWsict.De[(63

With all the gaheWAn1(erflica(the)-456.condu04(o)1.cthe)unrnWsit9(the)-456.surv97(n)27.eyWre3

5hegh427Td[(s52e)-6(autonomdu04(o)ous.0051e)-42acc.997(0i1e)-45re326(p)-27ime997(n)27s[(s52e)-6(5.

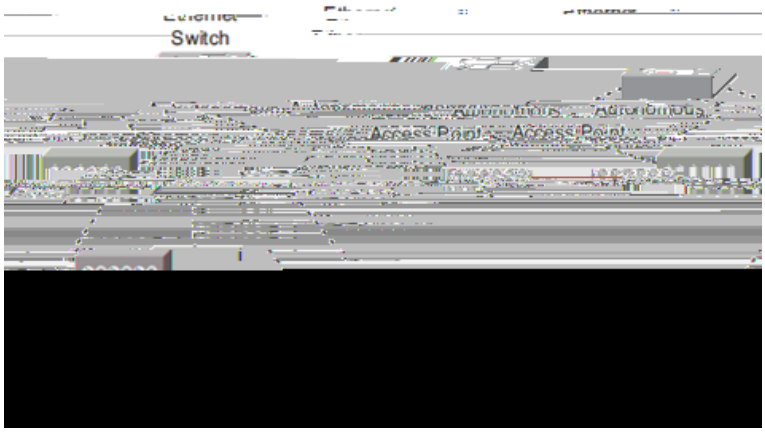

Figure 3.1: Autonomous access points o er distributed management and control [9]

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. men -ns.

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 B14ei45.98(hto)-05.98(c14ei58.005(arc318.005(hitecture)]TJ/ 3.001 w4thcoteus.

Chapter 4

Controller-based wireless architecture and introduction to Wireless LAN Controller

tures. Some of the main capabilities and features that Td[(ture.999(ansuLCres)-289.9shoul(a

cards, 802f11n APs. 3G/4G may be used in case of a failure of the LAN to WAN link.

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 APcome

guest tra c, meaning that authenticated tra c will be send to the wired network and the guest tra c 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 form one protected resource in the network to another.

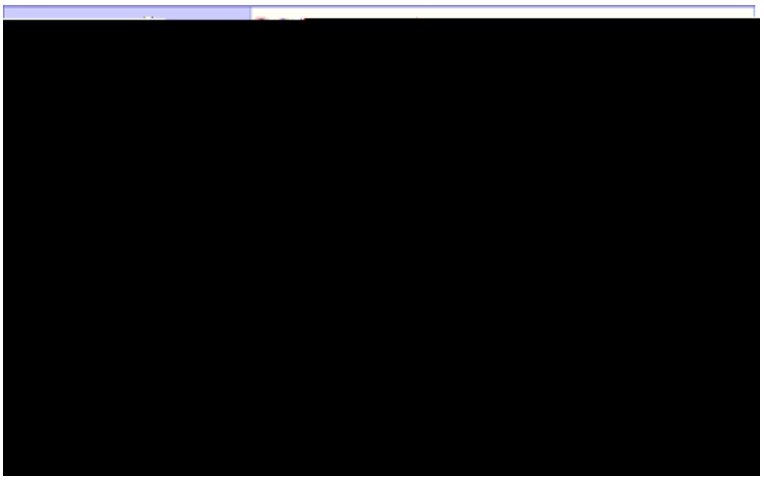

Figure 4.8: Controller-based system with split tra f c [13]eht19.

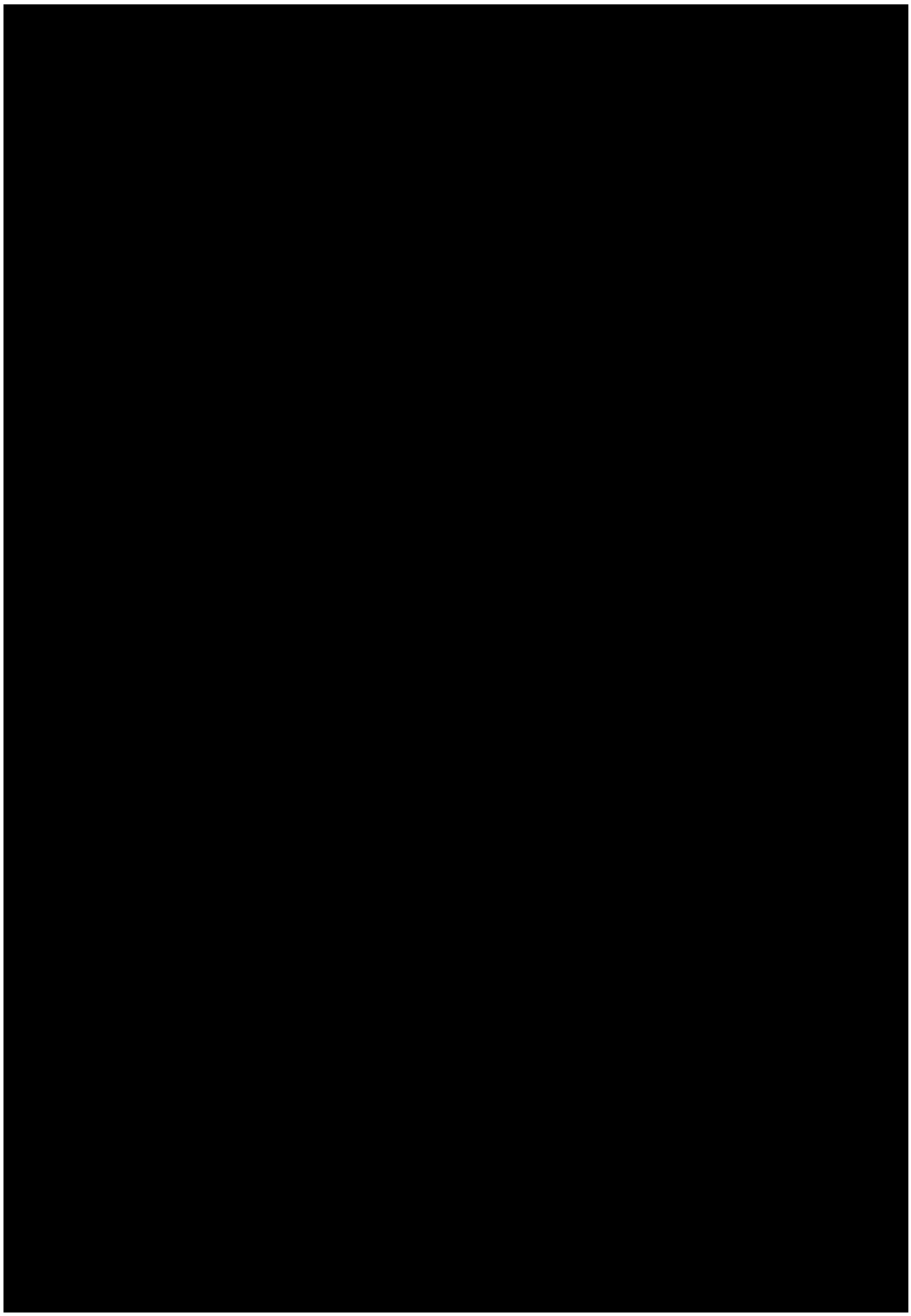

Table 5.1: Summerized information about Cisco controllers [16]

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

2500 Series

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

Figure 5.4: UniFi APs and users lists [19]

Also there are real-time statistics for the current state of the network, tra c, number of clients, etc.(Figure 5.5) which can be used for net(e)-418.002()]TJ-200.1 possibility for setting email notications and alerts fo keeping trac eve1,fOev

5.3 Meraki

Meraki was started by three MIT students (Sanjit Biswas, John Bicket, Hans Robertson) who worked on the MIT *Roofnet*

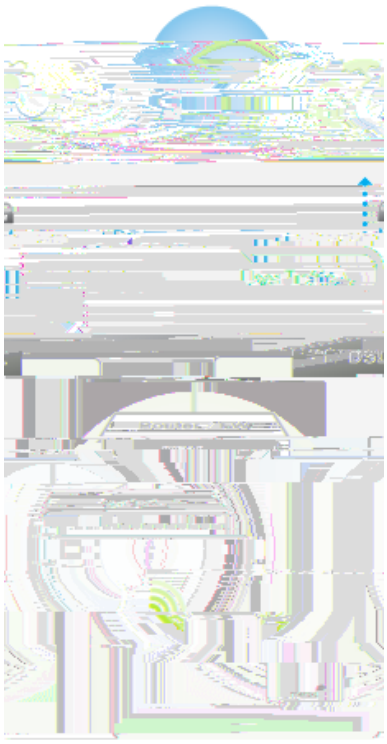

Figure 5.6: Meraki's out of band management architecture [20]

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

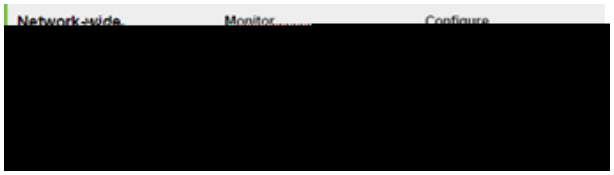

Figure 5.9: Meraki cloud management platform, network-wide tab and it's options

For each client attached to the network we can get a graphical explanation of its tra c, used applications and 7.009(en)26.992(t)-389.998(log)-391.001(with)-389.9

With the summary report we get statistics and graphical presentationl2(li00006-uith)--315.996366(the)-366(r

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 im-

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 net lters.

OpenWISP MiddleWare (OWMW): OWMW is a Sinatra application that helps for connection be-326.996(based)-32 404((O)32.ll404.995(foO-27.001(en,)SP)

Figure 5.14:

Updating OpenWRT sources.

Updating and installation of package feeds.

Con guration of the rmwnagepacagerces.

dati22ustom(t285j)84.996(p)-27.w(pac)27..reME2

[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 Uni Ubiquity* [Online], Available: http://nl.1a- rst-alternative.com/revolutionaire-wi -met-uni -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:,

[27] OpenVPN Technologies, Inc. (2002-2015), *HOWTO*