Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Diploma Thesis

Improvement security, usability and reliability of a business computer network

Bc. Viktor HARNACH

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Bc. Viktor Harnach

Informatics

Thesis title

Improvement security, usability and reliability of business network.

Objectives of thesis

The thesis focuses on analysis of security reliability and usability of business computer network. The main goal is to design and implement improvements for existing computer network. Part of the thesis contains case study of implementing selected solution.

Methodology

The thesis is based on study technology and scientific literature, technological articles and testing and own experience with administrating computer networks. Conclusion of the thesis is made by foundings from case study and analysis of sources.

The proposed extent of the thesis

60 – 80 stran

Keywords

router, security, networks, home, small business,administration, firewall, LAN

Recommended information sources

Free Routing Software: Smoothwall, Ebox, Openwrt, List of Router or Firewall Distributions, Hyperwrt, Clarkconnect, Xorp, Ipcop, Vyatta. 1. Mishawaka: Books LLC, 2010. ISBN 1155199162.

Guide to computer network security. 3rd. New York, NY: Springer Berlin Heidelberg, 2015. ISBN 9781447166535.

HOLT, Alan a Chi-Yu HUANG. Embedded Operating Systems. 1. London: Springer-Verlag London, 2014. ISBN 978-1-4471-6603-0.

NEMETH, Evi., Garth. SNYDER a Trent R. HEIN. Linux administration handbook. 2nd ed. Upper Saddle River, NJ: Prentice Hall, c2007. ISBN 9780131480049.

WONG, Angus. a Alan. YEUNG. Network infrastructure security. London: Springer, c2009. ISBN 1441901663.

Expected date of thesis defence

2017/18 WS – FEM (February 2018)

The Diploma Thesis Supervisor

Ing. Martin Havránek, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 31. 10. 2017	Electronic approval: 1. 11. 2017
Ing. Jiří Vaněk, Ph.D.	**Ing. Martin Pelikán, Ph.D.**
Head of department	Dean

Prague on 19. 11. 2017

Declaration

I declare that I have worked on my diploma thesis titled “Improvement security, usability and reliability of a business computer network" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the diploma thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on 30. 11. 2017

Bc. Viktor Harnach

Acknowledgement

I would like to thank my supervisor Ing. Martin Havránek, Ph.D. for his advices and support during my work on this thesis. Also, I would like to thank Ing. Pavlíčková Petra, Ph.D. and Ing. Alexandr Vasilenko, Ph.D. for their professional consultations.

Vylepšení bezpečnosti, použitelnosti a spolehlivosti firemní počítačové sítě

Souhrn

Práce se zabývá problematikou počítačové sítě konkrétní spolčenosti. Tato počítačová síť má mnoho nedostatků, ať už takových, které omezují uživatele a jejich práci, tak i takových které jsou v rozporu s mezinárodními normami. Zejména se jedná o nedostatky v oblasti zabezpečení, použitelnosti a spolehlivosti.

Hlavním cílem práce je analyzovat současnou situaci, navrhnout řešení a toto řešení aplikovat. Řešení musí splňovat požadavky mezinárodních norem ISO 27001 a 27002 a požadavky vedení firmy.

Vedlejším cílem je popsat krok po kroku celý proces analýzy, výběr vhodných řešení a posléze zařízení nebo služeb tak, aby na základě této práce mohl být postup zopakován pro podobné zadání, pouze s drobnými úpravami.

Klíčová slova: počítačová síť, zabezpečení, spolehlivost, použitelnost, router, multiwan, VPN, malý podnik, Turris Omnia, Cisco Meraki

Improvement security, usability and reliability of a business computer network

Summary

The diploma thesis deals with a topic of a computer network of an existing company. The computer network has several lacks. Starting with those which limit users and their work but also those which are inconsistent with international standards. Those lacks are mainly in areas of usability, reliability and security.

The main goal of this thesis is to analyse current state, design a solution and implement improvements for existing computer network of the selected company. The solution should fulfil requirements of international standards ISO 27001 and ISO 27002.

The other goal is to describe step by step whole process of analyses selecting suitable solution and later selecting devices or services in that manner that the thesis could be used as a guidance for similar projects.

Keywords: Computer network, security, reliability, usability, router, multiwan, VPN, small business, Turris Omnia, Cisco Meraki

Table of content

List of figures

List of tables

1 Introduction

At the end of year 2017, computers and all information technology are more and more important for our work, study etc. Almost in all companies some “IT solution” is used as a support for core business, like accounting, attendance check, elevator control etc. Besides that, many companies use computers also for their core business, which is also a case of the company described in this thesis - the Bär, s. r. o. – hereafter addressed just as the selected company.

A computer without any connection to other computers is rare today. It can be found just in some specific cases because of security or some other reasons (not needed for single purpose device such as an elevator).

Importance of a connection between computers is obvious. In the history, there were several types of how to connect computers, such as bus, ring, star, tree, mash and some others. [1]

In last years the most used network topology is “star” and “tree”, which is extended star. [2]. This topology is also used in the network of the selected company.

1.1 Description of the selected company

The selected company is Bär, s. r. o. A small business which deals with dubbing, voiceover subtitles and similar techniques how to transfer original movies, series and other audio-visual product into Czech language.

The company employs around ten staff members and several collaborators. The staff members are support personal such as an accountant but also core employees such as the director, record technicians, producer executive and so on. External collaborators work as actors (person who says the translated text), translators, modifiers and other.

2 Objectives and Methodology

To design a computer network of a good quality with a long-life expectancy, it is important to plan the network first. It is according to the author's own experience, according to Alton Hardin [3] and mainly according to ISO/IEC 27033-2:2012 - guidelines for the design and implementation of network security.

2.1 Objectives

The main goal of this thesis is to analyse current state of the network in the selected company, design solution and implement improvements. The solution must fulfil requirements of international standards ISO 27001 and ISO 27002.

The main goal will lead to the other goal, which is to describe step by step the whole process of analyses selecting suitable solution and later selecting devices or services in that manner that the thesis could be used as a guidance for similar projects. Obviously, any other company will have different requirements – so criterions will have different weights.

2.2 Methodology

Design of the computer network is not an easy task, so after several modifications, it was decided that this approach will lead to expected objectives:

Current state analyse is based on an expert estimate of the author of the thesis, who has worked at the selected company for almost 5 years. Part of the analysis is also collecting requirements from the company director and other employees.

Based on the analysis there are preselected suitable devices and types of services which are needed to fulfil the requirements and international standards for computer security and information security. From those devices and services, the best possible are chosen using multi-criteria decision approach.

First, important parameters for each category of compared solutions will be identified. Then those criterions should be figured out from a trustworthy source and normalised into a comparable form. Not all the criterions are equally important. Due to that it is necessary to employ a method to measure the importance of each criterion - Saaty's method of weighting criteria. Multiplying weight and normalised value of each parameter will then lead to a set of values which can be substracted and used as a score for the final decision made.

Once the best solution is identified, it should be bought and implemented. The steps of implementing are also part of the practical part of the thesis.

After implementing is done, the maintenance phase starts. In this phase it is required to be flexible, and if some mistake or a bug appears fix it as soon as possible. Because the case study is in the environment of a running business, there must not be any critical bugs which would cause malfunction of the network.

The final phase is to evaluate the implemented solution and discuss benefits for the selected company. Conclusion will be made based on the case study and previous analysis.

3 Theoretical basis

In this section will be introduced technology and individual solutions, which can be used for solving the goal of the thesis. Described technologies will be compared to each other and selected the best solution.

3.1 Network active elements

For communication between computers are necessary both – passive and active network elements. Passive elements are wires, connectors, sockets etc. Those parts are simple, and the thesis will not concentrate on it. The other parts of network communication are possible because of active network elements, such as switch (hub), router, bridge, repeater, access point etc. [4]

3.1.1 Switch

"Most business networks today use switches to connect computers, printers and servers within a building or campus. A switch serves as a controller, enabling networked devices to talk to each other efficiently. Through information sharing and resource allocation, switches save businesses money and increase employee productivity." [5]

Switch is active part of a network which interconnects other network devices, such as PCs, printers, servers, etc. A switch in most cases replaced older and "not so clever" device called hub. Switch works on second layer of the ISO/OSI model in star or tree topology.

Regarding the Cisco [5], there are two basic types of switches. Managed and unmanaged.

Unmanaged switches are usually in home, small business or anywhere, where is not necessary divide network communication. Unmanaged switches do not need any settings. When is the device unpacked, it is already ready to serve, just plug the switch into electricity and snapping the connectors of wanted devices.

Managed switches are configurable. It is possible to divide the network into VLANSs[1], QoS[2], link aggregation etc.

3.1.2 Router

“A router connects networks. Based on its current understanding of the state of the network it is connected to, a router acts as a dispatcher as it decides which way to send each information packet. A router is located at any gateway (where one network meets another), including each point-of-presence on the internet. A router is often included as part of a network switch.” [6]

One of the most important device in network. Without router, todays internet could not exist. The router is device over which must go all data and information which are sent or received to/from another network – internet. Router works on third layer of ISO/OSI network model.

Router usually contains more functions. Typically, NAT[3], bride, AP[4], DHCP[5] server, load balancing, multi wan[6] etc.

NAT is technology which allows connect more than one device to the internet using one internet connection – one IP[7] address. The service works on principle Public and Private IP addresses. Public address is usually one (but can be more) and NAT “remember” which

[1] Virtual Local Area Network

[2] Quality of Service

[3] Network Address Translator

[4] Access Point

[5] Dynamic Host Configuration Protocol

[6] Wide Area Network

[7] Internet Protocol

client communicate with which server. When remote server sends response, NAT based on its “memory” choose correct receiver and sends the response. [7]

Bridge is used to connect two or more technologies into one network. Usually it is Wi-Fi and ethernet, but can be also other technologies such as coaxial wire or other standards.

Access Point to network is such device, which spread the Wi-Fi signal in infrastructure wireless computer networks.

DHCP server take care about delivering some basic information about network and IP address to each connected device. DHCP simplify networking – without DHCP it would have to be this information set in every device.

Multi wan feature on router is useful when a network has more than one internet access. It can be because of request of uninterrupted internet access or because of increasing speed. Of course, also because of both reasons.

3.1.3 **Firewall**

“A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defence in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.” [8]

Regarding ICTsecurity.cz [9], firewall is system for manage network traffic, not just security device. It is difficult to decide whether to choose hardware or software firewall solution for network. The difference is just in that, that hardware solution contains not just firewall software, but also hardware part, which serves exclusively for the firewall purposes. This is the reason why is hardware solution considered as more secure – because the hardware does not share another application which could be thread or vulnerable target. Also dedicated hardware have advantage in higher performance – other application does not take CPU[8] time.

Figure 1 - Cisco Firewall RV 120W
(source: https://www.amazon.com/Cisco-RV120W-Wireless-N-Firewall-802-11b/dp/B003H05UZA)

A firewall is basic security device in network.

3.1.4 Powerline adapter

"Most home theatre components are not in the same room as a home network's router. That wasn't much of a problem until home theatre setups began to include network media players, media streamers, smart TVs, Blu-ray players and other home theatre components are able to access content from the internet and home PCs and media servers. As a result, it is now important to find a way to connect to your router to access the internet and stream photos, music and movies from media libraries on your home network." [10]

Powerline adapter is simple device which modulate the signal from ethernet wire into common electricity wire and then on the other end of electric wire, where the other powerline adapter is it again demodulate the signal back into ethernet. Whole process is transparent so

[8] Central Processing Unit

devices which are connected in such a way cannot even realize that they are not connected just by regular ethernet cable.

“Wireless networking, when it works, is a truly wonderful thing. However, it’s an unfortunate fact that it simply doesn’t work for everyone. This could be for any number of reasons; a lacklustre router, thick walls and floors or wireless interference can all easily lead to Wi-Fi dead zones plaguing your home.” [11]

Based on previous article and authors experience in environment of the selected company, Wi-Fi connection is not as it should be for nonstop use in the same place. It can be good solution for moving devices, but for fixed devices is better choice powerline.

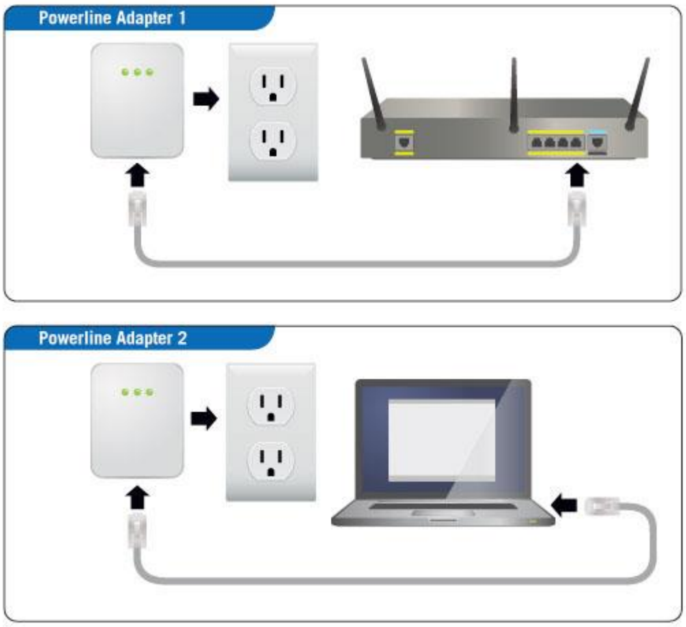


Figure 2 - Powerline adapters (source: https://www.lds.org/help/support/bc/clerksupport/image/article-images/PowerLine.jpeg)

3.1.5 Gateway

“Gateways are more versatile devices than routers. They perform protocol conversion between different types of networks, architectures, or applications and serve as translators and interpreters for network computers that communicate in different protocols and operate in dissimilar networks, for example, OSI and TCP/IP. Because the networks are different with different technologies, each network has its own routing algorithms, protocols, domain name servers, and network administration procedures and policies. Gateways perform all the functions of a router and more. The gateway functionality that does the translation between different network technologies and algorithms is called a protocol converter.” [12]

3.2 Proposed network devices

In this chapter will be listed some of network devices which could be used in the final solution as a main network device in the network. Mainly it is about gateway with multi wan ports, router and configurable switch. Some of devices have also wireless access point.

3.2.1 Turris Omnia

Turris Omnia is high-performance device which is primary router, but because of formidable accessories also multi-functional server.

Omnia was developed by Czech association CZ.NIC. This association oversees Czech top-level domain – ".cz". Also, some other activities including development of the DNSSEC technology, public education courses, "moved" service are products of CZ.NIC.

Figure 3 - Turris Omnia router
(source: https://omnia.turris.cz/cs/)

Association CZ.NIC developed first Turris as a part of service Turris. This service helps users with protection of their networks using mentioned device – router Turris. The service is free – non-profitable research project of the association.

Every user of the Turris service receives the router. Even the first Turris was powerful device, so next to common functions of home routers Turris analyses the traffic between local network and the internet. If the device detect suspect activity in the communication, notifies the Central (server which is obviously hosted by CZ.NIC). The Central has information from all the Turris routers, so if it detects threat, it distributes information and set of rules to whole Turris network. All networks covered by Turris routers are than protected from this threat.

On the beginning of the Turris was the service and Turris – the router. Today is the first router known as Turris 1.0, its evolution as a Turris 1.1 and today´s latest model as a Turris Omnia.

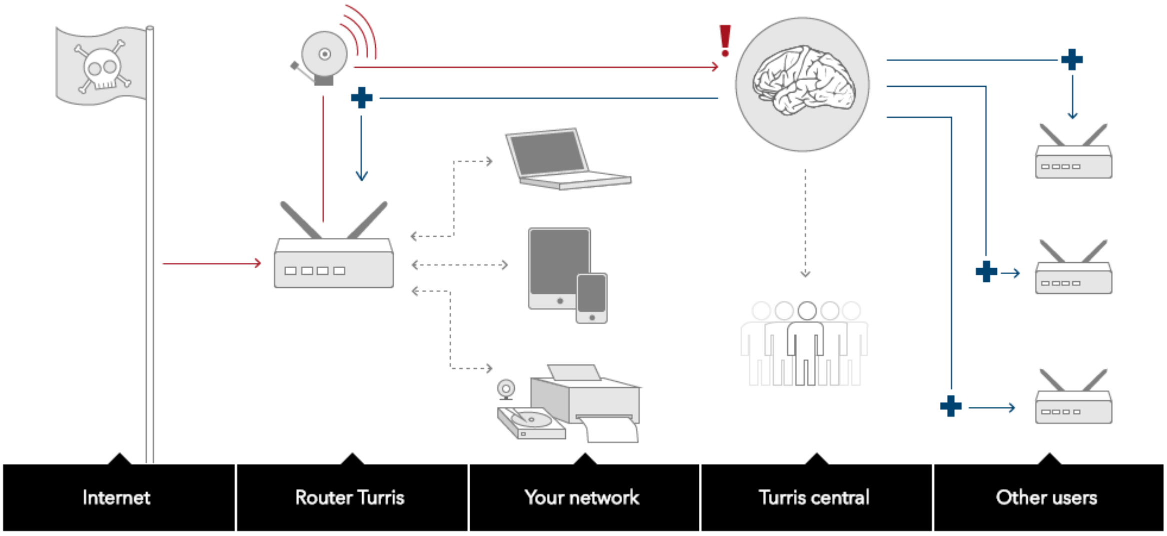


Figure 4 - Scheme of Turris network
(source: https://www.turris.cz/en/)

The first Turris was distributed to enthusiastic public of Czech Republic. It was possible to enter the project entering credentials on website of CZ.NIC and if you fulfilled necessary conditions, you could gain opportunity to participate and get the router for 1 CZK. The main conditions were [13]:

- The Turris router must be used as main gateway the internet (of the user network).
- User must have public IP address from his ISP[9].
- If user network needs any modem for internet connection, the modem must be fully transparent – in bridge mode.

[9] ISP – Internet Service Provider

- The router must be connected to the internet and turned on non-stop (there is some extra time for electricity blackouts, moving etc.).

The decision, if you get the opportunity was made based on population distribution - your geographical location, who is your ISP and how big the provider is (how many clients does he have). The CZ.NIC association wanted to have similar distribution of routers in homes as is distribution of internet access points in Czech Republic [13].

Hardware of those two routers was quite similar [14]. The main difference was adding USB 3 to newer version.

In the end of year 2017 is Turris Omnia the latest device of Turris family. Omnia was first commercial Turris router. Founds for development was gain in crowdfunding campaign on portal Indiegogo (https://www.indiegogo.com/). Currently is possible buy Omnia in retail stores such as alza.cz, amazon.de etc.

Hardware of Turris Omnia is powerful. Inside there is dual-core ARM CPU on 1.6 GHz, 1 or 2 GB DDR3 RAM, 8 GB internal flash storage, 6 Gait ports, 1 SFP port (which can only replace one of Giga bits ports), 2x USB 3.0, 3x Mini PCI Express (one of them can support mSATA, two of them are used for Wi-Fi cards), WIFI 3x3 MIMO 802.11ac, WIFI 2x2 MIMO 802.11b/g/n, SIM card slot, RTC with battery backup, crypto chip for generation secure random number, dimmable RGB LEDs, pin headers with GPIO, I^2C, SPI and more [15].

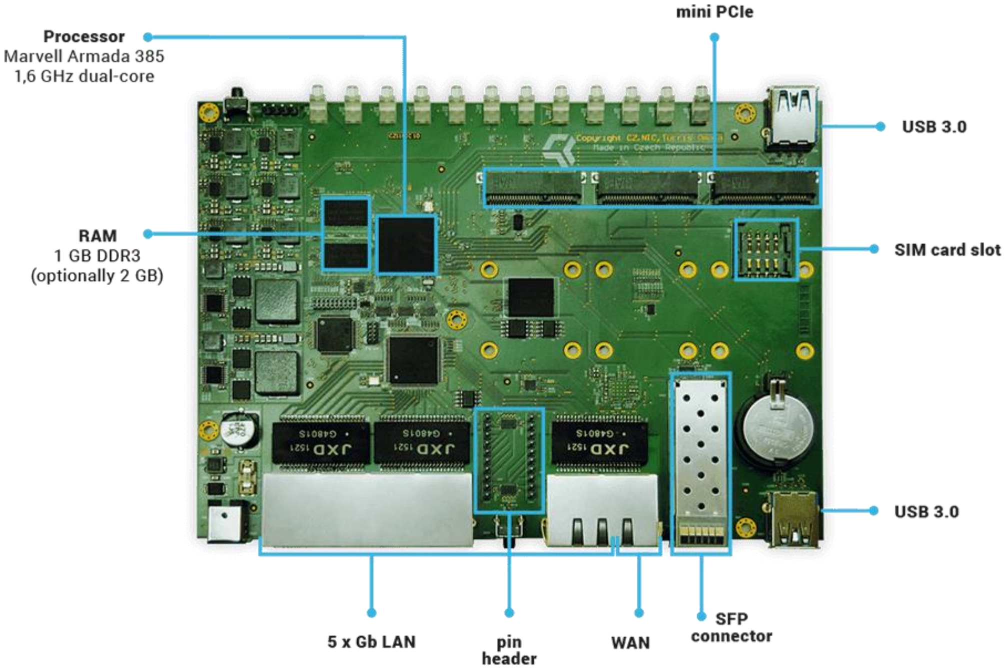


Figure 5 – Motherboard of Turris Omnia

(source: https://omnia.turris.cz/en/)

3.2.2 **CISCO RV320**

“The Cisco RV320 Dual Gigabit WAN VPN Router is the choice for any network in which performance, security, reliability, and adaptability top the list of requirements. The Cisco RV320 supports two connections to one service provider, delivering high performance by using load balancing, or to two different providers to deliver business continuity. High-capacity virtual private networks (VPNs) connect multiple offices and enable dozens of employees to access the information they need from any geographic location just as securely as if they were working at your main office.” [16]

Figure 6 - Cisco RV320

(source: https://www.cisco.com/c/en/us/products/collateral/routers/rv320-dual-gigabit-wan-vpn-router/data_sheet_c78-726132.html)

This router by Cisco company is device perfect quality based on testing of SmallNetBuilder.com [17]. The device has a lot of useful features such as 4 LAN 1Gbit/s ports, 2 USB 2.0 ports which can be used for 3G/4G modem, dual wan failover and load balancing mode (2x RJ 45), VLAN capable switch, QoS, SPF Firewall, DMZ functionality, VPN server (up to 10 clients), IPv6 support. All this is in nice web interface. There are no often reported troubles with this router. Last firmware was released on 15th September of 2017 which shows that Cisco still takes care about the router.

3.2.3 ZyXEL ZyWALL USG 40W

Regarding Small Net Builder [18], ZyWall 40W is one of the top all-in-one devices for small business. ZyXEL has 5 RJ-45 ports. One for WAN, one is configurable – another WAN or LAN and three others are for LAN. Those ports can be used for VLANs – up to eight different. Also, there is one USB port for 3G/4G modem for backup internet connection. ZyXEL supports IPv6. Routing ways are PPPoE, static routing, RIPv1/v2, policy-based and more. Wi-Fi part of the router is on 2.4 GHz, but in higher model (USG60W) can be dual band. Radius authentication is present. VPN server support two-step authentication and full tunnel mode.

“The ZyXEL USG Performance Series delivers enterprise grade Next Generation Firewall security without the hefty price tag.

It provides deep, extensive protection and effective control of Web applications-like Facebook, Google Apps and Netflix-with such anti-malware protection mechanisms as firewall, Anti-Virus, Anti-Spam, Content Filtering, IDP and Application Patrol.

Newly added Content Filtering 2.0 supports Geo IP Blocking to help propel detection rates from strength to strength. No longer do small businesses need to worry about threats, spam or social networking sites decreasing productivity.” [19]

Figure 7 - ZyXEL USG4W
(source: http://shop.zyxel.cz/upload/katalog/1626b_1.jpg)

3.3 Centralisation of the network

For network where are just couple computers is usually no need to employ any centralized network management tool. In larger networks, however, centralised solution can save a lot time for network administrator, and in some cases, it enables elsewise impossible settings.

There are two main types of how can be network administrate centralised. Cloud based solutions, such as MDM[10] or EMM[11]. And local, such as Windows or Linux server.

3.3.1 MDM

"Mobile device management (MDM) is the administrative area dealing with deploying, securing, monitoring, integrating and managing mobile devices, such as smartphones, tablets and laptops, in the workplace. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise, while simultaneously protecting the corporate network." [20]

Mobile device management tools are primary use for mobile devices such as mobile phones, tablets and laptops. However, there is no limitation use it also on desktop PC if OS[12] of the device is supported by specific MDM tool.

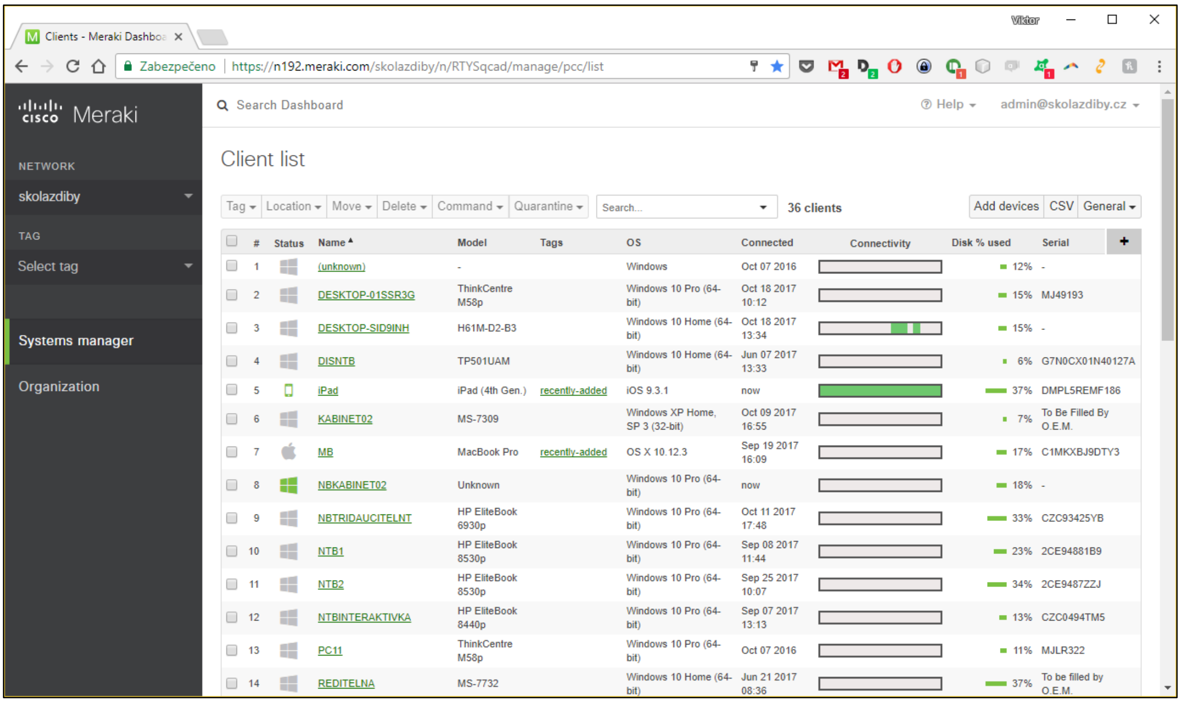
3.3.2 Cisco Meraki

"Cisco Meraki offers the only solution that provides unified management of mobile devices, Macs, PCs, and the entire network from a centralized dashboard. Enforce device security policies, deploy software and apps, and perform remote, live troubleshooting on thousands of managed devices." [21]

[10] Mobile Device Management

[11] Enterprise Mobility Management

[12] Operating System



#	Status	Name	Model	Tags	OS	Connected	Connectivity	Disk % used	Serial
1		(unknown)	-		Windows	Oct 07 2016		12%	-
2		DESKTOP-01SSR3G	ThinkCentre M58p		Windows 10 Pro (64-bit)	Oct 18 2017 10:12		15%	MJ49193
3		DESKTOP-SID9INH	H61M-D2-B3		Windows 10 Home (64-bit)	Oct 18 2017 13:34		15%	-
4		DISNTB	TP501UAM		Windows 10 Home (64-bit)	Jun 07 2017 13:33		6%	G7N0CX01N40127A
5		iPad	iPad (4th Gen.)	recently-added	iOS 9.3.1	now		37%	DMPL5REMF186
6		KABINET02	MS-7309		Windows XP Home, SP 3 (32-bit)	Oct 09 2017 16:55		7%	To Be Filled By O.E.M.
7		MB	MacBook Pro	recently-added	OS X 10.12.3	Sep 19 2017 16:09		17%	C1MKXBJ9DTY3
8		NBKABINET02	Unknown		Windows 10 Pro (64-bit)	now		18%	-
9		NBTRIDAUCITELNT	HP EliteBook 6930p		Windows 10 Pro (64-bit)	Oct 11 2017 17:48		33%	CZC93425YB
10		NTB1	HP EliteBook 8530p		Windows 10 Pro (64-bit)	Sep 08 2017 11:44		23%	2CE94881B9
11		NTB2	HP EliteBook 8530p		Windows 10 Pro (64-bit)	Sep 25 2017 10:07		34%	2CE9487ZZJ
12		NTBINTERAKTIVKA	HP EliteBook 8440p		Windows 10 Pro (64-bit)	Sep 07 2017 13:13		13%	CZC0494TM5
13		PC11	ThinkCentre M58p		Windows 10 Pro (64-bit)	Oct 07 2016		11%	MJLR322
14		REDITELNA	MS-7732		Windows 10 Home (64-bit)	Jun 21 2017 08:36		37%	To be filled by O.E.M.

Figure 8 - Cisco Meraki Dashboard

Meraki solution have huge advantage – in company with less than 100 devices it is free of a charge. [22] That could be the key decision factor in small companies which does not have huge monthly budget for such solutions.

All main features such as support of all major OS, BYOD[13] mode for devices, centralized mobile App management, centralized storage for Windows apps, mobile profiles (different settings for respective devices, based on tags, owner and other symptoms), Security Policies, Geofencing Policies and more are present. Also, one important and useful feature – Remote Desktop access to any of enrolled PC.

The main pros and cos by Tom’s it Pro [23]:

Pros: “Excellent user interface with fast device search; Addresses needs of small businesses more than other products tested; Easy to get up and running fast; Low internal (people) overhead to administer.”

[13] Bring Your Own Device

Cons: “Extensibility not a strong suit; Mobile Application Management missing and Content Management lacking; Features absent to avoid bumping heads (competitive overlap) with Cisco Enterprise.”

3.3.3 VMware AirWatch

Based on Tech Target [24], there are two major providers of EMM. EMM is extended MDM, which was explained in previous chapter. Enterprise Mobility Management combines Mobile Device Management, MAM[14], MCM[15], MIM[16], wireless networks and other business mobile computing services.

“Traditional approaches to Windows management are complex, costly and restrictive. Provisioning devices requires time consuming rip-and-replace imaging. Management is largely driven by Group Policies (GPOs), done on premises and only possible for network or domain-joined PCs. Before Windows 10, major OS updates were less frequent, and feature and security patches were put through extensive compatibility testing.” [25]

“With VMware AirWatch and Windows 10, a fundamentally different, cloud- and mobile-centric approach to simplify management and security is possible. Rethink traditional management practices and adopt unified endpoint management (UEM) as the standard management tool for any device running Windows 10.” [25]

[14] Mobile Application Management

[15] Mobile Content Management

[16] Mobile Identity Management

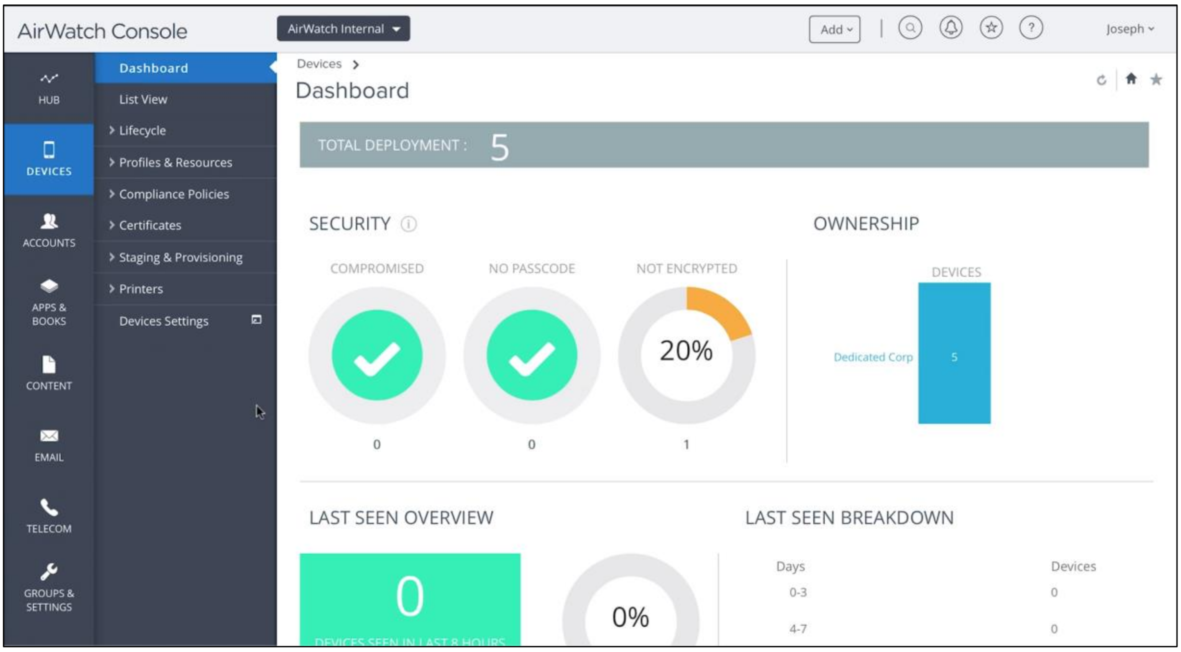


Figure 9 - AirWatch Dashboard

(source: https://www.dropbox.com/business/app-integrations/vmware-airwatch)

For secured access, AirWatch contains app catalogue where user can see all available applications which are available (allowed) in his company. Also, there is Content locker app which stores all business data, so business data such as word documents, pdfs, email attachments etc., are not mixed with personal data of employees. In case of lost or stolen device can corporate IT EMM remotely wipe the device, so the business data are protected from compromise or stolen. The data in Locker are of course encrypted so even if the internet connection is lost and remote wipe command cannot be performed, business documents are still protected.

Another feature are automatic reports based on symptoms of all devices. Some are All devices, compromised devices, offline devices. Those automatic reports use subscription, so the report can be regularly sent to specific user or to Business intelligence chosen user from other connected system.

AirWatch has also hundreds of predefined actions in case of fulfilment set conditions (location, lost flag, offline time length etc.). Every actions and conditions change are tracked and stored to meet audit and corporate standards. [26]

The price per one user is approximately 60 USD per year. [27]

3.3.4 Citrix XenMobile

“Deploy Citrix XenMobile in as little as two hours and get full access to mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), secure network gateway, and enterprise-grade mobile productivity apps in one comprehensive enterprise mobility management solution. XenMobile enhances the user experience on BYO or corporate devices, without compromising security.” [28]

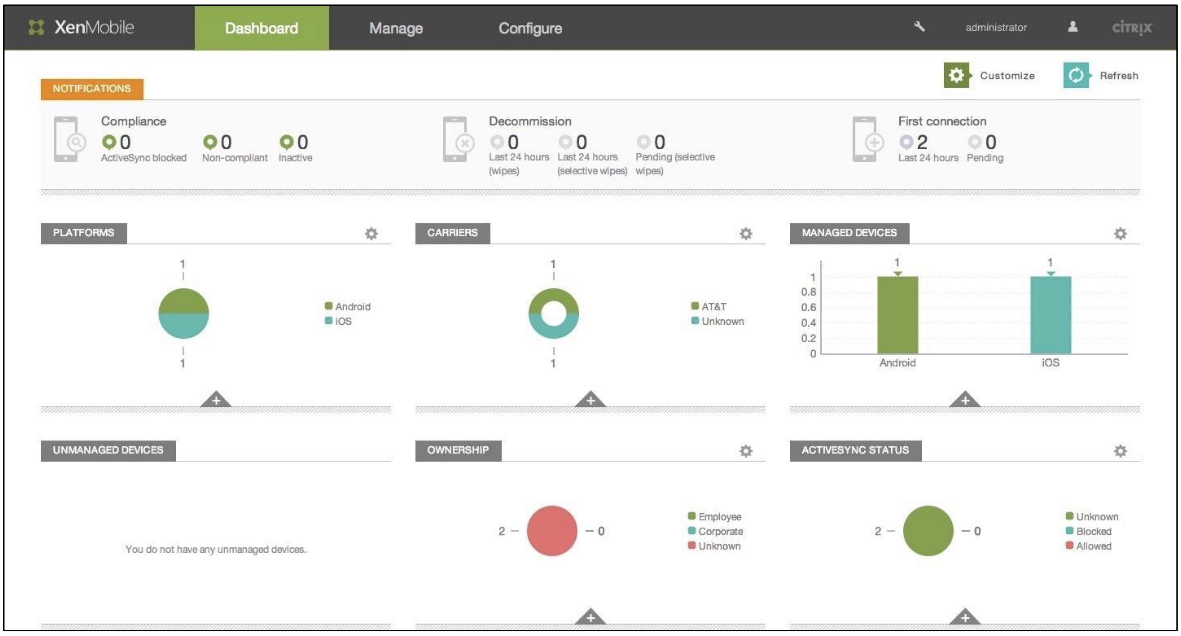


Figure 10 - XenMobile Dashboard
(source: https://www.citrix.com/blogs/2015/01/13/ten-benefits-xenmobile-10-offers-to-channel-partners)

XenMobile contains OS configuration management, remote wipe, application provisioning and more. „XenMobile EMM uses its WorxMail app to provide a containerized environment in which corporate data can safely interact with other Worx apps, such as those for note taking and file sharing.” [24]

The price for one user (max 10 devices per user) is 79 USD per year. [27]

3.4 Related ISO norms

In order to have secure, reliable and usable network is recommended to follow international standards. Those standards will ensure that during designing the network will not be omitted important steps or procedure.

ISO/IEC 27001 is information security standard which describes how should be information stored and protected inside of a company. In other words, instructions for establishing ISMS[17] - framework for best practices how to handle information security. Purpose of the standard is to preserve confidentiality, integrity and availability of the information base within a company.

Confidentiality in this case mean that only authenticated person with correct rights – with authorisation can access the information. Other attempts to reach the information must be denied. Integrity extends confidentiality and adds requirement for hold the state of the information in that stat, in which was left by authorised user. No data can be lost, modified, added or anyhow changed without necessary rights – authorisation. Also, information cannot be modified into state in which is not usable anymore or into state in which cannot be. Requirement for availability is about to not deny or not allow to access the information to any user who has necessary authorisation. This must not be due to any reason (system shutdown, breakdown, power outage etc.). [29]

The standard includes 133 controls and is divided into 8 main chapters and several subchapters. In a frame of information security, the standard and the ISMS contains best practises how to train employees, how to test the security or even how to prepare the data basis against nature disaster. Identified are also advices which information should be protected, why it should be protected, how to protect it and what can happen in case of failure of the duty. [30]

Another international standard is ISO/IEC 27002, which is close related to ISO/IEC 27001. Based on [31] is ISO 27002 is kind of guidance how to achieve ISO 27001

[17] Information Security Management System

certification, list of best practises. Also 27001 is formulate what you must to do to achieve certification, in 27002 is written what you should do.

Information Security Policy is the first class of ISO 27002 and its objective is "To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Based on [32] "Management should set the policy and visibly demonstrate commitment to information security. The policy should be in accordance with business requirements and relevant law and regulations. "

Once is the policy finished, it should be documented and approved by the top-level management of the organisation. Also, the norm reminds that just creating policy will not be sufficient while the policy is not communicated to all employees who could be influenced by the policy.

Policy document should contain [32]:

- Definition of Information Security and business objectives
- Statement of management intent in line with business strategy
- Framework for controls, including risk management
- Definition of responsibilities
- References to other policy and procedure documents
- Specific security policies, compliance requirements and violation consequences (Use/misuse of IT assets, Password control, use of e-mail and internet, Anti-virus maintenance, Other technical and non-technical policies (like clear desktop or locking computer in non-presence))

After setting and approving such policy it is necessary to continual improve it – PCDA[18]. The reviews should be at least annually, but also any time when there are any significant changes that could impact the policy. More often is in this case better.

[18] Plan – Do – Check - Act

4 Practical part – selecting solution

The company has two buildings. The main – the headquarter and two of three studios is in location “Na Borové” and the other one – with one studio is in “Spořilov” location.

4.1 Starting state of the network

For recording the audio output is used always one computer, which is on recommendation of the authorized supplier, disconnected from the internet. Specialized software and hardware are from The Merging company and its Pyramix software (http://www.merging.com/products/pyramix). This – recording – part is fully equipped and serviced by certificated supplier, so those computers will be excluded from the thesis.

After recording technician records whole work, he moves recorded data onto some storage media and physical brings it to the headquarters, in case of the Spořilov studio. In case of Na Borové, the technician copy files to company’s NAS[19]. Than is recorded audio uploaded directly to FTP[20] server of buyer.

In network at starting state are two kinds of devices. Devices which belongs to the company and are used for business, and devices which belongs to employees and collaborators and are not used for business. Company’s devices are PC[21], network printer,

[19] Network Attached Storage

[20] File Transfer Protocol

[21] Personal Computer

laptops, router, AP[22], switch, NAS etc. The rest devices on network are private devices, usually smart phones or PDA[23] connected via Wi-Fi[24].

Those devices are all connected to the internet by common home router TP-Link. This router provides some other services such as DHCP[25] server, but mainly routing and broadcasting Wi-Fi signal. The only exception from this is the PC of the director. Director's PC have two ethernet card and in case of failure he can access the internet using another ISP[26].

Because number of connected wired computers, one 16 port switch is present. Manufacture is also TP-Link, the switch is not possible to configure anyhow – it is just basic model with 1Gb/s speed on every port.

In mezzanine of headquarters there is network printer. Unfortunately, in mezzanine is no wired network, so printer is connected to the network by AP in client mode.

Another network device is NAS server with 4 hard drives. It is Western Digital My Cloud X4. The NAS is used as a transhipment. The staff download movies to the NAS for recording technics and recording technics sends back recorded audio track.

4.1.1 Services

The company is small, so they communicate via common mail account which they share all. They use protocol pop3 so once the email is downloaded from server, there is no way how to manage it between computers. Also, there is absence of syncing sent emails.

[22] Access Point

[23] Personal digital assistant

[24] Wireless fidelity

[25] Dynamic Host Configuration Protocol

[26] Internet Service Provider

In the network there is no domain controller, therefore windows work group and windows home group are used to simplify sharing network resources.

4.1.2 Starting Topology

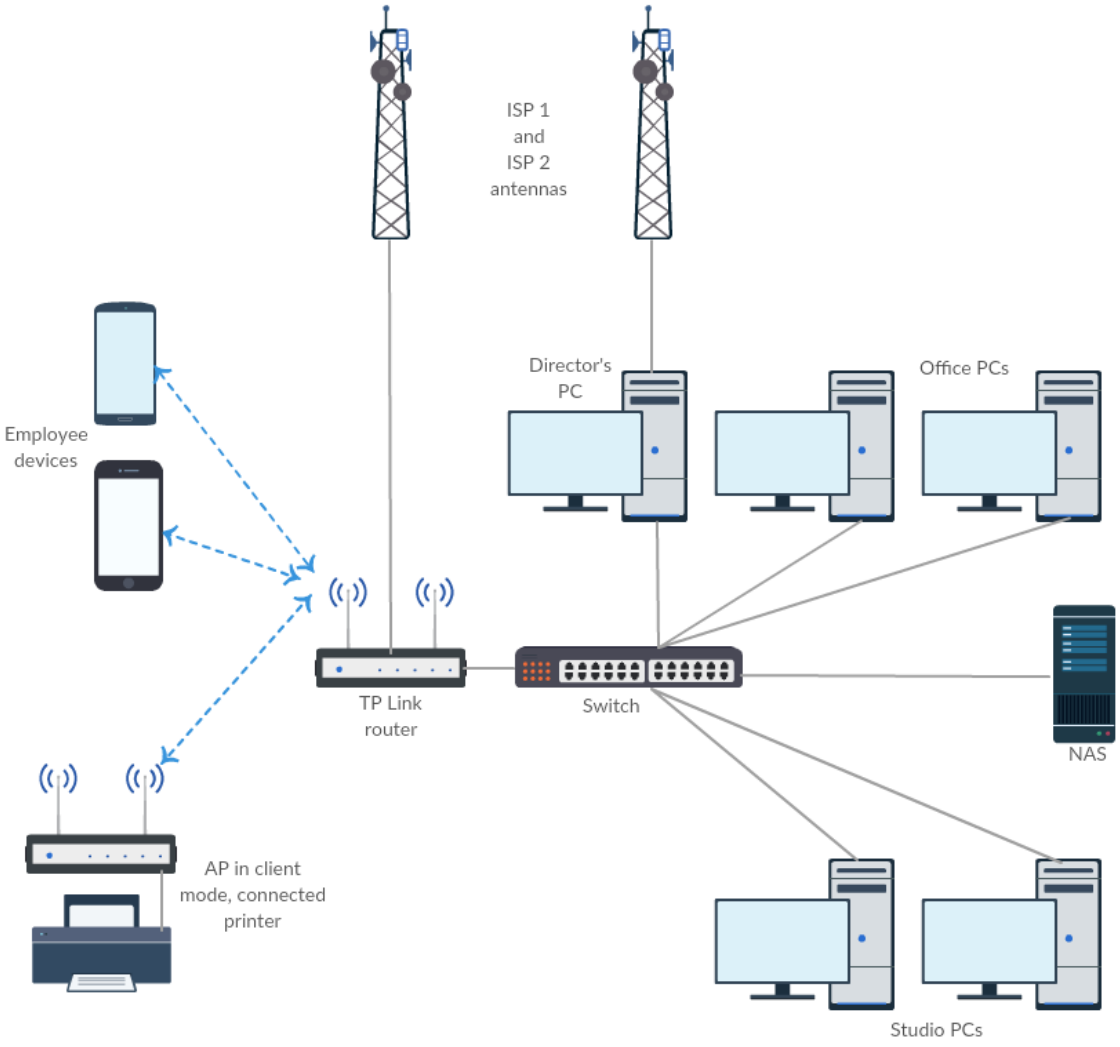


Figure 11 - Topology, starting state

(author: Viktor Harnach)

4.2 Requirements

This task is not solved just on academic level. The network and users are real. Therefore, all changes must follow the company (and its employees) needs and requirements. Besides that, in case of doing such changes, it is useful to search for “right” solution. “The right” solution should by based on international standards. Standards which are influencing these tasks are ISO 27001 – 27005, especially 27002:13.1 [33]

All needs came from some trouble with current state or wish for update.

4.2.1 Current state problems

- All devices share one network – security risk
- Access to NAS is slow (when two or more people are accessing at the same time)
- No backup internet connection for the rest of the network (only for director)
- The backup connection of director is almost all the time not used – wasting of payed and not used capacity
- Primary either secondary internet connection is not fast enough
- Recording technician from Spořilov studio must physically arrive and bring recorded data on data storage to submit their work

4.2.2 Expected future needs

- Possibility for some of office staff work from home – home office
- Centralized computer administration

4.2.3 Requirements based on problems and needs

- Dividing network into separate subnetworks, so that vulnerable devices which the company does not have under control are not dangerous for business (based on ISO 27002 13.1.3)
- Increase speed connection between NAS and switch, or modify the connection, so the speed would be sufficient

- Use both internet connection together for whole network. In normal conditions for increasing speed, in case of failure one of the connection to ensure that the company can continue and upload their production
- Prepare VPN[27] solution
- Implement some tool for centralized administrating of enrolled devices
- Create channel between both buildings for easy sharing

4.3 Selecting suitable solution – network gateway

In previous chapters were introduced some devices and services which should be good choice to fulfil requirements from chapter 4. This chapter will explain the way how was selected the network device and centralised network solution.

Both solutions must be selected based on several criterions. For this case is necessary to use some method for objective comparing.

In case of this diploma thesis, it was decided that Saaty's matrix will be used for generating individual weights for particular parameters.

4.3.1 Choosing of parameters

Parameters for comparing network device gateway/router were selected base on expert estimate author of the thesis and based on requirements for future state of the network. The compared parameters are:

- Switch speed (maximum speed of each individual port of the switch)
- # RJ-45 ports (how many ports on the switch are present – how many other devices can be connected to the particular device)
- Configurability of all ports (whether are all ports fully configurable for which purpose will be used – in which VLAN, or WAN)

[27] Virtual Private Network

- VLAN capability (whether is switch capable to divide ports between Virtual Local Area Network)
- Wi-Fi dual band (in case of Wi-Fi access point, if the AP can transmit in both Wi-Fi standardised zones – 2.4 GHz and 5 GHz)
- Wi-Fi guest network (if is possible on AP have at least two separate SSIDs and wireless networks for separate internal and external devices)
- VPN basic (whether is on the devices present Virtual Private Network server and whether is this feature included in purchase price)
- VPN advanced (rating of security, stability and other parameters of presented VPN solution)
- Multi-wan functionality (whether there is possibility to use multiple Internet Service Providers at the same time for load balancing and for failover use. Also, how many ISPs can be used at the same time – USB modems excluded)
- USB LTE backup (possibility of connecting 3G/4G USB modem for failover use)
- Extension possibility (how can be the device extended if need be – hardware extension and/or software package/service which could be added)

In those parameters is on purpose excluded one parameter – purchase price. The reason why is that for company decision are important usually annual or monthly common expenses. One-time expenses are usually budgeted in interval, as it was in this case. The one-time expense could be at maximum 10 000 CZK.

4.3.2 **Evaluating**

In evaluating the network device was considered all parameters and based on the official numbers from official sources was created table with all values.

The data sources for Turris Omnia 1 GB Wi-Fi are:

- https://omnia.turris.cz/cs/#features
- https://www.alza.cz/turris-omnia-1gb-d4480216.htm

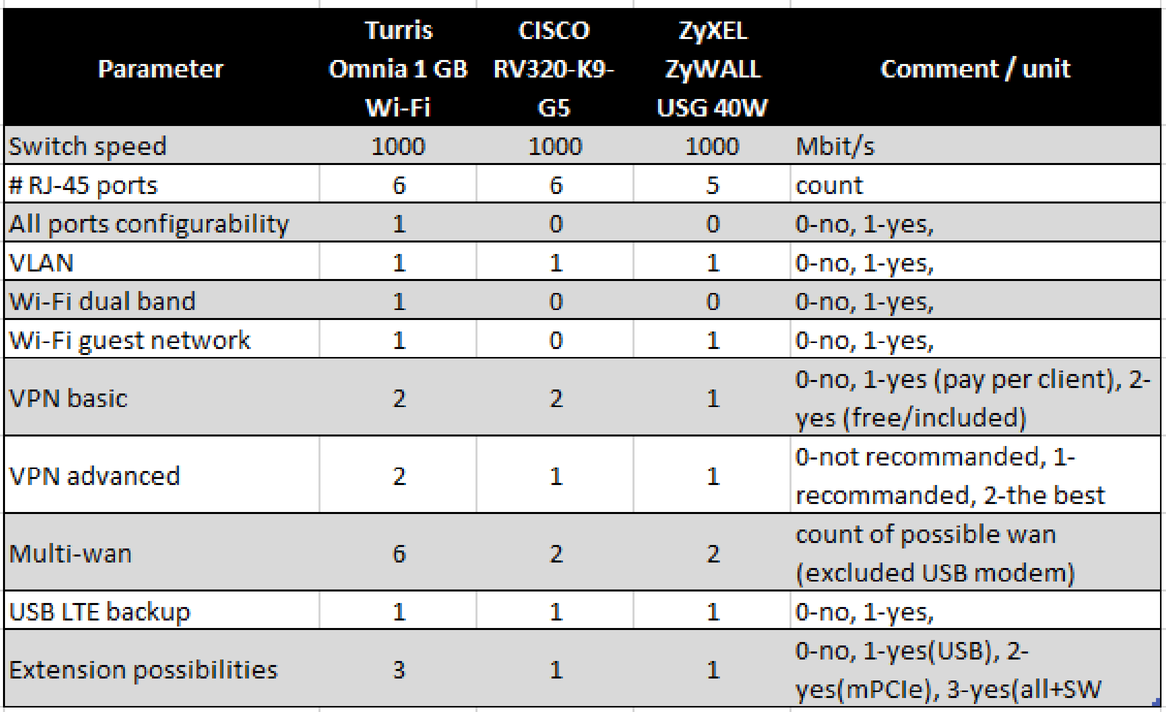
The data sources for Cisco RV320-K9-G5 are:

- https://www.cisco.com/c/en/us/products/collateral/routers/rv320-dual-gigabit-wan-vpn-router/data_sheet_c78-726132.html
- https://www.alza.cz/cisco-rv320-k9-g5-d510250.htm

The data sources for ZyXEL ZyWALL USG 40W are:

- https://www.zyxel.com/cz/cs/products_services/Next-Generation-Unified-Security-Gateway-Performance-Series-USG60W-60-40W-40/specifications#service
- https://www.alza.cz/zyxel-zywall-usg-40w-d2169998.htm#popis

Based on those sources was created summarized table.

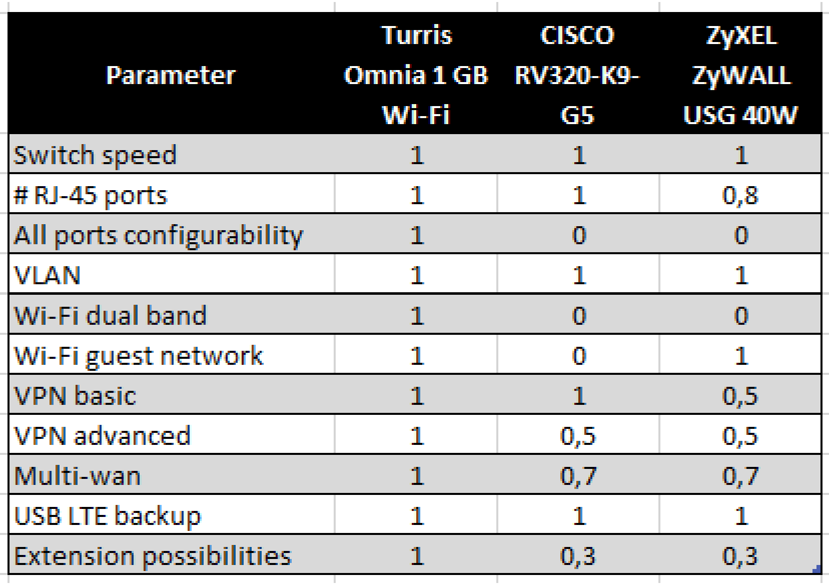


Parameter	Turris Omnia 1 GB Wi-Fi	CISCO RV320-K9-G5	ZyXEL ZyWALL USG 40W	Comment / unit
Switch speed	1000	1000	1000	Mbit/s
# RJ-45 ports	6	6	5	count
All ports configurability	1	0	0	0-no, 1-yes,
VLAN	1	1	1	0-no, 1-yes,
Wi-Fi dual band	1	0	0	0-no, 1-yes,
Wi-Fi guest network	1	0	1	0-no, 1-yes,
VPN basic	2	2	1	0-no, 1-yes (pay per client), 2-yes (free/included)
VPN advanced	2	1	1	0-not recommanded, 1-recommanded, 2-the best
Multi-wan	6	2	2	count of possible wan (excluded USB modem)
USB LTE backup	1	1	1	0-no, 1-yes,
Extension possibilities	3	1	1	0-no, 1-yes(USB), 2-yes(mPCIe), 3-yes(all+SW

Table 1 - Parameters of the gateways
(compiled by author)

All data in table above are based on official numbers (sources mentioned above). The VPN advanced rating is based on two expert articles [34] and [35].

Data in table above are rough data. In order to compare importance of each criterion and possibility to compare different unit it is necessary to "normalize" those data. The selected normalised method is to convert the value into value from interval 0 to 1 (<0,1>), where 1 is value of the highest value. 0 in case of not supported functionality.



Parameter	Turris Omnia 1 GB Wi-Fi	CISCO RV320-K9-G5	ZyXEL ZyWALL USG 40W
Switch speed	1	1	1
# RJ-45 ports	1	1	0,8
All ports configurability	1	0	0
VLAN	1	1	1
Wi-Fi dual band	1	0	0
Wi-Fi guest network	1	0	1
VPN basic	1	1	0,5
VPN advanced	1	0,5	0,5
Multi-wan	1	0,7	0,7
USB LTE backup	1	1	1
Extension possibilities	1	0,3	0,3

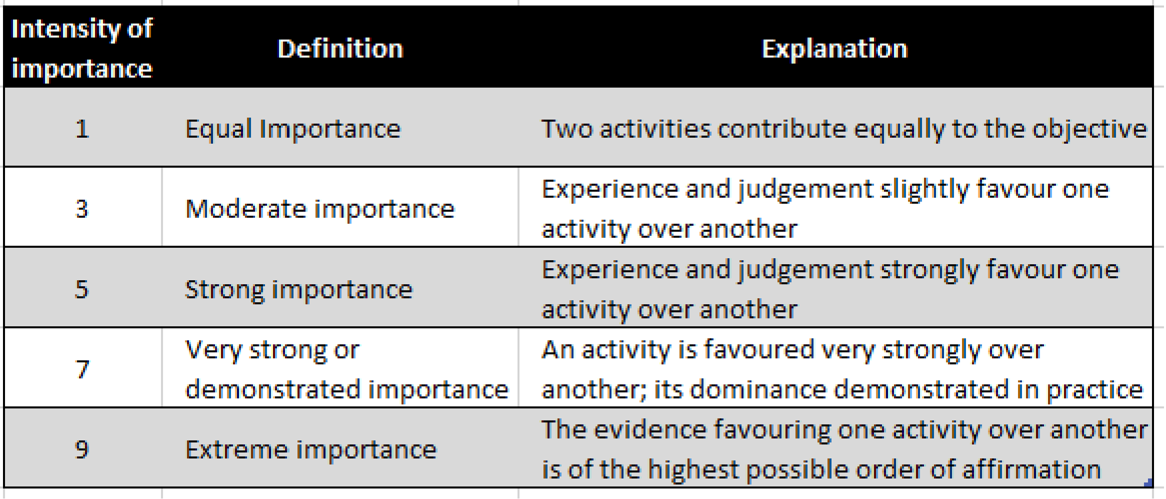
Table 2 - Parameters of the Gateways normalised
(normalised based on expert estimate)

In table above are normalised values which could be compared one to each other. In case of all parameters are equaly important this could be the last step of comparison. However, in most cases and also in case of the network gateways are not all parameters equaly important.

4.3.3 Determining weights of the parameters

For determining weights of each parameter is neccesary to employ particular method. In case of this comparism was choosed the Saaty's pairwise comparison method which is one of the best and one of the most used methods [36].

Satty's method is based on comparing two criterions and marking, which criterion is more important – and by how much is more important. For scale, how much Saaty introduced table:



Intensity of importance	Definition	Explanation
1	Equal Importance	Two activities contribute equally to the objective
3	Moderate importance	Experience and judgement slightly favour one activity over another
5	Strong importance	Experience and judgement strongly favour one activity over another
7	Very strong or demonstrated importance	An activity is favoured very strongly over another; its dominance demonstrated in practice
9	Extreme importance	The evidence favouring one activity over another is of the highest possible order of affirmation

Table 3 - Saaty's fundamental scale of absolute numbers

source: [37] page 86

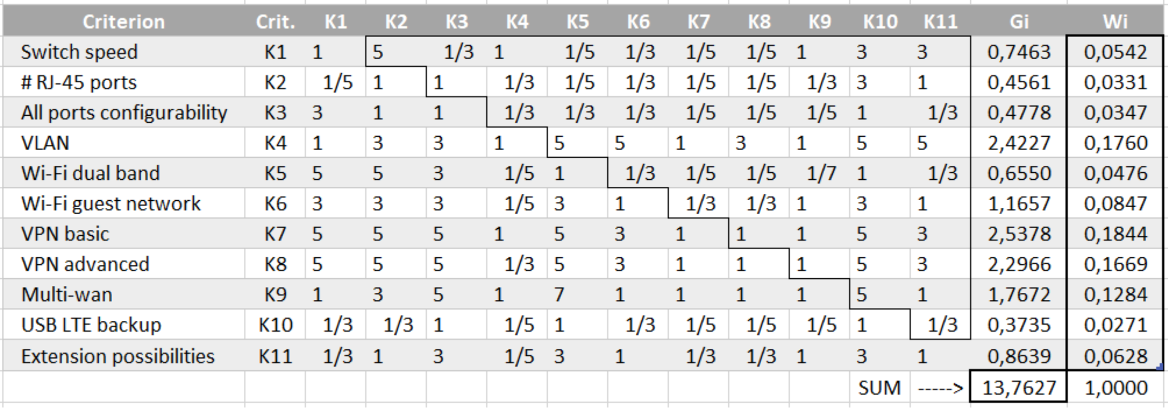
It would be possible to use also even numbers (2, 4, 6, 8) to even smaller differencing, but in this case, was odd numbers good enough to display differences between criterions.

Based on table above were compared all criterions and using particular formula

$$Gi = \sqrt[n]{\prod_{K=1}^{K11} K_{i,j}}$$

we gain G_i = Geometric mean for each criterion. The geometric mean than must be divided by summarization of geometric mean of all criterions. The weight we gain using formula

$$W_i = \frac{G_i}{\sum G}$$



Criterion	Crit.	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	Gi	Wi
Switch speed	K1	1	5	1/3	1	1/5	1/3	1/5	1/5	1	3	3	0,7463	0,0542
# RJ-45 ports	K2	1/5	1	1	1/3	1/5	1/3	1/5	1/5	1/3	3	1	0,4561	0,0331
All ports configurability	K3	3	1	1	1/3	1/3	1/3	1/5	1/5	1/5	1	1/3	0,4778	0,0347
VLAN	K4	1	3	3	1	5	5	1	3	1	5	5	2,4227	0,1760
Wi-Fi dual band	K5	5	5	3	1/5	1	1/3	1/5	1/5	1/7	1	1/3	0,6550	0,0476
Wi-Fi guest network	K6	3	3	3	1/5	3	1	1/3	1/3	1	3	1	1,1657	0,0847
VPN basic	K7	5	5	5	1	5	3	1	1	1	5	3	2,5378	0,1844
VPN advanced	K8	5	5	5	1/3	5	3	1	1	1	5	3	2,2966	0,1669
Multi-wan	K9	1	3	5	1	7	1	1	1	1	5	1	1,7672	0,1284
USB LTE backup	K10	1/3	1/3	1	1/5	1	1/3	1/5	1/5	1/5	1	1/3	0,3735	0,0271
Extension possibilities	K11	1/3	1	3	1/5	3	1	1/3	1/3	1	3	1	0,8639	0,0628
											SUM	----->	13,7627	1,0000

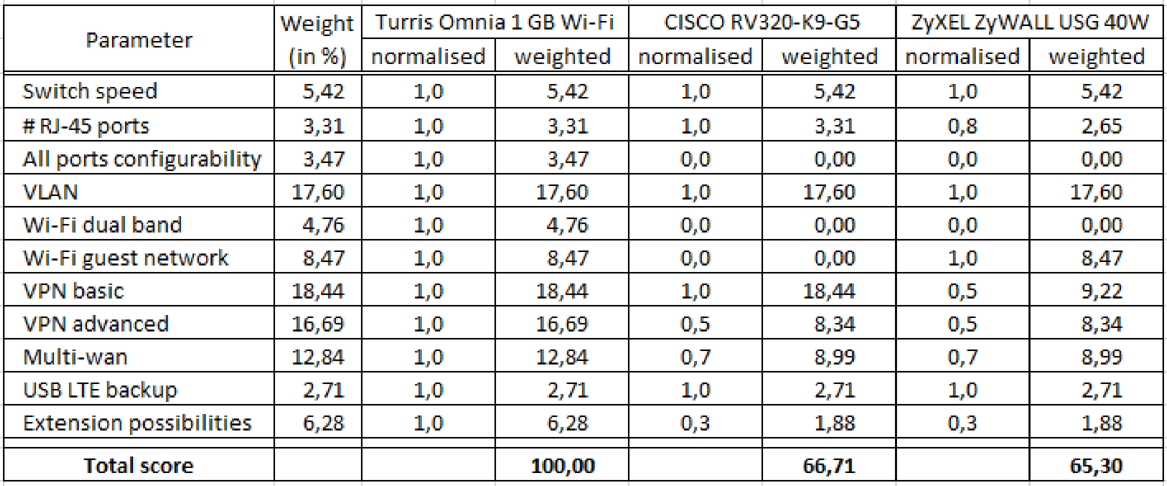
Table 4 - Saaty's matrix

(expert estimate)

In Saaty's matrix table is highlighted right top corner. The diagonal is occupied by "1" – every criterion is compared to it itself equally important. The left bottom corner is just reversed value of highlighted right top corner. So "Switch speed" (K1) has value "5" from Table 3 compared to "#RJ-45 ports" (K2). Than "#RJ-45 ports" has value "1/5" compared back to "Switch speed".

4.3.4 Comparing

After deriving weights of each criterion and after deriving normalised values of each criterion, it is possible to multiply those values and see summarization.



Parameter	Weight	Turris Omnia 1 GB Wi-Fi		CISCO RV320-K9-G5		ZyXEL ZyWALL USG 40W	
	(in %)	normalised	weighted	normalised	weighted	normalised	weighted
Switch speed	5,42	1,0	5,42	1,0	5,42	1,0	5,42
# RJ-45 ports	3,31	1,0	3,31	1,0	3,31	0,8	2,65
All ports configurability	3,47	1,0	3,47	0,0	0,00	0,0	0,00
VLAN	17,60	1,0	17,60	1,0	17,60	1,0	17,60
Wi-Fi dual band	4,76	1,0	4,76	0,0	0,00	0,0	0,00
Wi-Fi guest network	8,47	1,0	8,47	0,0	0,00	1,0	8,47
VPN basic	18,44	1,0	18,44	1,0	18,44	0,5	9,22
VPN advanced	16,69	1,0	16,69	0,5	8,34	0,5	8,34
Multi-wan	12,84	1,0	12,84	0,7	8,99	0,7	8,99
USB LTE backup	2,71	1,0	2,71	1,0	2,71	1,0	2,71
Extension possibilities	6,28	1,0	6,28	0,3	1,88	0,3	1,88
Total score			**100,00**		**66,71**		**65,30**

Table 5 - Comparing by normalised values and weights

The table above shows result of the comparison. Turris Omnia exceeds other two gateways. Due that, Turris Omnia was selected as the solution for computer network of the selected company.

4.4 Selecting suitable solution – centralising service

The same approach as was used for selecting network gateway was set to select tool (service) for centralising the network.

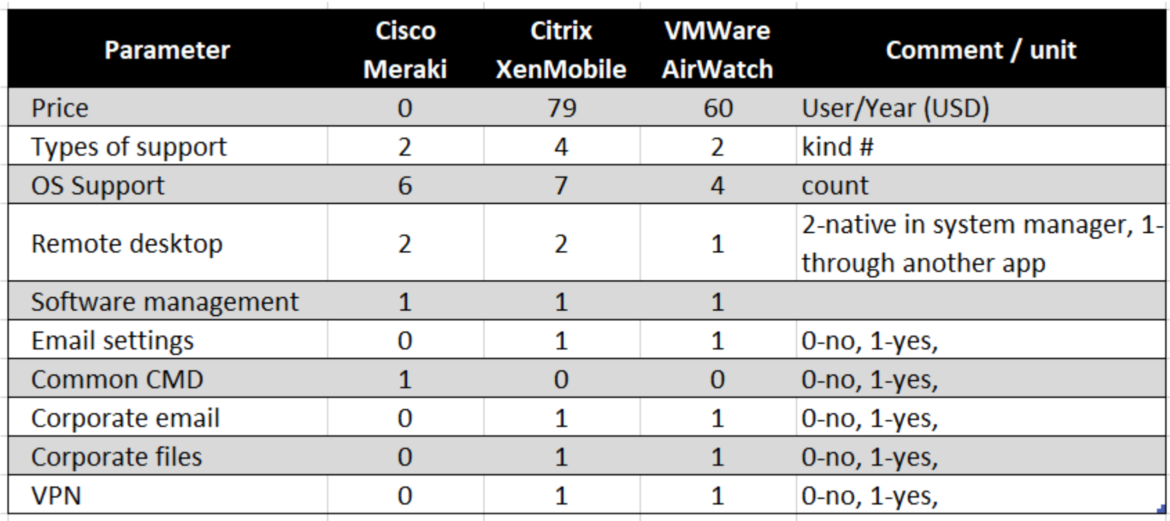
4.4.1 Parameters

As parameters for comparing were selected:

- Price (in this case price is not one-time purchase price but annual fee per one user)
- Types of support (how good is the support of the service – in how many ways can be support provided)
- OS Support (number of supported operating systems)
- Remote desktop (whether there is remote desktop client included in dashboard of the service or through another app or not present at all)
- Software management (if the service contains software manager ever for desktop operating systems such as Windows / Linux / Mac)
- Email settings (whether can be settings for mail client distributed by the service)
- Common CMD (possibility of remote use command line of enrolled devices – focused on Windows devices)
- Corporate email (own special mail client with advanced corporate features such as encryption or cloud attachments)
- Corporate files (own service for safe storing and sharing files inside company)
- VPN (whether there is included VPN solution)

4.4.2 Evaluating

For creating comparing table was used those sources: [23], [24], [26], [38]

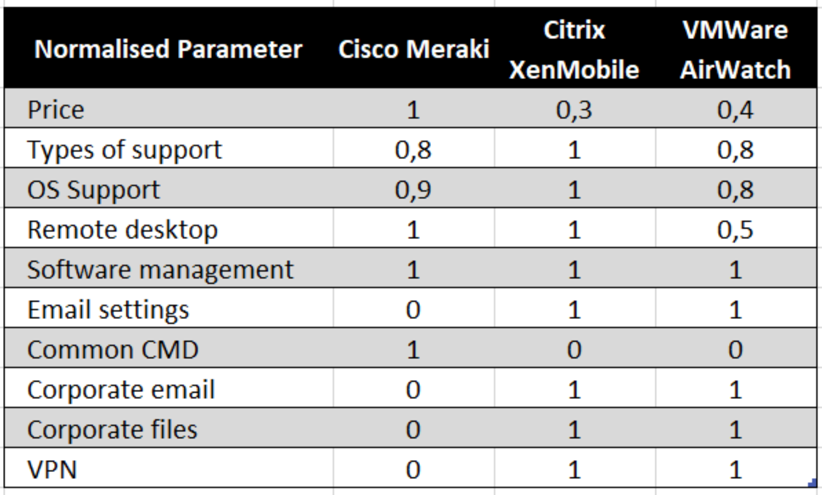


Parameter	Cisco Meraki	Citrix XenMobile	VMWare AirWatch	Comment / unit
Price	0	79	60	User/Year (USD)
Types of support	2	4	2	kind #
OS Support	6	7	4	count
Remote desktop	2	2	1	2-native in system manager, 1-through another app
Software management	1	1	1	
Email settings	0	1	1	0-no, 1-yes,
Common CMD	1	0	0	0-no, 1-yes,
Corporate email	0	1	1	0-no, 1-yes,
Corporate files	0	1	1	0-no, 1-yes,
VPN	0	1	1	0-no, 1-yes,

Table 6 - Parameters of the MDM

(compiled by author)

All data in table above are based on official numbers (sources mentioned above). As in the previous case, those data are rough data so in order to compare them it is necessary to normalise it.



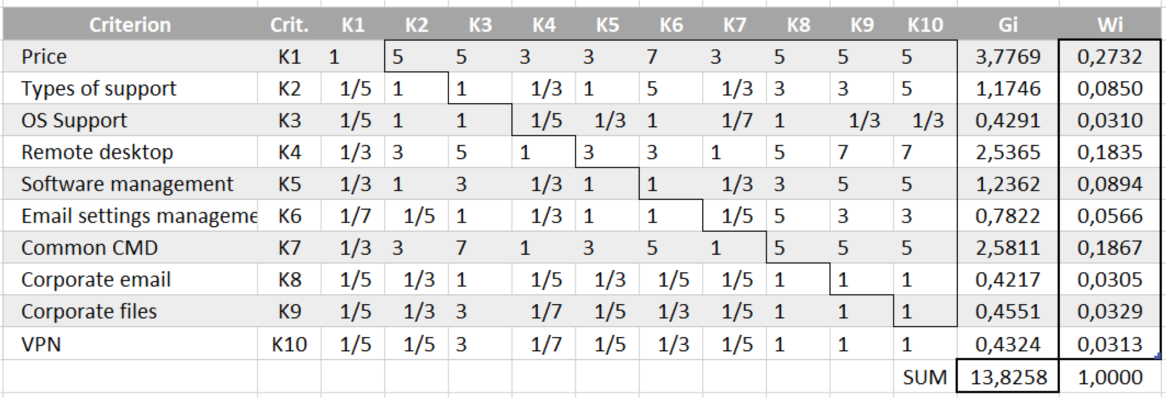
Normalised Parameter	Cisco Meraki	Citrix XenMobile	VMWare AirWatch
Price	1	0,3	0,4
Types of support	0,8	1	0,8
OS Support	0,9	1	0,8
Remote desktop	1	1	0,5
Software management	1	1	1
Email settings	0	1	1
Common CMD	1	0	0
Corporate email	0	1	1
Corporate files	0	1	1
VPN	0	1	1

Table 7 - Parameters of MDM normalised

(normalised based on expert estimate)

4.4.3 Determining weights of the parameters

Next step is to create Saaty's matrix which helps to determine weights of each parameter.

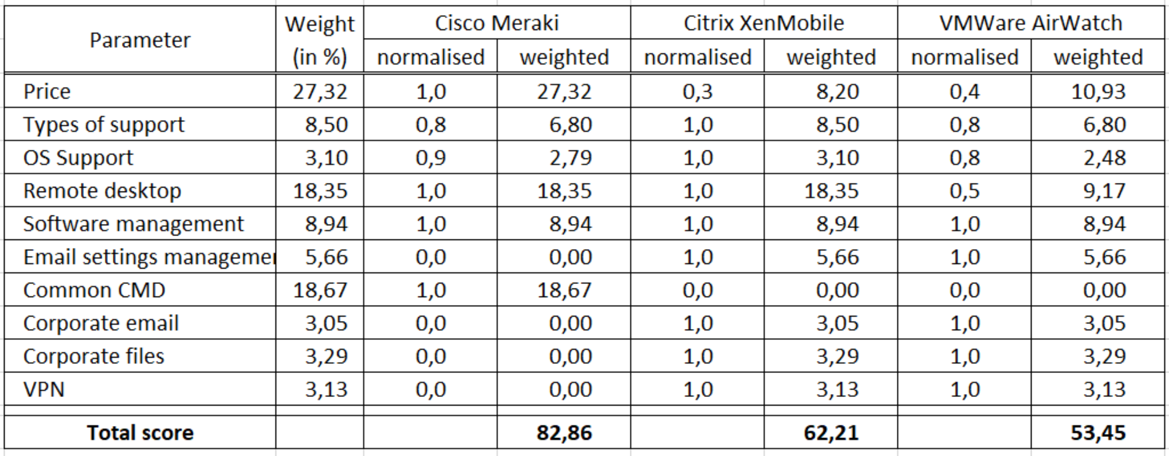


Criterion	Crit.	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	Gi	Wi
Price	K1	1	5	5	3	3	7	3	5	5	5	3,7769	0,2732
Types of support	K2	1/5	1	1	1/3	1	5	1/3	3	3	5	1,1746	0,0850
OS Support	K3	1/5	1	1	1/5	1/3	1	1/7	1	1/3	1/3	0,4291	0,0310
Remote desktop	K4	1/3	3	5	1	3	3	1	5	7	7	2,5365	0,1835
Software management	K5	1/3	1	3	1/3	1	1	1/3	3	5	5	1,2362	0,0894
Email settings manageme	K6	1/7	1/5	1	1/3	1	1	1/5	5	3	3	0,7822	0,0566
Common CMD	K7	1/3	3	7	1	3	5	1	5	5	5	2,5811	0,1867
Corporate email	K8	1/5	1/3	1	1/5	1/3	1/5	1/5	1	1	1	0,4217	0,0305
Corporate files	K9	1/5	1/3	3	1/7	1/5	1/3	1/5	1	1	1	0,4551	0,0329
VPN	K10	1/5	1/5	3	1/7	1/5	1/3	1/5	1	1	1	0,4324	0,0313
											SUM	13,8258	1,0000

Table 8 - Saaty's matrix
(expert estimate)

Saaty's matrix above show weights of each criterion. To see percentage impact on the final decision simply multiply weight by 100.

4.4.4 Comparing



Parameter	Weight (in %)	Cisco Meraki		Citrix XenMobile		VMWare AirWatch	
		normalised	weighted	normalised	weighted	normalised	weighted
Price	27,32	1,0	27,32	0,3	8,20	0,4	10,93
Types of support	8,50	0,8	6,80	1,0	8,50	0,8	6,80
OS Support	3,10	0,9	2,79	1,0	3,10	0,8	2,48
Remote desktop	18,35	1,0	18,35	1,0	18,35	0,5	9,17
Software management	8,94	1,0	8,94	1,0	8,94	1,0	8,94
Email settings managemeı	5,66	0,0	0,00	1,0	5,66	1,0	5,66
Common CMD	18,67	1,0	18,67	0,0	0,00	0,0	0,00
Corporate email	3,05	0,0	0,00	1,0	3,05	1,0	3,05
Corporate files	3,29	0,0	0,00	1,0	3,29	1,0	3,29
VPN	3,13	0,0	0,00	1,0	3,13	1,0	3,13
Total score			**82,86**		**62,21**		**53,45**

Table 9 - Comparing by normalised values and weights

In table above is shown comparison of MDM solutions for centralising of the network. Mainly because of the price wins Cisco Meraki solution which is free – has the maximum score in the most important parameter.

5 Practical part - applying

Based on Literature Research on the beginning of this thesis, starting state problems and expected future needs were derived requirements for new solution of computer network for the selected company. In this chapter will be analysed every requirement and determine, which solution – device or service could satisfy this requirement the best – or at least sufficiently.

As it is in real – non-academic conditions usually – also in the selected company is some budget constraint. The whole solution should be implemented for less than 10 000 CZK – approximately 380 EUR.

5.1 Network devices

It would be possible and maybe in some cases better to use in the network couple specialized devices – separate router, firewall, manageable switch and another devices. However, in order to keep the final solution simple an easy to manage, it was decided to use instead of it universal device – Turris Omnia.

5.1.1 Basic settings

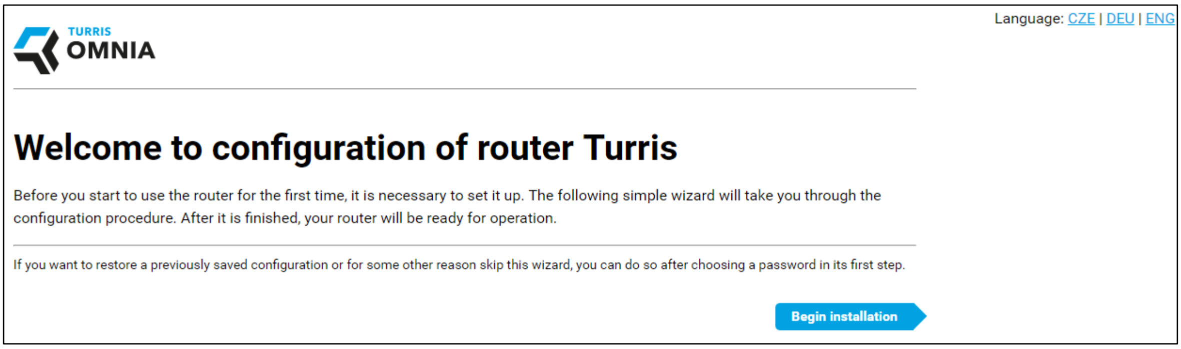
Omnia is not as common router. Many home users would be sad and angry because of Turris OS is still active in develop and sometimes developers release version which “brick” the router – the router is than necessary manually reset or sometimes even over flash with the newest fixed version.

Basic settings are however like setting of regular home router. Basic settings are done by Wizard. The wizard contains settings such as language, internet connection type and if necessary, details (DHCP, static IP, PPPoE[28]), time, time zone, password etc.

Those basic settings are enough in most cases to run the internet and to have working network, in case that no advanced functions are required. Probably none of Omnia users are

[28] Point-to-Point over Ethernet

however using just the wizard settings. Omnia is quite expensive for work which could handle just common home router.



Language: CZE | DEU | ENG

TURRIS OMNIA

Welcome to configuration of router Turris

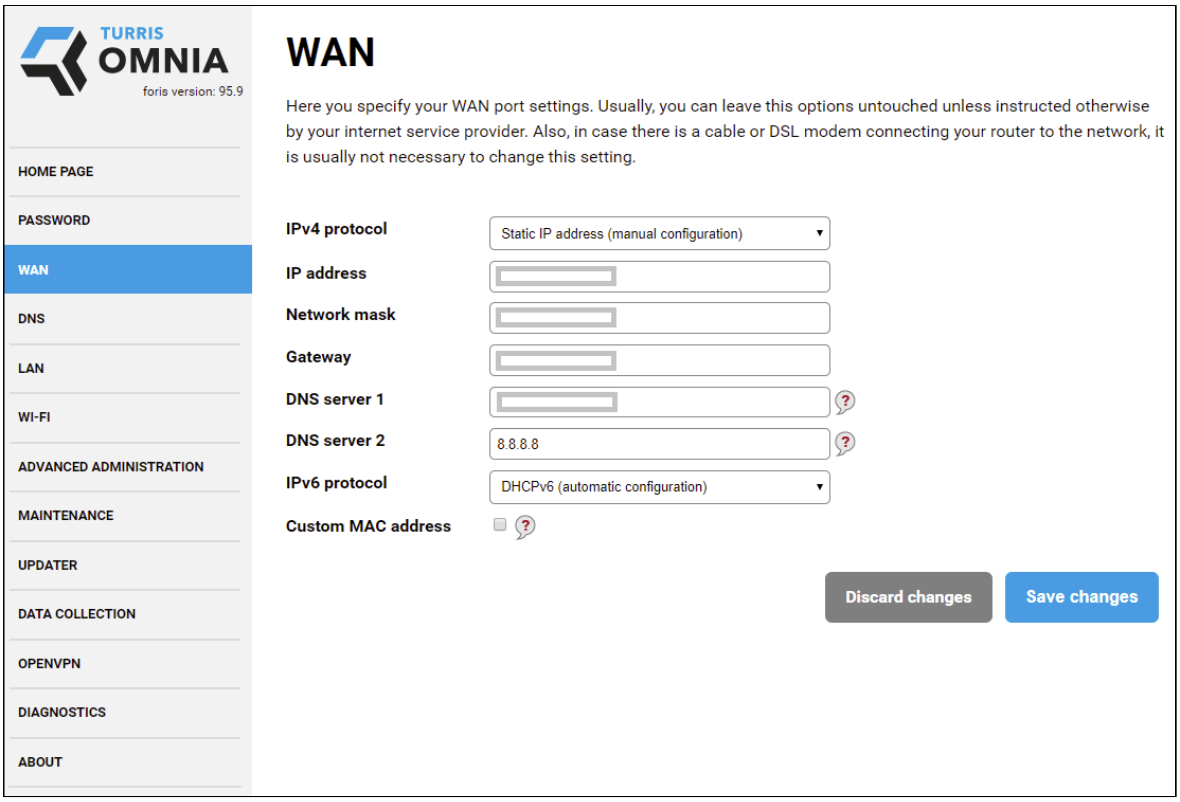
Before you start to use the router for the first time, it is necessary to set it up. The following simple wizard will take you through the configuration procedure. After it is finished, your router will be ready for operation.

If you want to restore a previously saved configuration or for some other reason skip this wizard, you can do so after choosing a password in its first step.

Figure 12 - Turris wizard

For more advance, but still basic settings have the router interface called Foris. Foris allows to set the same basic options which was in wizard and more. Specifically, administration password change, WAN settings, DNS (with connection tester), LAN settings such as router IP address, DHCP, guest network DHCP etc. Also, Wi-Fi section with independent settings for both Wi-Fi cards – for both bands (2,4 and 5 GHz).

Foris also includes maintenance settings. As was mentioned in chapter about Turris, all Turris routers have automatic firmware updates. In maintenance is possible to change how long to take between installing new update and restart. It happened couple times that upload was released by Turris team, but it bricked the router. Because of it, it was decided to set this option to maximum value – 10 days. In case of problematic update, the team have enough time to solve the trouble – which is in meantime reported by someone who already restarted the device after update.



WAN

Here you specify your WAN port settings. Usually, you can leave this options untouched unless instructed otherwise by your internet service provider. Also, in case there is a cable or DSL modem connecting your router to the network, it is usually not necessary to change this setting.

IPv4 protocol	Static IP address (manual configuration) ▾
IP address	[redacted]
Network mask	[redacted]
Gateway	[redacted]
DNS server 1	[redacted] ?
DNS server 2	8.8.8.8 ?
IPv6 protocol	DHCPv6 (automatic configuration) ▾
Custom MAC address	□ ?

Figure 13 - Foris - basic settings

In section Updater it is possible to tur automatic updates off. In business network, I think it could be possible to turn it off and regularly turn it back on every time, when administrator is present and is possible to restart the router after update, to make sure, that everything works again. Also in the same section is also possible to turn on/off some basic packages such as Tor, LuCI, Print server, device detection, Extension of network protocols, HTTP caching proxy Squid, OpenVPN package, Sound card, NAS extension allowing to connect disk and use Turris as a NAS, Home automation for smart home, Majordomo for monitoring connections of devices in local network. LXC utilities for virtualization, Access tokens and language packages.

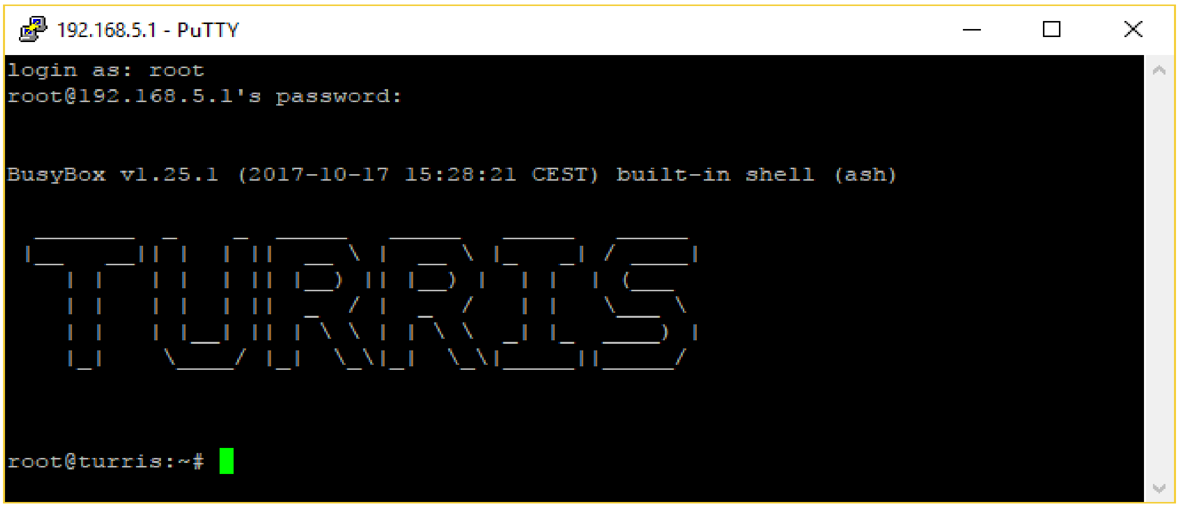
Data collection is about “With the Turris Omnia router you can join Project Turris which is a non-profit research project founded by the CZ.NIC association, a .CZ domain registry. By joining the project, your router will act as a probe which analyses traffic between your home network and the Internet and helps to identify malicious data flows. Once such a flow is detected your router notifies the Turris headquarters which can compare the flow with data from the rest of the probes and assign it a threat level. If the flow is identified as an attack Turris headquarters can prepare an update which is distributed to every Turris router and helps them to protect themselves against the attack." [39]

The section OpenVPN will pop up as soon as is OpenVPN package enabled in Updater section. In OpenVPN it is possible to enable and configure VPN server. Also, it is possible to get client configuration in one file with all certificates which are needed.

First is necessary to create CA[29], it is done just by clicking on button. When is CA ready, it is possible to set all necessary info such as IP address and subnet of the VPN, also is possible to route all traffic through VPN or allow VPN just for accessing local resources.

5.1.2 SSH access

SSH access is crucial while setting up the Turris. Some functionalities are possible to manage from LuCI or Foris, however some not typical use cases must be done through SSH. For SSH access was used PuTTY (0.67).



```
login as: root
root@192.168.5.1's password:


BusyBox v1.25.1 (2017-10-17 15:28:21 CEST) built-in shell (ash)

  _______  _    _  _____   _____   _____   _____
 |__   __|| |  | ||  __ \ |  __ \ |_   _| / ____|
    | |   | |  | || |__) || |__) |  | |  | (___
    | |   | |  | ||  _  / |  _  /   | |   \___ \
    | |   | |__| || | \ \ | | \ \  _| |_  ____) |
    |_|    \____/ |_|  \_\|_|  \_\|_____||_____/


root@turris:~#
```

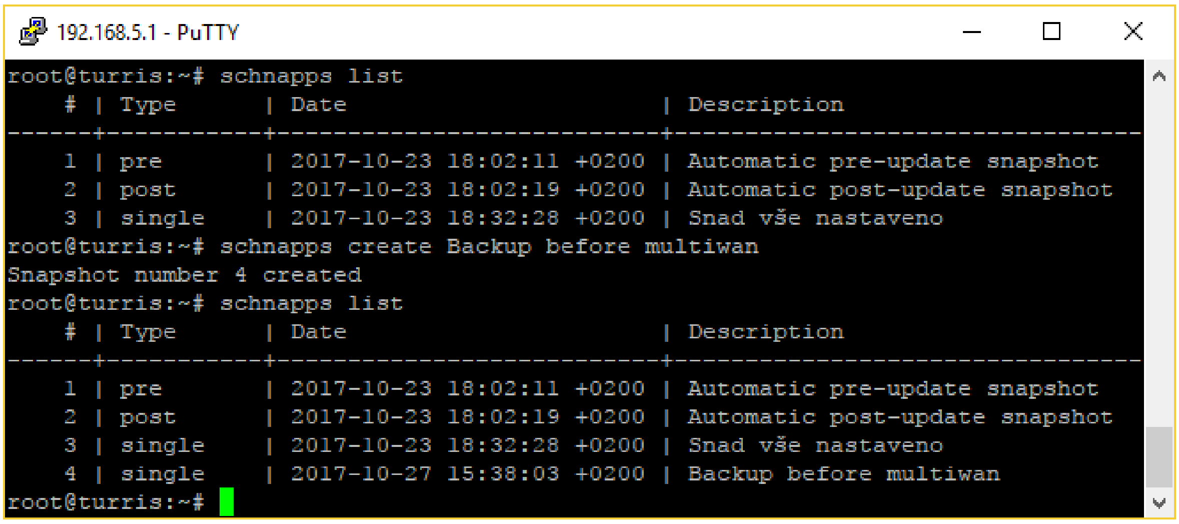
Figure 14 - SSH login Turris

Turris Omnia has nice utility called Schnapps.

[29] Certification Authority

“Schnapps is a tool for managing snapshots, which are states of the operating system at a given moment in time. Snapshots can be created manually - how to do that is explained in this article - but they are also created automatically whenever the system is updated and periodically once a week.

Thanks to Schnapps, it is possible to return to a previous version of the OS, for example, to test the functionality of this particular version or in case of OS failure. Therefore, if you plan to make major changes to the system, we recommend that you create a snapshot before hand, to which you can return if something goes wrong. You can also return to the latest snapshot simply by pressing the reset button until two diodes are light up and you can read about this simple rescue in Factory reset on Turris Omnia. This manual contains the instructions for a more advanced use of snapshots.” [40]



```
root@turris:~# schnapps list
    # | Type      | Date                      | Description
------+-----------+---------------------------+---------------------------------
    1 | pre       | 2017-10-23 18:02:11 +0200 | Automatic pre-update snapshot
    2 | post      | 2017-10-23 18:02:19 +0200 | Automatic post-update snapshot
    3 | single    | 2017-10-23 18:32:28 +0200 | Snad vše nastaveno
root@turris:~# schnapps create Backup before multiwan
Snapshot number 4 created
root@turris:~# schnapps list
    # | Type      | Date                      | Description
------+-----------+---------------------------+---------------------------------
    1 | pre       | 2017-10-23 18:02:11 +0200 | Automatic pre-update snapshot
    2 | post      | 2017-10-23 18:02:19 +0200 | Automatic post-update snapshot
    3 | single    | 2017-10-23 18:32:28 +0200 | Snad vše nastaveno
    4 | single    | 2017-10-27 15:38:03 +0200 | Backup before multiwan
root@turris:~#
```

Figure 15 - Schnapps creating backup Figure

Before any significant change is good to create a snapshot of system. In case of any trouble, it is possible to return to previous state easily.

5.1.3 LuCI

LuCI interface is something between Foris and SSH. In LuCI is almost everything what admin needs to for set up whole router. In case of the selected company was necessary to set up VLANs. VLANs divides network into several parts. Also, it matters on which level we talk about VLANs. On the switch of the router must be set three virtual networks.

One port of the switch is fixed assigned to wan0 – it is not possible to change this setting. The rest – 5 ports can be assigned to any VLAN.

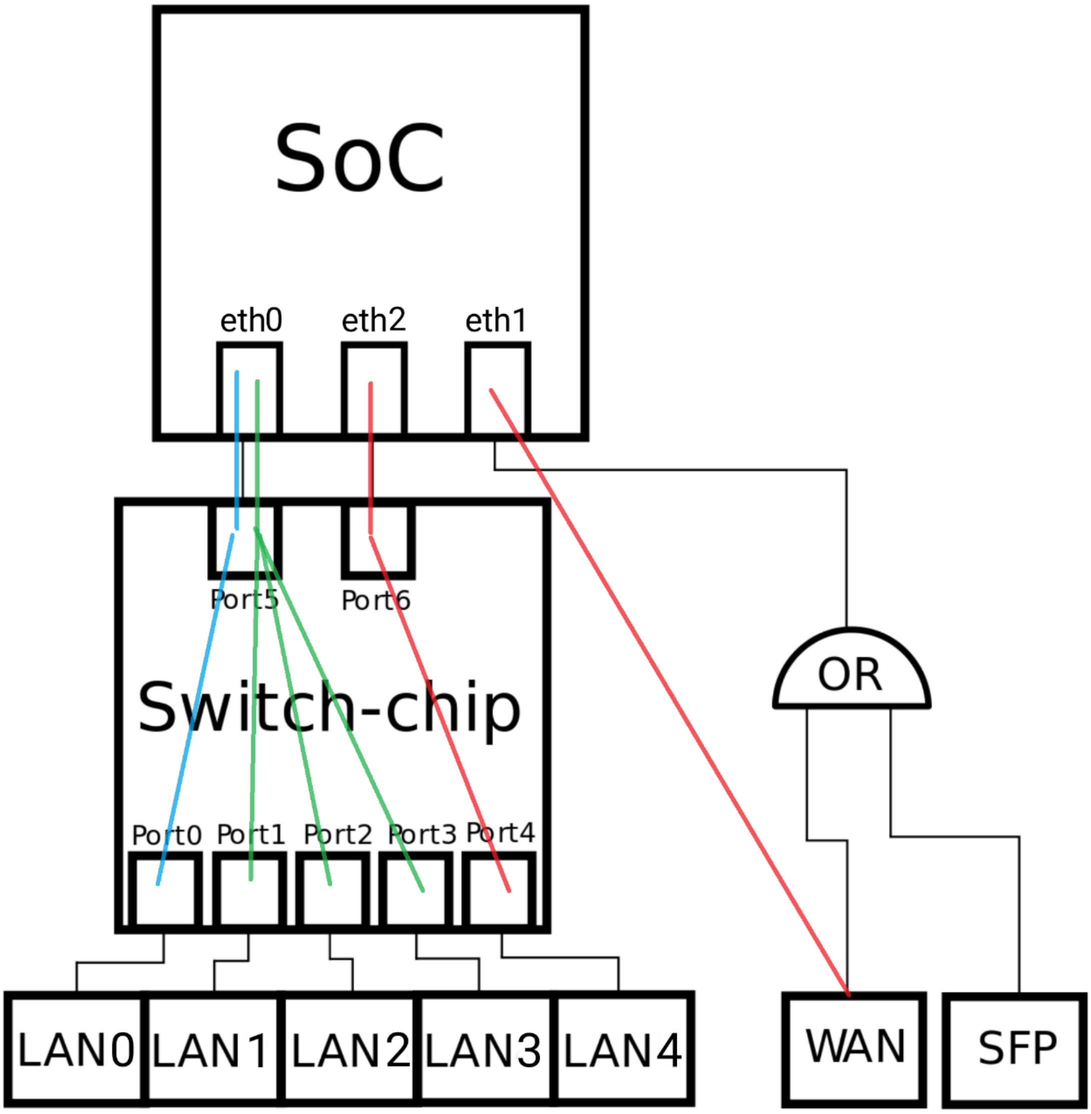
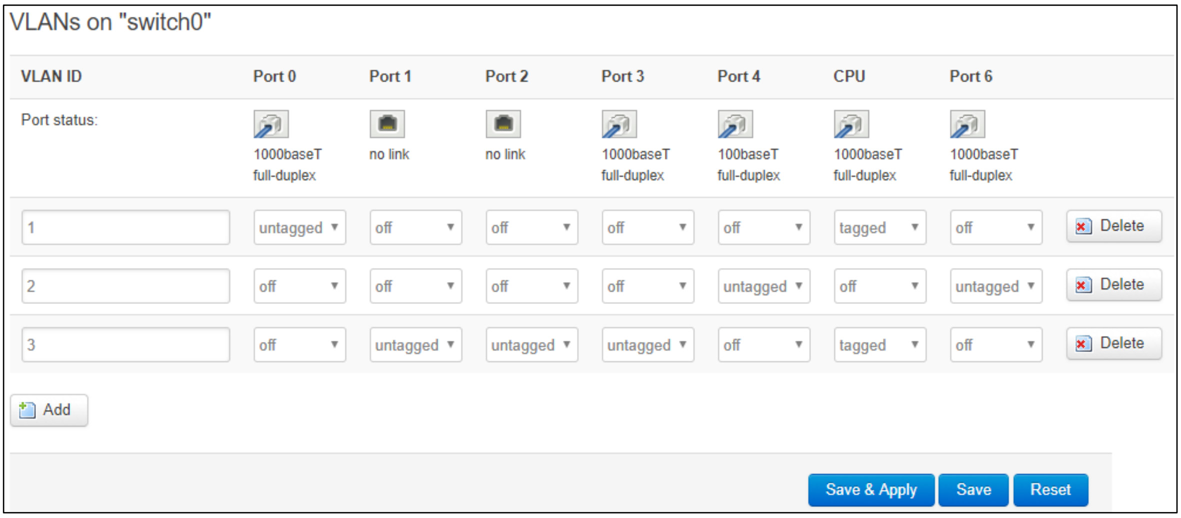


Figure 16 - Scheme of assigned ports to SoC and Switch-chip (source: https://www.turris.cz/doc/en/howto/vlan_settings_omnia, modified)

On the scheme above is shown how is the switch set up. Port LAN4 is used as WAN2 (red line), port LAN0 is used for whole Office network (after this is 16 ports unmanageable switch) (blue line) and ports 1, 2 and 3 belongs to separate VLAN for studios (green lines).



VLANs on "switch0"

VLAN ID	Port 0	Port 1	Port 2	Port 3	Port 4	CPU	Port 6	
Port status:	1000baseT full-duplex	no link	no link	1000baseT full-duplex	100baseT full-duplex	1000baseT full-duplex	1000baseT full-duplex	
1	untagged	off	off	off	off	tagged	off	Delete
2	off	off	off	off	untagged	off	untagged	Delete
3	off	untagged	untagged	untagged	off	tagged	off	Delete

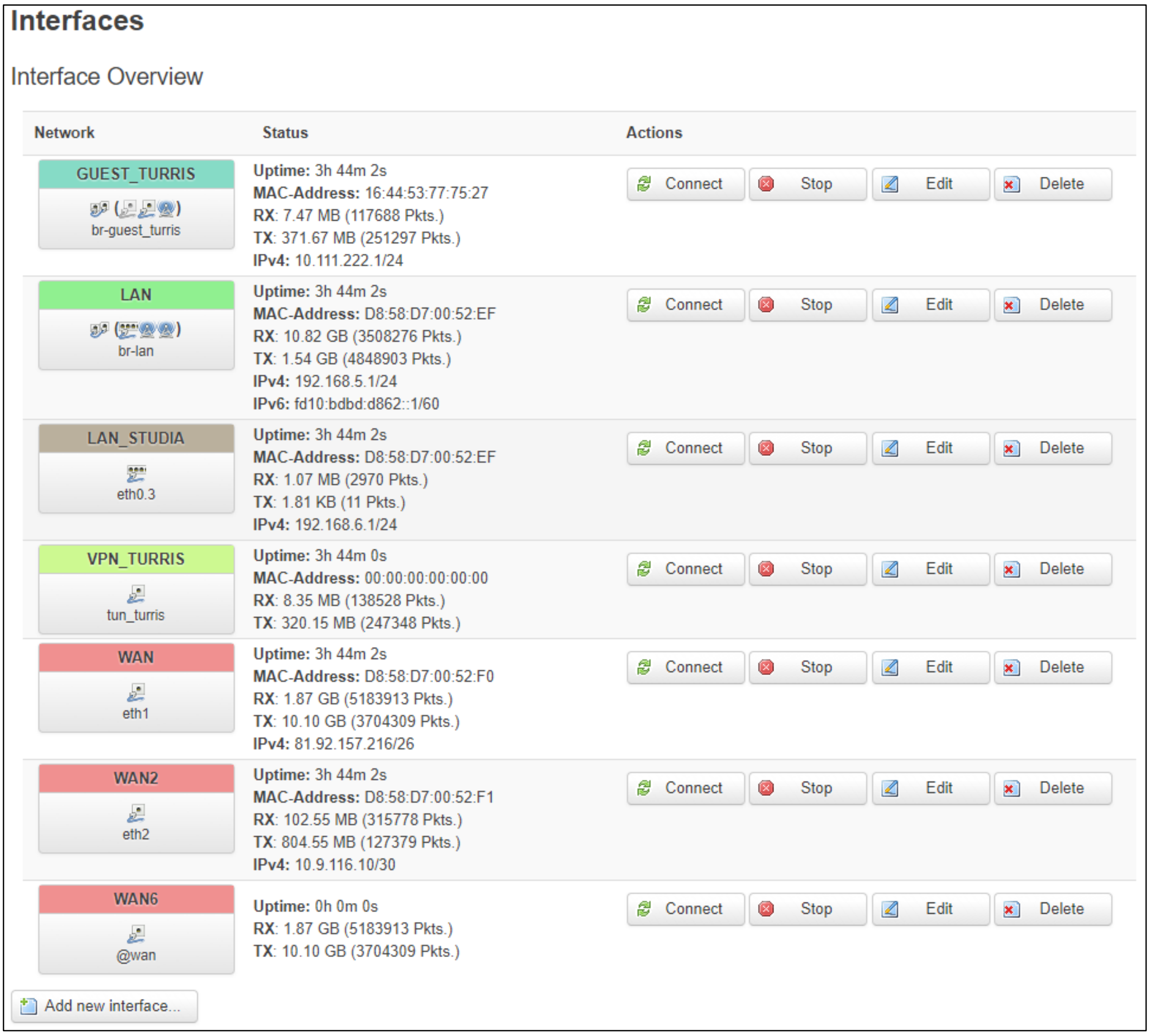
Figure 17 - Screenshot of settings VLANs on the switch

On the Figure above is shown settings of VLANs on the switch. If one port should belong to more than one VLAN, it must be marked as a “tagged” – in all VLANs where belongs. If a port belongs right to one VLAN, it will be marked as “untagged”. In case that the port is not related to the VLAN, the port is marked as “off”.

In case of the selected company, only port 5 – the CPU port is marked in two VLANs as “tagged”. That is because there are just two ports (5 and 6) which connects switch-chip and SoC.

For needed settings it is necessary also modify Interface section. On the picture below are shown all interfaces.

- GUEST_TURRIS – interface which is for providing Wi-Fi access and DHCP server to guest devices.
- LAN – office network for most of “support business” devices
- LAN_STUDIA – network for core business computers for recording
- VPN_TURRIS – VPN network. In firewall there is set to allow fluent communication between VPN and LAN (office)
- WAN – interface for one of ISP
- WAN2 – the other ISP
- WAN6 – IPv6 connection of primary ISP



Interfaces

Interface Overview

Network	Status	Actions
GUEST_TURRIS br-guest_turris	**Uptime:** 3h 44m 2s **MAC-Address:** 16:44:53:77:75:27 **RX**: 7.47 MB (117688 Pkts.) **TX**: 371.67 MB (251297 Pkts.) **IPv4:** 10.111.222.1/24	Connect Stop Edit Delete
LAN br-lan	**Uptime:** 3h 44m 2s **MAC-Address:** D8:58:D7:00:52:EF **RX**: 10.82 GB (3508276 Pkts.) **TX**: 1.54 GB (4848903 Pkts.) **IPv4:** 192.168.5.1/24 **IPv6:** fd10:bdbd:d862::1/60	Connect Stop Edit Delete
LAN_STUDIA eth0.3	**Uptime:** 3h 44m 2s **MAC-Address:** D8:58:D7:00:52:EF **RX**: 1.07 MB (2970 Pkts.) **TX**: 1.81 KB (11 Pkts.) **IPv4:** 192.168.6.1/24	Connect Stop Edit Delete
VPN_TURRIS tun_turris	**Uptime:** 3h 44m 0s **MAC-Address:** 00:00:00:00:00:00 **RX**: 8.35 MB (138528 Pkts.) **TX**: 320.15 MB (247348 Pkts.)	Connect Stop Edit Delete
WAN eth1	**Uptime:** 3h 44m 2s **MAC-Address:** D8:58:D7:00:52:F0 **RX**: 1.87 GB (5183913 Pkts.) **TX**: 10.10 GB (3704309 Pkts.) **IPv4:** 81.92.157.216/26	Connect Stop Edit Delete
WAN2 eth2	**Uptime:** 3h 44m 2s **MAC-Address:** D8:58:D7:00:52:F1 **RX**: 102.55 MB (315778 Pkts.) **TX**: 804.55 MB (127379 Pkts.) **IPv4:** 10.9.116.10/30	Connect Stop Edit Delete
WAN6 @wan	**Uptime:** 0h 0m 0s **RX**: 1.87 GB (5183913 Pkts.) **TX**: 10.10 GB (3704309 Pkts.)	Connect Stop Edit Delete

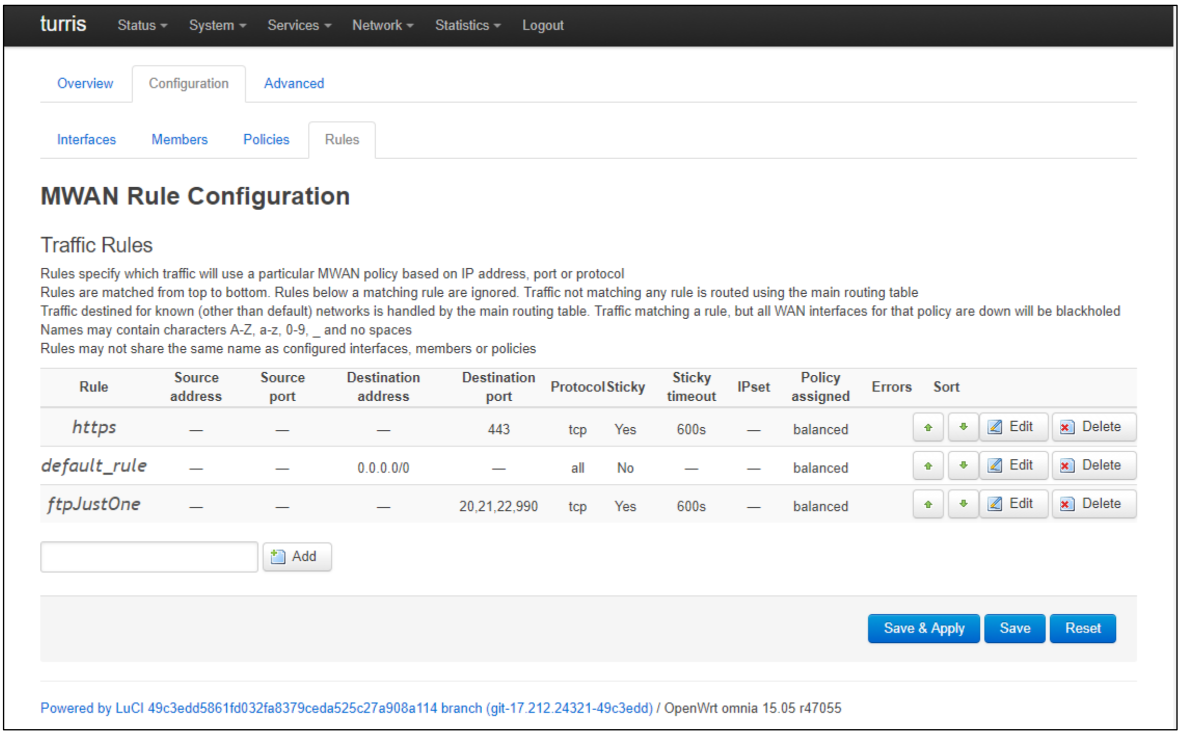
Add new interface...

Figure 18 - Interfaces - Turris Omnia LuCI settings

Based on the Turris documentation [41] and general documentation for Open WRT [42] was set the multi wan functionality. Before doing any changes to the router settings was necessary to fulfil pre-configuration. In this case it was set the VLANs and WAN interfaces in such way to have “wan” and “wan2” interfaces with working internet connection. About VLAN creation was already written in previous sections. Based on Open WRT official documentation about mwan3 package [42], it is important to set different metric on each wan interface, so it was done. Faster preferable interface should have lower metric.

After all pre-configuration conditions are met, is necessary to download mwan3 package in Turris software tab. Package called "luci-app-mwan3". Mwan functionality is than installed and after rebooting, in Network section than appears new section – Load

Balancing. The multiwan3 package is already preconfigured so it should work immediately after install. The only struggle with multi wan was during connection to FTP servers (via multiple protocols). FTP and mainly secured versions are sensitive to from which IP they transmit data. Data must be sent through the same IP all the time of the transportation. For this purpose (and others) is in mwan3 settings for “Rules” and for this specific trouble setting called “sticky”.



MWAN Rule Configuration

Traffic Rules

Rules specify which traffic will use a particular MWAN policy based on IP address, port or protocol
Rules are matched from top to bottom. Rules below a matching rule are ignored. Traffic not matching any rule is routed using the main routing table
Traffic destined for known (other than default) networks is handled by the main routing table. Traffic matching a rule, but all WAN interfaces for that policy are down will be blackholed
Names may contain characters A-Z, a-z, 0-9, _ and no spaces
Rules may not share the same name as configured interfaces, members or policies

Rule	Source address	Source port	Destination address	Destination port	Protocol	Sticky	Sticky timeout	IPset	Policy assigned	Errors	Sort
https	—	—	—	443	tcp	Yes	600s	—	balanced		
default_rule	—	—	0.0.0.0/0	—	all	No	—	—	balanced		
ftpJustOne	—	—	—	20,21,22,990	tcp	Yes	600s	—	balanced		

Powered by LuCI 49c3edd5861fd032fa8379ceda525c27a908a114 branch (git-17.212.24321-49c3edd) / OpenWrt omnia 15.05 r47055

Figure 19 - Screenshot Turris Omnia administration - Load balancing

Previous picture shows all rules applied on mwan load balancing. Two upper rules are set by default. The last is created especially for the selected company and their need of accessing FTP servers. The rule ensures that while connecting to any FTP or SFTP server (using the destination ports as a key), only one connection (IP address) is used for each FTP connection. This rule is necessary. Without the rule, FTP transfers often terminated with some security error.

5.1.4 Printer disconnecting

One of the requirements is about regular disconnecting of a printer. The issue is due to the way how the printer in mezzanine connected to the network. The printer is connected through the Wi-Fi. Current router – Access point is transmitting Wi-Fi network and another AP in client mode is connected. UTP wire cable than connect the other AP and the printer. Connecting this way is complicated and the collision domain is huge. Trouble can occur on the router, on the client AP or anywhere in the middle. Wi-Fi is still not as reliable as wire [11]. So, it was decided to use instead of unreliable Wi-Fi powerline solution.

Using all previous settings allowed to interconnect all devices in manner of ISO/IEC 27002. Result topology and way of connection can be seen from the picture bellow.

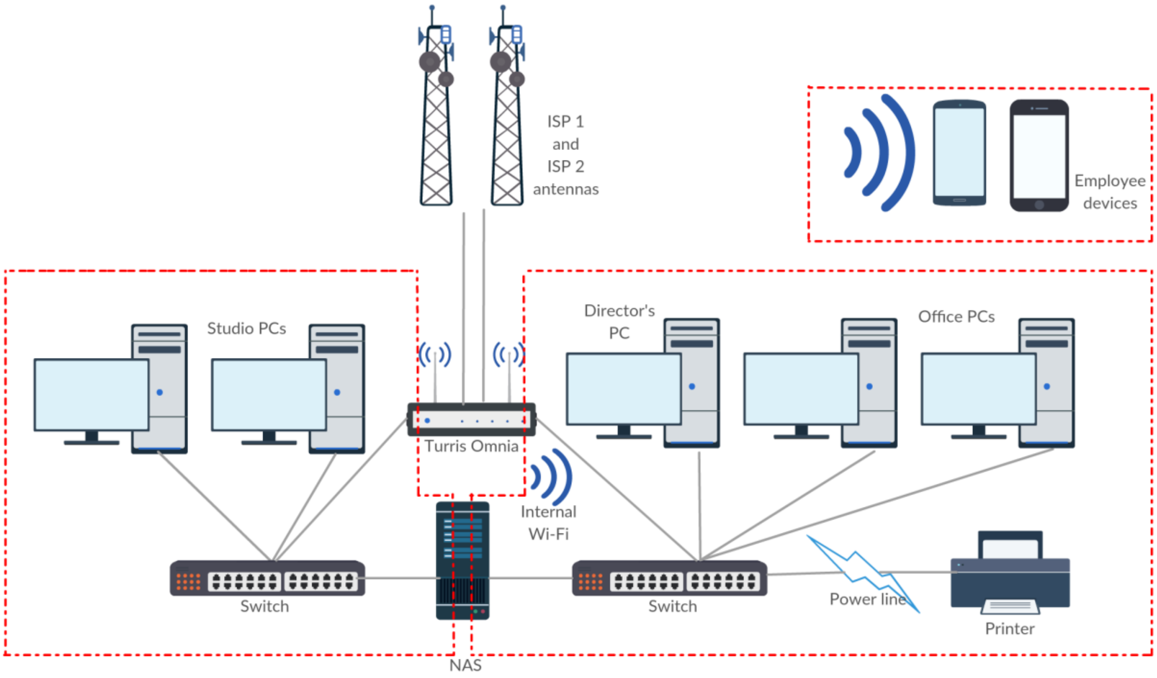


Figure 20 - Topology of proposed network solution

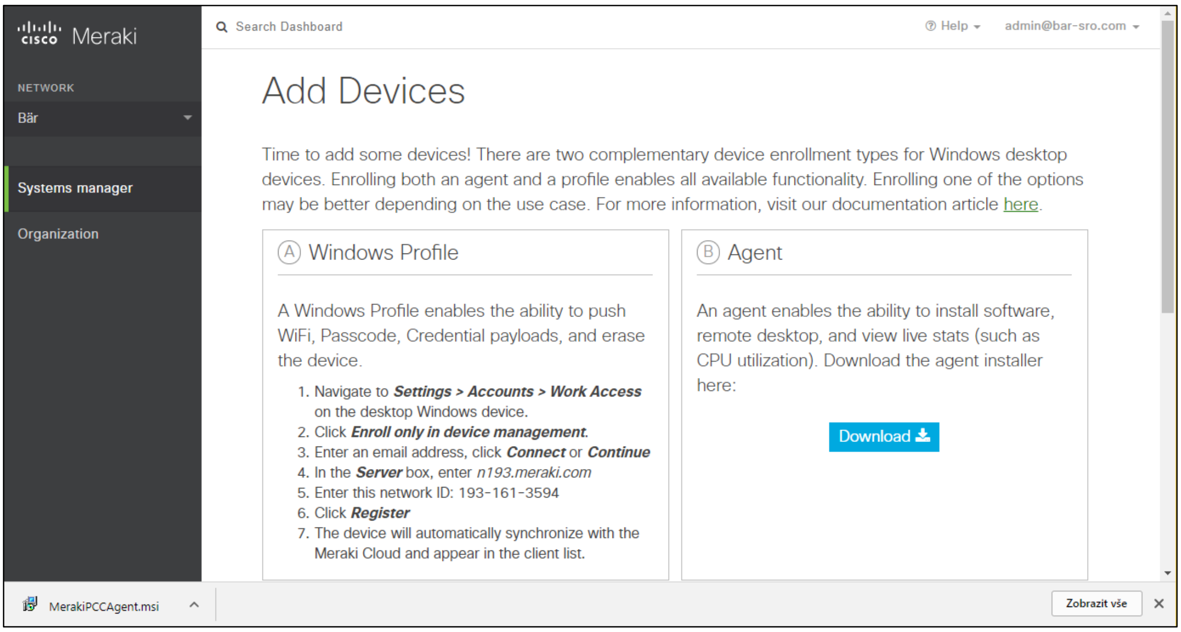
On the scheme above is shown that network is divided into several subnetworks. One subnetwork for guest devices and all other non-business-related devices. Another for studio PCs which are responsible for core business activities (recording). The last is the biggest and contains office PCs and network printers. Both business networks have their own connection to the NAS with separate wire.

Internet connection for whole network is provided by two ISP, the throughput is managed and divided between both ISPs by Turris Omnia router and its service mwan3.

The only AP in the network is also provided by Turris Omnia, which transmit three networks. One 2,4 GHz guest network and 2,4 GHz and 5 GHz internal Wi-Fi.

5.2 Centralization of network

Hence for selected company was selected solution of Cisco Meraki MDM, it was necessary to set all computers for cooperating with the System Manager of Meraki. For this purpose, it is for Windows PC platform used Meraki PCCAgent.



Add Devices

Time to add some devices! There are two complementary device enrollment types for Windows desktop devices. Enrolling both an agent and a profile enables all available functionality. Enrolling one of the options may be better depending on the use case. For more information, visit our documentation article here.

Ⓐ Windows Profile

A Windows Profile enables the ability to push WiFi, Passcode, Credential payloads, and erase the device.

1. Navigate to ***Settings > Accounts > Work Access*** on the desktop Windows device.
2. Click ***Enroll only in device management.***
3. Enter an email address, click ***Connect*** or ***Continue***
4. In the ***Server*** box, enter *n193.meraki.com*
5. Enter this network ID: 193-161-3594
6. Click ***Register***
7. The device will automatically synchronize with the Meraki Cloud and appear in the client list.

Ⓑ Agent

An agent enables the ability to install software, remote desktop, and view live stats (such as CPU utilization). Download the agent installer here:

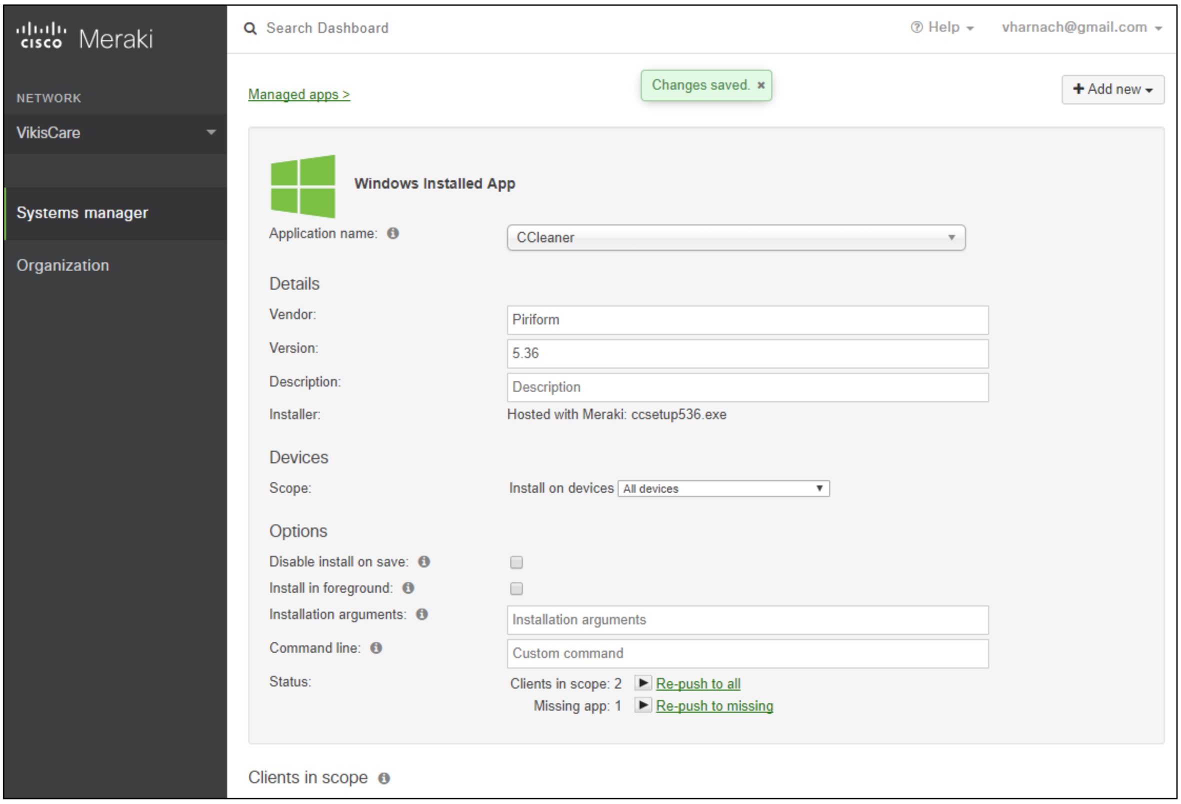
Figure 21 - Enrolling new device into Meraki MDM

After enrolling device, it is possible to perform tasks such as fetch list of processes currently running on specified PC, use command line, display network status, fetch screenshot or even use Remote desktop client. The RDC[30] is however still in beta testing. Also, it is possible to send notification to the PC or remotely restart or turn off the device.

Beside those functions which can be used for individual computers Meraki System manager also provides functionality for group actions such as command line which send performed command to all devices in scope command lines or installing applications.

[30] Remote desktop client

Using the command line in such way is very helpful. In the selected company it can be used for mapping network drive.



Windows Installed App

Application name: CCleaner

Details

Vendor: Piriform

Version: 5.36

Description: Description

Installer: Hosted with Meraki: ccsetup536.exe

Devices

Scope: Install on devices All devices

Options

Disable install on save: □

Install in foreground: □

Installation arguments: Installation arguments

Command line: Custom command

Status: Clients in scope: 2 ▶ Re-push to all
Missing app: 1 ▶ Re-push to missing

Clients in scope

Figure 22 - Meraki System Manager - managing applications

5.3 Applying standards

As it was discussed in chapter about international standards in Theoretical basis, it is important during phase of designing computer network not to forget applying those recommendations. In case of the selected company, one of the most important standard is ISO 27001 – Information security management.

ISO 27001 is influencing the selected company as any other company. Email conversation, accountant database etc. must be backup at a regular basis. Besides that, the company works with sensitive content of its client – episodes of series before television premiere. This is crucial, because in case of disclosure of any of the episode the trust of customer would be damaged. Also, there are legal consequences based on a contract between the selected company and its customers.

Therefore, the channel for interchanging audio-video content must be reliable secured. In an industry of voiceovering is standard to use FTP servers for such a content. All suppliers than connect to the FTP and download the source video. Than upload it back with new audio track. Hence the FTP protocol is not encrypted and can be overheard, for this purpose is unsatisfactory.

Plain FTP protocol must not be used due the security threat. Solution for the problem is using encrypted communication which is provided by SFTP (SSH FTP) or FTP with SSL/TLS encryption.

Hence the selected company is supplier for several clients, it connects to several FTP servers using different protocols and encryption. All clients with plain FTP should be contacted and asked for establishing secured connection.

Another threat to security of the entrusted work is in time between downloading and uploading back to the client. Before, after and during processing the video must be secure stored. Present state is that all audio/video files are stored on centralised device – NAS. Access to those files have just authorised users. The authorisation is based on user account and password authentication.

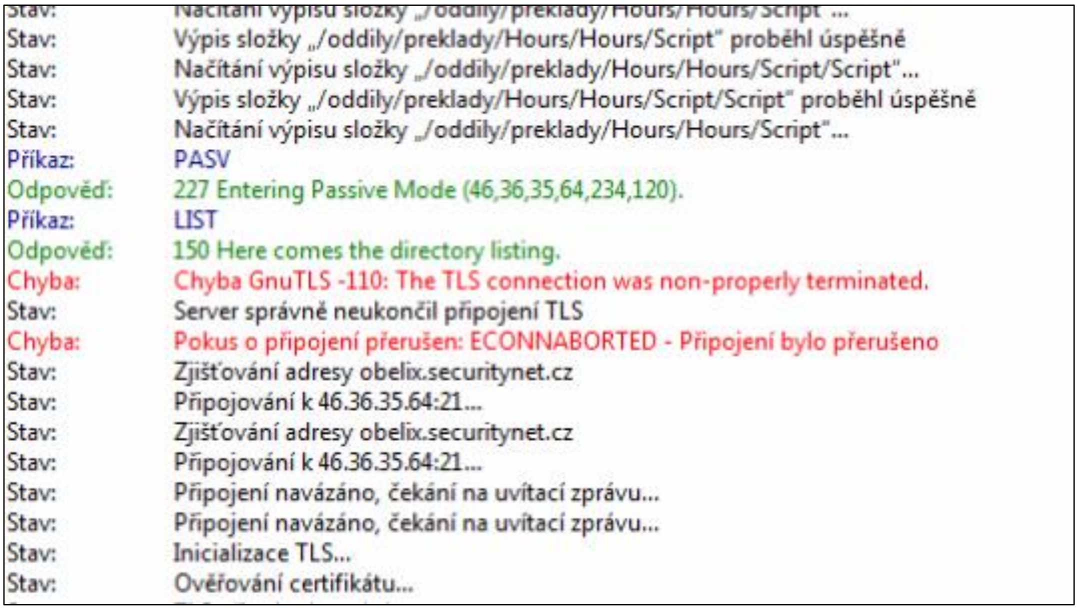
There are two kinds of privileges. For office staff (they download original files from clients) and for record technicians (they process the file and final version upload back to the NAS from which are completed tasks uploaded back to the customer). The privileges as low as it is possible to allow users to complete their task as the standards requires.

Also, another part of the ISO 27001 and ISO 27002 were applied (and similar information security norms). View the chapter with requirements for the network solution for more information.

6 Evaluation of results and recommendations

The main goal of this thesis was to design and implement improvements for the existing computer network of the selected company. This should be met by setting up the Turris Omnia router and setting up and enrolling company devices into MDM Cisco Meraki.

After implementing the Turris Omnia and all its features there were some troubles, mainly caused by using mwan3 package which allowed to use both internet connections at the same time in balance mode (also in case of failure one of them in failover mode). The trouble was in using secured protocols by both internet connections at the same time.



```
Stav:          Načítání výpisu složky „/oddily/preklady/Hours/Hours/Script“...
Stav:          Výpis složky „/oddily/preklady/Hours/Hours/Script“ proběhl úspěšně
Stav:          Načítání výpisu složky „/oddily/preklady/Hours/Hours/Script/Script“...
Stav:          Výpis složky „/oddily/preklady/Hours/Hours/Script/Script“ proběhl úspěšně
Stav:          Načítání výpisu složky „/oddily/preklady/Hours/Hours/Script“...
Příkaz:        PASV
Odpověď:       227 Entering Passive Mode (46,36,35,64,234,120).
Příkaz:        LIST
Odpověď:       150 Here comes the directory listing.
Chyba:         Chyba GnuTLS -110: The TLS connection was non-properly terminated.
Stav:          Server správně neukončil připojení TLS
Chyba:         Pokus o připojení přerušen: ECONNABORTED - Připojení bylo přerušeno
Stav:          Zjišťování adresy obelix.securitynet.cz
Stav:          Připojování k 46.36.35.64:21...
Stav:          Zjišťování adresy obelix.securitynet.cz
Stav:          Připojování k 46.36.35.64:21...
Stav:          Připojení navázáno, čekání na uvítací zprávu...
Stav:          Připojení navázáno, čekání na uvítací zprávu...
Stav:          Inicializace TLS...
Stav:          Ověřování certifikátu...
```

Figure 23 - FileZilla log

On the screen above the issue with TLS encrypted connection is shown while using both internet connections at the same time. The core trouble is that after establishing TLS connection fixed IP address of the client is on the server. Connecting with the same credentials but from the different IP address then causes terminating previous connection – and stopping communication.

This issue was worked around by setting the “sticky” mode for communication on all FTP ports. The sticky mode means that no connection is established with the same server using the other connection (and obviously other IP address) in the period of predefined time.

After handling with the issue of secured FTP connections, users are just happy and praise the increased speed of the internet connection.

From previous experience with the Turris Omnia it is known that the developer team sometimes releases a version of operation system update which breaks the settings of the router or bricks the whole device. Solution for this sporadic problem is to set automatic restart time to maximum – 10 days. So, the update is downloaded but not installed. Installation and restart are performed after ten days. Usually if any trouble with automatic update appears, community forum is full of complaints immediately after the release. So, in the case of a problematic version being released, there is enough time for Turris team to fix the issue and release a fixed version. The bad version is then overwritten by the fixed one and after restart and update everything works fine.

Another solution for any unpredictable failures is tool schnapps which allows to recover the state of the system into state which was before update (schnapps snapshot is automatically created by the router before every update).

Cisco Meraki solution for centralising the network was implemented without any issue. The only unexpected behaviour of the solution is that most of its features (such as common command line or remote desktop client) do not work in network without public IPv4. In the case of the selected company, however, there are two internet connections with public IP address, so the issue does not have any impact there.

Possible and wanted next step to improve the security of the network could be certifying the company for the international standard ISO 27001 or at least to create, approve and follow document Information Security Policy (ISO 27002).

7 Conclusion

The main goal of the thesis was to analyse, design a solution and implement improvements for an existing computer network of the selected company.

The analysis was done by gathering of all requirements for the future solution. Requirements were gathered based on user needs, expected future needs and requirements of international standards. Some of requirements were:

- Dividing network into separate subnetworks (based on ISO 27002 13.1.3)
- Increase speed connection between data storage and users
- Ensure security and reliability of the central data storage
- Use both internet connections together for the whole network. In normal conditions for increasing speed, in case of a failure one of the connection to ensure that the company can continue and upload their production
- Secure communication across networks using VPN solution (ISO 27033 5.1)
- Implement tool for a centralized administration of enrolled devices
- Create secured channel between both company buildings for an easy sharing

Next part was to design the suitable solution. It contains preselection of suitable devices and services, and multicriterial selection of the best solution. In preselection three network devices were selected:

- Turris Omnia
- CISCO RV320
- ZyXEL ZyWALL USG 40W

And three services:

- Cisco Meraki
- VMware AirWatch
- Citrix XenMobile

For both groups parameters (criterions) were selected based on devices/services compared. Importance of those criterions was set in the estimated value for the company, using Saaty's pairwise comparison method. Some of criterions for network device:

- VLAN capability (whether or not the switch is capable to divide ports between Virtual Local Area Network)
- VPN basic (whether or not Virtual Private Network server is present on the devices and if this feature is included in purchase price)
- Multi-wan functionality (whether or not there is a possibility to use multiple Internet Service Providers at the same time for load balancing and for failover use
- Extension possibility (how can be the device be extended if necessary – hardware extension and/or software package/service which could be added)

Also, centralised service selection had its own criterions. The main difference between those selections was the price. In the network device, price was excluded on purpose. By contrast, the annual fee in centralised service selection was one of the most important criterion. The reason is simple – the company has set budget for one-time expense. It was not possible to exceed it and saving money from the budget would not make any sense.

Values of all criterions were normalised in an interval <0,1> in order to have comparable values for all criterions (based on the Basic Variant Method). Final score the final selected solution was based on was gained by summing normalized values multiplied by particular weights (from Saaty’s matrix). In category network device Turris Omnia was selected, in centralised network solution Cisco Meraki.

Not negligible is also protection which provides the Turris Omnia router and its connection into Turris network. Firewall rules are updated automatically based on state in Turris network – network of routers by CZ.NIC, z. s. p. o. (more in chapter 3.2.1).

During implementation phase it was necessary to enrol all office devices into Cisco Meraki network, set basic setting on Turris Omnia (such as IP addresses, network masks, Wi-Fi settings etc.) and also advanced features. Advanced features include VPN settings, multiwan settings, separating network segments into VLANs and ensuring that all this works fine.

After implementing selected solutions and fixing initial troubles computer network of the selected company works perfectly. Users can see the difference experiencing continuous (never interrupted) internet access which is most of the time faster than ever before. Also increased speed of accessing files on central data storage (NAS) is significant. Another feature which benefits network users is VPN which can be used for home offices and for connecting the other studio which is located in other part of the city.

Beside those features which can employees experience there are also features added to improve security which are for users “invisible” but which are recommended by international standards ISO 27001 and ISO 27002. Some highlighted are separating network into subnetworks, so just devices with similar purpose are in the same subnetwork.

8 Bibliographies

[1] Introduction to Computer Network Topology. *Life Wire* [online]. New York: Bradley Mitchell, 2017 [cit. 2017-10-13]. Available from: https://www.lifewire.com/computer-network-topology-817884

[2] JOHNSON, Joel. What is the most popular type of topology?. In: *Tech Target* [online]. Atlanta: Joel Johnson, 2003 [cit. 2017-10-13]. Available from: http://searchnetworking.techtarget.com/answer/What-is-the-most-popular-type-of-topology

[3] Computer Networks Planning a Network. In: *YouTube* [online]. San Bruno, San Francisco: Alton Hardin, 2015 [cit. 2017-10-13]. Available from: https://www.youtube.com/watch?v=k-syi-L0k6k

[4] Aktivní prvky sítě. *Průvodce HW* [online]. České Budějovice: University of South Bohemia in České Budějovice, Faculty of Education, 2010 [cit. 2017-10-20]. Available from: http://www.pf.jcu.cz/stru/katedry/fyzika/prof/Tesar/diplomky/pruvodce_hw/komponenty/karty/sitovka/aktivni.htm

[5] What Is a Network Switch vs. a Router?. *Cisco* [online]. San Jose: Cisco Systems, Inc., 2017 [cit. 2017-10-18]. Available from: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/connect-employees-offices/network-switch-what.html

[6] Router. *Router* [online]. Atlanta: Margaret Rouse, TechTarget, 2016 [cit. 2017-10-18]. Available from: http://searchnetworking.techtarget.com/definition/router

[7] NAT. In: *ITBIZ* [online]. Prague: Nitemedia s.r.o., 2014 [cit. 2017-10-18]. Available from: http://www.itbiz.cz/slovnik/telekomunikace/nat

[8] What Is a Firewall. *Cisco* [online]. San Jose: Cisco Systems, Inc., 2017 [cit. 2017-10-18]. Available from: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

[9] PŘIBYL, Tomáš. Firewall: software nebo hardware. In: *ICT security* [online]. Prague: AVERIA, s. r. o., 2010 [cit. 2017-10-20]. Available from: http://www.ictsecurity.cz/odborne-clanky/3384-firewall-software-nebo-hardware

[10] GONZALEZ, Barb. What is a Powerline Adapter?. In: *Life Wire* [online]. New York: Life Wire, 2017 [cit. 2017-11-19]. Available from: https://www.lifewire.com/what-is-a-powerline-adapter-1846813

[11] EASTON, Richard. What is Powerline networking? And how fast is it versus Wi-Fi?. In: *Expert Reviews* [online]. London: Dennis Publishing, 2016 [cit. 2017-11-19]. Available from: http://www.expertreviews.co.uk/networks/powerline-networking/1404304/what-is-powerline-networking-and-how-fast-is-it-versus-wi-fi

[12] *Guide to computer network security*. 3rd. New York, NY: Springer Berlin Heidelberg, 2015. ISBN 9781447166535.

[13] FILIP, Mgr.,. *Nájemní smlouva - Turris*. 3. Praha, 2016. Dostupné také z: https://www.turris.cz/media/uploaded/Turris-smlouva_se_zakaznikem_v3.pdf

[14] Turris - Hardware details. *Turris* [online]. Prague: CZ.NIC, 2016 [cit. 2017-01-14]. Available from: https://www.turris.cz/en/hardware

[15] Turris Omnia - Features. *Turris Omnia* [online]. Prague: CZ.NIC, 2016 [cit. 2017-01-31]. Available from: https://omnia.turris.cz/en/#features

[16] Cisco RV320 Dual Gigabit WAN VPN Router Data Sheet. *Cisco* [online]. San Jose: Cisco, inc, 2017 [cit. 2017-11-01]. Available from:

https://www.cisco.com/c/en/us/products/collateral/routers/rv320-dual-gigabit-wan-vpn-router/data_sheet_c78-726132.html

[17] Cisco RV320 Dual Gigabit WAN VPN Router Reviewed. *Small Net Builder* [online]. New York: Doug Reid, 2014 [cit. 2017-11-01]. Available from: https://www.smallnetbuilder.com/lanwan/lanwan-reviews/32317-cisco-rv320-dual-gigabit-wan-vpn-router-reviewed

[18] ZyXEL USG40 Next-Gen Unified Security Gateway-Performance Series Reviewed. *Small Net Builder* [online]. New York: Doug Reid, 2014 [cit. 2017-11-01]. Available from: https://www.smallnetbuilder.com/lanwan/lanwan-reviews/32550-zyxel-usg40-next-gen-unified-security-gateway-performance-series-reviewed

[19] Next Generation Unified Security Gateway-Performance Series: USG40/40W/60/60W. *ZYXEL* [online]. Zyxel Communications Inc., Anaheim, CA [cit. 2017-11-01]. Available from: http://www.zyxel.com/us/en/products_services/usg60w_60_40w_40.shtml?t=p

[20] Mobile Device Management. In: *TechTarget* [online]. Atlanta: Margaret Rouse, 2013 [cit. 2017-10-18]. Available from: http://searchmobilecomputing.techtarget.com/definition/mobile-device-management

[21] Solutions: Mobile device management. *Cisco Meraki* [online]. San Jose: Cisco Systems, Inc., 2017 [cit. 2017-10-18]. Available from: https://meraki.cisco.com/solutions/mobile-device-management

[22] Systems Manager Free 100 Terms and Conditions. In: *Cisco Meraki: Support Policies* [online]. San Jose: Cisco Systems, Inc., 2017 [cit. 2017-10-20]. Available from: https://meraki.cisco.com/support/#policies:smfree100

[23] LINDER, Josh. Cisco Meraki Systems Manager Review. In: *Tom's IT PRO* [online]. New York: Tom's IT Pro, 2016 [cit. 2017-10-20]. Available from: http://www.tomsitpro.com/articles/cisco-meraki-systems-manager-review,2-1105.html

[24] SCHULZ, Matt. AirWatch vs. XenMobile EMM: Which is right for you?. In: *Tech Target* [online]. Atlanta: Tech Target, 2016 [cit. 2017-10-20]. Available from: http://searchmobilecomputing.techtarget.com/tip/AirWatch-vs-XenMobile-EMM-Which-is-right-for-you

[25] Modernize Windows Management and Security. *Windows 10 Management* [online]. Atlanta: VMWare, 2017 [cit. 2017-10-20]. Available from: https://www.air-watch.com/solutions/windows-10-management/

[26] AirWatch Mobile Device Management. In: *YouTube* [online]. San Francisco: MobisecTechnologies, 2013 [cit. 2017-10-22]. Available from: https://www.youtube.com/watch?v=VmgAlReJQ8s&t=16s

[27] Compare XenMobile vs. AirWatch. In: *Finances Online* [online]. Palo Alto: Finances Online, 2017 [cit. 2017-10-22]. Available from: https://comparisons.financesonline.com/xenmobile-vs-airwatch

[28] Deliver the most complete enterprise mobility management solution. *Citrix* [online]. Fort Lauderdale: Citrix Systems, Inc., 2017 [cit. 2017-10-20]. Available from: https://www.citrix.com/products/xenmobile/

[29] What is ISO 27001. In: *You Tube* [online]. San Bruno, San Francisco: Dejan Kosutic, 2012 [cit. 2017-11-20]. Available from: https://www.youtube.com/watch?v=AzSJyfjIFMw

[30] What is ISO 27001. In: *You Tube* [online]. San Bruno, San Francisco: Risk Factory, 2015 [cit. 2017-11-20]. Available from: https://www.youtube.com/watch?v=hPwmeYPE6VI

[31] *What is the difference between ISO/IEC 27001 and ISO/IEC 27002?* [online]. San Francisco: PECB, 2017 [cit. 2017-11-23]. Available from: https://www.youtube.com/watch?v=taXcjfulU-o

[32] *ISO27002 Foundation Preview* [online]. Nevada: Pink Elephant Netherlands, 2012 [cit. 2017-11-23]. Available from: https://www.youtube.com/watch?v=m0_A-Ptlyvc

[33] ISO/IEC 27002. *Information technology: Security techniques*. Second edition. Geneva: ISO copyright office, 2013.

[34] HOFFMAN, Chris. Which is the Best VPN Protocol? PPTP vs. OpenVPN vs. L2TP/IPsec vs. SSTP. In: *How To Geek* [online]. California: How-To Geek, LLC, 2015 [cit. 2017-11-18]. Available from: https://www.howtogeek.com/211329/which-is-the-best-vpn-protocol-pptp-vs.-openvpn-vs.-l2tpipsec-vs.-sstp/

[35] FAWKES, Guy. Srovnání VPN Protokolů: PPTP vs. L2TP vs. OpenVPN vs. SSTP vs. IKEv2. In: *VPN mentor* [online]. Washington: vpnMentor, 2017 [cit. 2017-11-18]. Available from: https://cs.vpnmentor.com/blog/srovnani-vpn-protokolu-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

[36] *Technological and Economic Development of Economy: Pairwise comparison matrix in multiple criteria decision making*. 2016, **1**(1). ISSN 2029-4913.

[37] *International Journal of Services Sciences: Decision making with the analytic hierarchy process*. Thomas L. Saaty, 2008, **1**(1). ISSN 1753-1454.

[38] Systems Manager Licensing. *Cisco Meraki Documentation* [online]. San Jose: Cisco Systems, Inc., 2017 [cit. 2017-11-22]. Available from: https://documentation.meraki.com/zGeneral_Administration/Licensing/Systems_Manager_Licensing

[39] Turris - Data collection. *CZ.NIC* [online]. Prague: CZ.NIC, z. s. p. o., 2017 [cit. 2017-11-02]. Available from: TurrisOmnia/foris/config/data-collection/

[40] Schnapps. *Project:Turris/doc* [online]. Prague: CZ.NIC, z. s. p. o., 2017 [cit. 2017-11-02]. Available from: https://www.turris.cz/doc/en/howto/schnapps

[41] Failover to LTE using mwan3. *Project Turris: Documentation* [online]. Prague: CZ.NIC, z. s. p. o., 2017 [cit. 2017-11-05]. Available from: https://www.turris.cz/doc/en/howto/multiwan

[42] How to use multiple WAN connections using the mwan3 package. *OpenWRT: Wireless Freedom* [online]. San Francisco: Open WRT forum user "cmalcolm", 2017 [cit. 2017-11-05]. Available from: https://wiki.openwrt.org/doc/howto/mwan3

9 Appendix

9.1 Network Config file content

```
config interface 'loopback'
     option ifname 'lo'
     option proto 'static'
     option ipaddr '127.0.0.1'
     option netmask '255.0.0.0'

config globals 'globals'
     option ula_prefix 'fd10:bdbd:d862::/48'

config interface 'lan'
     option force_link '1'
     option type 'bridge'
     option proto 'static'
     option netmask '255.255.255.0'
     option ip6assign '60'
     option ipaddr '192.168.5.1'
     option _orig_ifname 'eth0 eth2 wlan0 wlan1'
     option _orig_bridge 'true'
     option ifname 'eth0.1'

config interface 'wan'
     option ifname 'eth1'
     option proto 'static'
     option ipaddr '81.92.157.216'
     option netmask '255.255.255.192'
     option gateway '81.92.157.254'
     list dns '8.8.8.8'
     list dns '81.92.155.1'
     option metric '15'

config interface 'wan6'
     option ifname '@wan'
     option proto 'dhcpv6'

config switch
     option name 'switch0'
     option reset '1'
     option enable_vlan '1'

config switch_vlan
     option device 'switch0'
     option vlan '1'
     option vid '1'
     option ports '0 5t'

config switch_vlan
     option device 'switch0'
     option vlan '2'
     option vid '2'
     option ports '4 6'

config interface 'guest_turris'
     option enabled '1'
     option type 'bridge'
     option ifname 'guest_turris_0 guest_turris_1'
     option proto 'static'
     option ipaddr '10.111.222.1'
     option netmask '255.255.255.0'
     option bridge_empty '1'

config interface 'vpn_turris'
     option ifname 'tun_turris'
     option proto 'none'
     option auto '1'

config interface 'wan2'
     option _orig_ifname 'eth0.2'
     option _orig_bridge 'false'
     option proto 'static'
     option netmask '255.255.255.252'
     option gateway '10.9.116.9'
     option ipaddr '10.9.116.10'
     option ifname 'eth2'
     option metric '10'

config switch_vlan
     option device 'switch0'
     option vlan '3'
     option vid '3'
     option ports '1 2 3 5t'

config interface 'lan_studia'
     option ifname 'eth0.3'
     option _orig_ifname 'eth0.3'
     option _orig_bridge 'false'
     option proto 'static'
     option ipaddr '192.168.6.1'
     option netmask '255.255.255.0'
```

9.2 Multiwan configuration file content

```
config interface 'wan2'
     list track_ip '8.8.8.8'
     list track_ip '208.67.220.220'
     option reliability '1'
     option count '1'
     option timeout '2'
     option interval '5'
     option down '3'
     option up '8'
     option enabled '1'

config interface 'wan'
     list track_ip '8.8.4.4'
     list track_ip '8.8.8.8'
     list track_ip '208.67.222.222'
     list track_ip '208.67.220.220'
     option reliability '2'
     option count '1'
     option timeout '2'
     option interval '5'
     option down '3'
     option up '8'
     option enabled '1'

config member 'wan_m1_w3'
     option interface 'wan'
     option metric '1'
     option weight '3'

config member 'wan_m2_w3'
     option interface 'wan'
     option metric '2'
     option weight '3'

config member 'wan2_m1_w2'
     option interface 'wan2'
     option metric '1'
     option weight '2'

config member 'wan2_m2_w2'
     option interface 'wan2'
     option metric '2'
     option weight '2'

config policy 'wan_only'
     list use_member 'wan_m1_w3'

config policy 'wan2_only'
```

```
     list use_member 'wan2_m1_w2'

config policy 'balanced'
     list use_member 'wan_m1_w3'
     list use_member 'wan2_m1_w2'

config policy 'wan_wan2'
     list use_member 'wan_m1_w3'
     list use_member 'wan2_m2_w2'

config policy 'wan2_wan'
     list use_member 'wan_m2_w3'
     list use_member 'wan2_m1_w2'

config rule 'https'
     option sticky '1'
     option dest_port '443'
     option proto 'tcp'
     option use_policy 'balanced'

config rule 'default_rule'
     option dest_ip '0.0.0.0/0'
     option use_policy 'balanced'

config rule 'ftpJustOne'
     option dest_port '20,21,22,990'
     option sticky '1'
     option use_policy 'balanced'
     option proto 'tcp'
```