Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Diplomová práce

Zabezpečení chytré domácí sítě

Bc. Lucie Bobková

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Lucie Bobková

Informatika

Název práce

Zabezpečení chytré domácí sítě

Název anglicky

Smarthome network security

Cíle práce

Hlavním cílem diplomové práce je zabezpečit chytrou domácnost s využitfm nástrojů pro správu domácí počítačové sítě a konfigurace jejích síťových prvků.
Cílem teoretické části je popis typů útoků a hrozeb, které mohou nastat při nedostatečném zabezpečení sítě. Dále definice pojmu chytré domácnosti, spolu s analýzou prvků chytré domácnosti. V neposlední řadě je cílem popis problematiky počítačových sítf, síťových prvků, zabezpečení sítf a samotného fungování sítf.
Cílem praktické části je vytvoření blokového schématu, který bude reprezentovat rozdělení celé domácí sítě na jednotlivé bloky, které budou nést své vlastní zabezpečující prvky a svou specifickou konfiguraci.
Přínosem práce je poskytnutf návrhu řešení zabezpečení chytré domácnosti s využitfm podsítf, správy přístupu do jednotlivých bloků a konfigurace síťových prvků.

Metodika

Metodika řešeného problému v diplomové práci vychází z analýzy a studia odborných informačních zdrojů. V teoretické části práce je vytvořen teoretický podklad pro praktickou část. Jsou definovány pojmy týkající se chytré domácnosti, počítačových sítf a zabezpečení, dále jsou rozebrány útoky a hrozby, které mohou nastat při nezabezpečení chytré domácí sítě. V části praktické jsou vytvořeny podsítě pomocí subnetování. Vzniklé sítě jsou zakresleny do blokového schématu a je navržena vhodná konfigurace. Následně je toto schéma vytvořeno v softwaru Packet Tracer, kde je ověřena konektivita, zabezpečení a navržená konfigurace.

Doporučený rozsah práce

60-80 stran

Klíčová slova

bezpečnost, IoT, chytrá domácnost, počítačová síť, firewall, subnetting, Packet Tracer

---

Doporučené zdroje informací

DOSTÁLEK, Libor. KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. Brno: Computer Press, 2012. ISBN 978-80-251-2236-5.

CHEW, Daniel. The Wireless Internet of Things: A Guide to the Lower Layers. 2018. Spojené Státy Americké: Standards Information Network. ISBN: 978-1119260578

CHOU, Timothy. Precision: Principles, Practices and Solutions for the Internet of Things. 2020. Spojené Státy Americké: lulu.com. ISBN: 978-1329843561

VANDOME, Nick. Smart Homes in easy steps: Master smart technology for your home. 2018. Spojené Státy Americké: In Easy Steps Limited. ISBN: 978-1840788259

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Ing. Dana Vynikarová, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 31. 10. 2022

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 28. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 30. 03. 2023

Čestné prohlášení

Prohlašuji, že svou diplomovou práci ‚Zabezpečení chytré domácí sítě' jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 10.2.2023 _____

Poděkování

Ráda bych touto cestou poděkovala Ing. Daně Vynikarové, Ph.D. z Katedry informačního inženýrství za vedení, odborné rady, veškerý věnovaný čas a trpělivost po celý proces tvorby práce.

Zabezpečení chytré domácí sítě

Abstrakt

Tato diplomová práce se zabývá problematikou zabezpečení sítě pro chytrou domácnost. V teoretické části je vysvětlen pojem internet věcí (IoT), jeho vznik, historie a jeho další vývoj. Také jsou uvedeny příklady jeho užití se zaměřením na využití IoT v domácnostech. Na základě analýzy odborných zdrojů jsou vysvětleny technologie přenášení dat v IoT a uvedeny příklady používaných protokolů. Jsou vypsány možné komponenty chytré domácnosti, jejich funkce a účel. V práci je dále rozebrána bezpečnost IoT a popsána technologie blockchain. Je vysvětlen pojem počítačových sítí a jejich fungování. Je popsán referenční model ISO/OSI a vysvětleny funkce jednotlivých vrstev v modelu. Síťový model TCP/IP je definován spolu s protokoly. Tato práce také vysvětluje princip ip adresace, pojem podsítí a také popisuje techniku subnettingu. V neposlední řade je rozebráno samotné zabezpečení počítačových sítí. Jsou popsány typy síťových útoků a hrozeb. Následně jsou rozebrány metody, postupy a nástroje, kterými lze počítačovou síť chránit před těmito hrozbami. V závěru teoretické části je popsán software Packet Tracer, ve kterém bude na závěr testován výsledný návrh zabezpečení chytré domácí sítě. V praktické části této diplomové práce je řešeno samotné zabezpečení chytré domácí sítě s využitím konfigurace síťových prvků a subnettingu. Návrh rozdělení sítě je vyobrazen pomocí blokového schématu a je zobrazen proces vytvoření podsítí pomocí subnettingu. Konfigurace síťových prvků, spolu s užitými příkazy, je popsána a zároveň je vysvětlena funkce použitých příkazů. Výsledný návrh je nasimulován v softwaru Packet Tracer. Je ověřena konektivita síťových prvků, jejich zabezpečení, konfigurace a také funkčnost celé sítě.

Klíčová slova: IoT, chytrá domácnost, počítačová síť, zabezpečení sítě, firewall, subnetting, Packet Tracer

Smarthome network security

Abstract

This diploma thesis deals with the issue of network security for the smart home. The concept of the Internet of Things (IoT), its origin, history and further development is explained in the theoretical part. Examples of its use are also given, focusing on the use of IoT in households. Based on the analysis of professional sources, the technologies of data transfer in IoT are explained and examples of the protocols used are given. Possible components of a smart home, their functions and purpose are listed. IoT security is further discussed in the thesis and blockchain technology is described. The concept of computer networks and their functioning is explained. The ISO/OSI reference model is described and the functions of individual layers in the model are explained. The TCP/IP network model is defined along with the protocols. This thesis also explains the principle of ip addressing, the concept of subnetting and also describes the technique of subnetting. Last but not least, the security of computer networks itself is discussed. Types of network attacks and threats are described. Subsequently, the methods, procedures and tools that can be used to protect the computer network from these threats are discussed. At the end of the theoretical part, the Packet Tracer software is described, in which the resulting smart home network security proposal will be tested. In the practical part of this thesis, the security of the smart home network itself is addressed using the configuration of network elements and subnetting. The design of network partitioning is illustrated using a block diagram and the process of creating subnets using subnetting is shown. The configuration of the network elements, together with the commands used, is described and at the same time the function of the commands used is explained. The resulting design is simulated in Packet Tracer software. The connectivity of network elements, their security, configuration, and the functionality of the entire network are verified.

Keywords: IoT, smart home, computer network, network security, firewall, subnetting, Packet Tracer

Obsah

1 Úvod

Svět se stává čím dál tím více propojený a digitální. Tento vývoj zastihnul i domácnosti, kdy byla snaha propojit a digitalizovat naše domácí prostředí a tak vznikl trend chytrá domácnost. Chytré domácnosti jsou vybavené zařízeními, které jsou připojené k internetu a ovládají se na dálku pomocí chytrých telefonů, tabletů či pomocí automatizačních technologií. Lze takto ovládat různé aspekty domácího prostředí, od osvětlení a teploty až po bezpečnostní systémy, hudbu či si na dálku zkontrolovat stav lednice. I když inteligentní domácnosti nabízejí mnoho výhod, jako je pohodlí a energetická účinnost, přicházejí také s novými bezpečnostními riziky, které je třeba řešit.

Chytré domácí sítě jsou bez řádného zabezpečení velice zranitelné vůči řadě bezpečnostních hrozeb, jako třeba malware, kybernetické útoky či hackeři. Tyto hrozby mohou způsobit neoprávněný přístup k citlivým informacím, jako třeba čísla kreditních karet, rodná čísla, čísla telefonů, hesla a jiné důležité informace. Také je zde riziko, že neoprávněná osoba získá přístup k ovládání chytrého domu a tím může například ovládat bezpečnostní kamery, otevřít chytré zámky či vypnout vytápění nebo chlazení a rozsvěcet světla dle libosti.

Právě zvyšující se počet chytrých zařízeních v domácnostech vytváří širokou škálu potenciálních terčů, které jsou zranitelné vůči útokům. Tato široká škála dává větší prostor pro útoky, což ztěžuje zabezpečení sítě. Proto je čím dál tím více důležité dbát na správné a efektivní zabezpečení chytré domácí sítě a předejít tak možným škodám.

Cílem této práce je vytvořit účinná bezpečnostní opatření pro chytrou domácí síť, které výrazně sníží rizika napadení. V první kapitole je popsána historie internetu věcí, využití, budoucí vývoj a jeho architektura pro bližší seznámení s konceptem jako takovým. Tato kapitola se také věnuje přenosovým technologiím, které se využívají pro přenos dat mezi chytrými zařízeními. Jsou vysvětleny protokoly jako je Z-Wave, Bluetooth či WiFi. Dále jsou vyjmenovány komponenty chytré domácnosti a je pojednáno o bezpečnosti internetu věcí jako takového. V druhé kapitole jsou popsány počítačové sítě a jejich náležitosti. Od vysvětlení referenčního modelu ISO/OSI, po síťový model TCP/IP, kde jsou rozebrány vrstvy a protokoly těchto modelů. Je vysvětlen pojem ip adresace a technika subnettování. Třetí kapitola je věnována samotnému zabezpečení sítí, kde jsou popsány metody, opatření a nástroje pro zvýšení bezpečnosti počítačových sítí. Jsou popsány typy útoků, které mohou nastat. Útoky jako je DoS (Denial of service) útok či MiM (man in the middle) útok. Část

této kapitoly je také věnována konfiguraci síťových prvků a vypsání základních příkazů pro jejich nastavení. Poslední kapitola je věnována samotnému vytvoření návrhu zabezpečení. Pomocí techniky subnettingu je síť rozdělena na menší, lépe spravovatelné celky, které jsou zakresleny v blokovém schématu. Následuje konfigurace síťových prvků, které nesou svá bezpečnostní opatření, pro zajištění bezpečnosti celé sítě. Konečnou fází je testování celého návrhu v softwaru Packet tracer, kde se ověřuje konektivita, zvolená konfigurace u jednotlivých zařízeních a celková funkčnost sítě.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem diplomové práce je zabezpečit chytrou domácnost s využitím nástrojů pro správu domácí počítačové sítě a konfigurace jejích síťových prvků. Cílem teoretické části je popis typů útoků a hrozeb, které mohou nastat při nedostatečném zabezpečení sítě. Dále definice pojmu chytré domácnosti, spolu s analýzou prvků chytré domácnosti. V neposlední řadě je cílem popis problematiky počítačových sítí, síťových prvků, zabezpečení sítí a samotného fungování sítí.

Cílem praktické části je vytvoření blokového schématu, který bude reprezentovat rozdělení celé domácí sítě na jednotlivé bloky, které budou nést své vlastní zabezpečující prvky a svou specifickou konfiguraci.

Přínosem práce je poskytnutí návrhu řešení zabezpečení chytré domácnosti s využitím podsítí, správy přístupu do jednotlivých bloků a konfigurace síťových prvků.

2.2 Metodika

Metodika řešeného problému v diplomové práci vychází z analýzy a studia odborných informačních zdrojů. V teoretické části práce je vytvořen teoretický podklad pro praktickou část. Jsou definovány pojmy týkající se chytré domácnosti, počítačových sítí a zabezpečení, dále jsou rozebrány útoky a hrozby, které mohou nastat při nezabezpečení chytré domácí sítě. V části praktické jsou vytvořeny podsítě pomocí subnetování. Vzniklé sítě jsou zakresleny do blokového schématu a je navržena vhodná konfigurace. Následně je toto schéma vytvořeno v softwaru Packet Tracer, kde je ověřena konektivita, zabezpečení a navržená konfigurace.

3 Teoretická východiska

3.1 Internet věcí

Internet věcí (IoT) je komplexní síť objektů, které jsou vzájemně propojeny pomocí internetu. Všechny tyto objekty shromažďují data, která jsou následně sdílena po síti. Tato sdílená data jsou opět využívána jinými objekty. Tato data představují velmi širokou škálu informací z reálného světa, informace o prostředí, o pohybu, ale také o podmínkách a způsobech používání konkrétního zařízení. Za objekty lze považovat jak zařízení, tak osoby. Tyto vzájemně propojené a komunikující objekty mají vždy svůj účel. Tento účel je většinou vždy určen člověkem a může jím být například zjednodušení výroby, úspora nákladů a energie, hledání trendů či vzorů, rychlejší reakce v logistických centrech, mapování trasy objektů nebo prostě zpříjemnění či zjednodušení běžných lidských činností.

Pojem internet věcí spojuje velké množství technologií a dohromady tvoří ucelený koncept, který svou komplexností a širokou dostupností nabízí obrovský technologický potenciál a dosud neobjevené možnosti. Dá se říci, že internet věcí je technologie, která postupně utváří naši budoucnost.

3.1.1 Historie IoT

Samotná myšlenka, kdy stroje spolu komunikují a spolupracují při minimálním zásahu člověka, aby za nás vykonávaly různé úkony a tím nám ušetřily čas a energii, existovala ještě předtím, než byl zavedený odborný název a než se vůbec začal tento koncept považovat za ucelenou technologii, která má obrovský potenciál pro budoucí rozvoj technologického odvětví. Již na počátku 19. století byl sestrojen elektromagnetický telegraf, taktéž byl nazýván jako bezdrátový telegraf. V polovině 20. století začal vývoj samotných počítačů, o pár let později vzniká ARPANET, který se v 80. letech otevírá pro veřejnost a dává tak možnost k vývoji internetu, jak je znán dnes. V druhé polovině 20. století vzniká doménový systém, koncept M2M komunikace, Global Positioning Satellites (GPS), protokol TCP/IP a samotný World Wide Web, přičemž všechny tyto technologie nás posouvají k momentu, kdy se samotná myšlenka komunikujících a autonomních strojů začíná stávat realizovatelným konceptem. Této myšlence se říkalo například vestavěný internet nebo všudypřítomný computing. (19), (20), (21)

Mezi první IoT zařízení lze zařadit automat na nápoje Coca-cola, který byl vytvořen studenty na univerzitě Carnegieho-Mellonových v roce 1982. Tito studenti propojili tento automat s internetem a naprogramovali ho tak, aby jim hlásil, zda je nápoj k dispozici a zda je nápoj vychlazený, aby si ušetřili cestu k automatu, kdyby tomu tak nebylo. Jako další zařízení lze uvést chytrý toaster, který byl vytvořen Johnem Romkey v roce 1990. Tento toaster bylo možno ovládat přes internet. V roce 2000 společnost LG začala vyrábět chytrou lednici, která kontrolovala počet potravin. Jednalo se o první chytré zařízení pro domácnost, které se mělo sériově vyrábět, ale kvůli vysoké pořizovací ceně se tento produkt neprodával dobře a jeho výroba byla zastavena. (19), (20), (21), (22)

Název, který tento koncept nese dnes, byl vytvořen Kevinem Ashtonem v roce 1999. Ashton tímto termínem nazval svou prezentaci, při které prezentoval novou technologii RFID (Radio Frequency Identification) pro společnost Procter&Gamble. Při prezentaci také vyslovil svou myšlenku, že by data na internetu mohla být využívána ve firmách pro zlepšení efektivity práce a také by mohli ušetřit náklady a energii. Přičemž by tato data byla sdílena mezi stroji a zároveň by stroje data samotná poskytovaly ostatním zařízením. Ashtonovi se podařilo získat pozornost některých osob ve vedení společnosti, ale samotný termín se rozšířil až o pár let později. (21), (22)

V roce 2003 přední firmy začínají používat IoT označení místo dosud užívaného termínu M2M, zároveň se termín IoT začíná vyskytovat v uznávaných publikacích jako The Guardian, Scientific American nebo třeba Boston Globe. IoT se tedy dostává do povědomí široké veřejnosti i mnoha společnostem a jsou zakládány různé projekty, které si kladou za úkol s touto technologií pracovat a implementovat ji do zařízení z různých odvětví. (19), (20)

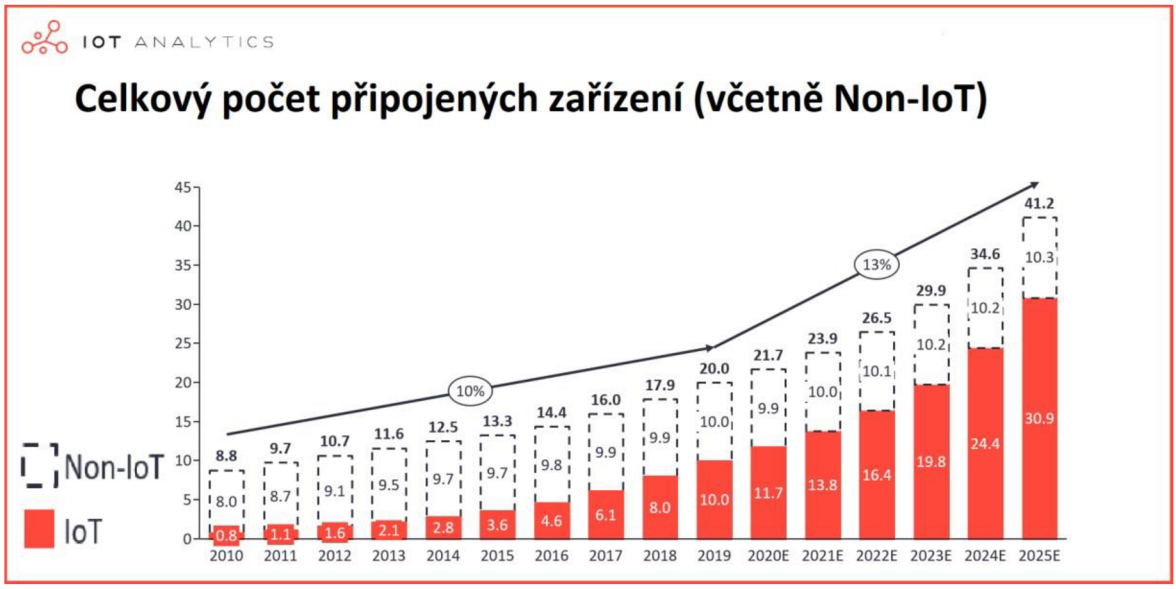
V roce 2008 je zformována nezisková organizace IPSO Alliance (The Internet Protocol for Smart Objects Alliance), která vznikla za účelem podpořit používání stejného internetového protokolu v sítích tvořených chytrými zařízeními a umožnit tak fungování internetu věcí. Do této aliance vstoupilo více než 50 firem. Mezi členy můžeme jmenovat například společnosti jako Cisco, Bosh, Ericsson, Intel, Google a Fujitsu. Tato organizace v dnešní době pracuje na zdokonalování, objevování a implementaci nových nápadů do IoT sektoru. Období mezi roky 2008 a 2009 je považováno za zrod internetu věcí, kdy počet připojených zařízení k internetu přesáhl celkový počet obyvatel na planetě. A tento počet se

dokonce v roce 2015 zdvojnásobil, kdy součet připojených zařízení byl 13,3 miliard. (19), (20)

Rok 2011 znamenal pro internet věcí důležitý milník v jeho rozvoji. V tomto roce byl veřejně spuštěn protokol IPV6, který navyšoval adresový prostor na internetu, dovolující tak mnoha soukromým firmám i finančním agenturám začít využívat benefity internetu věcí a expandovat v této technologii. Tento protokol umožňuje 2^{128} adres na internetu. Dalším milníkem pro internet věcí je přelom roků 2013 a 2014, kdy IoT zařízení začínají využívat senzory. Díky senzorům lze měřit přesná data okolního prostředí, také dovolují chytrým termostatům a chytrému osvětlení reagovat a přizpůsobovat se momentální situaci okolí. V roce 2014 společnost Amazon představuje Alexu, hlasového asistenta pomocí kterého lze ovládal chytrou domácnost. Stále čím dál tím více firem začíná investovat do rozvoje IoT technologií a spolu s rozvojem internetu, přenosových technologií či hardwarových i softwarových možností internet věcí nalézá stále více uplatnění v různých odvětví lidského působení. V minulém roce, tj. rok 2020 bylo podle odhadů připojeno k internetu přes 20 miliard zařízení s tím, že se odhaduje 13% růst tohoto čísla každým rokem. (19), (20)

3.1.2 Budoucí vývoj IoT

V posledních letech zaznamenává IoT sektor rapidní růst jak ve vývoji, tak v užívání, ať už ve spotřebitelské, podnikové, zemědělské či zdravotní sféře. Je v povědomí široké veřejnosti a mnohé firmy investují do IoT vybavení, aby zefektivnili svou výrobu či služby. Rok 2020 a příchod covidové pandemie tento rozvoj více popohnal dopředu, jelikož zde byla nutnost zajistit online fungování většiny firem, služeb a zároveň zde byla nutnost rychleji rozšířit 5G sítě, aby byla zajištěna stabilní rychlost a dostupnost internetu v době, kdy vše začalo přecházet do online módu. IoT zařízení stále přibývají, stejně tak jako přibývají nové firmy zabývající se výrobou chytrých produktů, což zajišťuje konkurenci pro stávající výrobce. Ceny klesají a IoT se stává dostupnějším. Dále se rozšiřují způsoby využívání chytrých věcí. V roce 2020 poprvé přesáhl počet IoT zařízení počet non-IoT zařízení a podle odborníků tento trend bude už jenom stoupat, viz obrázek 1. (22)



Obrázek 1 - Graf počtu připojených zařízení (41)

IoT bude nadále expandovat do mnoha odvětví. Velký nárůst IoT zařízení zaznamená zdravotní péče. Pandemická krize zapříčinila nutnost omezení kontaktu mezi pacienty a lékaři a právě chytrá zařízení nám dovolují sledovat stav pacienta na dálku. Tyto technologie se budou nadále rozvíjet, kdy zařízení, která bude mít pacient na sobě, budou sledovat například jeho srdeční tep, teplotu či tlak. Tato data se budou odesílat do nemocnic nebo k určitému doktorovi a ten následně data vyhodnotí a určí jaké kroky třeba podniknout nebo zda je nutná osobní návštěva u doktora. Další možné rozšíření je i do způsobů výuky. Například virtuální prohlídka muzea uprostřed hodiny či efektivnější sdílení výukových materiálů a poznatků. IoT zařízení také umožní virtuální návštěvu přednášejícího ve třídě a tak možnost studentům přednést svůj výklad, aniž by musel cestovat do určitého města či země. Rozvoj IoT nastane i v průmyslu, kdy se bude více přecházet na chytrou výrobu a využívání IoT v logistice. Chytrá zařízení budou snižovat náklady, monitorovat stav opotřebení strojů a komponentů, predikovat poruchu, ale i vykonávat úkoly, které jsou pro lidi obtížné nebo i zdraví škodlivé. (23), (24), (25)

Vzhledem k neustálému růstu IoT technologií bude třeba vyřešit otázky týkající se bezpečnosti. Díky své distribuované povaze je IoT náchylné k útokům a ztrátě dat. Predikce odborníků se tedy shodují na tom, že se trh s IoT bude více zaměřovat na zvýšení bezpečnosti IoT sítí. Bude se jednat zejména o vylepšování a využívání technologie blockchain, která je již využívána například finančními institucemi. Tato technologie, také

nazývána jako technologie účetní knihy, je navržena pro systémy, kde spolu komunikuje mnoho jednotek. Tato komunikace je zaznamenávána v neměnných řetězcích a následně sdílena skrz celý systém bez možnosti jakékoliv změny. Tímto způsobem zajišťuje blockchain zabezpečený přenos dat v síti. Zároveň se předpokládá růst popularity technologie digital twins. Technologie digitálních dvojčat vytváří přesnou kopii objektu či procesu ve virtuálním prostoru, kde tato kopie má stejné vlastnosti i funkce jako její předloha. V tomto virtuálním prostoru lze testovat a nanečisto si vyzkoušet různé druhy vylepšení výroby, přidání nebo odebrání výrobní linky či zařazení nového výrobního postupu. Virtuální dvojče využívá nasbíraná data z reálného světa a simuluje situaci ve virtuálním světě. Ukazuje nám, co by nastalo, kdybychom chtěné změny provedli v realitě. Na základě nasbíraných dat pomocí chytrých zařízení nám digital twins pomáhají s rozhodováním. Tento proces ušetří výdaje a ukazuje zisk či ztrátu ještě před tím, než dané změny provedeme v realitě. (23), (24)

Jako vize do budoucna je stále prioritou rozšiřování 5G sítě. Sítě 5G znamenají pro internet věcí velký skok dopředu. Tato síť disponuje většími kanály, které zajišťují výrazné zrychlení dat, zároveň má 5G síť nízkou latenci, která poskytuje lepší odezvu. K této síti lze zapojit mnohem více zařízení najednou, tato vlastnost se převážně využije k zapojení senzorů a více chytrých zařízení, aniž by se síť přetížila. Další důležitou technologií pro internet věcí je cloud computing. Technologie cloud computing nashromážděná data odesílá na hlavní cloudový server, kde jsou tato data zpracována a odesílána zpět do zařízení. Tyto data jsou odesílána i na dlouhé vzdálenosti, což zvyšuje latenci. Vysoká letence může působit problémy při zpracovávání dat v reálném čase, kdy je rychlá odezva velmi důležitá. Do budoucna se odhaduje přecházení k edge computingu, kdy nashromážděná data se vyhodnocují přímo na zařízení, které je získá. Tato technologie je možná právě díky neustále se zvyšujícímu výpočetnímu výkonu chytrých zařízení. Jedná se o decentralizovaný systém, kdy odpadá jakékoliv odesílání dat na centrální server. Tímto se eliminují problémy s vysokou latencí, šířkou pásma, ale také se zlepšuje ochrana dat. (23), (24)

Internet věcí se posouvá od sběru a sdílení dat k vyhodnocování těchto získaných dat a následného použití výsledků. Vyhodnocená data pak využívá k vykonání určité činnosti, rozhodnutí a navržení možného řešení nebo okamžitého vybrání nejlepší varianty. Zde hraje velkou roli umělá inteligence a její spojování s IoT technologiemi. Postupně se termín Internet of Things posouvá k termínu Internet of Everything, kdy chytré prostředí

bude reagovat na každý náš pohyb či na každou změnu v okolí, kde každý podnět bude zpracováván a vyhodnocován. (24), (25)

3.1.3 Architektura IoT

Všechna IoT zařízení pracují s daty, což je odlišuje od běžných automatizovaných zařízení. Vzhledem k přítomnosti dat, zde musí být jistá architektura, která určí, kam data půjdou, jaký formát použijí, jak se dostanou na cílové místo a jakou akci vykonat na základě těchto dat. Jsou zde jisté vlastnosti, které by měla splňovat každá IoT architektura pro správné a efektivní fungování. Těmito prvky jsou funkčnost, škálovatelnost, dostupnost a udržovatelnost celého systému. (26)

IoT architekturu lze rozdělit do čtyř po sobě jdoucích stádií. Tyto čtyři úrovně popisují proces, kterým data projdou od senzorů až do cloudového úložiště. První úroveň je začátkem celého procesu. Zde hrají největší roli senzory a aktuátory. Senzory sbírají informace ze svého okolí v reálném světě. Může se jednat o vlhkost vzduchu, teplotu, tok vody v potrubí, rychlost výrobního pásu, úroveň paliva v nádrži, atd. Senzor tyto informace přemění na data, která jsou následně analyzována a zpracovávána na dalších úrovních dané architektury. Co se týče aktuátoru, tak ten je schopen reagovat na tyto informace a ihned vykonat akci, která se promítne do reálného světa. Aktuátor například vypne světlo nebo zvýší teplotu v místnosti na základě nasbíraných informací ze svého okolí. V druhé úrovni se jedná o systémy agregace dat ze senzorů a následný převod z analogové formy dat do dat v digitální podobě. Na této úrovni se data formátují, filtrují, ale také jsou komprimovány na optimální velikost pro přenos. Přenos takto upravených dat probíhá přes internetové brány. Tyto brány jsou zodpovědné za řízení oboustranného toku informací v systému a s řádným šifrováním a dalšími zabezpečujícími prvky mohou zabránit úniku dat a snížit riziko vnějších útoků na tento systém. Tímto se zvyšuje zabezpečení systému. Ve třetí úrovni, kdy už data jsou zdigitalizována a agregována, přichází na řadu koncové zařízení IoT systému, které data předběžně zpracuje před fází vstupu do datového centra. Součástí takového zpracování je i rozšířená analýza dat a další komprimace objemu dat. Zároveň toto koncové zařízení může poskytovat zpětnou vazbu do systému a průběžně vylepšovat samotný proces, aniž by čekalo na odezvu z datového centra nebo cloudu. Čtvrtá a zároveň poslední úroveň zařizuje analýzu, správu a ukládání dat. Hlavní procesy probíhají v datovém centru nebo cloudu. Jedná se tedy o podrobnou analýzu dat a následnou revizi zpětné vazby. Zpětnou

vazbou jsou například příchozí data, která mohou naznačovat žádoucí změny v nastavení určitých zařízení nebo mohou poukazovat na způsoby optimalizace procesu. V této úrovni se zpracovává ohromné množství dat a pro jejich analýzu jsou využívána velmi výkonná zařízení a jsou používány mechanismy strojového učení, tzv. machine learning. Pro hlubší analýzu jsou zde data kombinována z více senzorů či zdrojů z jiných provozních míst. Tento postup pak přináší širší obraz o celém IoT systému a zároveň poskytuje užitečné informace jak chytrým zařízením, tak manažerům, vedoucím či analytikům. Z těchto dat lze vyčíst například klíčové trendy, vzory nebo odhalit anomálie. Výstupem celého procesu jsou tedy informace, ale již ve své zpracované a zanalyzované formě. (26), (27)

Obrázek 2 - IoT architektura

3.1.4 Využití IoT

Internet věcí má velmi širokou škálu využití a používá se v mnoha odvětvích. Tato využitelnost se neustále rozšiřuje s tím, jak se IoT rozvíjí a přizpůsobuje se novým odvětvím. Internet věcí lze rozdělit do různých skupin užití. Nejznámějšími skupinami jsou industriální IoT a spotřebitelské IoT. V roce 2017 vzniká IoBT – Internet of Battlefield Things, což znamená využití IoT v armádě. Dále lze uvést IoT pro zemědělství, byznys, zdravotní péči, logistiku a transport. Spotřebitelské IoT nám nabízí možnost udělat naše prostředí chytřejší a propojenější. Do spotřebitelského IoT lze zařadit například chytrá auta, chytré kanceláře, chytré budovy a samozřejmě chytré domácnosti. Industriální IoT (IIoT) je často označováno jako čtvrtá průmyslová revoluce, kdy se chytrá zařízení začínají používat ve výrobě k optimalizaci výrobních procesů a snižování celkových nákladů na produkci. S příchodem technologie 5G internetu se začíná více realizovat i další odvětví IoT, chytrá města. (28), (29)

Za první chytré město se považuje Dublin, kdy se v roce 2014 vedení města rozhodlo využít funkce chytrých zařízení a konceptu IoT ke zlepšení funkcí samotného města. Byly zavedeny senzory na měření hluku, měření úrovně hladiny vody a také chytré odpadkové koše, které ukazovaly stupeň naplnění. Možnosti využití internetu věcí ve městech stále rostou a přibývají. Můžeme jmenovat například automatizovanou hromadnou dopravu, chytré systémy pro správu energie, distribuci vody, chytré dopravní značení, chytré semafory, monitorování životního prostředí a také zvýšení bezpečnosti města, pomocí chytrých kamer a mnohé další. Díky těmto technologiím lze lépe spravovat dopravu, energii, vodu či odpad ve městech nebo poskytnout možnost zobrazení volných parkovacích míst. Využíváním chytrých zařízení lze předejít nebo zcela odstranit každodenní či budoucí problémy, jako například dopravní zácpu, výpadky elektřiny, znečištění a obecné poruchy veřejných zařízení. Stále více měst přijímá tyto inovace, aby se stala úspornější a chytřejší. (28), (29)

V zemědělství se využívají převážně senzory, které nám měří například vlhkost půdy, úroveň kyselosti půdy, množství minerálů a vody v půdě a poté data odesílají. Tyto poznatky se pak využívají třeba k určení optimálního množství hnojiva nebo k lepší návratnosti investic do osázení půdy. V hospodářství se například sleduje zdravotní stav chovného dobytka a tím lze předcházet rozšiřování nemocí mezi zvířaty. (28), (29)

Ve zdravotnictví s využitím chytrých zařízení lze sledovat stav pacienta nepřetržitě, ať je kdekoliv. V případě naměření negativních hodnot se například hned zavolá záchranná služba nebo se kontaktuje doktor, který data vyhodnotí a navrhne následné řešení či doporučení. Zároveň nasbíraná data o jedinci lze využít pro podrobnější analýzu jeho zdravotního stavu. V některých nemocnicích již využívají chytré postele, které neustále měří teplotu, tlak, tep či okysličení organismu. (28), (29)

Výše zachycené možnosti využívání jsou jen zlomkem toho, co nám internet věcí nabízí a v čem všem ho lze najít. Vzhledem k povaze konceptu IoT, která je charakterizována zlepšováním procesů, rychlostí, pohodlím či bezpečností na všech úrovních, lze tuto technologii využít téměř všude.

3.1.5 Technologie přenosu dat v IoT

Internet věcí, jak z definice vyplývá, je seskupení zařízení, která mezi sebou komunikují, respektive si posílají data a tvoří vzájemně propojenou síť. Aby tato síť mohla vůbec fungovat, je zcela nezbytné, aby tato zařízení komunikovala stejným jazykem. Tuto problematiku nám řeší technologie pro přenos dat, které zajišťují komunikaci, propojení a přenos dat uvnitř dané sítě, kterou tvoří chytrá zařízení. Tyto technologie se dělí na drátové a bezdrátové. Drátové technologie pro přenos dat využívají fyzické kabelové propojení mezi zařízeními. Bezdrátové technologie využívají ke svému přenosu dat radiové vlny různé frekvence.

3.1.5.1 Kabelové provedení

V dnešní době se veškeré technologie vyvíjejí tak, aby kabely nebyly zapotřebí. Trendem současnosti je bezdrátové propojení, avšak stále je tu minimálně půlka zařízení, která fungují na kabelech a tyto linky jsou již zavedené. Proto se i drátové technologie stále rozvíjí a zlepšují. Zlepšuje se jejich dosah i rychlost. I přes veškerou popularizaci bezdrátových technologií, má v dnešní době kabelové provedení stále své jisté místo, a to kvůli své spolehlivosti a rychlosti. (30)

Všechna chytrá zařízení jsou propojena speciálním kabelem, který sbírá data a ty pak přenáší do výkonného zařízení. Jako příklady speciálních kabelů lze uvést optické kabely, koaxiální kabely či kroucené dvojlinky. Optický kabel lze považovat za nejrychlejší datový přenašeč, který funguje na bázi využívání světelných impulsů. Co se rychlosti týče, je potenciál optických kabelů opravdu vysoký. V laboratorních podmínkách se podařilo naměřit až 111 Gb/s. Kroucená dvojlinka je nejvíce známá a také nejvíce používaná, ale v současné době je priorita ji nahradit optickými kabely. Kroucená dvojlinka dosahuje rychlosti až 1 Gb/s. Posledním zmíněným zástupcem je koaxiální kabel, který je nejstarší používanou technologií z výše vyjmenovaných. V současné době se používá převážně jen na přenos televizního signálu. (32)

Některé z jejich výhod stále ještě nebyly překonány bezdrátovou konkurencí. K jejich nesporným výhodám patří bezpečnost. Data se přenáší po kabelech, většinou zabudovaných ve zdech či ve vnitřních prostorách budovy. Data se nevysílají vzduchem, kde mohou být ukradena či napadena. Vzhledem k fyzickému přenosu, je tato síť více spolehlivá,

méně náchylnější k výpadkům a naprosto odolná vůči kolizím s ostatními sítěmi. Kabelové provedení nám nabízí vyšší rychlost, právě kvůli tomu, že kabely nejsou ovlivněny tloušťkou zdi, materiálem zdi, zástavbou budovy, délkou pokoje či rušením od ostatních elektronických zařízení, jak tomu je u bezdrátového provedení. Na úkor těchto výhod existuji jisté nevýhody. Toto řešení je mnohem dražší než bezdrátové, kvůli nutnosti investice do kabelů, vypracování projektu zapojení či údržby a výměny kabelů při poškození. Kabely jsou zapracované do zdí, podlah či stropů, takže přidání či odebrání dalšího chytrého zařízení vyžaduje fyzický vstup do zástavby a znovu nakonfigurování systému. V porovnání s bezdrátovou technologií je kabelová mnohem méně flexibilní a hůře upravovatelná. (31)

3.1.5.2 Bezdrátové provedení

Komunikační bezdrátové technologie používají k přenosu dat rádiové vlny. Vytváří lokální síť, kde jsou spolu chytrá zařízení propojená, což jim umožňuje vzájemně si posílat a přijímat zprávy. V dnešní době existuje mnoho různých bezdrátových technologií, které se mezi sebou liší různými aspekty. Mezi tyto aspekty se rozhodně řadí jejich dosah, spotřeba energie, počet připojených zařízení, rychlost přenosu dat a frekvence. Mezi nejznámější a pro IoT používané technologie patří Wi-Fi, Bluetooth, ZigBee, Z-Wave, Thread, SigFox, LoRaWAN a NB-IoT. (1), (33)

Nespornou výhodou bezdrátového provedení je fakt, že instalace je velmi jednoduchá, není třeba projekt jako u kabelového řešení a také tuto technologii lze jednoduše implementovat do již postavené budovy, aniž bychom fyzicky zasahovali do stavby. Do bezdrátového řešení lze snadno přidávat a odebírat chytrá zařízení oproti kabelovému řešení. Z těchto vlastností vyplývá, že bezdrátové provedení je mnohem flexibilnější a lépe se přizpůsobuje požadavkům klienta. Vzhledem k tomu, že neinvestujeme do kabelového projektu a ani do samotných kabelů, je bezdrátové provedení levnější. Jelikož se data přenášejí pomocí radiových vln, je bezdrátové provedení více náchylné na útoky a krádeže informací. Možnou nevýhodou může být vznik kolize s ostatními sítěmi a vytvoření „hluchého“ místa. (1), (33)

3.1.5.2.1 Dálkové nízkoenergetické přenosové technologie

Do této kategorie spadají technologie určené k přenosu dat na velké vzdálenosti, které jsou označovány jako LPWAN (Low Power Wide Area Network). SigFox technologie má dosah až 50 km ve volné krajině, v zástavbě se tento dosah snižuje na 10 km. SigFox síť funguje na podobném principu jako sítě mobilních operátorů, proto musela být vystavěna fyzická síť vysílačů, aby se k ní IoT zařízení mohla připojovat. V České republice má SigFox 89% pokrytí a poskytuje i roamingový přenos dat. Jeho přenosová rychlost a spotřeba energie jsou velmi nízké. Tato technologie pracuje ve frekvenčním pásmu 868 MHz. Podporuje pouze omezenou obousměrnou komunikaci a je odolná vůči rušení. Další zástupcem dálkové přenosové technologie je LoRaWAN. Tato síť má dosah 5 až 10 km a pracuje ve frekvenčním pásmu 868 MHz. LoRa má otevřený standard, který nabízí zájemci možnost postavit si a provozovat vlastní LoRa síť, přičemž musí dodržovat LoRAWAN standard. Oproti SigFoxu nabízí LoRa plnohodnotnou obousměrnou komunikaci. NB-IoT patří k novějším technologiím, proto na trhu najdeme jen velmi málo výrobků, které tuto technologii podporují. Tato síť pracuje v licenčním frekvenčním pásmu 868 MHz, což zajišťuje bezpečný přenos dat. V České republice má 100% pokrytí. Vývoj a rozšíření této technologie podporují velké společnosti, jako například Huawei, Ericsson a Qualcomm. (34)

3.1.5.2.2 Z-Wave

Komunikační protokol Z-Wave, spadající pod společnost Silicon Labs, je bezdrátová přenosová technologie používající se převážně pro automatizaci domácností. Z-Wave tedy zajišťuje komunikaci mezi chytrými zařízeními v domácnosti, jako jsou světla, zámky, termostat, okenní rolety či garážová vrata. Díky velmi nízké spotřebě energie je také vhodný pro zařízení (např. senzory), která jsou napájena pomocí externích zdrojů, jako jsou například baterie. K síti Z-Wave může být připojeno až 232 zařízení. Tato síť funguje na principu mesh sítě, což znamená, že všechna zařízení spolu dokážou vzájemně komunikovat. Díky této vlastnosti si chytrá zařízení dokážou přeposílat zprávy, i když koncové zařízení není v dosahu. Toto přeposíláni je ale omezeno pouze na čtyři uzly, kde pátý uzel je koncový. Z-wave vždy upřednostňuje tu nejkratší a nejrychlejší cestu. Dosah této sítě je až sto metrů. Tento dosah je samozřejmě ovlivněn zástavbou a také materiálem zástavby, proto je pro optimální efektivitu doporučováno mít Z-Wave zařízení od sebe maximálně 30 stop. Z-wave

síť pracuje v přenosovém pásmu 868 MHz, takže zde nehrozí kolize s Wi-Fi sítí. Vzhledem k nižší nosné frekvenci dosahuje Z.Wave síť rychlosti až 100 kbit/s. Tuto síť lze spravovat přes aplikaci v mobilu, tabletu, počítači a také pomocí hlasových příkazů. (1), (35), (36)

Z-Wave protokol disponuje uzavřeným standardem, což znamená, že jeho zdrojový kód je uzavřený a neposkytuje tedy výrobcům možnost tento kód měnit. Touto vlastností se zajišťuje interoperabilita mezi zařízeními od různých výrobců. V praxi to znamená, že každé zařízení, které podporuje protokol Z-Wave, je schopno komunikace s každým starým i novým zařízením fungujícím na této komunikační technologii. Na současném trhu existuje již více než 2400 produktů používajících tento protokol od více než 450 výrobců, kteří jsou sdruženi v Z-wave Alliance. Tato aliance zajišťuje správu kompatibility produktů i jejich certifikaci. (1), (35)

Obrázek 3- Schéma Z-Wave domácnosti (42)

3.1.5.2.3 ZigBee

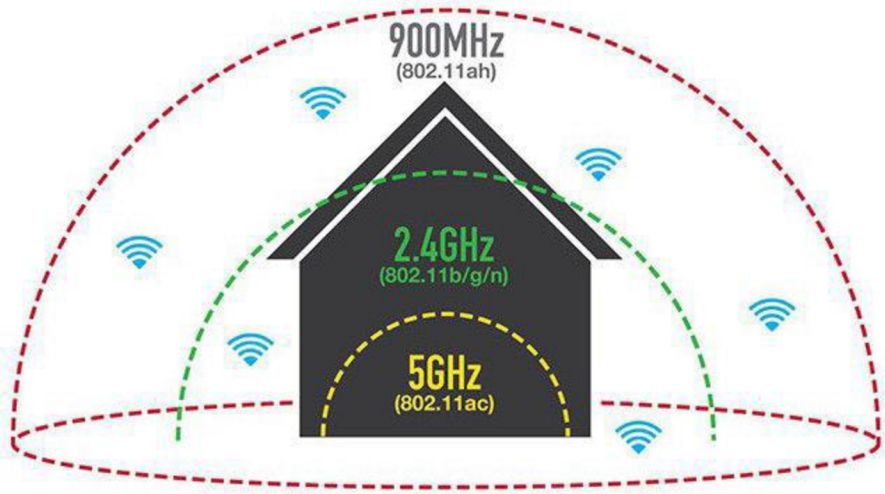
Přenosový protokol ZigBee, vyvíjený od roku 2002 ZigBee Aliancí, je bezdrátová komunikační technologie založená na standardu IEEE 802.15.4. Tato technologie se využívá pro vybudování personální sítě neboli PAN (Personal Area Networks). ZigBee tedy zajišťuje propojenost a komunikaci mezi všemi prvky chytré domácnosti, které jsou založeny na tomto protokolu. Jedná se o chytrá světla, termostaty, různé senzory, bezpečnostní zařízení či monitorování spotřeby vody a energie. Pro svou velmi nízkou energetickou náročnost nalézá uplatnění nejen v chytrých domácnostech, ale také i v menších průmyslových zónách. Zde se jedná převážně o sběr dat z bezdrátových senzorů. Nízká energetická spotřeba jde ruku v ruce s krátkou přenosovou vzdáleností. Síť ZigBee má dosah do vzdálenosti zhruba 75 metrů. Tato síť je založena na principu mesh sítě, což zajišťuje vzájemnou komunikaci všech zařízení v této síti. ZigBee síť je schopna pojmout až 65 000 chytrých produktů. Prvky v síti jsou schopné tzv. retranslace, přičemž zpráva může být přeposlána 64 krát a 65. zařízení je zde konečné. Tuto funkci nemohou využívat zařízení, která mají externí zdroj napájení, jelikož by museli být neustále činná a tím by se zvyšovala jejich spotřeba. ZigBee síť pracuje v přenosovém pásmu 2,4 GHz, což je stejné pásmo jako síť Wi-Fi, takže hrozí vznik hluchých míst. Toto přenosové pásmo síti Zigbee poskytuje přenosovou rychlost až 250 kbit/s. (1), (36), (37)

Protokol ZigBee je otevřený standard, dovolující výrobcům upravovat jeho zdrojový kód. Toto řešení vedlo v minulosti k mnoha problémům s kompatibilitou zařízení. Přesněji řečeno, bylo třeba kupovat zařízení pouze od jednoho výrobce, aby tato zařízení spolu mohla komunikovat. V roce 2015 byl vydán unifikovaný protokol ZigBee 3.0, který řeší tyto problémy a zajišťuje kompatibilitu napříč všemi výrobky, nehledě na výrobce. Tito výrobci jsou sjednoceni pod ZigBee Alliance, která čítá přes 300 firem. Na trhu lze nalézt přes 2500 produktů fungujících na protokolu ZigBee. (1), (36), (37)

Obrázek 4- ZigBee schéma (43)

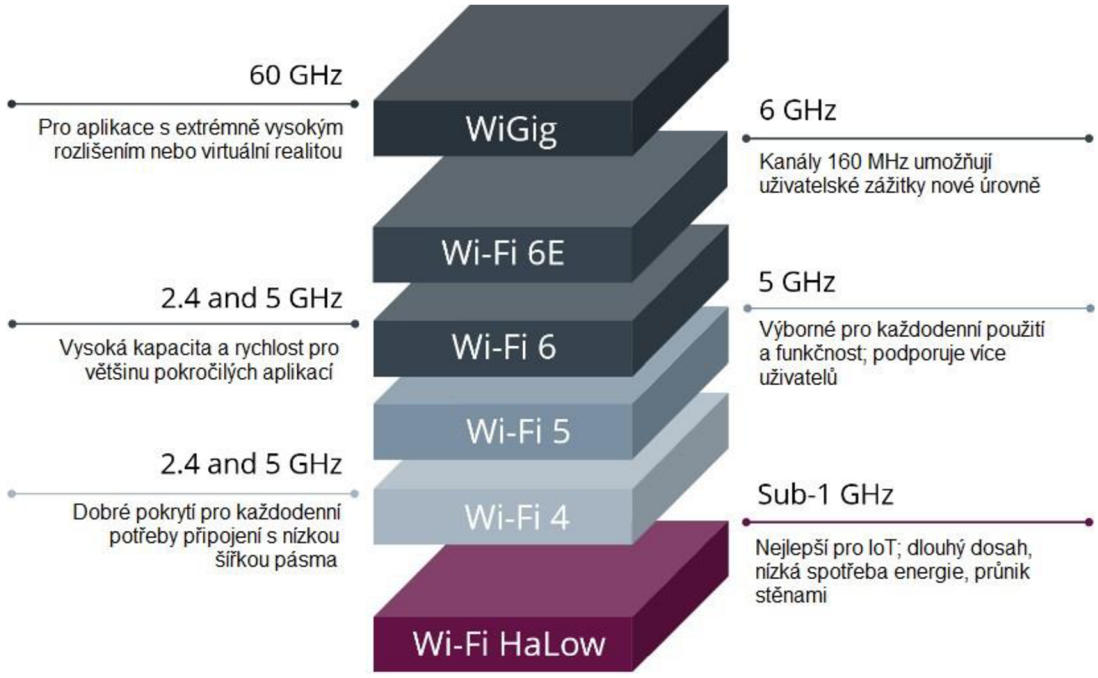
3.1.5.2.4 Wi-fi

Wi-fi je jedna z nejrozšířenějších bezdrátových technologií, nabízející velmi široké pokrytí. Její nejčastější užití je pro připojení zařízení k internetu, kdy je využíván router pro kódování signálu. Tento protokol funguje na standardu IEEE 802.11. Tyto standardy se neustále rozvíjejí a každá verze tohoto standardu nabízí jiné doplňky a rozšíření. Wi-fi má otevřený standard, který je aktualizován a neustále rozvíjen organizací Wi-Fi Alliance, aby byla zajištěna interoperabilita mezi produkty od různých výrobců. Tato aliance má na starost i certifikaci produktů. Wi-fi operuje ve frekvenčním pásmu 2,4 GHz nebo 5 GHz. Tyto frekvence jsou velmi využívané a právě díky tomu může dojít ke kolizi mezi zařízeními fungujícími na těchto frekvencích a výsledkem je, že ani jedno ze zařízení nedostane požadovanou šířku pásma. Sice tyto frekvence nabízejí vyšší datový tok, ale na úkor dosahu. Čím vyšší frekvence, tím je dosah kratší, viz obrázek 9. Klasický a domácnostmi využívaný wi-fi standard, ať už operující na 2,4 GHz nebo 5 GHz, je velmi náročný na energii, což silně omezuje využití wi-fi sítě pro chytrá zařízení, která jsou napájena bateriemi. (1), (38), (39)



Obrázek 5 - Dosah frekvenčních pásem (44)

Z výše uvedených informací je jasné, že vysokofrekvenční standardy wi-fi nejsou pro chytrou domácnost dobré řešení. Wi-fi Alliance proto vytvořila standard IEEE 802.11ah neboli Wi-Fi HaLow. Tento standard byl vyvinut speciálně pro využití v IoT. Wi-fi HaLow pracuje ve frekvenčním pásmu do 1 GHz, u nás je to pásmo 868 MHz. Tento protokol je vyvíjen s ohledem na spotřebu energie a poskytuje různé úsporné režimy. Pro svoji energetickou nenáročnost je tedy vhodný i pro chytrá zařízení, která jsou napájena bateriemi. Zároveň poskytuje větší dosah. Tento protokol nedisponuje vysokou rychlostí přenosu dat, což vzhledem k malému objemu odesílaných dat ze senzorů a čidel nevytváří žádný zásadní problém. Nízkofrekvenční radiové vlny mají i tu vlastnost, že lépe proniknou skrz zeď a další možné překážky vyskytující se v domácnostech. Zabezpečení wi-fi HaLow je stejné jako u ostatních standardů a také pravidelně aktualizované. Vzhledem k rozšířenosti wi-fi je pro uživatele jednoduší si přivyknout a vyznat se v tomto standardu. To samé platí pro instalaci, kdy se jenom přidají chytrá zařízení do již existující lokální sítě. Problém může nastat tehdy, kdy současný router či modem tuto frekvenci nepodporuje a je potřeba zařízení dokoupit. (1), (38), (39)



Obrázek 6 - Typologie wi-fi standardů (45)

3.1.5.2.5 Bluetooth

Bluetooth je klasifikován jako bezdrátová přenosová technologie, která byla vytvořena v roce 1994 k přímé komunikaci mezi zařízeními na krátkou vzdálenost. U menších zařízení se jedná o vzdálenost do 10 metrů, u větších zařízení o vzdálenost do 100 metrů. Tato vzdálenost se zdvojnásobuje u standardu Bluetooth 5.0, avšak záleží na překážkách a zástavbě prostoru. Bluetooth pracuje v oblíbeném pásmu 2,4 GHz. Bluetooth je energeticky náročný, jelikož udržuje zařízení neustále spárovaná, je zde tedy neustálý tok bitů. Kvůli tomuto negativu byl vyvinut nový standard Bluetooth Low Energy, který spojení mezi zařízeními udržuje v režimu spánku do doby, kdy zařízení nezačnou odesílat data. Díky tomuto vylepšení se výrazně snížila spotřeba energie a Bluetooth lze využívat i v chytrých domácnostech. Bluetooth Low Energy standard dosahuje přenosové rychlosti až 2 Mb/s a oproti klasickému Bluetooth standardu, který čítá 79 kanálů, má tato verze pouze 40 kanálů. Bluetooth rozděluje odesílaná data do těchto kanálů, snižuje se tak riziko kolize se sítěmi fungujícími na stejné frekvenci. Bluetooth je chráněnou značkou společnosti SIG (Special Interested Group), pod kterou jsou sloučeny všechny členské firmy, které chtějí vyrábět produkty s podporou Bluetooth technologie. Díky rozšířenosti tohoto globálního standardu existuje na trhu velmi mnoho výrobků, které podporují tento protokol. (38), (40)

Tabulka 1 - Porovnání Bluetooth verzí (46)

	Bluetooth Low Energy (LE)	Bluetooth Classic
Počet kanálů	40 kanálů	79 kanálů
Spotřeba energie	~0.01x to 0.5x z reference	1 (referenční hodnota)
Rychlost přenosu dat	LE 2M PHY: 2 Mb/s LE 1M PHY: 1 Mb/s LE Coded PHY (S=2): 500 Kb/s LE Coded PHY (S=8): 125 Kb/s	EDR PHY (8DPSK): 3 Mb/s EDR PHY (π/4 DQPSK): 2 Mb/s BR PHY (GFSK): 1 Mb/s
Maximální vysílací výkon	Class 1: 100 mW (+20 dBm) Class 1.5: 10 mW (+10 dbm) Class 2: 2.5 mW (+4 dBm) Class 3: 1 mW (0 dBm)	Class 1: 100 mW (+20 dBm) Class 2: 2.5 mW (+4 dBm) Class 3: 1 mW (0 dBm)

3.1.5.2.6 Thread

Thread je bezdrátová přenosová technologie, založená na standardu IEEE 802.15.4 a vyznačuje se tím, že používá IP adresaci. IP adresace zajišťuje vyšší bezpečnost přenosu dat, zároveň se jedná o technologii, která je velmi známá a rozšířená. IP adresování zajišťuje komunikaci bez použití brány. Jinak řečeno, chytré zařízení se díky své unikátní IP adrese připojí přímo k internetu, netřeba další zařízení, které bude dělat prostředníka mezi Thread protokolem a internetem. Thread je otevřený standard, dovolující vývojářům zdrojový kód vylepšovat a upravovat. Thread pracuje v pásmu 2.4 GHz s dosahem až 30 m a rychlostí 250 kb/s. Tato technologie funguje na principu mesh sítě, stejně jako ZigBee a Z-Wave. Oproti těmto standardům má vyšší spotřebu energie. Thread síť dokáže pojmout až 16 352 chytrých zařízení. Všechny partnerské firmy, které vyrábějí produkty s Thread podporou, jsou sjednoceny do Thread Group. Thread Group zajišťuje certifikaci produktů a jejich kompatibilitu. (36), (38)

3.1.6 Komponenty chytré domácnosti

Na trhu se neustále objevují nové a nové komponenty do chytré domácnosti, které nabízí nejrůznější funkce, rozličný vzhled, různé parametry a vlastnosti. Zajišťují tak široký výběr pro sestavení chytré domácnosti přizpůsobené požadavkům většiny spotřebitelů. Stále více firem investuje do vývoje a výroby chytrých zařízení pro domácnost a nejen pro ni. Zvyšuje se tak konkurence schopnost a výrobky jsou stále více cenově dostupnější pro běžné spotřebitele.

Lze vyjmenovat esenciální komponenty pro chytrou domácnost. Jedná se o komponenty, které zajišťují převážně bezpečí a úspory energie. Mezi takové zařízení patří chytrá centrální jednotka, chytrý termostat, chytré osvětlení, chytré kamery, chytré detektory, chytré zásuvky a chytré zámky. Mezi komponenty poskytující převážně úsporu času a komfort lze zařadit chytré domácí spotřebiče, chytrý garážový systém, chytrá multimediální zařízení, chytré zavlažovací systémy, chytré klimatizace a ventilátory, chytré okenní rolety a mnoho dalších. (36)

Chytré termostaty uživatelům dopřávají jak komfort, tak napomáhají snižování výdajů za energii. Součástí chytrých termostatů jsou senzory, které jsou umístěny do místností, které se obývají nejčastěji. Teplota je tak řízena podle těchto místností a ne podle umístění termostatu, jak tomu je u běžných termostatů. Chytrý termostat navíc dokáže sám detekovat, jestli je v domácnosti přítomna nějaká osoba a kde se momentálně nachází. Na základě těchto informací tento termostat operuje. Chytré osvětlení uživatelům dovoluje ovládat osvětlení na dálku, intenzitu světla, barvu osvětlení a nastavovat automatické zapnutí či vypnutí v určitý čas. Lze použít chytré žárovky nebo chytré spínače světla. Chytré spínače jsou lacinější, ale často mají náročnější instalaci. Chytré žárovky jsou dražší, ale jsou jednoduší na instalaci, mají větší životnost než běžné žárovky a nabízejí více možností přizpůsobování světla. Chytré kamery monitorují dění uvnitř domácnosti i dění v nejbližším okolí budovy. Lze skrz ně kontrolovat děti nebo domácí mazlíčky, ale také dokážou detekovat vstup neznámé osoby na pozemek. Některé chytré kamery nabízejí i možnost rozpoznávání osob a tak například při zaznamenání určité osoby automaticky odemknout vstupní branku či dveře. Chytré detektory při zaznamenání kouře, plynu či vody ihned pošlou notifikaci a lze hned obratem kontaktovat příslušnou pohotovost. Nabízejí i funkci navigace ze zakouřené místnosti pomocí světelných signalizací. Chytré zásuvky dokážou z každého zařízení, které je napájeno skrz zásuvku, udělat jeho chytřejší verzi. Lze je pak na dálku

ovládat. Chytré zámky uživatelům dovolují zkontrolovat, jestli zamkli a případně i zamknout na dálku. Existuje hodně chytrých zařízení, která nabízejí mnoho funkcí a využití. Výše uvedená chytrá zařízení jsou výčtem těch nejzákladnějších. (36)

3.1.7 Bezpečnost IoT

Zabezpečení IoT se týká opatření zavedených k ochraně připojených zařízení, sítí a dat používaných v aplikacích IoT. Účelem zabezpečení IoT je zabránit neoprávněnému přístupu, zneužití a modifikaci dat a zařízení připojených k internetu.

Zařízení internetu věcí jsou zranitelná vůči řadě bezpečnostních hrozeb, včetně hackerů, narušení dat, útoků malwaru a fyzické manipulace. Tyto bezpečnostní hrozby představují značná rizika pro organizace a jednotlivce, včetně finančních ztrát, porušení soukromí a poškození pověsti. Proto je zabezpečení IoT zásadní pro zajištění bezpečnosti zařízení internetu věcí a dat, která generují. Bezpečnost IoT čelí několika výzvám, které komplikují implementaci účinných bezpečnostních opatření. (3), (4)

Systémy internetu věcí jsou složité, s více vrstvami hardwaru a softwaru, což ztěžuje zabezpečení všech komponent. Dále jsou tyto systémy často nasazovány ve velkém měřítku s tisíci nebo miliony zařízení připojenými k internetu, což ztěžuje jejich správu a zabezpečení. Zařízení IoT se dodávají v různých tvarech, velikostech a typech, z nichž každé má své jedinečné požadavky na zabezpečení, takže je obtížné vyvinout univerzální řešení zabezpečení, které by vyhovovalo všem. Další výzvou je fakt, že mnoho zařízení IoT je postaveno pomocí zastaralých technologií, což je činí zranitelnými vůči bezpečnostním hrozbám. Neexistují žádné standardizované bezpečnostní protokoly pro IoT, což ztěžuje vývoj komplexních bezpečnostních řešení. (3), (4)

Pro adresování výzev bezpečnosti internetu věcí v organizaci, existují osvědčené postupy, kterýma se lze řídit a snížit tak bezpečnostní rizika. Prvním doporučením je provádění hodnocení rizik, aby se identifikovaly potenciální bezpečnostní hrozby a zranitelnosti. Zařízení IoT by měla používat silné metody ověřování, jako je dvoufaktorová autentizace, aby se zabránilo neoprávněnému přístupu. Dále by zařízení IoT měla používat šifrování k zabezpečení dat při přenosu. Organizace by měly zavést opatření řízení přístupu, aby omezily přístup k zařízením a datům internetu věcí. Všechna Zařízení IoT by měla používat aktualizovaný software k řešení bezpečnostních slabin a chyb. Organizace by měly nepřetržitě monitorovat zařízení IoT, aby detekovaly bezpečnostní hrozby a anomálie.

V neposlední řadě by organizace měly školit své zaměstnance o osvědčených postupech zabezpečení IoT, aby se snížilo riziko lidské chyby. (3), (4)

3.1.7.1 Blockchain

Blockchain v IoT je inovativní technologie, která umožňuje bezpečnou a spolehlivou správu a sdílení dat mezi různými zařízeními připojenými k internetu. V kombinaci s internetem věcí může blockchain pomoci vytvořit nové příležitosti pro účinnou kontrolu zabezpečení a automatizaci průmyslových procesů, a tím snížit náklady a zvýšit produktivitu. (5), (6)

Blockchain je distribuovaný systém ukládání dat, který zajišťuje bezpečné ukládání informací a zároveň umožňuje snadné a efektivní sdílení dat mezi různými zařízeními. V IoT může blockchain fungovat jako distribuovaná účetní kniha, která ukládá všechny transakce mezi zařízeními a zároveň zajišťuje, že tyto transakce jsou bezpečné. (5) (6)

Blockchain v IoT umožňuje ovládání zařízení, sledování dat a zabezpečení sítě. To pomáhá při řízení průmyslových procesů, jako je automatizace výroby, monitorování a řízení dodavatelského řetězce a správa inteligentních domácností. V průmyslu lze například blockchain využít k vytváření spolehlivých a bezpečných transakcí mezi různými průmyslovými zařízeními, což pomáhá optimalizovat výrobu a snižovat náklady. Další využití blockchainu v IoT by mohlo být v oblasti bezpečnosti. Vzhledem k tomu, že blockchain je decentralizovaný systém, který nevyžaduje centrální autoritu, lze jej použít pro zabezpečení dat a sítě. To pomáhá předcházet kybernetickým útokům a podvodům. Používání blockchainu v IoT však přináší také výzvy a omezení. Problémem v některých aplikacích IoT může být například omezená kapacita sítě a latence transakcí. Vytvoření a údržba blockchainové sítě navíc vyžaduje vysoké náklady na hardware, software a energii. (5), (6)

3.2 Počítačové sítě

Počítačové sítě jsou dnes nezbytnou součástí našeho každodenního života. Tato technologie umožňuje lidem komunikovat a sdílet informace v reálném čase, což je obzvláště důležité v době digitalizace a globalizace.

Počítačové sítě fungují na základě komunikace mezi různými zařízeními, jako jsou počítače, telefony, tablety, routery a další. Tyto zařízení jsou propojeny pomocí kabelů, bezdrátových signálů nebo optických vláken, které umožňují přenos dat z jednoho zařízení na druhé.

Existují různé druhy počítačových sítí, jako jsou LAN (Local Area Network), WAN (Wide Area Network) a WLAN (Wireless Local Area Network). Každý typ sítě má své vlastní výhody a nevýhody, a proto je důležité zvolit ten správný typ sítě pro konkrétní situaci. (2)

Využití počítačových sítí zahrnuje mnoho oblastí, jako jsou podnikové informační systémy, telekomunikační sítě, vzdělávací instituce a zdravotnická zařízení. Tato technologie umožňuje efektivní a rychlé sdílení informací mezi různými zařízeními a umožňuje lidem pracovat společně na projektech a sdílet soubory.

Bezpečnost počítačových sítí je také velmi důležitá, protože nedostatečné zabezpečení sítě může vést k zneužití a krádeži dat, krádeži identity a dalším nežádoucím následkům. Proto je důležité mít k dispozici kvalitní antivirové programy, firewall a další bezpečnostní opatření.

Vývoj počítačových sítí stále pokračuje a mnoho odborníků v oblasti informačních technologií pracuje na vylepšení sítí pro lepší výkon a bezpečnost. Tato technologie se stává stále důležitější pro naši každodenní interakci a komunikaci a bude mít stále větší vliv na naše životy v budoucnu.

3.2.1 Referenční model ISO/OSI

Model ISO/OSI, také známý Open Systems Interconnection model, je standardní referenční model pro komunikační protokoly používané v počítačových sítích. Tento model byl vyvinut Mezinárodní organizací pro standardizaci (ISO) jako standardní způsob popisu a kategorizace jednotlivých prvků, procesů a protokolů v počítačových sítích. Model ISO/OSI je rozdělen do sedmi abstraktních vrstev, z nichž každá poskytuje specifické funkce a interaguje s ostatními vrstvami za účelem přenosu dat v rámci sítě. První vrstva je vrstva fyzická, která je zodpovědná za přenos dat mezi fyzickými prvky sítě, jako jsou kabely, spoje a konektory. Zajišťuje správnou úroveň signálu a přenosovou rychlost. Druhá vrstva je linková. Tato vrstva je zodpovědná za přenos dat mezi uzly ve stejné síti. Řídí přenos dat mezi fyzickými prvky sítě a řeší problémy jako je detekce chyb při přenosu dat. Třetí vrstva se nazývá síťová vrstva a vrstva řídí přenos dat mezi různými sítěmi a zajišťuje optimální

cestu pro přenos dat přes různé uzly a sítě. Zajišťuje správné adresování a směrování paketů. Čtvrtá vrstva je vrstva transportní. Tato vrstva zajišťuje spolehlivý přenos dat mezi dvěma koncovými body v síti a řeší problémy, jako je ztráta dat nebo opakovaný přenos dat. Následuje vrstva relace, která spravuje relace a připojení mezi koncovými body v síti, jako jsou webové relace, e-mailové relace a podobně. Prezentační vrstva je vrstvou předposlední a zabývá se formátováním dat a zajišťuje převod dat do standardního formátu pro přenos mezi různými zařízeními a operačními systémy. Poslední vrstva je aplikační vrstva, která poskytuje skutečnou funkčnost aplikace a umožňuje interakci mezi aplikacemi v síti. (2), (7)

ISO/OSI model poskytuje standardizovaný způsob popisu a kategorizace jednotlivých prvků, procesů a protokolů v počítačových sítích. Tento model umožňuje vytvářet standardizované protokoly a komunikační metody, které lze použít napříč různými zařízeními a operačními systémy, čímž podporuje interoperabilitu mezi různými systémy. Rozdělením sítě na různé vrstvy umožňuje model ISO/OSI lepší řešení problémů a identifikaci problémů, které mohou v síti nastat. Celkově je model ISO/OSI základním nástrojem pro návrh, implementaci a správu sítě. (2), (7)

3.2.1.1 Fyzická vrstva

Fyzická vrstva je první vrstvou v modelu ISO/OSI a je zodpovědná za přenos bitů přes komunikační kanál. Jakožto nejzákladnější vrstva stanovuje základ pro všechny ostatní vrstvy modelu. Fyzická vrstva určuje, jak jsou data přenášena přes síťové médium. Dále definuje fyzické vlastnosti přenosového média, jako je typ kabelu, typ konektoru, způsob signalizace a rychlost přenosu dat. Fyzická vrstva také definuje úrovně napětí používané k reprezentaci bitů na médiu. (2), (7)

Fyzická vrstva pracuje na bitové úrovni a její primární funkcí je přenášet bity z jednoho zařízení do druhého. Pro splnění tohoto úkolu je fyzická vrstva zodpovědná za kódování a dekódování dat do a ze signálů, které mohou být přenášeny přes síťové médium. Tento proces kódování a dekódování je známý jako modulace a demodulace. Modulace je proces převodu digitálních dat na analogový signál a demodulace je proces převodu analogového signálu zpět na digitální data. Jedním z nejdůležitějších aspektů fyzické vrstvy je použití protokolů, které definují konkrétní detaily přenosu dat přes médium. Nejběžnější protokoly fyzické vrstvy jsou Ethernet, Wi-Fi a Bluetooth. Tyto protokoly určují formát

přenášených dat, úrovně napětí používané k reprezentaci bitů, fyzické konektory používané k připojení zařízení k síti a přenosovou rychlost. (2), (7)

Fyzická vrstva je také zodpovědná za detekci a opravu chyb. Pro zajištění integrity dat se na této vrstvě používají techniky jako kontrola parity a kontrola cyklické redundance, aby se detekovaly a opravovaly chyby při přenosu. Jednou z největších výzev fyzické vrstvy je řešení poruch přenosových médií, jako je útlum, zkreslení a šum. Tato narušení mohou způsobit ztrátu dat nebo chyby během přenosu a Fyzická vrstva musí zajistit, aby byla data přenášena spolehlivě i přes tato omezení. (2), (7)

Celkově je fyzická vrstva základní vrstvou modelu ISO/OSI, která udává základ pro všechny ostatní vrstvy. Zajišťuje, že data jsou přenášena přesně a spolehlivě tím, že definuje fyzické charakteristiky sítě a kóduje a dekóduje data do a ze signálů, které lze přenášet přes médium. Bez fyzické vrstvy by komunikace přes počítačové sítě nebyla možná.

3.2.1.2 Linková vrstva

Linková vrstva je druhá vrstva v modelu ISO/OSI a je zodpovědná za poskytování spolehlivého a bezchybného přenosu dat mezi přímo připojenými zařízeními. Zodpovídá za rámování datových paketů, detekci a opravu chyb. Tato vrstva zajišťuje správný tok dat mezi zařízeními. (2), (7)

Linková vrstva je rozdělena do dvou podvrstev: podvrstva Media Access Control (MAC) a podvrstva Logical Link Control (LLC). Podvrstva MAC je zodpovědná za řízení přístupu k přenosovému médiu, zatímco podvrstva LLC poskytuje služby síťové vrstvě. Linková vrstva je zodpovědná za rozdělení dat přijatých ze síťové vrstvy do rámců, které lze přenášet přes fyzické médium. Každý rámec obsahuje záhlaví, data a zápatí. Záhlaví obsahuje řídicí informace, jako je zdrojová a cílová adresa, pořadová čísla a kódy detekce chyb. Datová část rámce obsahuje aktuální přenášená data a zápatí obsahuje informace o detekci chyb a opravách. (2), (7)

Linková vrstva obsahuje mechanismy pro regulaci toku dat, které zajišťují, že data jsou přenášena rychlostí, která je přijatelná pro cílové zařízení. Regulace toku dat je zajištěna pomocí technik, jako je klouzající okénko (sliding window), které umožňuje přijímajícímu zařízení informovat odesílající zařízení o množství dat, které lze v daném okamžiku přenést. Jednou z nejdůležitějších funkcí linkové vrstvy je detekce a oprava chyb. Toho je dosaženo

zahrnutím kódů detekce chyb, jako jsou cyklické kontroly redundance (CRC), do zápatí každého rámce. Cílové zařízení používá tyto kódy k detekci a opravě chyb, které se mohly vyskytnout během přenosu. (2), (7)

Další důležitou funkcí linkové vrstvy je kontrola přístupu podvrstvy MAC k přenosovému médiu. To se provádí pomocí mechanismů pro řízení přístupu, jako je vícenásobný přístup pomocí Carrier Sense s detekcí kolize (CSMA/CD) a Carrier Sense Multiple Access s předcházením kolize (CSMA/CA). (2), (7)

Linková vrstva je nezbytná pro zajištění spolehlivého přenosu dat mezi zařízeními v síti. Poskytuje detekci a opravu chyb, řízení toku a mechanismy pro řízení přístupu, které zajišťují přesný a efektivní přenos dat. Bez této vrstvy by byl přenos dat v síti nespolehlivý, pomalý a náchylný k chybám.

3.2.1.3 Síťová vrstva

Síťová vrstva je třetí vrstvou v modelu ISO/OSI a je zodpovědná za poskytování end-to-end komunikace mezi zařízeními, která nejsou přímo propojena. Tato vrstva je zodpovědná za směrování a předávání dat mezi různými sítěmi a k tomu využívá internetový protokol (IP). Tato vrstva zapouzdřuje data do paketů. Hlavní funkcí síťové vrstvy je poskytovat logické adresování a směrování. Je zodpovědná za přidělování IP adres zařízením v síti a za směrování datových paketů do jejich cílů pomocí nejefektivnější cesty. Síťová vrstva používá směrovací protokoly, jako je Border Gateway Protocol (BGP) a Open Shortest Path First (OSPF), aby určila nejlepší cestu pro datové pakety k dosažení jejich cíle. (2), (7)

Síťová vrstva také poskytuje služby fragmentace a opětovného sestavení. Když je datový paket příliš velký na to, aby jej bylo možné přenést po síti jako jeden kus, rozdělí se na menší fragmenty. Síťová vrstva je zodpovědná za opětovné sestavení těchto fragmentů v cíli. Tento proces zajišťuje, že data mohou být přenášena přes sítě s velikostí maximální přenosové jednotky (MTU). Další důležitou funkcí síťové vrstvy je kontrola zahlcení. Síťová vrstva používá různé techniky, jako je traffic shaping či plánování paketů, k řízení toku dat a zabránění zahlcení sítě. Tyto techniky jsou důležité zejména ve vytížených sítích s velkých provozem. (2), (7)

Síťová vrstva poskytuje mechanismy kvality služeb (QoS), které zajišťují, že různé typy přenosu budou mít prioritu na základě jejich důležitosti. Například přenos v reálném čase, jako je hlas a video, může mít vyšší prioritu než jiné typy přenosu. Síťová vrstva je také zodpovědná za řešení bezpečnostních problémů. Poskytuje služby, jako je šifrování, ověřování a řízení přístupu k ochraně dat před neoprávněným přístupem, krádeží a úpravami dat. (2), (7)

Síťová vrstva je klíčovou vrstvou v modelu ISO/OSI, která poskytuje služby logického adresování, směrování, fragmentace a opětovného sestavení. Je odpovědná za směrování datových paketů na místo určení pomocí nejefektivnější cesty a za zajištění spolehlivého a efektivního přenosu dat napříč sítěmi. Schopnost síťové vrstvy zvládat přetížení, poskytovat QoS a řešit bezpečnostní problémy z ní činí základní součást moderních počítačových sítí.

3.2.1.4 Transportní vrstva

Transportní vrstva je čtvrtou vrstvou v modelu OSI (Open Systems Interconnection). Jeho primární funkcí je poskytovat spolehlivé služby přenosu dat typu end-to-end pro aplikace, které běží na různých médiích. Tato vrstva zajišťuje, že datové pakety jsou doručovány přesně a v pořadí, bez chyb, duplikace nebo ztráty. Transportní vrstva toho dosahuje segmentováním dat z vrstvy relace do menších jednotek známých jako segmenty. Tyto segmenty jsou pak přenášeny po síti pomocí služeb nižších vrstev, jako je síťová vrstva. (2), (7)

Transportní vrstva také poskytuje řízení toku, řízení chyb a mechanismy řízení zahlcení, aby bylo zajištěno spolehlivé doručování dat. Existují dva hlavní protokoly, které fungují na transportní vrstvě: Transmission Control Protocol (TCP) a User Datagram Protocol (UDP). TCP je protokol orientovaný na spojení, který vytváří spolehlivé virtuální spojení mezi dvěma hostiteli. Poskytuje spolehlivé služby přenosu dat tím, že zajišťuje, aby byly všechny segmenty doručeny ve správném pořadí, bez chyb a bez duplicit. TCP také poskytuje mechanismy řízení toku pro regulaci toku dat mezi hostiteli a mechanismy řízení přetížení, aby se zabránilo přetížení sítě. Na druhé straně UDP je protokol bez spojení, který před přenosem dat nenavazuje virtuální připojení. Neposkytuje spolehlivé služby přenosu dat ani neposkytuje mechanismy řízení toku nebo přetížení. UDP se často používá pro

aplikace, které vyžadují nízkou latenci, jako jsou online hry, streamování videa a VoIP. (2), (7), (8)

Transportní vrstva hraje klíčovou roli při zajišťování spolehlivého a efektivního přenosu dat po síti. Bez transportní vrstvy by bylo obtížné zaručit, že data budou doručena přesně a včas, což by mohlo vést ke ztrátě nebo poškození dat.

3.2.1.4.1 TCP

TCP (Transmission Control Protocol) je široce používaný přenosový protokol orientovaný na spojení, který poskytuje spolehlivé a uspořádané doručování dat mezi dvěma koncovými body v síti. Funguje na transportní vrstvě modelu OSI (Open Systems Interconnection) a je jedním ze dvou nejběžnějších transportních protokolů, druhým je UDP (User Datagram Protocol). TCP naváže virtuální spojení mezi dvěma koncovými body před přenosem dat a zahrnuje mechanismy pro detekci chyb, opravu a řízení toku. Zajišťuje, že data jsou dodávána přesně a úplně, takže je ideální pro aplikace, které vyžadují spolehlivé služby přenosu dat, jako je přenos souborů, e-mail, procházení webu a další aplikace, které vyžadují přesný a úplný přenos dat. TCP používá třícestný handshake k navázání spojení mezi dvěma koncovými body. Nejprve klient odešle na server paket SYN (Synchronize). Server odpoví paketem SYN-ACK (Synchronize-Acknowledge), kterým potvrdí požadavek klienta a naváže spojení. Nakonec klient odešle ACK (Acknowledge) paket pro potvrzení připojení. TCP zahrnuje mechanismy řízení zahlcení, které zabraňují přetížení sítě omezením počtu paketů, které lze přenášet. To pomáhá zajistit, že síť zůstane stabilní a citlivá. TCP je základní protokol používaný v Internet Protocol Suite (TCP/IP), který je základem moderního internetu. Je široce používán v síťové komunikaci a je nezbytný pro poskytování spolehlivých služeb přenosu dat. (2), (7), (8)

3.2.1.4.2 UDP

UDP (User Datagram Protocol) je nespojený přenosový protokol, který funguje na transportní vrstvě modelu OSI (Open Systems Interconnection). Je to jeden ze dvou nejběžnějších transportních protokolů, přičemž druhým je TCP (Transmission Control Protocol). UDP poskytuje rychlé a efektivní doručování dat mezi dvěma koncovými body po síti, ale nezaručuje spolehlivé nebo chybově kontrolované doručení dat. Často se používá pro aplikace, které mohou tolerovat určitou ztrátu dat, jako je streamování v reálném čase,

videokonference, online hry a další aplikace, které upřednostňují rychlost před přesností. Na rozdíl od TCP, UDP nenavazuje virtuální spojení mezi dvěma koncovými body před přenosem dat a nezahrnuje mechanismy pro detekci chyb, opravu a řízení toku. To znamená, že data mohou přijít ve špatném pořadí nebo nemusí dorazit vůbec. UDP je rychlejší než TCP, protože neobsahuje mechanismy kontroly chyb a oprav, které mohou způsobit zpoždění v sítích s vysokou latencí. Je také méně náročný na zdroje a vyžaduje méně prostředků k přenosu dat. UDP neposkytuje spolehlivé služby přenosu dat, takže je méně ideální pro aplikace, které vyžadují přesný a úplný přenos dat. Jeho rychlost a efektivita jej však činí ideální pro aplikace v reálném čase, kde jsou malá zpoždění nebo chyby méně kritické než rychlost a odezva. (7), (8)

3.2.1.5 Relační vrstva

Relační vrstva je pátou vrstvou modelu OSI a je zodpovědná za správu relací mezi aplikacemi na různých hostitelích. Vrstva relací poskytuje služby, které umožňují dvěma nebo více aplikacím navázat, používat a ukončit připojení nebo relaci a vyměňovat si data během relace. Relační vrstva je zodpovědná za zakládání a rušení relací, což jsou logická spojení mezi dvěma aplikacemi. Během relace tato vrstva zajišťuje, že data odeslaná jednou aplikací obdrží druhá aplikace ve správném pořadí a bez chyb. Relační vrstva také poskytuje služby pro kontrolní body, které aplikaci umožňují uložit svůj aktuální stav, aby v ní bylo možné pokračovat později v relaci. (7), (8)

Tato vrstva není vždy přítomna ve všech síťových implementacích, protože její funkce mohou být implementovány v jiných vrstvách modelu OSI, jako je transportní vrstva. V některých síťových architekturách, jako je sada protokolů ISO, je však vrstva relací samostatnou vrstvou. Tato vrstva poskytuje několik důležitých funkcí v síťové komunikaci. Jednou z těchto funkcí je vytvoření a správa relací, kdy je vrstva relací zodpovědná za vytváření, udržování a ukončování relací mezi aplikacemi. Řídí tok dat mezi aplikacemi během relace a zajišťuje, že data jsou doručována přesně a ve správném pořadí. Další a neméně důležitou funkcí je synchronizace relací, kdy vrstva relací poskytuje služby pro synchronizaci relací mezi aplikacemi a zajišťuje, že každá aplikace během relace ví o stavu té druhé. Vrstva relací také spravuje připojení mezi aplikacemi a umožňuje jim podle potřeby vytvářet, udržovat a ukončovat připojení. Mezi další služby, které tato relace

poskytuje, patří obnova relací, které byly přerušeny v důsledku selhání sítě nebo jiných problémů. (7), (8)

3.2.1.6 Prezentační vrstva

Prezentační vrstva je šestou vrstvou modelu OSI. Hlavním úkolem této vrstvy je transformovat data z aplikační vrstvy do formátu, který lze přenášet po síti. Tato vrstva je také zodpovědná za převod přijatých dat ze sítě do formátu, kterému přijímající aplikace rozumí. Jednou z hlavních funkcí této vrstvy je kódování a komprese dat. To zahrnuje převod dat do standardního formátu, který mohou rozpoznat všechna síťová zařízení, a jejich kompresi, aby byl umožněn efektivní přenos po síti. Prezentační vrstva je také zodpovědná za šifrování a dešifrování dat, aby byl zajištěn bezpečný přenos citlivých informací, jako jsou osobní či finanční údaje. Další důležitou funkcí prezentační vrstvy je překlad dat. To zahrnuje převod dat mezi různými formáty používanými různými aplikacemi. Prezentační vrstva může například převádět data z jedné znakové sady do druhé nebo z jednoho formátu obrázku nebo videa do jiného. Prezentační vrstva je také zodpovědná za formátování dat způsobem, který může přijímající aplikace správně interpretovat. To zahrnuje přidání záhlaví, zápatí a dalších informací o formátování k datům. Stojí za zmínku, že ne všechny síťové implementace zahrnují Prezentační vrstvu. Některé jeho funkce mohou být implementovány v jiných vrstvách modelu OSI. Nicméně v některých síťových architekturách, jako je sada protokolů ISO, je prezentační vrstva samostatnou vrstvou. (2), (7), (8)

3.2.1.7 Aplikační vrstva

Aplikační vrstva je sedmou a nejvyšší vrstvou modelu OSI a je zodpovědná za poskytování síťových služeb aplikacím koncových uživatelů. Vrstva je zodpovědná za propojení mezi softwarovou aplikací a sítí, což umožňuje aplikacím komunikovat s jinými aplikacemi v síti. Na aplikační vrstvě mohou aplikace přistupovat k síťovým službám nabízeným nižšími vrstvami modelu OSI, včetně šifrování dat, komprese dat, opravy chyb a řízení toku. Tyto služby se používají k zajištění spolehlivé a efektivní komunikace mezi aplikacemi v síti. (2), (7), (8)

Aplikační vrstva je také zodpovědná za správu autentizace a autorizace uživatelů a zajišťuje, že pouze oprávnění uživatelé mají přístup k síťovým zdrojům. Tato vrstva poskytuje různé funkce zabezpečení, jako je šifrování a dešifrování dat přenášených po síti, ověřování uživatelů a řízení přístupu. Aplikační vrstva navíc podporuje protokoly na aplikační úrovni, jako je HTTP, SMTP, FTP a Telnet. Tyto protokoly poskytují standardní způsob vzájemné komunikace různých aplikací bez ohledu na platformu nebo operační systém, na kterém běží. Aplikační vrstva poskytuje uživatelské rozhraní, které umožňuje koncovému uživateli interakci s aplikací. Spravuje formátování a prezentaci dat, v případě potřeby převádí data mezi různými formáty a poskytuje funkce, jako je grafika a zvuk. Aplikace, které fungují na aplikační vrstvě, zahrnují webové prohlížeče, e-mailové klienty, aplikace pro přenos souborů a aplikace pro rychlé zasílání zpráv. Tyto aplikace používají různé protokoly na aplikační úrovni ke komunikaci s jinými aplikacemi v síti. (2), (7), (8)

3.2.2 Síťový model TCP/IP

TCP/IP je sada komunikačních protokolů, které poskytují základ pro komunikaci přes internet. Skládá se ze dvou hlavních protokolů, Transmission Control Protocol (TCP) a Internet Protocol (IP), spolu s dalšími podpůrnými protokoly, jako je User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) a Address Resolution Protocol (ARP). TCP/IP je vrstvený protokol, což znamená, že je rozdělen do různých vrstev, z nichž každá má vlastní sadu funkcí. Sada protokolů TCP/IP se řídí čtyřvrstvou architekturou, která zahrnuje aplikační vrstvu, transportní vrstvu, internetovou vrstvu a síťovou přístupovou vrstvu. (2), (8), (9)

Aplikační vrstva je nejvyšší vrstvou a poskytuje služby na podporu síťových aplikací. Je zodpovědná za komunikaci mezi aplikacemi a sítí. Příklady aplikací, které používají aplikační vrstvu, zahrnují e-mail, protokoly přenosu souborů (FTP) a procházení webu (HTTP). Transportní vrstva poskytuje aplikacím služby, které dodávají end-to-end data. Zodpovídá za to, že data jsou dodána spolehlivě a ve správném pořadí. TCP je nejběžněji používaný protokol transportní vrstvy a je zodpovědný za zajištění spolehlivého doručení dat. Síťová vrstva je zodpovědná za směrování a adresování služeb pro datové pakety. Je zodpovědná za přenos dat mezi sítěmi. Nejběžněji používaný protokol v síťové vrstvě je IP. Vrstva síťového rozhraní, nebo také vrstva fyzická, je nejnižší vrstvou v sadě

protokolů TCP/IP. Je zodpovědná za přenos dat po fyzické síti. Tato vrstva se zabývá úkoly, jako je elektrická signalizace, kabeláž a síťová rozhraní. (2), (8), (9)

TCP/IP je základem pro komunikaci přes internet a stal se standardní sadou protokolů pro moderní počítačové sítě. TCP/IP je používaný prakticky všemi moderními počítačovými sítěmi. Poskytuje výkonnou a flexibilní sadu protokolů, které umožňují komunikaci mezi různými zařízeními, operačními systémy a sítěmi. TCP/IP je komplexní a výkonná sada protokolů a neustále se vyvíjí. Do sady jsou přidávány nové protokoly, které řeší nové potřeby a výzvy, a stávající protokoly jsou aktualizovány, aby se zlepšil výkon a zabezpečení. (2), (8), (9)

3.2.2.1 Síťové protokoly

V modelu TCP/IP existují různé síťové protokoly, které fungují na různých vrstvách modelu. Nejčastěji používané protokoly jsou internet protocol, transmission control protocol, user datagram protocol, address resolution protocol, internet control message protocol, domain name System, simple mail transfer protocol, post office protocol, file transfer protocol, hypertext transfer protocol, simple network management protocol, border gateway protocol. (2), (8), (9)

Internet protocol (IP) je protokol, který funguje na síťové vrstvě modelu TCP/IP. Je zodpovědný za směrování paketů dat napříč různými sítěmi. IP poskytuje jedinečnou adresu pro každé zařízení v síti, známou jako IP adresa. (2), (9)

Transmission control protocol (TCP) je protokol, který funguje na transportní vrstvě modelu TCP/IP. Je zodpovědný za zajištění spolehlivého přenosu dat mezi zařízeními v síti. TCP používá třícestný handshake k navázání spojení mezi zařízeními a rozděluje data na menší segmenty pro přenos. (2), (9)

User datagram protocol (UDP) je protokol, který také funguje na transportní vrstvě modelu TCP/IP. Na rozdíl od TCP neposkytuje UDP spolehlivost ani kontrolu chyb. Používá se pro aplikace, kde je rychlost důležitější než spolehlivost, jako je streamování videa nebo zvuku. (2), (9)

Address resolution protocol (ARP) je protokol, který funguje na síťové vrstvě modelu TCP/IP. Používá se k překladu IP adresy na fyzickou adresu, jako je MAC adresa. ARP používají zařízení k nalezení fyzické adresy jiného zařízení ve stejné síti. (2), (9)

Protokol ICMP (Internet Control Message Protocol) je protokol, který také funguje na síťové vrstvě modelu TCP/IP. Používá se pro účely diagnostiky a hlášení chyb, například když je zařízení nedostupné nebo když je síť přetížená. (2), (9)

Domain Name System (DNS) je protokol, který je využíván na aplikační vrstvě modelu TCP/IP. Zodpovídá za překlad názvů domén, jako je www.nazev.com, na adresy IP, kterým síť rozumí. DNS umožňuje uživatelům přistupovat k webovým stránkám a dalším zdrojům pomocí uživatelsky přívětivých jmen namísto IP adres. (2), (9)

Simple mail transfer protocol (SMTP) je protokol, který funguje na aplikační vrstvě modelu TCP/IP a používá se k odesílání a přijímání e-mailových zpráv. Je zodpovědný za přenos e-mailových zpráv mezi poštovními servery a klienty. (2), (9)

Post office protocol (POP) je protokol, který také funguje na aplikační vrstvě modelu TCP/IP a používá se k načítání e-mailových zpráv z poštovního serveru. Umožňuje uživatelům stahovat zprávy z poštovního serveru do jejich místního zařízení pro offline přístup. (2), (9)

File transfer protocol (FTP) je protokolem fungujícím na aplikační vrstvě modelu TCP/IP a používá se k přenosu souborů mezi zařízeními v síti. Umožňuje uživatelům nahrávat a stahovat soubory ze vzdáleného serveru. (2), (8), (9)

Hypertext transfer protocol (HTTP) je protokolem aplikační vrstvy modelu TCP/IP a používá se k přenosu dat přes World Wide Web. Je to protokol, který se používá pro přístup k webovým stránkám a dalším zdrojům na internetu. (2), (8), (9)

Simple Network Management Protocol (SNMP) je protokolem aplikační vrstvy modelu TCP/IP a používá se ke správě a monitorování síťových zařízení. Poskytuje standardizovaný způsob správy síťových zařízení, jako jsou směrovače a přepínače. (2), (9)

Border Gateway Protocol (BGP) je protokol, který se používá na síťové vrstvě modelu TCP/IP a využívá se k výměně informací o směrování mezi různými autonomními systémy na internetu. Je zodpovědný za směrování provozu mezi různými sítěmi. (2), (8), (9)

3.2.3 IP adresace

IP adresování je základním aspektem sady protokolů TCP/IP. IP adresa je číselný štítek přiřazený každému zařízení připojenému k síti, která ke komunikaci používá

internetový protokol (IP). IP adresa tedy slouží jako jedinečný identifikátor zařízení a používá se ke směrování datových paketů do jejich zamýšleného cíle. (2), (8)

V současnosti se používají dvě verze IP adres: IPv4 a IPv6. IPv4 je původní verze protokolu a používá 32bitový formát adresy, který umožňuje přibližně 4,3 miliardy jedinečných adres. IPv6 na druhou stranu používá 128bitový formát adresy, který umožňuje enormní počet jedinečných adres, tedy přibližně 3,4 × 10^38. (2)

Adresa IPv4 je 32bitové číslo vyjádřené v desítkové soustavě s tečkami, což znamená, že se skládá ze čtyř sad desetinných čísel oddělených tečkami. Každá sada desetinných čísel představuje 8 bitů adresy. Například IP adresa 192.168.1.1 je reprezentována binárně jako 11000000.10101000.00000001.00000001. IPv4 adresy jsou rozděleny na dvě části: síťovou část a hostitelskou část. (2)

IPv4 adresy jsou rozděleny do pěti tříd: A, B, C, D a E. Každá třída má jiný rozsah adres, které lze přiřadit zařízením v síti. Třídy A, B a C se používají pro unicast adresy, zatímco třída D se používá pro multicast adresy a třída E je vyhrazena pro budoucí použití. Adresy třídy A mají první oktet v rozsahu 1-126 a síťová část adresy je reprezentována prvním oktetem. Adresy třídy B mají první oktet v rozsahu 128-191 a síťová část adresy je reprezentována prvními dvěma oktety. Adresy třídy C mají první oktet v rozsahu 192-223 a síťová část adresy je reprezentována prvními třemi oktety. V prvních třech třídách existují určité rozsahy IP adres, které jsou vyhrazeny pro použití v privátních sítích. Tyto adresy nejsou směrovatelné na veřejném internetu a lze je používat pouze v privátních sítích. Rozsahy privátních IP adres pro IPv4 jsou:

10.0.0.0 – 10.255.255.255 (třída A)

172.16.0.0 – 172.31.255.255 (třída B)

192.168.0.0 – 192.168.255.255 (třída C) (2), (8), (10)

Adresa IPv6 je 128bitové číslo vyjádřené v hexadecimálním zápisu, což znamená, že se skládá z osmi sad hexadecimálních čísel oddělených dvojtečkami. Každá sada hexadecimálních čísel představuje 16 bitů adresy. Například IP adresa 2001: 0db8: 85A3: 0000: 0000: 8A2E: 0370: 7334 je zastoupena v binárním 0010000000000000 0001011011010000000011011010010000001101110100110000101101010011000011011 101001100 000. (2), (8)

Sítě se svými maskami lze zjednodušeně zapsat pomocí notace CIDR. IP adresy a masky podsítě lze pohodlně reprezentovat pomocí zápisu CIDR (Classless Inter-Domain

Routing). Podsíť je reprezentována počtem úvodních bitů v masce podsítě. Například IP adresa 192.168.1.1 s maskou podsítě 255.255.255.0 může být zapsána jako 192.168.1.1/24 v notaci CIDR, kde 24 označuje počet úvodních bitů masky sítě. (2), (8)

3.2.3.1 Podsítě

Podsíť je součástí větší sítě, která byla v počítačové síti rozdělena na menší části. To se často provádí za účelem zvýšení zabezpečení sítě, správy nebo výkonu sítě. Velikost rozsahu IP adres každé podsítě je závislá na velikosti celkové sítě a počtu zařízení, která k ní budou připojena. Tento rozsah obvykle volí správce sítě. Každá podsíť je spravována jako samostatná síť s vlastním ID sítě a adresou vysílání. To může zvýšit efektivitu a snížit přetížení sítě, protože to umožňuje zařízením v podsíti komunikovat mezi sebou přímo, bez nutnosti procházet celou sítí. (2), (8), (10)

K identifikaci podsítě se používá maska podsítě, což je 32bitová hodnota, která identifikuje velikost podsítě. V kombinaci s IP adresou se maska podsítě používá k určení, která část adresy identifikuje síť a která hostitele. Například síť s rozsahem IP adres 192.168.0.0 – 192.168.255.255 lze rozdělit na menší podsítě. Když je maska podsítě nastavena na 255.255.255.0, síť je rozdělena na 256 podsítí, z nichž každá má rozsah 256 adres IP. To umožňuje lepší řízení síťového provozu a zvyšuje výkon sítě. (2), (8), (10)

3.2.3.2 Subnetting

Subnetting je proces rozdělování sítě na menší podsítě. Tento proces se provádí vypůjčením bitů z hostitelské části IP adresy a jejich použitím k vytvoření nové síťové části. Subnetting je široce používán v počítačových sítích ke zlepšení výkonu sítě, škálovatelnosti a zabezpečení. Podsítě umožňují správcům sítě řídit a organizovat síť efektivněji tím, že ji rozdělí na menší, lépe spravovatelné podsítě. (2), (8), (10)

Hostitelská část IP adresy identifikuje konkrétní zařízení v rámci sítě, zatímco síťová část identifikuje samotnou síť. Vypůjčením bitů z hostitelské části lze síťovou část rozšířit, což umožňuje vytvoření menších podsítí v rámci původní sítě. Pro vytvoření podsítě, musí správce sítě nejprve určit počet podsítí a počet požadovaných zařízení na podsíť. To určuje počet bitů, které je třeba si vypůjčit z hostitelské části IP adresy. Počet vypůjčených bitů se nazývá maska podsítě. Po určení masky podsítě, může správce sítě rozdělit rozsah IP adres

na menší podsítě pomocí nové masky podsítě. Každá podsíť bude mít svou vlastní jedinečnou síťovou adresu a zařízením v této podsíti budou přiděleny IP adresy z rozsahu IP adres této podsítě. Takto vytvořená podsíť poskytuje správcům sítě několik výhod. Umožňuje lepší výkon sítě snížením přetížení sítě, což zvyšuje rychlost sítě. Zlepšuje také zabezpečení sítě omezením velikosti vysílacích domén, což pomáhá předcházet síťovým útokům, jako je ARP spoofing a útoky denial-of-service. (2), (8), (10)

3.2.3.2.1 Síťové prvky

Základní kámen efektivity sítě spočívá ve fyzických síťových zařízeních, která usnadňují síťové připojení, správu a ovládání. Tato nepostradatelná zařízení poskytují infrastrukturu pro bezproblémový přenos dat a komunikaci mezi síťovými zařízeními. Mezi tato zařízení patří mimo jiné přepínače, směrovače, brány firewall, rozbočovače, modemy a bezdrátové přístupové body. Každé zařízení plní specifickou funkci a je nezbytné pro správné fungování sítě. (2), (11)

Síťové přepínače (switch) jsou integrální zařízení, která umožňují připojení zařízení místní sítě (LAN). Přepínače fungující jako centrální rozbočovače, které usnadňují komunikaci mezi zařízeními. Tato zařízení jsou dostupná v různých velikostech a konfiguracích a mohou sahat od malých stolních přepínačů až po ty podnikové. (2), (11)

Sítě se propojují přes směrovače neboli routery. Tato zařízení se starají o směrování datového provozu a výběr nejúčinnější cesty pro přenos dat. Směrovače jsou nezbytné pro propojení různých LAN a WAN sítí a pro připojení sítí k internetu. (2), (11)

Pro ochranu sítě před potenciálními riziky, jako je malware, viry a hackování, jsou nasazovány brány firewall jako bariéra mezi sítí a internetem. Firewall filtruje příchozí i odchozí komunikaci a tím zajišťuje, že se do sítě dostane pouze autorizovaný síťový provoz. (11)

Rozbočovače fungují jako centrální bod pro přenos dat a připojení více zařízení v síti LAN. Tento síťový komponent již není tak používaný, jelikož je skoro vždy nahrazený přepínačem (switchem). (2), (11)

Modemy slouží k převodu digitálních signálů z počítače na analogové signály, které lze přenášet po telefonních linkách, kabelových vedeních nebo jiných komunikačních kanálech pro připojení počítačů nebo sítí k internetu. (2), (11)

Bezdrátové přístupové body (WAP) se používají k připojení bezdrátových zařízení k sítím. Fungují jako bezdrátový rozbočovač a umožňují zařízením, jako jsou notebooky, smartphony a tablety, připojit se k síti bez potřeby kabelů. (2), (11)

3.2.4 Zabezpečení počítačové sítě

V moderní době, kdy je všudypřítomnost internetu a propojení standardem, se zabezpečení sítě stalo klíčovým aspektem informačních technologií. S neustále rostoucím využíváním počítačových sítí pro sdílení informací, vzdálený přístup či obchodní transakce se stalo zabezpečení sítě důležitější než kdykoli předtím.

Bezpečnost sítě je komplexní a neustále se transformuje díky neustálému vývoji nových technologií a také stále novým druhům hrozeb. Zabezpečení sítě zahrnuje užití různých technologií, zásad a postupů k ochraně počítačové sítě před kybernetickými hrozbami, jako jsou viry, malware, phishingové útoky a krádeže dat. Avšak nejedná se o pouze o postupy proti virtuálním rizikům, ale také proti fyzickým hrozbám, jako je fyzické zabezpečení zařízení, ochrana proti přírodním jevům či správné umístění zařízení. K ochraně proti těmto hrozbám se používá řada nástrojů a opatření. Tato opatření mohou mimo jiné zahrnovat nasazení firewallů, systémů detekce narušení, antivirového softwaru, šifrování a autentizačních postupů. (12), (13), (14)

Jedním z klíčových cílů síťové bezpečnosti je aby osobní data, důvěrná firemní data či další důležitá a střežená data byla chráněna před neoprávněným zneužitím či krádeží. To znamená, že k citlivým datům by měli mít přístup pouze oprávnění uživatelé. Lze tedy implementovat zásady řízení přístupu, a tím zajistit, že k určitým datům mohou přistupovat pouze povolené osoby. Dále lze využít šifrovací techniky a tím chránit data při přenosu v síti. Dalším důležitým cílem zabezpečení sítě je zachování integrity dat. To znamená, že data by neměla být žádným způsobem upravována nebo pozměňována bez řádného povolení. Aby byla zajištěna integrita dat, lze implementovat kontrolní součty, digitální podpisy nebo jiné metody ověřování pravosti dat. Zabezpečení sítě má také za cíl zajistit dostupnost síťových zdrojů. To znamená, že uživatelé by měli mít přístup k síti a jejím zdrojům, když to potřebují. K dosažení tohoto cíle lze použít opatření proti ztrátě či nedostupnosti dat, jako jsou zálohovací systémy nebo mechanismy pro přepnutí při selhání, aby se zajistilo, že síť zůstane dostupná i v případě selhání hardwaru nebo jiného problému. (12), (13), (14)

3.2.4.1 Typy útoků

Síťové útoky jsou záměrné akce provedené za účelem narušení, poškození nebo získání neoprávněného přístupu k počítačové síti a jejím datům. Existují různé typy síťových útoků a každý typ využívá různé zranitelnosti v síťové infrastruktuře. Typ útoku, který zahltí síť nebo server provozem, který pak není chopen reagovat na legitimní požadavky, se nazývá denial of service attack(DoS). Tento útok pak může narušit síťový provoz a zabránit tak přístupu ke kritickým službám či funkcím sítě. Podobným útokem jako DoS je DDoS (Distributed denial of service) útok. Hlavním rozdílem je, že DDOoS používá více zařízení k zaplavení sítě, což následně ztěžuje zmírnění útoku. Dalším typem je útok Man-in-the-middle (MitM), který zachycuje a odposlouchává komunikaci mezi dvěma stranami, což útočníkovi umožňuje ukrást citlivé informace nebo upravit komunikaci bez vědomí zúčastněných stran. Phishingové útoky jsou útoky, které jsou navržené tak, aby přiměly uživatele prozradit citlivé informace, jako jsou přihlašovací údaje nebo finanční údaje. Tyto útoky obvykle zahrnují odesílání e-mailů, které vypadají, že pocházejí z legitimního zdroje, jako je banka nebo internetový prodejce, ale ve skutečnosti jsou podvodné. Dalším typem útoku je malware. Malware je jakýkoli škodlivý software určený k narušení nebo poškození počítačového systému nebo sítě. Mezi typy malwaru patří viry, červi, trojské koně a ransomware. Útoky zvané SQL injection využívají zranitelnosti webových aplikací k získání přístupu k citlivým datům uloženým v databázích. Tyto útoky zahrnují vložení škodlivého kódu SQL do webového formuláře nebo dotazu, což útočníkovi umožní obejít autentizační opatření a získat tak přístup k citlivým datům. Útok DNS spoofing zahrnuje přesměrování webového provozu uživatele na podvodnou webovou stránku, což umožňuje útočníkovi ukrást citlivé informace nebo nainstalovat malware do počítače uživatele. Síťových útoku existuje mnohem více, ale výše jmenované se vyskytují nejvíce. (13), (14)

Aby se zmírnilo riziko síťových útoků, měla by se vždy zavést komplexní strategie zabezpečení sítě, která zahrnuje kombinaci technologií, nástrojů a osvědčených postupů. To může zahrnovat nasazení firewallů, systémů detekce a prevence narušení, VPN a šifrovacích technologií, stejně jako implementaci přísných kontrol přístupu, mechanismů ověřování a zásad hesel. Také je třeba dbát na pravidelné aktualizování zabezpečení a testování zranitelnosti, které může pomoci identifikovat potenciální bezpečnostní slabiny v síti. Také je vhodné zaškolit všechny uživatele, kteří k síti přistupují a tím snížit riziko lidské chyby. (14)

3.2.4.2 Ochrana sítě

Ochrana sítě zahrnuje použití různých metod a opatření k zajištění bezpečnosti dané sítě. Mezi nejčastěji používané metody lze zařadit řízení přístupu, nasazení firewallu, systémy pro detekci a prevence rušení (IDPS), virtuální privátní síť (VPN), šifrování, systémy pro správu zabezpečení a testování zabezpečení. (14)

Řízení přístupu je proces omezování toho, kdo má přístup k síti a ke kterým zdrojům má přístup. Toho lze dosáhnout různými metodami, jako je autentizace, autorizace a sledování přístupů. Autentizace ověřuje identitu uživatele nebo zařízení před povolením přístupu k síti. Autorizace určuje, ke kterým zdrojům má uživatel nebo zařízení přístup. Sledování přístupů sleduje a zaznamenává aktivitu uživatelů v síti. (14), (15)

Firewall je zařízení pro zabezpečení sítě, které monitoruje a filtruje příchozí a odchozí síťový provoz na základě předem definovaných pravidel zabezpečení. Brány firewall se běžně používají k zabránění neoprávněnému přístupu k síti nebo k omezení přístupu k určitým typům provozu. (14)

Systém detekce a prevence narušení (IDPS) slouží pro zabezpečení sítě, které monitoruje síťový provoz a kontroluje zda nevykazuje známky podezřelé aktivity. Tento systém dokáže odhalit a upozornit na potenciální narušení bezpečnosti a také přijmout preventivní opatření k blokování škodlivého provozu. (14)

Virtuální privátní sítě (VPN) se používají k vytvoření zabezpečeného a šifrovaného spojení mezi dvěma nebo více zařízeními přes internet. VPN lze použít k připojení vzdálených pracovníků k firemní síti nebo k vytvoření zabezpečeného spojení mezi dvěma nebo více geograficky oddělenými sítěmi. (14), (15)

Šifrování je proces převodu prostého textu na šifrovaný text, který může číst pouze někdo, kdo má klíč k jeho dešifrování. Šifrování se běžně používá k ochraně citlivých dat před neoprávněným přístupem nebo krádeží. Systémy pro správu bezpečnostních informací a událostí (SIEM) slouží k analyzování bezpečnostních výstrah generovaných síťovým hardwarem a aplikacemi v reálném čase. Systémy SIEM se používají k identifikaci bezpečnostních hrozeb a reakci na ně v reálném čase. (14)

Testování zabezpečení je proces vyhodnocování bezpečnosti sítě pokusem o zneužití zranitelností v síti. To může zahrnovat penetrační testování, skenování zranitelnosti a etické hackování. (14)

Kromě těchto metod existuje mnoho dalších opatření, která lze využít pro zvýšení ochrany sítě. Avšak je důležité poznamenat, že žádná jediná metoda nebo opatření nemůže zajistit úplnou ochranu sítě. Vícevrstvý přístup využívající více metod a opatření je nejlepším způsobem, jak zajistit řádnou ochranu sítě. (14)

3.2.4.3 Switch a jeho konfigurace

Switche jsou síťová zařízení, která se používají k propojení více zařízení dohromady v síti. Jsou navrženy tak, aby spojovaly zařízení, jako jsou počítače, tiskárny, IoT zařízení a servery v místní síti. Tím se usnadňuje komunikace a přenos dat mezi těmito zařízeními. Switche fungují na linkové vrstvě modelu OSI a jsou zodpovědné za přenos dat mezi zařízeními. Přepínače fungují tak, že načtou adresy MAC (Media Access Control) každého zařízení připojeného k síti a poté předávají datové pakety na správné místo na základě MAC adresy. Tento proces je známý jako switching a umožňuje switchům poskytovat vyhrazenou šířku pásma každému zařízení, což vede ke zlepšení výkonu sítě. Existují dva typy switchů, spravované a nespravované. Spravované switche nabízejí více funkcí a možností konfigurace než nespravovatelné switche, takže jsou vhodnější pro větší sítě se složitými požadavky. Nespravovatelné switche jsou na druhou stranu jednodušší a snáze se používají, takže jsou ideální pro menší sítě. (17)

Pro konfiguraci switche je třeba provést několik kroků. Prvním krokem je samozřejmě připojení napájení a následně připojení požadovaných zařízení. Nastavení switche lze provést pomocí webového rozhraní, rozhraní příkazového řádku (CLI) nebo protokolu SNMP (Simple Network Management Protocol). Následuje konfigurace základního nastavení switche, jako je IP adresa, maska podsítě a výchozí brána. Také lze nakonfigurovat porty switche pro přiřazení sítí VLAN. Dalším krokem je nakonfigurovat bezpečnostní opatření pro síť. Což je například filtrování MAC adres, zabezpečení portů či nastavení správy přístupu. Po nakonfigurování všech chtěných funkcí je třeba tuto konfiguraci otestovat, zda vše funguje, jak má. Konfigurace switche se může zdát jako složitý proces, ale se správným plánováním a znalostí základních konfiguračních nastavení a pokročilých funkcí lze vytvořit optimalizovanou a zabezpečenou síť. (17)

3.2.4.3.1 Základní příkazy pro konfiguraci cisco switche

Pro efektivní nastavení switche je zapotřebí znát základní příkazy pro konfiguraci tohoto zařízení. Každý switch může vyžadovat jinou podobu příkazů, proto je za potřebí si ověřit jakou formu příkazy mají mít. Pro tuto práci jsou zvoleny switche společnosti Cisco. Základní příkazy pro tyto switche jsou:

1. „enable“: Tento příkaz umožňuje vstoupit do privilegovaného režimu EXEC, který je vyžadován pro většinu konfiguračních úloh. (16), (17)
2. „configure terminal“: Tento příkaz umožňuje vstoupit do režimu globální konfigurace, kde se mohou provádět změny v konfiguraci switche. (16), (17)
3. „interface <*rozhraní*>“: Tento příkaz umožňuje vybrat konkrétní rozhraní, jako je Ethernet nebo FastEthernet, pro konfiguraci. (16), (17)
4. „ip address <*ip addresa*> <*maska sítě*>“: Tento příkaz umožňuje konfigurovat IP adresu a masku sítě pro určené rozhraní. (16), (17)
5. „no shutdown“: Tento příkaz aktivuje vybrané rozhraní a přepne jej do režimu online. (16), (17)
6. „show interfaces“: Tento příkaz zobrazí stav a konfiguraci všech rozhraní na přepínači. (16), (17)
7. „show running-config“: Tento příkaz zobrazí aktuální spuštěnou konfiguraci přepínače. (16), (17)
8. „copy running-config startup-config“: Tento příkaz uloží aktuální spuštěnou konfiguraci do spouštěcí konfigurace, která se načte automaticky při zapnutí nebo restartu přepínače. (16), (17)
9. „hostname <*name*>“: Tento příkaz nastavuje název pro switch. (16), (17)
10. „enable password <*heslo*>“: Tento příkaz nastavuje heslo pro switch. (16), (17)
11. „enable secret <*heslo*>“: Tento příkaz nastavuje zašifrované heslo pro switch. (16), (17)
12. „line vty 0 4“: Tento příkaz umožňuje konfigurovat virtuální terminálové linky pro vzdálený přístup. (16), (17)
13. „password <*heslo*>“: Tento příkaz nastavuje heslo pro přístup k virtuálnímu terminálu. (16), (17)
14. „show interfaces“: Tento příkaz zobrazí stav a konfiguraci všech rozhraní na přepínači. Poskytuje informace o MAC adrese, IP adrese, rychlosti a nastavení duplexu pro každé rozhraní. (16), (17)

15. „show vlan“: Tento příkaz zobrazí informace o sítích VLAN nakonfigurovaných na switchi, včetně ID VLAN, názvu a portů přiřazených každé VLAN. (16), (17)
16. „interface <*interface-id*>“: Tento příkaz umožňuje vstoupit do režimu konfigurace rozhraní pro zadané rozhraní. Například rozhraní GigabitEthernet1/0/1 vstoupí do konfiguračního režimu pro rozhraní GigabitEthernet1/0/1. (16), (17)
17. „switchport mode access“: Tento příkaz nastaví zadané rozhraní do režimu přístupu, což znamená, že může být přiřazeno pouze jedné VLAN síti. (16), (17)
18. „switchport access vlan <*vlan-id*>“: Tento příkaz přiřadí zadanou VLAN k přístupovému portu. Například switchport access vlan 10 by přiřadil VLAN 10 k přístupovému portu. (16), (17)
19. „switchport mode trunk“: Tento příkaz nastaví specifikované rozhraní do trunk módu, což znamená, že může být přiřazen pro více VLAN sítí. (16), (17)
20. „switchport trunk allowed vlan <*vlan-list*>“: Tento příkaz určuje, které VLAN mohou procházet portem trunk. (16), (17)

3.2.4.3.2 Packet tracer

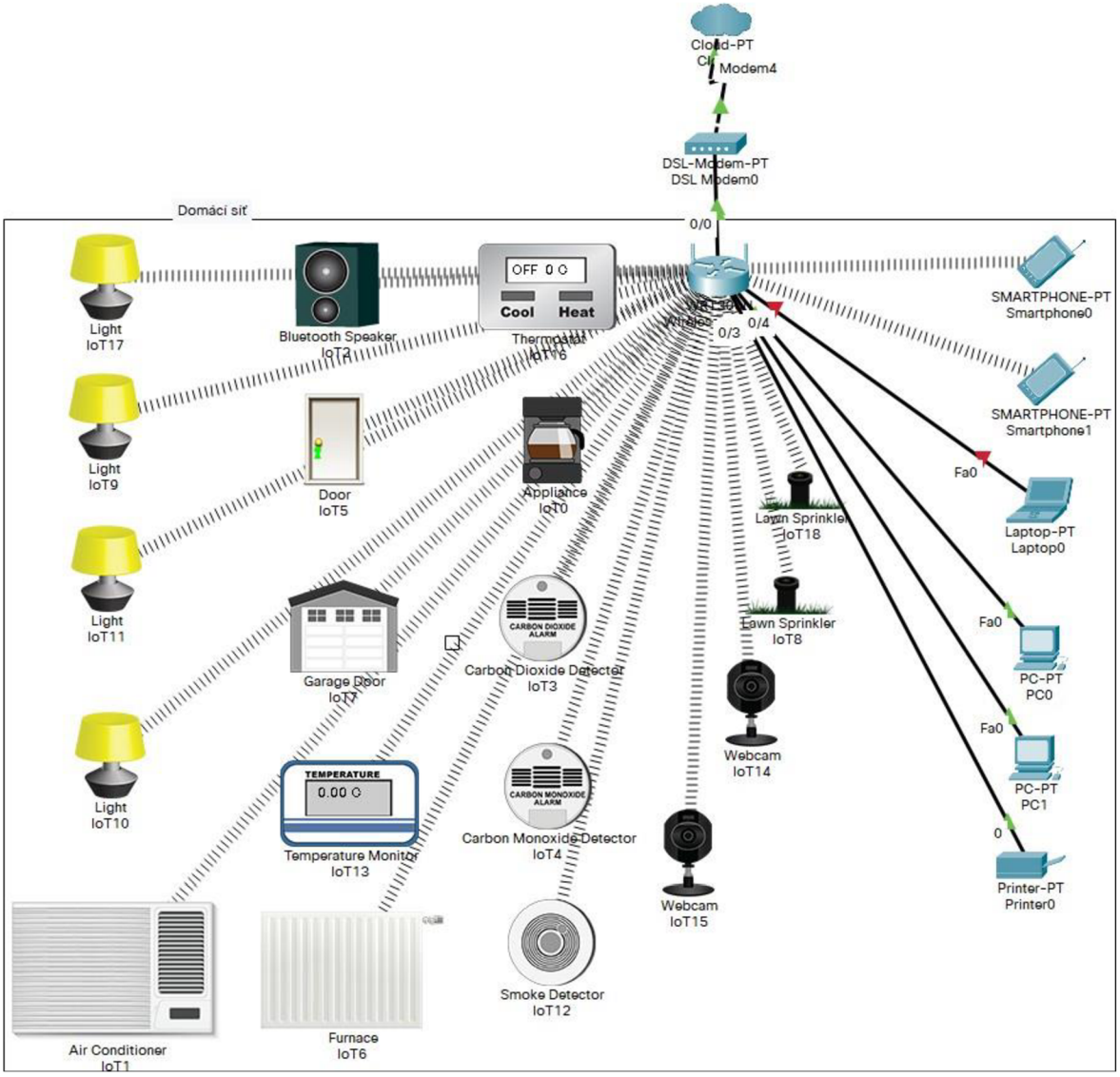
Packet Tracer je software pro simulaci počítačové sítě, který byl vyvinutý společností Cisco Systems. Tento software umožňuje navrhovat, konfigurovat a odstraňovat problémy v počítačových sítích. Poskytuje simulované prostředí, ve kterém lze vytvářet a manipulovat se síťovými topologiemi, zařízeními a konfiguracemi bez potřeby fyzického hardwaru. Díky tomu je ideálním nástrojem pro výuku, ale i pro testování a ověřování návrhů sítí před implementací. Packet Tracer je navržen tak, aby podporoval kurikulum Cisco Networking Academy a je široce používán v kurzech sítě Cisco jako učební pomůcka. Poskytuje tedy platformu pro experimentování s různými konfiguracemi sítě a protokoly v bezpečném a kontrolovaném prostředí. Kromě toho nabízí funkce, jako je vizualizace sítě v reálném čase a ohodnocení sítě. Některé z klíčových funkcí Packet Traceru zahrnují schopnost vytvářet a konfigurovat virtuální síťová zařízení, jako jsou routery, switche, firewally a servery. Podporuje širokou škálu síťových protokolů včetně TCP/IP, DHCP, DNS, OSPF a EIGRP. V tomto softwaru lze také vytvářet a konfigurovat topologie sítí a simulovat síťový provoz za účelem testování výkonu sítě a odstraňování problémů. Packet Tracer také poskytuje řadu nástrojů pro hodnocení sítě a řešení problémů. Obsahuje nástroj pro ladění, který umožňuje identifikovat a řešit problémy se sítí. Packet tracer také nabízí režim simulace, který umožňuje sledovat chování sítě v reálném čase. (18)

4 Vlastní práce

V praktické části této práce je hlavním cílem vytvořit účinné zabezpečení chytré domácí sítě. V první kapitole této části je popsán současný stav chytré domácí sítě. Je vytvořena logická topologie nynějšího stavu sítě v softwaru packet tracer. V této logické topologie je znázorněno jaká zařízení jsou k síti připojena a pomocí jakého rozhraní. V kapitole druhé jsou vytvořeny podsítě pomocí subnettování. Jedná se například o podsíť pro chytrá zařízení, podsíť pro počítače či podsíť pro hosty. Proces subnettování je popsán a výsledek je následně znázorněn pomocí blokového schématu, kde je síť již rozdělena a jsou přiřazené IP adresy k jednotlivým zařízením, ale také k podsítím. Ve třetí kapitole je vytvořena logická topologie podle výsledného blokového schématu v softwaru packet tracer. Následuje konfigurace všech zařízení, jako například přiřazení IP adres, masek sítě, nastavení virtuálních sítí, bezpečnostní nastavení routeru, nastavení správných rozhraních nebo správa přístupu. V poslední kapitole je otestována konektivita a propojení zařízeních pomocí pingů na určitou ip adresu zařízení. Je ověřeno správné nastavení všech ACL pravidel a jsou ověřeny přístupy do jednotlivých podsítí, pomocí nástrojů v softwaru packet tracer.

4.1 Počáteční stav chytré domácí sítě

Na obrázku číslo sedm je vyobrazena současná logická topologie chytré domácí sítě. Jedná se o primární stav, kdy se všechna zařízení připojí k routeru buď kabelem nebo pomocí wifi. Síť je bez jakékoli konfigurace a zabezpečení. Tato topologie je vytvořena v softwaru packet tracer. Všechna zařízení v domácnosti jsou připojené k jednomu routeru a vše je tak v jedné domácí síti. IoT zařízení jako je chytrý termostat, chytré osvětlení, chytrý zámek, chytrý zavlažovač, chytré detektory, chytrá garážová vrata či chytré kamery jsou připojené k routeru pomocí wifi. Dva počítače, tiskárna a laptop jsou připojeny k routeru pomocí kabelu. Pomocí wifi jsou připojeny i dva chytré mobily. Není zde řešeno z jakého zařízení mohou být IoT prvky sítě ovládány, takže je může ovládat každý, kdo se do sítě dostane. Tudíž chybí zde jakákoliv správa přístupu k IoT zařízením. IoT zařízení a domácí počítače nejsou v oddělených sítích, tudíž pokud je například počítač napaden, tak útočník získává rovnou přístup do celé sítě ke všem zařízením, a naopak. Z tohoto důvodu je síť rozdělena na podsítě, kdy každá podsíť nese své vlastní zabezpečující nastavení.



Obrázek 7- Počáteční stav chytré domácí sítě

4.2 Rozdělení chytré domácí sítě

Pomocí techniky subnettingu je chytrá domácí síť rozdělena do podsítí. Síť, která je rozdělována je privátní síť typu C 198.168.0.0. Pomocí subnettingu vznikají oddělené a samostatně spravovatelné celky, které nesou svou vlastní IP adresu a specifickou konfiguraci. Pro určení počtu podsítí a také počtu zařízeních v každé podsíti bylo třeba určit podobná zařízení, určit jaká komunikace je potřeba pro daná zařízení, jakou rychlost přenosu potřebují a jaká zařízení mohou či nemohou posílat zprávy, a komu. Pro takto rozřazená zařízení v podsítích lze pak snadněji řešit pravidla pro celou podsíť.

První podsíť zahrnuje kabelem připojená zařízení, kterými jsou osobní počítače, laptopy a tiskárna. Tato síť může komunikovat jak na internet, tak v domácí síti. Podrobnosti této komunikace jsou ošetřeny v ACL (Acces Control List) pravidlech. Důvodem pro oddělení této sítě je izolace od IoT zařízeních. Také tato zařízení nepotřebují omezovat rychlost připojení k internetu. Pro tuto podsíť je vytvořena i wifi síť, která bude kopírovat její konfiguraci. Další podsítě jsou vytvořeny pro IoT zařízení, která jsou připojeny pomocí wifi sítě. Podsíť pro chytré osvětlení je určena pro chytré žárovky a další typy světelných prvků v síti. Tato podsíť nebude moct komunikovat na internet, pouze v místní síti a pouze do určených podsítí. Tyto pravidla jsou dále upřesněny v ACL. Světla budou moci být ovládány pouze z podsítě osobních počítačů a mobilů, tudíž žádné jiné IoT zařízení nebude moct manipulovat se světelnými prvky v této síti. Také naopak, pokud například jedna z žárovek bude napadena, nebude moct ovládat či jinak narušit chod ostatních chytrých zařízeních. V této podsíti lze upravit rychlost připojení, jelikož chytré osvětlení nepotřebuje plnou rychlost připojení. Podobná omezení nese i další podsíť, která zahrnuje chytrý zámek, garážová vrata a kamery. Pro tuto síť je nastavena vyšší přenosová rychlost, právě kvůli kamerám. Tato podsíť také nemá přístup k internetu. Tímto se docílilo toho, že elektronický zabezpečovací systém bude izolován a tím pádem do určité míry odolný vůči vnějším kyberútokům a hrozbám, ale i vnitřním pokusům o nepovolenou komunikaci, jelikož jsou nastavena pravidla pro přístup do této podsítě. Zařízení jako chytrá lednice, chytrá trouba, chytrý kávovar, chytrý termostat, chytrý radiátor či klimatizace jsou zařazena do podsítě, kde je komunikace na internet sice povolená, ale omezená rychlostí. Komunikace je povolená z důvodu zajištění správy na dálku pomocí chytrého telefonu či pro komunikaci zařízení s určitou databází či pro aktualizace softwaru pro jednotlivá zařízení. Tato podsíť má omezenou komunikaci v místní síti, která je omezena pravidly ACL. Poslední skupinou, pro kterou je nutno vytvořit podsíť, jsou senzory a detektory. Do této podsítě tedy patří detektory kouře a plynu, senzory teploty, senzory měřící vlhkost či úroveň vody a také jsou zde zařazeny kropiče zahrady. Tato podsíť má povolenou komunikaci skrz internet kvůli případnému bezpečnostnímu hlášení detektorů. Komunikace v místní síti je povolena, ale také omezena na komunikaci se specifickými zařízeními.

Každé podsíti je přiřazeno rozmezí IP adres a také maska sítě, která je zvolena podle počtu prvků v jednotlivých podsítích. Jednotlivé adresy jsou vypsány v blokovém schématu,

kde jsou vyznačeny rozhraní pro jednotlivé podsítě, IP adresy bran jednotlivých podsítí a také jsou sepsány základní ACL pravidla.

4.2.1 Blokové schéma chytré domácí sítě

Obrázek číslo osm je reprezentací rozdělení chytré domácí sítě. Jsou zde zakresleny jednotlivé podsítě, IP adresy, rozhraní, identifikátory bezdrátové sítě a také základní ACL. Pro úsporu kabelů a síťových prvků se síť rozdělila do virtuálních místních sítí (vlan). Virtuální místní síť je logické rozdělení sítě bez potřeby zasahování do fyzického uspořádání síťových prvků a zařízeních. Každá virtuální místní síť je podsítí celé sítě. Pro přehlednost a jednoduchou orientaci je každá vlan označena jako *vlan* a příslušné číslo IP adresy podsítě, to znamená, jestliže je podsíti přiřazena IP adresa 192.168.100.0, označení vlan bude *vlan 100*. Masky podsítí jsou zapisovány pomocí CIDR notace.

Router je připojen k externí síti poskytovatele internetu, ve které nese svou externí IP adresu. K routeru jsou připojeny dva osobní počítače, jeden notebook a jedna tiskárna pomocí kabelu. Tato zařízení jsou v podsíti vlan 100. Rozhraní pro tato zařízení jsou Gi1/1-4 (GigabitEthernet 1/ 1-4). Pomocí příkazu access jsou tato rozhraní zařazena do příslušné vlan 100. Gateway (GW) pro tuto vlan nese adresu 192.168.100.1/25. Maska podsítě je zvolena na /25, tato síť má k dispozici 128 IP adres, takže lze připojit 125 zařízení. Tři IP adresy z tohoto rozsahu jsou vždy rezervované pro gateway, podsíť a broadcast adresu.

Do routeru jsou pomocí kabelů zapojeny dva AP (access pointy) pro vysílání wifi sítě. Pro tyto prvky se využívá rozhraní Gi1/7-8. Tyto rozhraní jsou konfigurovány pomocí trunk příkazu, aby přenášely více vlan sítí. Tyto AP mají šest SSID (Service Set Identifier) a každé je určeno jiné vlan síti.

SSID *Doma* je určeno pro vlan 100, která je určena například pro mobily, tablety či chytré hodinky. Gateway pro tuto vlan je stále stejná, jako pro „kabelovou“ verzi vlan 100.

SSID *IoT-Svetla* je určená pro vlan 101, na kterou se připojují chytré osvětlovací prvky. IP adresa GW je 192.168.101.1/26. Tato síť poskytuje 64 IP adres a lze k ní tedy připojit 61 zařízení.

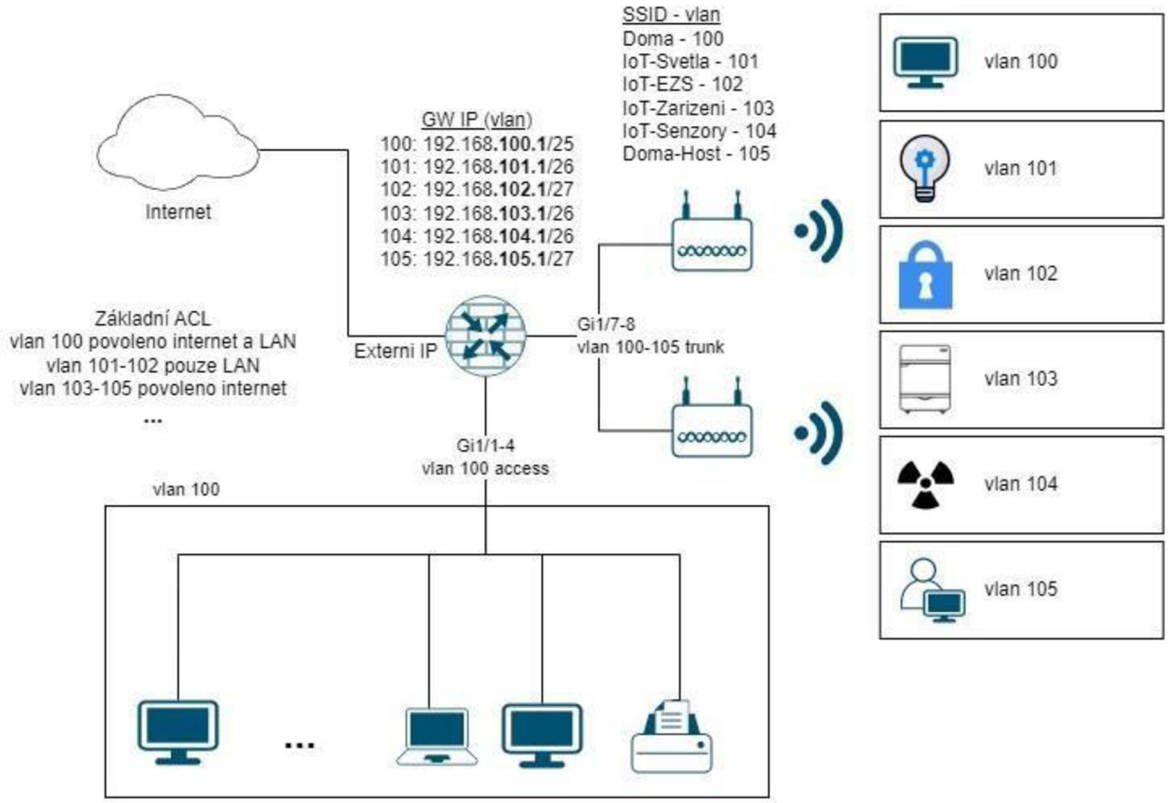
SSID *IoT-EZS* je určena pro vlan 102, kam se připojují chytré prvky zajišťující převážně zabezpečení pro domácnost. Tím se myslí chytrý zámek, chytrá garážová vrata a chytré kamery. Pro tuto vlan má GW IP adresu 192.168.102.1/27. Pro síť s maskou /27 jsou k dispozici IP adresy v množství 32. K této síti lze připojit až 29 prvků.

SSID *IoT-Zarizeni* je určena pro vlan 103. IP adresa GW pro tuto vlan je 192.168.103.1/26. Vlan 103 poskytuje 64 IP adres a lze připojit 61 prvků do této sítě. Tato podsíť je určena pro chytré spotřebiče jako pračka, trouba, lednice či kávovar. Chytré termostaty spolu s chytrými radiátory a klimatizací jsou také připojeny do této sítě.

SSID *IoT-Senzory* je určena pro vlan 104. K této vlan se připojují chytrá zařízení jako chytré senzory na detekci kouře či plnu, senzory vlhkosti a také chytré zavlažovače zahrady. Gateway pro tuto vlan nese IP adresu 192.168.104.1/26 poskytující 64 IP adres a lze k ní tedy připojit 61 zařízení.

SSID *Doma-Host* je přiřazena k vlan 105. IP adresa GW pro tuto vlan je 192.168.105.1/27. Pro síť s maskou /27 jsou k dispozici IP adresy v množství 32. K této síti lze tedy připojit až 29 prvků. Vlan 105 je určena pro hosty.

Masky podsítí jsou zvoleny tak, aby vždy v každé podsíti byla rezerva minimálně 25 zařízení. Tím, že síť je dělená na devátém bitu, není problém síť kdykoliv rozšířit a navýšit tak počet připojených zařízeních k určité síti. Ve schématu jsou vypsány základní pravidla ACL. Podrobněji jsou rozvedena u samotné konfigurace těchto pravidel.



Obrázek 8 - blokové schéma chytré domácí sítě

4.3 Konfigurace síťových prvků v chytré domácí síti

V této části práce jsou ukázány výtažky kódů, které jsou pro konfiguraci nejdůležitější. V první řadě je vždy nastaveno základní zabezpečení síťových prvků pomocí příkazu *enable secret,* který vytváří šifrované heslo pro přístup do síťového prvku. Zařízení jsou konfigurována postupně. Jako první jsou vytvořeny a nakonfigurovány vlan sítě, jsou jim přiřazeny IP adresy dle schématu. Rozhraní jsou přiděleny do určených vlan sítí a určitá rozhraní spojující hlavní síťové prvky jsou nakonfigurovány tak, aby nesly komunikaci všech vlan sítí pomocí příkazu *switchport mode trunk*. Dále probíhá nastavení access pointů a vytvoření více bezdrátových sítí, které jsou vysílány právě access pointami. Každá bezdrátová síť nese své SSID, které je spojeno s danou vlan dle blokového schématu. Jsou nakonfigurovány DHCP pooly pro přidělování IP adres pro určité vlan sítě. Natavená jsou také subrozhraní na routeru. Pomocí příkazu *ip dhcp snooping limit* <*číslo*> je limitován příjem packetů za sekundu a tím je síť chráněna před útoky jako IP a DHCP spoofing a DHCP starvation. V poslední řadě jsou nastavena ACL pravidla pro správu přístupu. Ověření konfigurace a konektivity modelu je prováděno v další kapitole praktické části.

První zařízení, které je nakonfigurováno je switch. Na switchi se konfigurují vlan sítě, přiřazují se IP adresy GW a taky IP adresy pro každou podsíť. Dle schématu jsou zařízení zapojena přímo do routeru, avšak packet tracer nemá možnost konfigurace vlan sítí pro router, proto je do modelu přidán switch. V CLI (command-line interface) switche je zadán příkaz *enable*, který nám dovolí vstoupit do privilegovaného režimu EXEC, který je vyžadován pro většinu konfiguračních úloh. Dalším příkazem je *configure terminal,* tento příkaz umožňuje vstoupit do režimu globální konfigurace, kde se mohou provádět změny v konfiguraci. V tomto režimu lze vytvořit vlan sítě. Na obrázku číslo devět lze vidět příkaz *vlan* a preferované číslo vlan sítě. Dle schématu jsou vlany pojmenovány podle IP adres, které nesou. Po příkazu *vlan 100* je založena vlan 100 a následně je i takto pojmenována. Postupně jsou takto vytvořeny všechny požadované vlan sítě. Pomocí příkazu *show vlan* jsou zobrazeny všechny vla sítě, které jsou na switchi vytvořeny. Vlan 1 neboli default je automaticky vytvářena vlan síť do které jsou přiřazeny veškerá rozhraní.

```
Switch(config)#vlan 100
Switch(config-vlan)#name vlan100
Switch(config-vlan)#vlan 101
Switch(config-vlan)#name vlan101
Switch(config-vlan)#vlan 102
Switch(config-vlan)#name vlan102
Switch(config-vlan)#vlan 103
Switch(config-vlan)#name vlan103
Switch(config-vlan)#vlan 104
Switch(config-vlan)#name vlan104
Switch(config-vlan)#vlan 105
Switch(config-vlan)#name vlan105
Switch(config-vlan)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Obrázek 9- Založení a pojmenování vlan

Na obrázku číslo deset lze vidět výstup příkazu *show vlan*. Nově vytvořené vlany ještě nemají přiřazená rozhraní a lze vidět, že veškerá rozhraní jsou v defaultní vlan.

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
100  vlan100                          active
101  vlan101                          active
102  vlan102                          active
103  vlan103                          active
104  vlan104                          active
105  vlan105                          active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
 --More--
```

Obrázek 10- Výstup příkazu show vlan

Obrázek číslo jedenáct ukazuje přiřazení určitých rozhraní do vlan 100. V režimu konfigurace je zadán příkaz *interface FastEthernet 0/1* (zkráceně *int fa0/1*) a pro toto

rozhraní je pomocí příkazu *switchport mode access* povoleno přirazení k určité vlan síti. Následující příkazem *switchport access vlan 100* je rozhraní přiřazeno do této virtuální podsítě. Do switche jsou kabelem ještě připojena tři zařízení, notebook, tiskárna a ještě jeden osobní počítač. Počítač je připojen do rozhraní fa0/2, notebook do rozhraní fa0/3 a tiskárna do rozhraní fa0/4. Tato rozhraní jsou také přidána do vlan 100. Pomocí příkazu *interface range FastEthernet 0/2-4* (*int r fa0/2-4*) se všechna tato rozhraní staly také součástí vlan 100. Obrázek číslo dvanáct ukazuje výstup příkazu *show lan* a lze vidět přiřazená rozhraní do vlan 100. Pro přiřazení rozhraní do ostatních vlan je třeba nastavit AP (access pointy) a vytvořit SSID (Service Set Identifier) a poté je přiřadit k jednotlivým vlan jako rozhraní.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 100
Switch(config-if)#int r fa0/2-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 100
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Obrázek 11- Přiřazení rozhraní vlan 100

```
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
100  vlan100                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
101  vlan101                           active
102  vlan102                           active
```

Obrázek 12- Výstup show vlan příkazu

Takto vytvořeným vlan sítím je za potřebí přidělit na switchi jejich IP adresy. Na obrázku číslo třináct lze vidět postup při přidělování IP adres. V konfiguračním režimu se vstoupí pomocí příkazu *interface vlan 100* (*int vlan 100*) do nastavení daného rozhraní.

Příkazem *int vlan 100* se vstoupilo do nastavení vlan 100. V tomto rozhraní se nastaví IP adresa 192.168.100.2 pomocí příkazu *ip address 168.192.100.2 255.255.255.128*, tento příkaz vyžaduje i masku podsítě, nelze ji zadat v CIDR notaci. Adresa je zvolena na základě druhého čísla v pořadí, jelikož číslo jedna je rezervováno pro adresu GW. IP adresy jsou tímto způsobem přiřazeny všem vlan sítím, kdy IP adresy jsou předem určeny v blokovém schématu.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 100
Switch(config-if)#ip address 192.168.100.2 255.255.255.128
Switch(config-if)#int vlan 101
Switch(config-if)#ip address 192.168.101.2 255.255.255.192
Switch(config-if)#int vlan 102
Switch(config-if)#ip address 192.168.102.2 255.255.255.224
Switch(config-if)#int vlan 103
Switch(config-if)#ip address 192.168.103.2 255.255.255.192
Switch(config-if)#vlan 104
Switch(config-vlan)#ip address 192.168.104.2 255.255.255.192
                   ^
% Invalid input detected at '^' marker.

Switch(config-vlan)#int vlan 104
Switch(config-if)#ip address 192.168.104.2 255.255.255.192
Switch(config-if)#int vlan 105
Switch(config-if)#ip address 192.168.105.2 255.255.255.224
Switch(config-if)#
Switch(config-if)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Obrázek 13- Přiřazení IP adres vlan sítím

Router je nakonfigurován, aby zařízením v síti dynamicky přiřazoval IP adresy z daného rozsahu. Lze říci, že router funguje i jako DHCP server. Obrázek číslo čtrnáct ukazuje postup této konfigurace. V konfiguračním režimu pomocí příkazu *ip dhcp pool* <název-vlan> se vstoupí do nastavení DHCP poolu pro rozdělování IP adres pro danou vlan a zadají se parametry, podle kterých jsou IP adresy rozdělovány. Příkazem *ip dhcp pool vlan101* se vstoupí do nastavení DHCP poolu pro vlan 101. V tomto režimu se nastaví IP adresa podsítě a také IP adresa default-routeru. Pro vlan 101 je nastavena IP adresa podsítě 192.168.101.0 s maskou sítě 255.255.255.192 a IP adresa routeru 198.168.101.1. Síťová maska zde není vyžadovaná. První adresa v sítí je rezervovaná pro router neboli gateway v tomto modelu. Pomocí stejných příkazů jsou nastaveny i vlan 100, vlan 102, vlan 103, vlan 104 a vlan 105. Pro vlan 100 je přiřazena IP adresa sítě 192.168.100.0 s maskou sítě

255.255.255.128. Pro vlan 102 je nastavena IP adresa sítě 192.168.102.0 s maskou 255.255.255.224. Pro vlan 103 je IP adresa sítě ve tvaru 192.168.103.0 a její maska je 255.255.255.224. Vlan 104 má IP adresu sítě 192.168.104.0 a masku sítě 255.255.255.192. Poslední vlan 105 má přiřazenou adresu sítě 192.168.105.0 s maskou sítě 255.255.255.224. Adresy routeru jsou vždy nastaveny na první adresu v síti, tudíž na 1.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool vlan100
Router(dhcp-config)#network 192.168.100.0 255.255.255.128
Router(dhcp-config)#default-router 192.168.100.1
Router(dhcp-config)#exit
Router(config)#ip dhcp pool vlan101
Router(dhcp-config)#network 192.168.101.0 255.255.255.192
Router(dhcp-config)#default-router 192.168.101.1
Router(dhcp-config)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool vlan102
Router(dhcp-config)#network 192.168.102.0 255.255.255.224
Router(dhcp-config)#default-router 192.168.102.1
Router(dhcp-config)#exit
Router(config)#ip dhcp pool vlan103
Router(dhcp-config)#network 192.168.103.0 255.255.255.224
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool vlan103
Router(dhcp-config)#network 192.168.103.0 255.255.255.224
Router(dhcp-config)#default-router 192.168.103.1
Router(dhcp-config)#exit
Router(config)#ip dhcp pool vlan104
Router(dhcp-config)#network 192.168.104.0 255.255.255.192
Router(dhcp-config)#default-router 192.168.104.1
Router(dhcp-config)#exit
Router(config)#ip dhcp pool vlan105
Router(dhcp-config)#network 192.168.105.0 255.255.255.224
Router(dhcp-config)#default-router 192.168.105.1
Router(dhcp-config)#exit
Router(config)#
```

Obrázek 14- Nastavení dhcp poolu

Pro založení a správu AP (Access point) je za potřebí do modelu přidat WLC (wireless LAN controller) prvek. Cisco packet tracer nepodporuje přímé nastavení AP a je vyžadováno užití WLC zařízení pro správu bezdrátových sítí. Do switche se přidá WLC prvek, který je zapojen do rozhraní fa0/23. Cisco WLC zařízení podporují pouze LAG (Link Aggregation Group) a proto je za potřebí nastavit rozhraní do kterého je WLC zapojeno jako LAG. Na obrázku číslo patnáct je zobrazena konfigurace LAG. Je vybráno rozhraní, které

do této skupiny náleží a následně pomocí příkazu *channel-group 1 mode on* je vytvořeno nové rozhraní port-channel 1.

```
Switch(config)#int r f0/23-24
Switch(config-if-range)#channel-goup 1 mode on
                       ^
% Invalid input detected at '^' marker.

Switch(config-if-range)#channel-group 1 mode on
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
```

Obrázek 15- nastavení channel group

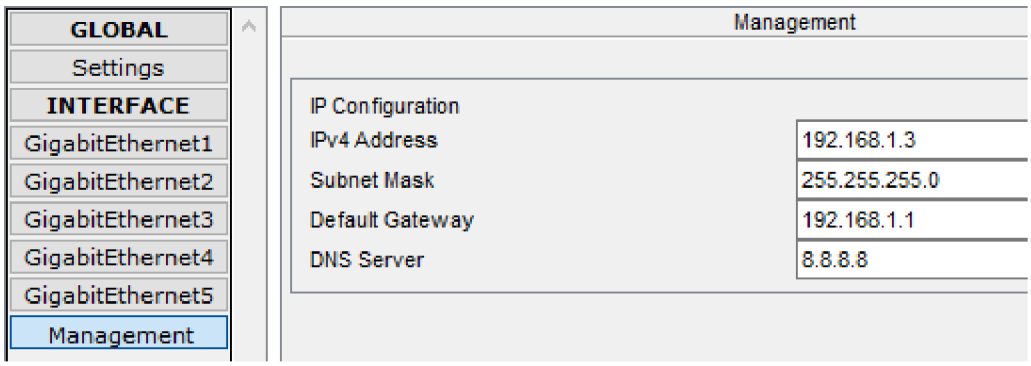
Aby všechny vytvořené vlan sítě mohli komunikovat do routeru, je rozhraní mezi routerem a switchem nastaveno jako trunk port. Rozhraní, kterým je připojen switch k routeru je konfigurováno pomocí příkazu pro tvorbu trunk portu, jak lze vidět na obrázku číslo šestnáct. V konfiguračním režimu pomocí příkazu interface Gig0/1 se vstoupí do nastavení tohoto rozhraní. Zde je zadán příkaz *switchport mode trunk* pro nastavení trunk spojení mezi routerem a switchem. Na obrázku číslo šestnáct také vidět uložení dosavadní konfigurace pomocí příkazu *copy run start,* který lze zadat pouze v privilegovaném režimu.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int gig0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Obrázek 16- Nastavení trunk portu

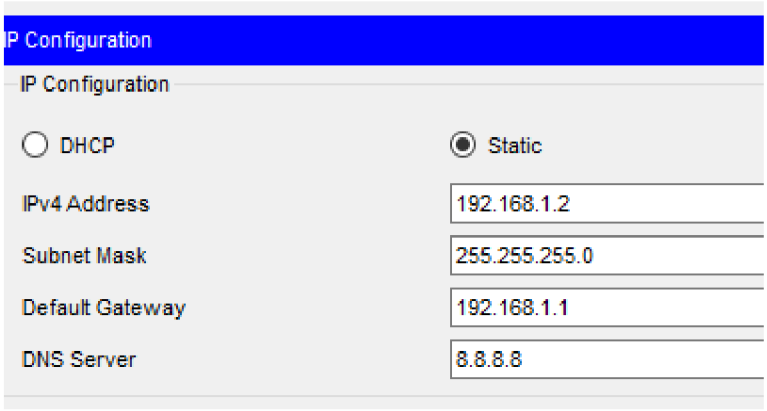
Pro vytvoření více SSID (Service Set Identifier) na AP (Access Point) je za potřebí přidat do modelu WLC (Wireless LAN Controller) a také DHCP server pro přidělení IP adresy Access pointům. Cisco packet tracer neumožňuje nastavit IP adresu pro AP ručně v nastavení, proto je IP adresa přidělena pomocí DHCP serveru. Obrázek číslo sedmnáct ukazuje IP nastavení pro WLC prvek. Tomuto síťovému prvku je přiřazena IP adresa 192.168.1.3. Tato adresa je zvolena tak, aby nezasahovala do adres, které jsou určeny pro

vlan sítě podle blokového schématu. Defaultní gateway adresa je stanovena na 192.168.1.1, jakožto první adresa v dané síti. Pro DNS server je zvolena IP adresa 8.8.8.8. Tato adresa je primární adresou DNS serveru společnosti google a je veřejná.



Obrázek 17- IP konfigurace WLC prvku

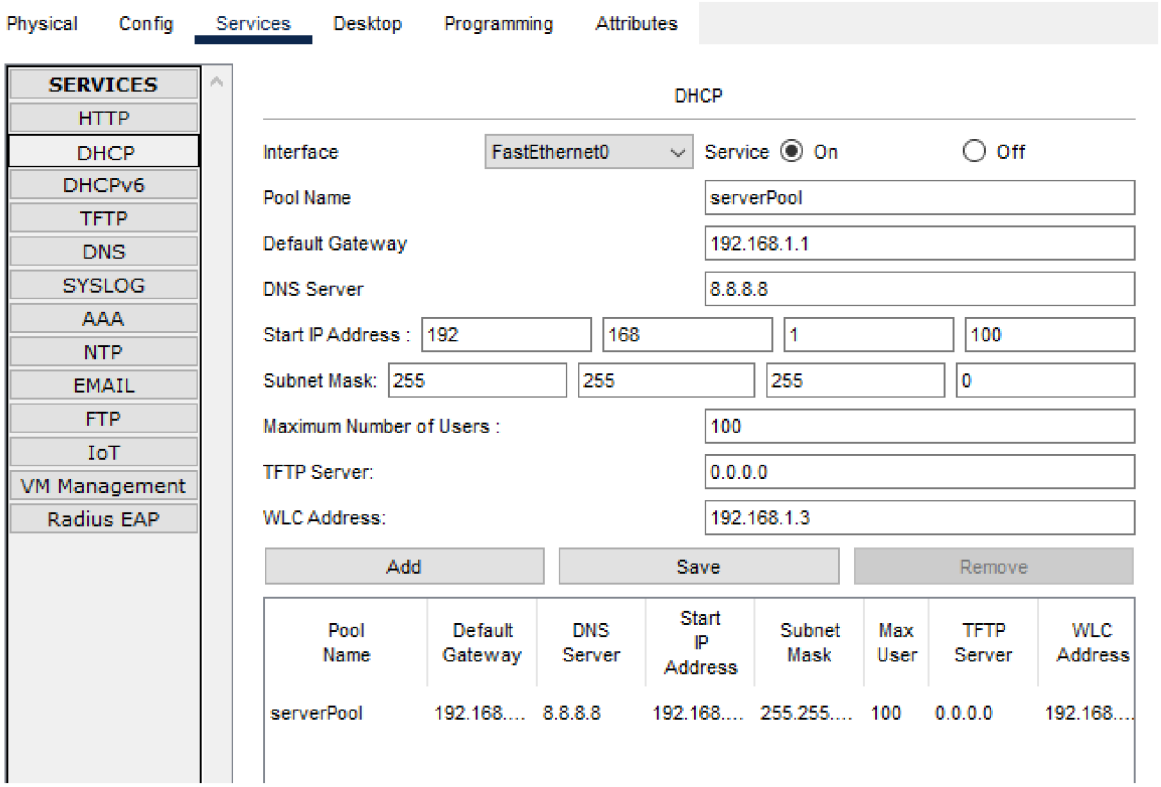
Na obrázku číslo osmnáct je vyobrazena IP konfigurace samotného DHCP serveru. Tomuto serveru je přiřazena druhá adresa v síti, tudíž IP adresa 192.168.1.2. Defaultní gateway a DNS server má stejné adresy jako WLC prvek.



Obrázek 18- IP konfigurace DHCP serveru

Konfigurace DHCP služby je zobrazena na obrázku číslo devatenáct. Adresa default gateway a adresa DNS serveru je stejná jako při IP konfiguraci DHCP serveru. Startovní IP adresa, od které začne DHCP server rozdělovat adresy, je stanovena na 192.168.1.100. Pro přehlednost se IP adresy začnou přiřazovat od 100. Počet možných rozdělených adres je nastaven na 100. Pokud se budou přidávat další AP, je zajištěna rezerva pro ně. Aby AP prvky věděly, jaká adresa je pro jejich ovládací zařízení, je v kolonce WLC address

nastavena IP adresa, která byla přiřazena WLC prvku v síti, tudíž 192.168.1.3. Konfigurace je uložena pomocí tlačítka save.



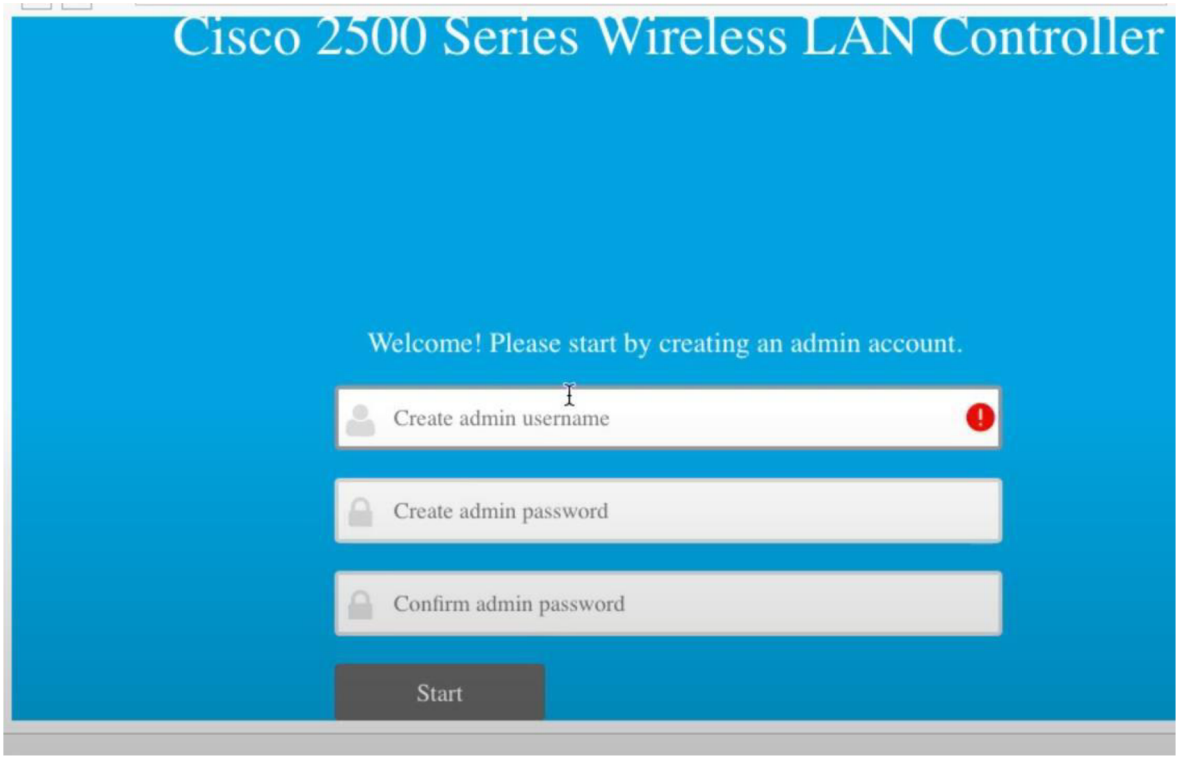
Obrázek 19- Nastavení DHCP služby

Obrázek číslo dvacet dokazuje funkčnost DHCP serveru. Po povolení DHCP protokolu u Access pointů se jim přiřadila IP adresa ve zvoleném DHCP poolu. Lze vidět, že AP obdržel IP adresu 192.168.1.100. Tento AP také zná adresu svého WLC zařízení. Na obrázku číslo dvacet je tato informace zapsána ve formě CAPWAP Status: Connected to 192.168.1.3, což je adresa řídícího prvku WLC.

```
Device Name: doma-ap1
Device Model: 3702i

Port                Link   IP Address          MAC Address
GigabitEthernet0    Up     192.168.1.100/24    0001.63BE.A301
Dot11Radio0         Up     <not set>           0001.63BE.A302

CAPWAP Status: Connected to 192.168.1.3
Providing WLANs:
    doma (doma)

Physical Location: Intercity > Home City > Corporate Office > Main
```

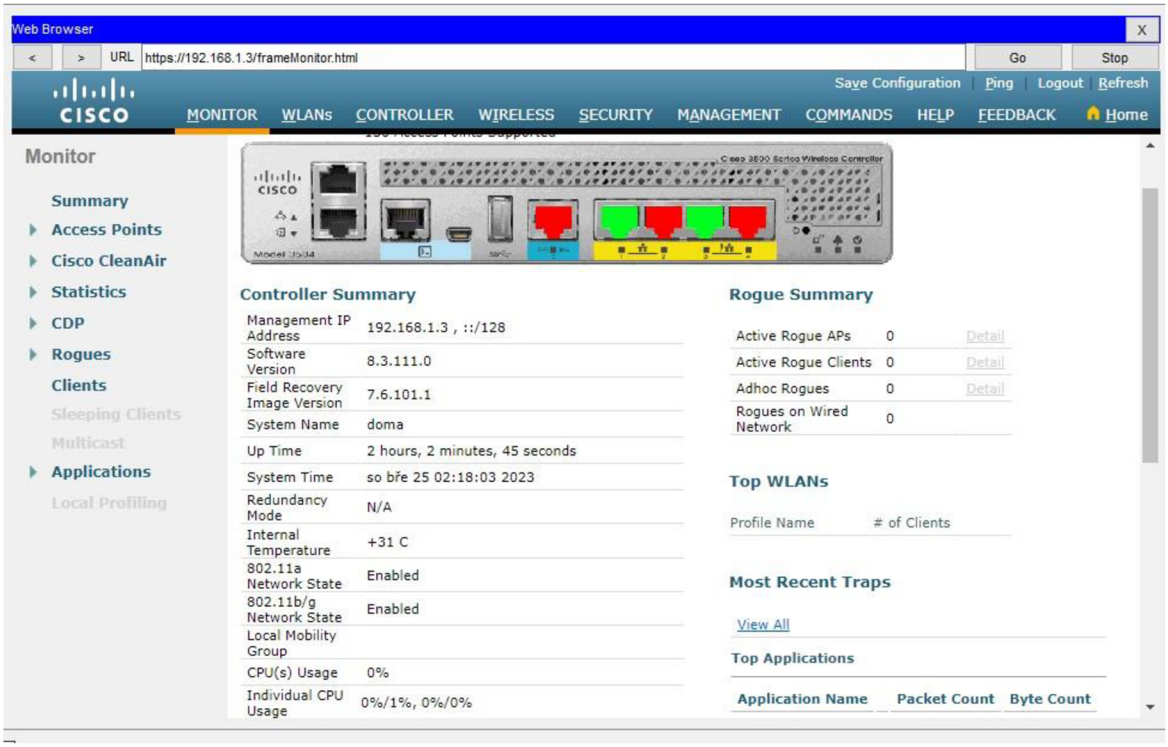
Obrázek 20- IP adresa AP

Po zadání IP adresy WLC prvku do webového prohlížeče připojeného osobního počítače do stejné sítě, se otevře nabídka se základním konfiguračním nastavením pro WLC zařízení. Obrázek číslo dvacet jedna ukazuje úvodní stránku nastavení. Je zvoleno uživatelské jméno a heslo. Je provedena základní konfigurace WLC, jakou je například přiřazení IP adres, defaultní gateway, DNS server či jméno bezdrátové sítě.

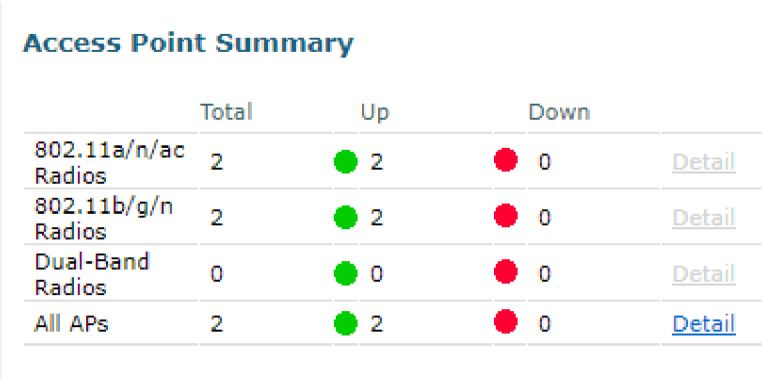


Obrázek 21- Počáteční nastavení WLC

Po provedení základní konfigurace lze vstoupit do nastavení bezdrátových sítí, tudíž lze nastavit nová SSID pro access pointy. Obrázek číslo dvacet dva ukazuje, jak vypadá úvodní obrazovka pro nastavení bezdrátové sítě. Jsou zde základní informace o zařízení samotném, jako je jeho IP adresa, doba provozu, využití CPU (central processing unit) a paměti, jaké sloty jsou fyzicky osazené či teplotu samotného zařízení. Obrázek číslo dvacet tři ukazuje propojení WLC a Access pointů.

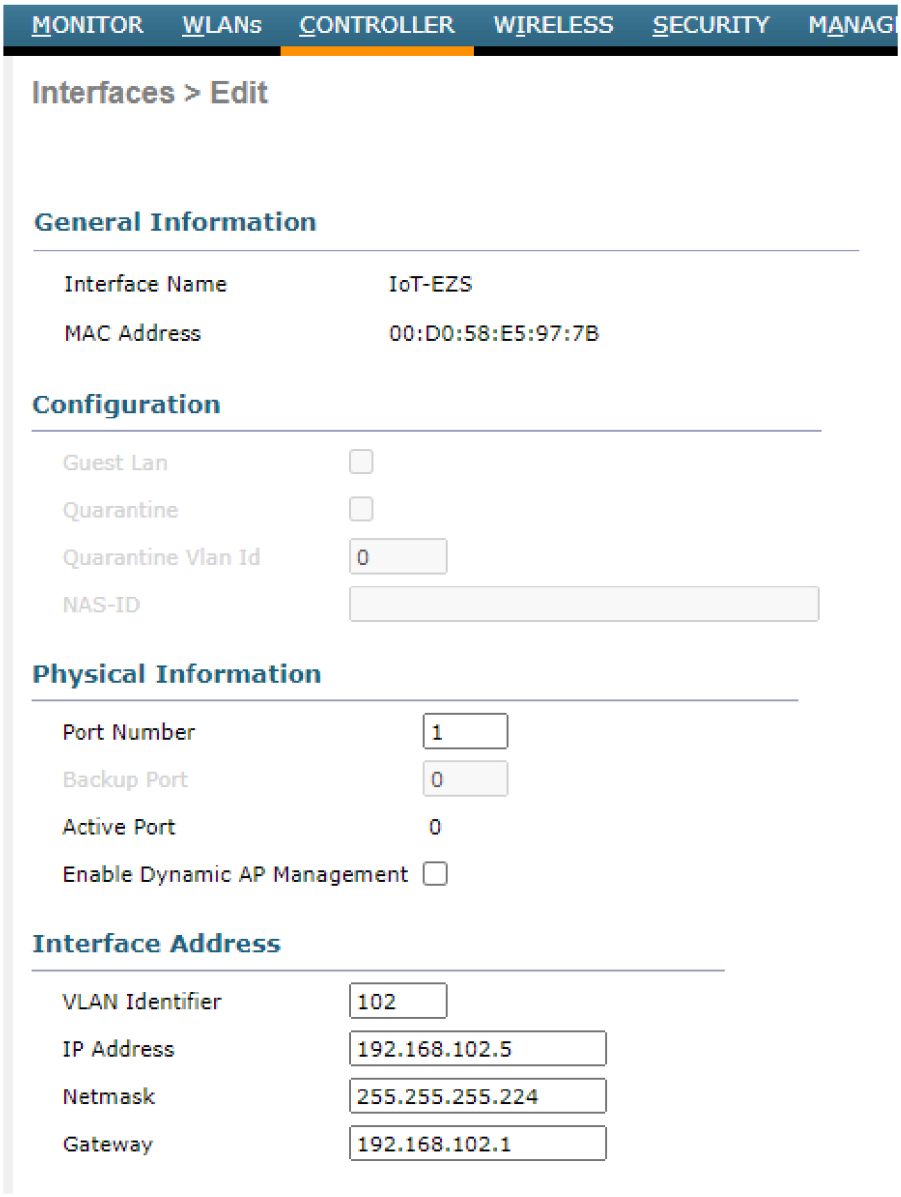


Obrázek 22- Úvodní obrazovka pro WLC správu



Obrázek 23- Access point status

V záložce controller jsou vytvořena rozhraní pro potřebná SSID. Na obrázku číslo dvacet čtyři je ukázána tvorba a nastavení nového rozhraní pro vlan 102, tedy SSID IoT-EZS. Je nastaveno příslušné číslo vlan sítě, do které toto SSID patří. Nastaveny jsou IP adresy pro defaultní gateway a také pro samotné rozhraní. Takto jsou vytvořená rozhraní pro všechny vlan sítě. Obrázek číslo dvacet pět ukazuje výsledný souhrn vytvořených rozhraní.

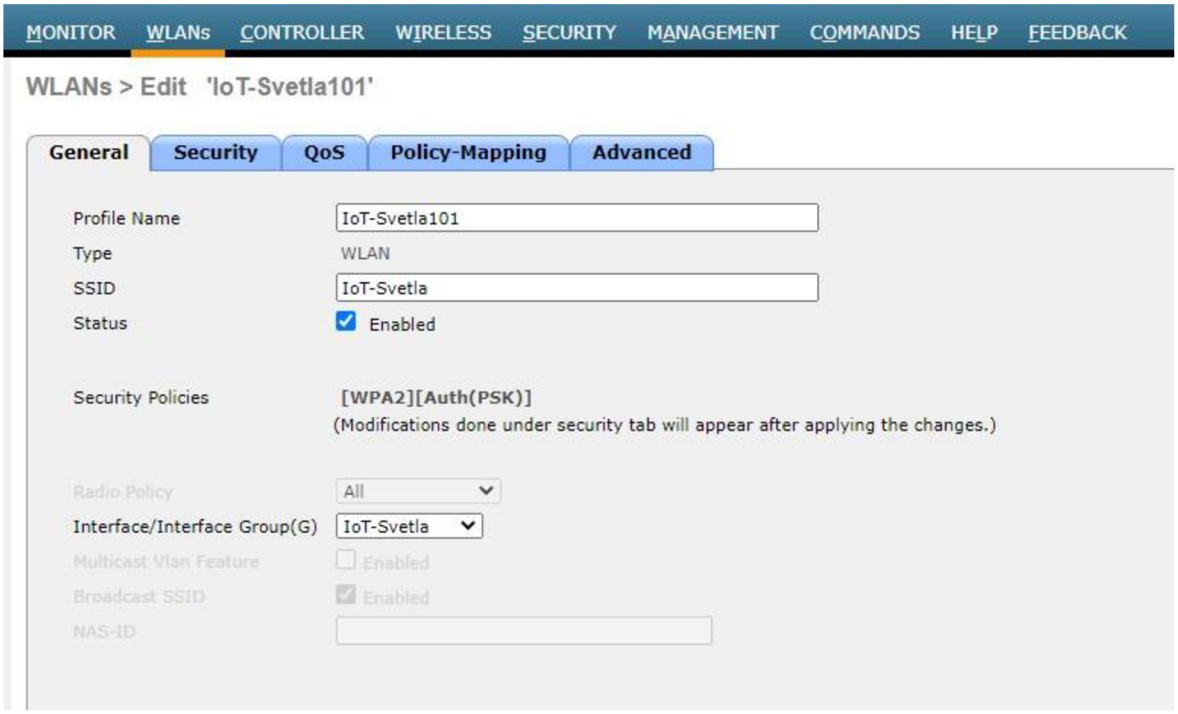


Obrázek 24- Tvorba rozhraní pro vlan 102

Interface Name	VLAN Identifier	IP Address	Interface Type
Doma	100	192.168.100.5	Dynamic
Doma-Host	105	192.168.105.5	Dynamic
IoT-EZS	102	192.168.102.5	Dynamic
IoT-Senzory	104	192.168.104.5	Dynamic
IoT-Svetla	101	192.168.101.5	Dynamic
IoT-Zarizeni	103	192.168.103.5	Dynamic

Obrázek 25- Vytvořená rozhraní pro všechny vlan sítě

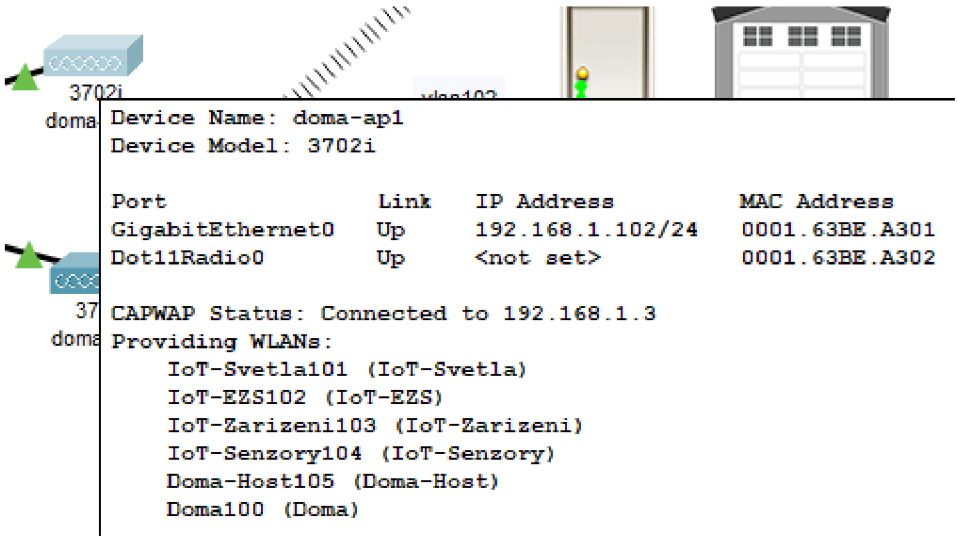
V záložce WLANs se k těmto rozhraním vytvoří bezdrátová síť. Obrázek číslo dvacet šest ukazuje základní nastavení WLAN pro rozhraní IoT-Svetla. Pro tuto síť bylo nastaveno zabezpečení WPA2 (Wifi protected access) v záložce security a je nastaveno PSK (Phase-shift Key) neboli heslo pro síť. Pro zbývající vlan sítě je postup konfigurace opakován a na obrázku číslo dvacet sedm lze vidět výsledek.



Obrázek 26- Konfigurace vlan 101

Obrázek 27- Přehled vytvořených WLAN sítí

Obrázek číslo dvacet sedm ukazuje, že access point již nabízí všechny sít, které bylo potřeba vytvořit podle blokového schématu. Všechna chytrá zařízení se připojí k určeným sítím dle schématu. V nastavení zařízení je nastaveno SSID ke kterému je dané zařízení přiřazeno a je zadáno potřebné heslo pro připojení k dané bezdrátové síti.



Obrázek 28- AP WLAN sítě

Na obrázku číslo dvacet devět a třicet lze vidět konfiguraci subrozhraní pro router. Pro dostupnost GW pro každé zařízení je nastavena IP adresa pro daná subrozhraní. V konfiguračním režimu je zadán příkaz *int g0/1.100* pro vstup do nastavení tohoto rozhraní. Příkazem *encapsulation dot1q 100* je přiřazena vlan 100. Následně je příkazem *ip address 192.168.100.1 255.255.255.128* přiřazena adresa pro toto rozhraní. Tyto příkazy jsou použity pro konfiguraci všech ostatních subrozhraní. Nastavení je následně uloženo. Rozhraní, které spojuje switch a AP je pomocí příkazu *switchport mode trunk* změněno na trunk port a je tak zajištěna komunikace a přenos více vlan sítí.

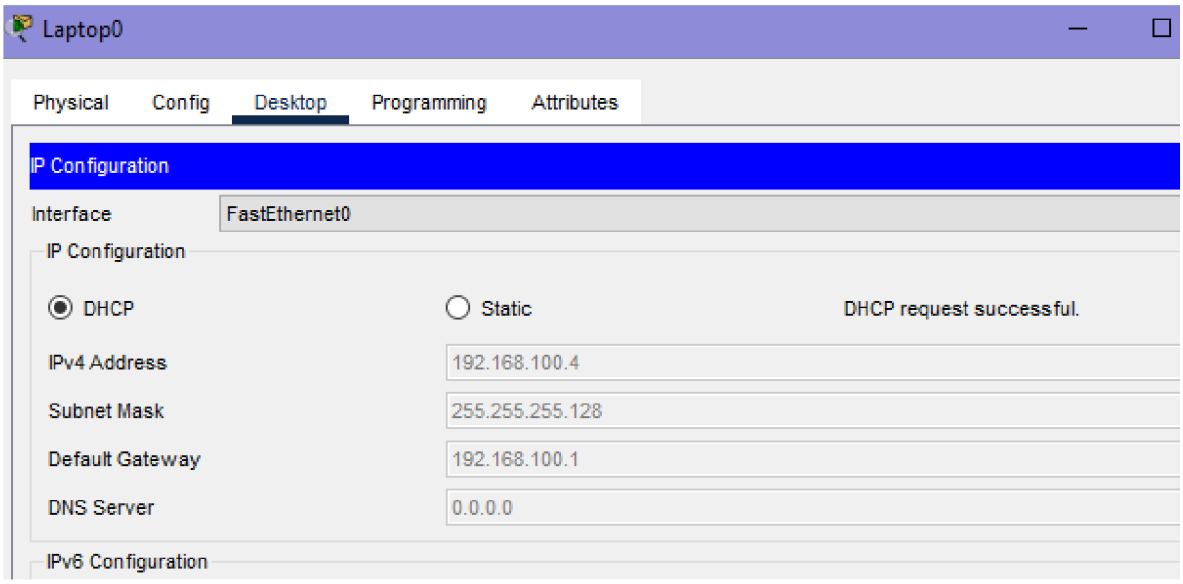
```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/1.100
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.100, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.100, changed state to up

Router(config-subif)#encapsulation dot1q 100
Router(config-subif)#ip address 192.168.100.1 255.255.255.128
Router(config-subif)#int gig0/1.101
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.101, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.101, changed state to up

Router(config-subif)#encapsulation dot1q 101
Router(config-subif)#ip address 192.168.101.1 255.255.255.192
Router(config-subif)#int gig0/1.102
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.102, changed state to up
```

Obrázek 29- Router- Konfigurace subrozhraní 1

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.102, changed state to up

Router(config-subif)#encapsulation dot1q 102
Router(config-subif)#ip address 192.168.102.1 255.255.255.224
Router(config-subif)#int gig0/1.103
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.103, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.103, changed state to up

Router(config-subif)#encapsulation dot1q 103
Router(config-subif)#ip address 192.168.103.1 255.255.255.192
Router(config-subif)#int gig0/1.104
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.104, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.104, changed state to up
encapsulation dot1q 104
Router(config-subif)#encapsulation dot1q 104
Router(config-subif)#ip address 192.168.104.1 255.255.255.192
Router(config-subif)#int gig0/1.105
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.105, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.105, changed state to up

Router(config-subif)#encapsulation dot1q 105
Router(config-subif)#ip address 192.168.105.1 255.255.255.224
```

Obrázek 30- Router- Konfigurace subrozhraní 2

Po připojení všech zařízení k síti je u každého prvku v síti povolena funkce DHCP. Každé zařízení pošle žádost o svou IP adresu na router a ten jim adresu přidělí z dříve nastavených IP poolů. Na obrázku číslo třicet jedna lze vidět, že DHCP žádost byla úspěšná a zařízení, v tomto případě notebook, dostalo svou IP adresu. Rozhraní notebooku je přiřazeno k vlan 100 a proto zařízení dostalo adresu 192.168.100.4.



Obrázek 31- DHCP žádost

Pro lepší zabezpečení sítě jsou nastavena ACL pravidla. Tato pravidla spravují přístup do sítě a v síti. Nastavení nejdůležitějších pravidel lze vidět na obrázku číslo třicet dva a třicet tři. Pro vlan 101 se nastaví ACL pomocí příkazu *access-list 101* a vypíší se veškeré zakázané a povolené adresy nebo adresy subnetů. Pro ostatní vlan se postup opakuje. Na obrázku číslo třicet tři lze vidět nastavení ACL pro vlan 102, kde je zakázána komunikace s vlan 101-105, pro vlan 100 je udělaná výjimka pro jeden počítač na který kamey přesouvají svůj záznam, další komunikace na tuto vlan je zakázána. Například další výjimka je udělána pro senzory, které mohou odesílat notifikace pouze na určitý chytrý telefon, ostatní komunikace je zakázána. Jednotlivé ACL jsou přiřazeny na určitá rozhraní pomocí příkazu *ip access-group <číslo-ACL> in.*

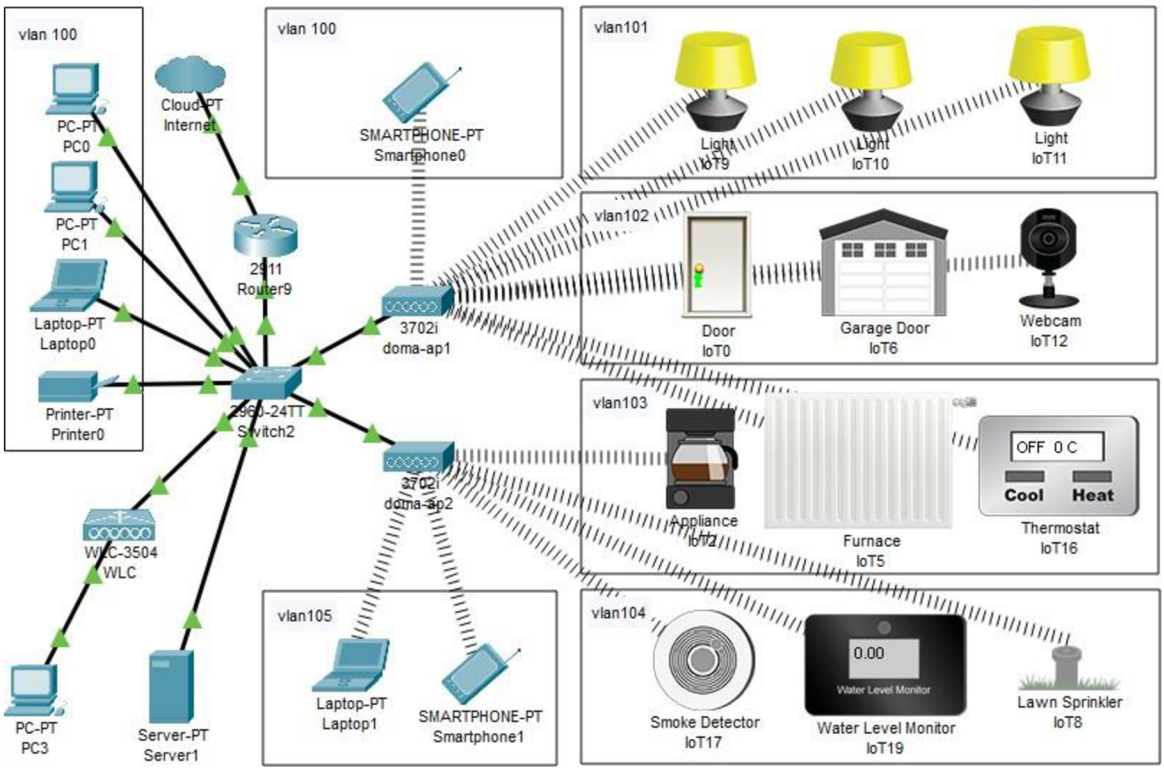
```
Router(config)#
Router(config)#access-list 101 deny ip 192.168.101.0 0.0.0.63 192.168.100.0 0.0.0.127
Router(config)#access-list 101 deny ip 192.168.101.0 0.0.0.63 192.168.102.0 0.0.0.31
Router(config)#access-list 101 deny ip 192.168.101.0 0.0.0.63 192.168.103.0 0.0.0.63
Router(config)#access-list 101 deny ip 192.168.101.0 0.0.0.63 192.168.104.0 0.0.0.63
Router(config)#access-list 101 deny ip 192.168.101.0 0.0.0.63 192.168.105.0 0.0.0.31
Router(config)#int g0/1.101
Router(config-subif)#ip access-group 101 in
Router(config-subif)#exit
Router(config)#access-list 102 deny ip 192.168.102.0 0.0.0.31 192.168.105.0 0.0.0.31
Router(config)#access-list 102 deny ip 192.168.102.0 0.0.0.31 192.168.101.0 0.0.0.63
Router(config)#access-list 102 deny ip 192.168.102.0 0.0.0.31 192.168.103.0 0.0.0.63
Router(config)#access-list 102 deny ip 192.168.102.0 0.0.0.31 192.168.104.0 0.0.0.63
Router(config)#access-list 102 permit ip 192.168.102.0 0.0.0.31 host 192.168.100.3
Router(config)#access-list 102 deny ip 192.168.102.0 0.0.0.31 192.168.100.0 0.0.0.63
Router(config)#access-list 102 permit ip any any
Router(config)#int g0/1.102
Router(config-subif)#ip access-group 102 in
Router(config-subif)#
```

Obrázek 32- ACL pravidla 1

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 103 deny ip 192.168.103.0 0.0.0.63 192.168.105.0 0.0.0.31
Router(config)#access-list 103 deny ip 192.168.103.0 0.0.0.63 192.168.104.0 0.0.0.63
Router(config)#access-list 103 deny ip 192.168.103.0 0.0.0.63 192.168.102.0 0.0.0.31
Router(config)#access-list 103 deny ip 192.168.103.0 0.0.0.63 192.168.101.0 0.0.0.63
Router(config)#access-list 103 permit ip any any
Router(config)#int g0/1.103
Router(config-subif)#ip access-group 103 in
Router(config-subif)#exit
Router(config)#access-list 104 deny ip 192.168.104.0 0.0.0.63 192.168.101.0 0.0.0.63
Router(config)#access-list 104 deny ip 192.168.104.0 0.0.0.63 192.168.102.0 0.0.0.31
Router(config)#access-list 104 deny ip 192.168.104.0 0.0.0.63 192.168.103.0 0.0.0.63
Router(config)#access-list 104 deny ip 192.168.104.0 0.0.0.63 192.168.105.0 0.0.0.31
Router(config)#access-list 104 permit ip 192.168.104.0 0.0.0.63 host 192.168.100.7
Router(config)#access-list 104 deny ip 192.168.104.0 0.0.0.63 192.168.100.0 0.0.0.127
Router(config)#access-list 104 permit ip any any
Router(config)#int g0/1.104
Router(config-subif)#ip access-group 104 in
Router(config-subif)#exit
Router(config)#access-list 105 deny ip 192.168.105.0 0.0.0.31 192.168.101.0 0.0.0.63
Router(config)#access-list 105 deny ip 192.168.105.0 0.0.0.31 192.168.102.0 0.0.0.31
Router(config)#access-list 105 deny ip 192.168.105.0 0.0.0.31 192.168.103.0 0.0.0.63
Router(config)#access-list 105 deny ip 192.168.105.0 0.0.0.31 192.168.104.0 0.0.0.63
Router(config)#access-list 105 deny ip 192.168.105.0 0.0.0.31 192.168.100.0 0.0.0.127
Router(config)#access-list 105 permit ip any any
Router(config)#int g0/1.105
Router(config-subif)#ip access-group 105 in
Router(config-subif)#exit
Router(config)#
```

Obrázek 33- ACL pravidla 2

4.4 Finální topologie chytré domácí sítě



Obrázek 34- Finální topologie chytré domácí sítě

4.5 Ověření konektivity a zabezpečení chytré domácí sítě

Poslední část vlastní práce spočívá v ověření konektivity, konfigurace prvků a správy přístupů. Konektivita je ověřena v softwaru packet tracer pomocí tlačítka add simple PDU (protocol data unit), která ověřuje, zda zařízení spolu komunikují a mají k sobě cestu. Na obrázku číslo třicet pět je ukázán výstup ověřování, zda zařízení z každé vlan sítě může komunikovat s routerem, tudíž svou GW. Před nasazení ACL pravidel je ověřena konektivita všech prvků v síti, to znamená, zda každý prvek sítě může komunikovat s každým zařízením v síti. Také je ověřena komunikace prvků uvnitř každé vlan sítě.

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	Successful	PC0	Router9	ICMP		0.000	N
	Successful	IoT9	Router9	ICMP		0.000	N
	Successful	IoT0	Router9	ICMP		0.000	N
	Successful	IoT2	Router9	ICMP		0.000	N
	Successful	IoT17	Router9	ICMP		0.000	N
	Successful	Smartph...	Router9	ICMP		0.000	N
	Successful	Smartph...	Router9	ICMP		0.000	N

Obrázek 35- Ověření konektivity- router

Pravidla ACL jsou ověřena stejnou funkcí packet traceru jako konektivita v síti. Jsou ověřeny komunikace, které mají být zakázané a které mají být povolené. Obrázek číslo třicet šest ukazuje část testování. Lze vidět, že zařízení IoT9, které patří do vlan 101 selhalo v komunikaci na osobní počítač, tedy do vlan 100. Zařízení IoT0, které patří do vlan 102, úspěšně komunikovalo s osobním počítačem, který byl v pravidlech povolen. Dále lze vidět, že to samé zařízení selhalo v komunikaci s druhým osobním počítačem ze stejné sítě jako PC0. Stejným příkladem je zařízení IoT17, které patří do vlan 104 a má povoleno komunikovat pouze s určitým chytrým telefonem a do zbytku sítě komunikovat nemůže. Takto se postupně ověřila veškerá pravidla access listu. Omezený přístup zajišťuje, že pokud je síť napadena, tak se útočník nedostane do celé sítě a síť je tak stále funkční.

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	Failed	IoT9	PC0	ICMP		0.000	N
	Failed	IoT11	PC1	ICMP		0.000	N
	Failed	IoT10	Printer0	ICMP		0.000	N
	Successful	IoT0	PC0	ICMP		0.000	N
	Failed	IoT0	PC1	ICMP		0.000	N
	Successful	IoT17	Smartphone0	ICMP		0.000	N
	Failed	IoT17	PC0	ICMP		0.000	N
	Failed	IoT9	IoT0	ICMP		0.000	N
	Failed	IoT9	IoT2	ICMP		0.000	N
	Failed	IoT2	IoT17	ICMP		0.000	N

Obrázek 36- Ověření ACL pravidel

5 Závěr

Tato diplomová práce se zabývá problematikou zabezpečení sítě pro chytrou domácnost. V teoretické části byl vysvětlen pojem internet věcí (IoT), popsán jeho vznik a historie. Následně byl predikován jeho další vývoj. Byly uvedeny možné příklady využití internetu věcí se zaměřením na chytré domácnosti. Byly vysvětleny technologie přenášení dat v IoT, a to bezdrátové i drátové. Tyto technologie byly popsány a byly uvedeny jejich výhody a nevýhody. Uvedeny byly příklady nejčastěji používaných protokolů pro přenos dat, jako například LoRaWAN, Z-wave, Wi-fi či Bluetooth. Byly vypsány možné komponenty chytré domácnosti, jejich funkce a účel. V práci byla rozebrána bezpečnost IoT a také popsána technologie blockchain, pomocí které lze zvýšit bezpečnost chytrých zařízení.

Téma této diplomové práce je úzce spojeno s problematikou počítačových sítí. Problematika počítačových sítí byla vysvětlena a popsána v druhé části teoretických východisek. Byl vysvětlen pojem počítačových sítí a jejich fungování. Popsán byl také referenční model ISO/OSI a byly vysvětleny funkce jednotlivých vrstev v modelu. Síťový model TCP/IP byl definován spolu s protokoly, které fungují na jeho vrstvách. Tato práce také vysvětlila princip ip adresace, pojem podsítí a techniku subnettingu, kterou lze rozdělit síť na menší, lépe spravovatelné celky. V neposlední řade bylo rozebráno samotné zabezpečení počítačových sítí. Popsány byly typy síťových útoků a hrozeb. Následně byly rozebrány metody, postupy a nástroje, kterými lze počítačovou síť chránit před těmito hrozbami. Jednou z metod bylo zabezpečení síťových prvků a proto byly vypsány základní příkazy pro konfiguraci těchto zařízení. V závěru teoretické části byl popsán software Packet Tracer, ve kterém byl testován výsledný návrh zabezpečení chytré domácí sítě.

V praktické části diplomové práce bylo řešeno samotné zabezpečení chytré domácí sítě s využitím konfigurace síťových prvků a subnettingu. Návrh rozdělení sítě byl vyobrazen pomocí blokového schématu a byl zobrazen proces vytvoření podsítí pomocí subnettingu. Konfigurace síťových prvků, spolu s užitými příkazy, byla popsána a zároveň vysvětlena funkce použitých příkazů. Výsledný návrh byl nasimulován v softwaru Packet Tracer. Ověřena byla konektivita síťových prvků, jejich zabezpečení, konfigurace a také funkčnost celé sítě.

Hlavním cílem této diplomové práce bylo navrhnout a vytvořit účinná bezpečnostní opatření pro chytrou domácí síť, která výrazně sníží rizika a dopady napadení. Tohoto cíle

bylo dosaženo rozdělením sítě do menších, samostatně spravovatelných podsítí. Tyto podsítě byly vytvořeny jako virtuální podsítě a nepotřebovaly tedy dodatečný hardware k jejich oddělení. Každé této virtuální síti byly přiřazeny přístupová pravidla, tím se docílilo kontroly nad jednotlivými přístupy do všech sítí. Pokud zařízení z jedné virtuální sítě bylo napadeno, tato pravidla zařídila, že nelze napadnout zařízení z dalších virtuálních sítí. V pravidlech pro přístup byly nastaveny výjimky pro určitá zařízení, která mohou být kontaktována z jiných virtuálních sítí. Například chytrý detektor kouře může poslat notifikaci o nebezpečí požáru na určený chytrý telefon, ale na jiný prvek z této sítě komunikace selže, je zablokována. Pomocí příkazů na omezení počtu přijímaných packetů za sekundu bylo zamezeno útokům typu IP a DHCP spoofing či DHCP starvation.

Vedlejším cílem této diplomové práce bylo ověřit konektivitu a zabezpečení této konfigurace. V softwaru packet tracer byl vytvořen simulační model, kterým se ověřila konektivita mezi prvky a také přiřazená pravidla přístupu pro jednotlivé virtuální sítě.

Přínosem této diplomové práce je poskytnutí návrhu řešení zabezpečení chytré domácnosti s využitím podsítí, správy přístupu do jednotlivých bloků a konfigurace síťových prvků.

6 Seznam použitých zdrojů

1. CHEW, Daniel. *The Wireless Internet of Things: A Guide to the Lower Layers.* 2018. Spojené Státy Americké: Standards Information Network. ISBN: 978-1119260578
2. KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5. aktualizované vydání. Brno: Computer Press, 2012. ISBN 978-80-251-2236-5.
3. 10 IoT Security Challenges and Solutions for your Cybersecurity Team!. *Sectrio* [online]. 2022 [cit. 2023-03-10]. Dostupné z: https://sectrio.com/top-10-iot-security-challenges-and-solutions/
4. 5 Big IoT Security Challenges (And How To Overcome Them). *Crn* [online]. 2021 [cit. 2023-01-10]. Dostupné z: https://www.crn.com/slide-shows/internet-of-things/5-big-iot-security-challenges-and-how-to-overcome-them-?itc=refresh
5. How does IoT work with blockchain?. *Ibm* [online]. 2021 [cit. 2023-01-11]. Dostupné z: https://www.ibm.com/topics/blockchain-iot
6. Benefits and Challenges of Blockchain in IoT. *Originstamp* [online]. 2023 [cit. 2023-01-11]. Dostupné z: https://originstamp.com/blog/benefits-and-challenges-of-blockchain-in-iot/
7. The OSI Reference Model Explained. *Learncisco* [online]. [cit. 2023-01-12]. Dostupné z: https://www.learncisco.net/courses/ccna/part-1-internetworking/the-osi-reference-model.html
8. COMER, Douglas. *Internetworking with TCP/IP Volume One* [online]. 6. vydání. New Jersey: Pearson, 2013 [cit. 2023-01-12]. ISBN 978-0-13-608530-0.
9. TCP/IP Model. *Ipcisco* [online]. 2020 [cit. 2023-01-12]. Dostupné z: https://ipcisco.com/lesson/tcp-ip-model/
10. Configure IP Addresses and Unique Subnets for New Users. *Cisco* [online]. 13.02.2023 [cit. 2023-02-18]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html
11. All Enterprise Networks Products. *Cisco* [online]. [cit. 2023-02-13]. Dostupné z: https://www.cisco.com/c/en/us/solutions/enterprise-networks/product-listing.html

12. CHOUDARY, Archana. What is Network Security: An introduction to Network Security. *Edureka* [online]. [cit. 2023-03-03]. Dostupné z: https://www.edureka.co/blog/what-is-network-security/
13. Network Security: What Is It, Why Does It Matter and What Can You Do to Make Networks More Secure?. *Comptia* [online]. [cit. 2023-03-03]. Dostupné z: https://www.comptia.org/content/guides/network-security-basics-definition-threats-and-solutions
14. STALLINGS, William. *Network Security Essentials: Applications and Standards*. 6th Edition. New Jersey: Pearson, 2016. ISBN 978-0134527338.
15. Network Infrastructure Security Guide. *Defense.gov* [online]. June 2022 [cit. 2023-03-14]. Dostupné z: https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF
16. ABHISHEKG25. Cisco Switch Configuration basic commands. *Geeksforgeeks* [online]. 2020 [cit. 2023-03-04]. Dostupné z: https://www.geeksforgeeks.org/cisco-switch-configuration-basic-commands/
17. Using the Command-Line Interface. *Cisco* [online]. [cit. 2023-03-04]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/b_consolidated_3850_3se_cg_chapter_01.html
18. What is Cisco Packet Tracer. *Geeksforgeeks* [online]. 2020 [cit. 2023-03-05]. Dostupné z: https://www.geeksforgeeks.org/what-is-cisco-packet-tracer/
19. The Rise of IoT: The History of the Internet of Things. *Simoniot* [online]. 20.11.2020. [cit. 2023-03-04]. Dostupné z: https://www.simoniot.com/history-of-iot/
20. Internet of Things (IoT) History. Postscapes. [online]. [cit. 2023-03-04]. Dostupné z: https://www.postscapes.com/iot-history/
21. FOOTE, D. Keith**.** A Brief History of the Internet of Things. *Dataversity* [online]. 16.08.2016. [cit. 2023-03-04]. Dostupné z https://www.dataversity.net/brief-history-internet-things/#
22. LUETH, Knud Lasse. Why the Internet of Things is called Internet of Things: Definition, history, disambiguation. *Iot-analytics* [online]. 19.12.2014. [cit. 2023-03-04]. Dostupné z: https://iot-analytics.com/internet-of-things-definition/

23. NEWMAN, Daniel. The 4 Stages of IoT Architecture. *forbes* [online]. 31.07.2020. [cit. 2023-03-04]. Dostupné z: https://www.forbes.com/sites/danielnewman/2020/11/25/5-iot-trends-to-watch-in-2021/?sh=1e6fc499201b
24. MENDOZA, N.F. The future of IoT: 5 major predictions for 2021. *techrepublic* [online]. 28.08.2020. [cit. 2023-02-04]. Dostupné z: https://www.techrepublic.com/article/the-future-of-iot-5-major-predictions-for-2021/
25. TAMSONS, Asa. My IoT predictions for 2021: Smarter tech will make better business. *ericsson* [online]. 15.01.2020. [cit. 2023-02-04]. Dostupné z: https://www.ericsson.com/en/blog/2021/1/iot-predictions-2021
26. STOKES, Paul. *4* Stages of IoT architecture explained in simple words. *datadriveninvestor* [online]. 05.12.2018. [cit. 2023-02-04]. Dostupné z: https://medium.datadriveninvestor.com/4-stages-of-iot-architecture-explained-in-simple-words-b2ea8b4f777f
27. JAHNKE, Alec. 5 IoT Trends To Watch In 2021. *digi* [online]. 25.11.2020. [cit. 2023-02-04]. Dostupné z: https://www.digi.com/blog/post/the-4-stages-of-iot-architecture
28. The 9 most important applications of the Internet of Things (IoT). *fracttal* [online]. [cit. 2023-02-04]. Dostupné z: https://www.fracttal.com/en/blog/the-9-most-important-applications-of-the-internet-of-things
29. 10 Real World Applications of Internet of Things (IoT) – Explained in Videos. *analyticsvidhya.* [online]. 26.08.2016. [cit. 2023-02-04]. Dostupné z: https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/
30. AUDIN, Gary. Managing Wired IoT Devices in a Wireless World. *nojitter* [online]. 06.03.2020. [cit. 2023-02-04]. Dostupné z: https://www.nojitter.com/internet-things/managing-wired-iot-devices-wireless-world
31. The Truth About IoT Implementations - Wireless vs. Wired. *Senseware* [online]. [cit. 2023-02-04]. Dostupné z: https://blog.senseware.co/2017/10/10/iot-implementations-wireless-vs-wired

32. BENZL, Lukáš. Optické připojení k internetu pod lupou. *rychlost* [online]. 07.01.2020. [cit. 2023-02-04]. Dostupné z: https://rychlost.cz/clanek/2018-06-opticke-pripojeni-k-internetu-pod-lupou/
33. 6 Leading Types of IoT Wireless Tech and Their Best Use Cases. *behrtech* [online]. [cit. 2023-02-04]. Dostupné z: https://behrtech.com/blog/6-leading-types-of-iot-wireless-tech-and-their-best-use-cases/
34. RAY, Brian. Four types of IoT wireless networks. *iotacommunications* [online]. 24.03.2020. [cit. 2023-02-04]. Dostupné z: https://www.iotacommunications.com/blog/types-of-iot-networks/
35. Z-Wave. *Z-Wave.* [online]. [cit. 2023-02-04]. Dostupné z: https://www.z-wave.com/learn
36. VANDOME, Nick. *Smart Homes in easy steps: Master smart technology for your home.* 2018. Spojené Státy Americké: In Easy Steps Limited. ISBN: 978-1840788259
37. Zigbee. *csa-iot* [online]. [cit. 2023-02-04]. Dostupné z: https://csa-iot.org/all-solutions/zigbee/
38. CHOU, Timothy. *Precision: Principles, Practices and Solutions for the Internet of Things.* 2020. Spojené Státy Americké: lulu.com. ISBN: 978-1329843561
39. Wi-Fi HaLow™: Wi-Fi® for IoT applications (2020). *wi-fi.* [online]. [cit. 2023-02-04]. Dostupné z: https://www.wi-fi.org/downloads-registered-guest/Wi-Fi_HaLow_White_Paper_20200518_0.pdf/36881
40. Learn about Bluetooth. *Bluetooth* [online]. [cit. 2023-02-04]. Dostupné z: https://www.bluetooth.com/learn-about-bluetooth/radio-versions/
41. *Iot-analytics.* [online]. 2020 [cit. 2023-03-20]. Dostupné z: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/
42. *Thinkprotection* [online]. [cit. 2023-03-20]. Dostupné z: https://thinkprotection.com/shop/equipment/added-services/z-wave-technology/
43. *Geekdad* [online]. 2015 [cit. 2023-03-20]. Dostupné z: https://geekdad.com/2015/08/critical-flaw/
44. *Transistor-man* [online]. [cit. 2023-03-20]. Dostupné z: https://transistor-man.com/long_wifi_adventures.html

45. *Microcontrollertips* [online]. 2022 [cit. 2023-03-20]. Dostupné z: https://www.microcontrollertips.com/wi-fi-by-the-numbers-faq/
46. *Randomnerdtutorials* [online]. 2019 [cit. 2023-03-20]. Dostupné z: https://randomnerdtutorials.com/esp32-bluetooth-low-energy-ble-arduino-ide/

7 Seznam obrázků, tabulek a zkratek

7.1 Seznam obrázků

7.2 Seznam tabulek

7.3 Seznam použitých zkratek

DHCP - Dynamic Host Configuration Protocol)

DNS – systém doménových jmen

EIGRP - Enhanced Interior Gateway Routing Protocol

IEEE - Institut pro elektrotechnické a elektronické inženýrství (Institute of Electrical and Electronics Engineers)

IoT- internet věcí (Internet of Things)

ISO/OSI- International Organization for Standardization/Open Systems Interconnection

LAN – lokální počítačová síť

LED - elektroluminiscenční dioda (Light-Emitting Diode)

OSPF - Open Shortest Path First

TCP/IP- Transmission Control Protocol/Internet Protocol

VLAN – virtuální lokální síť

WAN - rozlehlá síť spojující LAN a MAN sítě

WLAN- bezdrátová lokální síť