Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Návrh domácí počítačové sítě

Štěpán Unger

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Štěpán Unger

Informatika

Název práce

Návrh domácí počítačové sítě

Název anglicky

Design of a Home Computer Network

Cíle práce

Hlavním cílem práce je navržení efektivní a bezpečné počítačové sítě pro domácnost.

Dílčí cíle:
Provedení analýzy a průzkumu současného trhu technologií pro využití v domácích sítích.
Návrh a výběr optimální síťové topologie pro domácnost
Specifikace a výběr vhodných zařízení pro domácí síť
Konfigurace základních síťových služeb
Návrh a zabezpečení domácí sítě

Metodika

Teoretická část práce je zaměřena na studium a analýzu odborných a vědeckých zdrojů. Obsahuje přehled nejpoužívanějších technologií a nástrojů v domácích počítačových sítích.

Praktická část je zaměřena na návrh a konfiguraci síťových prvků pro domácí síť. Zahrnuje výběr zařízení, jejich konfiguraci, vzájemnou integraci a nastavení síťových služeb. Součástí je také implementace bezpečnostních opatření a ověření funkčnosti navržené sítě v modelových podmínkách.

Doporučený rozsah práce

40 – 50 stran

Klíčová slova

počítačové sítě, zabezpečení, síťová topologie, síťové prvky, konfigurace sítě, domácí síť

Doporučené zdroje informací

HUAWEI Technologies Co., Ltd. Data Communications and Network Technologies. c2022. ISBN 978-981-19302-9-4

Karygiannis, T. T., & Owens, L. Wireless Network Security: 802.11, Bluetooth and Handheld Devices (NIST Special Publication 800-48). National Institute of Standards and Technology. 2002.

Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8. edition). Pearson.

MCMILLAN, Troy a EBRARY, INC. *Cisco networking essentials : e-book.* Indianapolis, Ind.: John Wiley & Sons, Inc., 2012. ISBN 978-1-118-09759-5.

ODOM, Wendell. CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press, 2019. ISBN-13: 978-1-58714-713-5.

Předběžný termín obhajoby

2025/26 LS – PEF

Vedoucí práce

doc. Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 19. 06. 2025

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 25. 06. 2025

prof. Ing. Lukáš Čechura, Ph.D.

Děkan

V Praze dne 03. 03. 2026

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Návrh domácí počítačové sítě" jsem vypracoval samostatně pod vedením vedoucího bakalářské 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 autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14.3.2026 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu mé bakalářské práce, panu doc. Ing. Jiřímu Vaňkovi, Ph.D. za odborné vedení, cenné rady a věcné připomínky, které mi poskytl v průběhu zpracování této práce. Dále bych chtěl vyjádřit upřímné poděkování své mamince za její neutuchající podporu, trpělivost a zázemí, které mi po celou dobu studia i během psaní této práce poskytovala.

Návrh domácí počítačové sítě

Abstrakt

Bakalářská práce se zaměřuje na návrh a zabezpečení počítačové sítě v domácím prostředí. V teoretické části práce představuje a popisuje klíčové pojmy a parametry související s moderními domácími sítěmi, včetně síťových standardů, topologií a aktuálních bezpečnostních hrozeb. V praktické části práce je vytvořen konkrétní návrh síťové infrastruktury, který zahrnuje výběr vhodných hardwarových prvků a jejich následnou konfiguraci. Pozornost je také věnována implementaci bezpečnostních opatření, jako je nastavení firewallu a zabezpečení bezdrátového přenosu. Navržené řešení je v závěru podrobeno testování, které ověřuje funkčnost a stabilitu sítě v modelových podmínkách s cílem zajistit bezpečné digitální prostředí pro koncového uživatele.

Klíčová slova: počítačové sítě, zabezpečení, síťová topologie, síťové prvky, konfigurace sítě, domácí síť

Design of a home computer network

Abstract

The bachelor's thesis focuses on the design and security of a computer network in a home environment. In the theoretical part of the thesis, it presents and describes key concepts and parameters related to modern home networks, including network standards, topologies and current security threats. In the practical part of the thesis, a specific design of the network infrastructure is created, which includes the selection of suitable hardware elements and their subsequent configuration. Attention is also paid to the implementation of security measures, such as firewall settings and wireless transmission security. The proposed solution is finally subjected to testing, which verifies the functionality and stability of the network in model conditions in order to ensure a safe digital environment for the end user.

Keywords: computer networks, security, network topology, network elements, network configuration, home network

Obsah

1 Úvod 11

2 Cíl práce a metodika 13

2.1 Cíl práce 13

2.2 Metodika 13

3 Teoretická východiska 14

3.1 Počítačová síť 14

3.1.1 Typy počítačových sítí podle rozsahu 14

3.1.2 Typy počítačových sítí podle topologie 15

3.2 Referenční model ISO/OSI 17

3.2.1 Aplikační vrstva 17

3.2.2 Prezentační vrstva 18

3.2.3 Relační vrstva 18

3.2.4 Transportní vrstva 18

3.2.5 Síťová vrstva 19

3.2.6 Spojová vrstva 19

3.2.7 Fyzická vrstva 19

3.3 TCP/IP 19

3.3.1 Aplikační vrstva 20

3.3.2 Transportní vrstva 20

3.3.3 Síťová vrstva 21

3.3.4 Vrstva síťového rozhraní 21

3.4 Ethernet 21

3.4.1 Koaxiální kabel 22

3.4.2 Kroucená dvojlinka 22

3.4.3 Optické vlákno 22

3.5 Wi-Fi 23

3.5.1 Wi-Fi standardy 23

3.5.2 Frekvence 23

3.5.3 Zabezpečení Wi-Fi 24

3.6 Zařízení v počítačové síti 24

3.6.1 Směrovač (Router) 25

3.6.2 Přepínač (Switch) 25

3.6.3 Modem 25

3.6.4 Zesilovač (Repeater) 25

3.6.5 Rozbočovač (Hub) 25

3.7 Základní funkce v počítačových sítích 26

3.7.1 IP Adresa 26

3.7.2 MAC Adresa ... 26
3.7.3 DHCP ... 27
3.7.4 DNS ... 27
3.7.5 Firewall ... 27
3.7.6 NAT ... 28
3.8 Zabezpečení sítí z pohledu uživatele ... 28
3.8.1 Antivirus ... 28
3.8.2 Aktualizace ... 29
3.9 Standardní domácí síť ... 29
3.10 Shrnutí ... 30

4 Vlastní práce ... 31
4.1 Modelový scénář a požadavky ... 31
4.1.1 Specifikace internetového připojení ... 31
4.1.2 ISP Modem ... 31
4.1.3 Prostředí a topologie sítě ... 31
4.2 Průzkum trhu ... 32
4.2.1 Specifikace MikroTik hAP ax² ... 33
4.3 Konfigurace zařízení ... 33
4.3.1 Připojení k routeru a prvotní nastavení ... 34
4.3.2 Vytvoření uživatele a nastavení hesla. ... 34
4.3.3 Nastavení identity routeru ... 34
4.3.4 Nastavení WAN rozhraní (DHCP Client) ... 35
4.3.5 Aktualizace systému RouterOS ... 35
4.3.6 Nastavení domácí Wi-Fi ... 35
4.3.7 Nastavení sítě pro hosty ... 36
4.3.8 Nastavení síťového mostu ... 37
4.3.9 Nastavení LAN DHCP ... 38
4.3.10 Konfigurace DHCP pro síť hostů ... 38
4.3.11 Nastavení firewall pravidel ... 39
4.3.12 Vypnutí nepotřebných služeb ... 40
4.3.13 Konfigurace modemu ... 41

5 Výsledky a diskuse ... 42
5.1 Bezpečnostní limity a minimalizace rizik ... 42
5.2 Konfigurovatelnost a nezávislost na poskytovateli ... 42
5.3 Náročnost a proveditelnost implementace ... 43
5.4 Měření rychlosti a latence ... 43
5.4.1 Metodika měření ... 43
5.4.2 Výsledky měření ... 44
5.4.3 Zhodnocení měření ... 44

6 Závěr **46**

7 Seznam použitých zdrojů **48**

Seznam obrázků a tabulek **50**

7.1 Seznam obrázků 50

7.2 Seznam tabulek 50

1 Úvod

V dnešní době, kdy se naše životy neoddělitelně proplétají s digitálním světem, se počítačové sítě staly naprosto nepostradatelnou součástí téměř každé domácnosti. Ať už jde o prosté prohlížení webu, plynulé streamování filmů a seriálů, intenzivní hraní online videoher, nebo o komplexní systémy chytré domácnosti. Téměř každé zařízení v našem domě dnes využívá přístup k internetu prostřednictvím lokální sítě. Toto propojení nám sice usnadňuje život, ale zároveň otevírá dveře potenciálním hrozbám. Pokud síť není dostatečně zabezpečená, vystavujeme se riziku nejrůznějších nástrah a útoků z internetu.

Mnoho uživatelů při pořízení nového internetového připojení postupuje velmi podobně: dostanou zařízení od svého poskytovatele internetu, zapojí ho do elektrické sítě a datové přípojky, nastaví si heslo na Wi-Fi a začnou ho používat. Pro nenáročné uživatele, kteří internet využívají jen základním způsobem, se tento postup může jevit jako dostatečný. Je však důležité si uvědomit, že takové nastavení obvykle spoléhá na velmi jednoduché zabezpečení poskytnuté internetovým poskytovatelem. Toto základní zabezpečení nemusí být dostatečné pro ochranu před sofistikovanějšími kybernetickými hrozbami a často neumožňuje plně využít potenciál moderních domácích sítí.

Z těchto důvodů se doporučuje jít nad rámec základního nastavení od poskytovatele. Zařízení od providera je často nejlepší chápat jen jako "bránu" mezi domácí sítí a internetem. Pro skutečně efektivní a bezpečnou domácí síť je výhodné investovat do vlastního síťového zařízení. Takové řešení nabízí mnohem širší škálu možností, jak důkladně zabezpečit domácí síť proti nejrůznějším útokům, optimalizovat její výkon a přizpůsobit ji přesně uživatelským potřebám. Zároveň poskytuje plnou kontrolu nad zařízením, což umožňuje detailnější analýzu provozu a pokročilou správu při využívání domácí sítě.

Důležitým aspektem při výběru správného zařízení pro domácí síť jsou především očekávání a potřeby uživatele. Správný výběr je klíčový, jelikož zvolené zařízení musí být dostatečně výkonné na správu a obstarání veškerého síťového provozu. Při rozhodování je nejdůležitější zohlednit několik faktorů: především poměr ceny a výkonu, dostupné funkce, uživatelskou přívětivost při nastavení a každodenním používání, jaké typy připojení zařízení poskytuje, frekvenci aktualizací a průběžného zabezpečení vydávaných výrobcem a samozřejmě také celkovou pořizovací cenu.

Aby však bylo možné plně využít výhod vybraného zařízení, je nezbytné věnovat se i podrobnému nastavení zabezpečení uvnitř zařízení. Bezpečnost by měla být vždy na prvním místě. Základním pravidlem pro její dosažení je: zakázat vše, co není nezbytně nutné pro správné fungování, a povolit pouze to, co je skutečně potřeba. Tímto způsobem minimalizujeme bezpečnostní rizika a získáme maximální ochranu proti případným útokům.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je navržení efektivní a bezpečné počítačové sítě pro domácnost. Dílčími cíli je provedení analýzy a průzkumu současného trhu technologií pro využití v domácích sítích, návrh a výběr optimální síťové topologie pro domácnost. Dalšími cíli je Specifikace a výběr vhodných zařízení pro domácí síť, konfigurace základních síťových služeb, návrh a zabezpečení domácí sítě.

2.2 Metodika

Teoretická část práce je zaměřena na studium a analýzu odborných a vědeckých zdrojů. Obsahuje přehled nejpoužívanějších technologií a nástrojů v domácích počítačových sítích.

Praktická část je zaměřena na návrh a konfiguraci síťových prvků pro domácí síť. Zahrnuje výběr zařízení, jejich konfiguraci, vzájemnou integraci a nastavení síťových služeb. Součástí je také implementace bezpečnostních opatření a ověření funkčnosti navržené sítě v modelových podmínkách.

3 Teoretická východiska

Oblast počítačových sítí se vyznačuje rozsáhlou sadou pojmů a technologií, z nichž každá plní specifickou funkci v rámci síťové architektury. Pro efektivní návrh a správu domácí sítě je nezbytná orientace v této terminologii a porozumění principům, na nichž jednotlivé technologie fungují. Tato kapitola se proto zaměří na klíčové koncepty a funkce relevantní pro běžné domácí sítě, detailněji popíše jejich charakteristiky a praktické využití. Cílem je poskytnout teoretický základ nezbytný pro pochopení následného návrhu a zabezpečení domácí počítačové sítě.

3.1 Počítačová síť

Počítačová síť je systém vzájemně propojených elektronických zařízení a systémů, které mají schopnost efektivní komunikace a výměny dat a sdílení zdrojů prostřednictvím společného přenosového média. Jejím primárním účelem je zajištění interkonektivity mezi jednotlivými síťovými uzly pro výměnu informací, spolupráci a sdílení centralizovaných i distribuovaných zdrojů.

3.1.1 Typy počítačových sítí podle rozsahu

Počítačové sítě lze klasifikovat na základě jejich geografického rozsahu, topologie a typu propojení což ovlivňuje jejich charakteristiky, účel a technologie:

- **Privátní síť (PAN)** – Privátní sítě (Personal Area Network) jsou nejmenší typy sítí, které se používají výhradně pro osobní účely. Nejčastěji jde o propojení jednoho uživatele s jeho zařízeními. Mezi příklady PAN sítě patří připojení pomocí Bluetooth nebo infračerveného záření.[1] Příkladem PAN sítě může být propojení mobilního telefonu s bezdrátovými sluchátky pomocí Bluetooth technologie.
- **Lokální síť (LAN)** – Lokální síť (Local Area Network) je typ počítačové sítě, která slouží k propojení zařízení v malé geografické oblasti, jako je například domácnost nebo kancelář. Sítě LAN se obvykle skládají z uživatelských zařízení, tiskáren, síťových úložišť nebo chytrých zařízení. Tato zařízení bývají propojena pomocí kabelů nebo bezdrátovou technologií Wi-Fi. LAN je klasickým příkladem domácí sítě. Hlavním cílem této sítě je umožnit zařízení komunikovat mezi sebou v rámci jedné sítě.
- **Bezdrátová lokální síť (WLAN)** – Bezdrátová lokální síť (Wireless Local Area Network) je typ sítě podobný tradiční LAN, avšak s tím rozdílem, že místo kabelového

propojení využívá bezdrátovou technologii pro připojení zařízení k síti. Pro tento účel se nejčastěji používá technologie Wi-Fi.

- **Metropolitní síť (MAN)** – Metropolitní síť (Metropolitan Area Network) je počítačová síť, která pokrývá rozsáhlejší geografickou oblast, typicky univerzitní či firemní kampus, obec nebo město. Jejím účelem je propojení více lokálních sítí (LAN) v rámci dané metropolitní oblasti. Infrastruktura MAN často využívá vysokorychlostní páteřní optické sítě a slouží k poskytování sdílených služeb nebo k propojení poboček organizací. Internetoví poskytovatelé často provozují MAN sítě pro distribuci internetového připojení v rámci města, přičemž tyto MAN jsou následně propojeny do rozsáhlejších WAN sítí.
- **Rozlehlá síť (WAN)** – Rozlehlá síť (Wide Area Network) je typ počítačové sítě, která propojuje geograficky velmi vzdálené lokality, kterými jsou města, státy nebo kontinenty. Na rozdíl od LAN a MAN využívá WAN často externí telekomunikační infrastrukturu a veřejné přenosové linky. Nejznámějším a nejrozsáhlejším příkladem WAN je internet, který představuje globální propojení milionů menších sítí. Kromě internetu existují i privátní WAN sítě, které spojují pobočky velkých korporací napříč kontinenty.

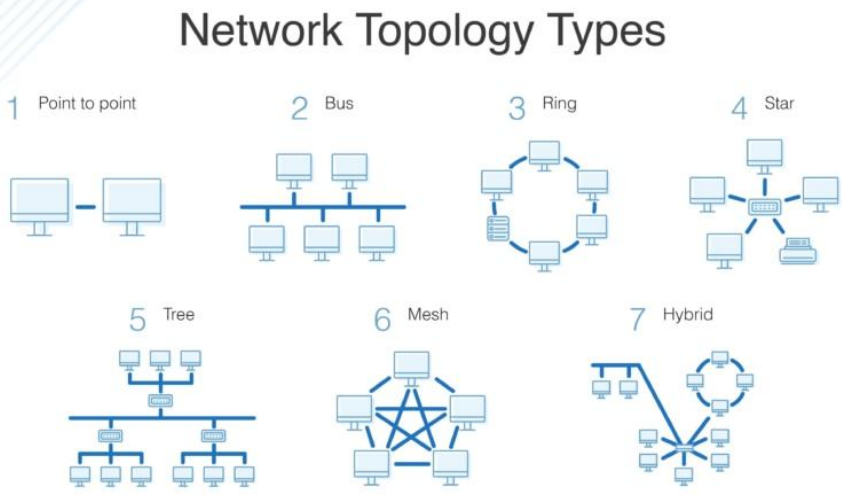
3.1.2 Typy počítačových sítí podle topologie

Počítačové sítě lze klasifikovat také na základě jejich topologie, která definuje fyzické nebo logické uspořádání síťových prvků a způsob jejich vzájemného propojení. Volba konkrétní síťové topologie má zásadní dopad na spolehlivost, výkon, škálovatelnost a celkovou komplexnost implementace sítě.[2]

- **Sběrnicová topologie (Bus)** – Jedná se o nejstarší a nejjednodušší typ síťové topologie, kde jsou všechna zařízení připojena k jednomu společnému přenosovému médiu (sběrnici). Data se šíří po sběrnici oběma směry a jsou přijímána pouze cílovým zařízením.[2]
- **Kruhová topologie (Ring)** – V kruhové topologii jsou zařízení propojena do uzavřeného kruhu, přičemž každé zařízení je připojeno ke dvěma sousedním. Data putují po kruhu jedním směrem a každé zařízení data přijímá, zpracuje (pokud je cílem) a předá dál k dalšímu zařízení.[2]
- **Hvězdicová topologie (Star)** – Hvězdicová topologie je v současnosti nejčastěji využívaným typem zapojení, zejména v lokálních a domácích sítích. Všechna

uživatelská zařízení jsou připojena k jednomu centrálnímu síťovému prvku, kterým je typicky směrovač (router) nebo přepínač (switch).[2]

- **Stromová topologie (Tree)** – Stromová topologie je hierarchická struktura, která vychází z kombinace hvězdicové a sběrnicové topologie. Skládá se z několika hvězdicových sítí, které jsou propojeny sběrnicovým způsobem prostřednictvím centrálních přepínačů nebo směrovačů. Vytváří tak rozvětvenou strukturu připomínající strom.[2]
- **Smíšená topologie (Mesh)** – V této topologii je každé zařízení v síti propojeno s každým dalším zařízením. Tento typ topologie vytváří mnoho redundantních cest pro data.[2]
- **Hybridní topologie (Hybrid)** – Hybridní topologie je nejčastěji se vyskytující typ topologie v reálných, komplexních sítích. Jedná se o kombinaci dvou nebo více základních topologií, které jsou navrženy tak, aby splňovaly specifické požadavky na výkon, spolehlivost a efektivitu. Příkladem je propojení několika hvězdicových sítí sběrnicovou architekturou, nebo kombinace hvězdicové a bezdrátové topologie.[2]



Obrázek 1: Topologie sítí. Zdroj: dnsstuff.com [3]

3.2 Referenční model ISO/OSI

Konceptuální model standardizace funkce komunikačního systému v počítačových sítích byl vyvinut mezinárodní organizací ISO (International Organization for Standardization) a poprvé publikován v roce 1984. Tento model je strukturován do sedmi logických vrstev, z nichž každá plní specifickou úlohu v rámci komunikace mezi zařízeními. Hlavním cílem modelu je sjednocení komunikace mezi zařízeními od různých výrobců, a to prostřednictvím definování jasných pravidel a zásad. Vrstvy mezi sebou vzájemně komunikují jak vertikálně, tak horizontálně. Je však zásadní, že jednotlivé vrstvy na stejné úrovni mohou komunikovat mezi sebou, ale není přípustné, aby komunikovaly vrstvy nacházející se na různých úrovních. [4]

Obrázek 2: ISO/OSI model. Zdroj: [Vlastní Zpracování]

3.2.1 Aplikační vrstva

Aplikační vrstva je nejvyšší vrstvou referenčního modelu ISO/OSI. Jejím primárním účelem je poskytovat síťové služby přímo uživatelským aplikacím, čímž slouží jako rozhraní mezi softwarem uživatele a síťovou infrastrukturou. Nezahrnuje samotné aplikace, ale spíše

definuje protokoly a standardy, které aplikace využívají pro síťovou komunikaci. Mezi klíčové protokoly pracující na této vrstvě patří HTTP/HTTPS pro webové prohlížení, FTP pro přenos souborů, SMTP/POP3/IMAP pro elektronickou poštu, DNS pro překlad doménových jmen na IP adresy, SSH pro zabezpečený vzdálený přístup a další. [4]

3.2.2 Prezentační vrstva

Prezentační vrstva modelu OSI má za cíl standardizovat a převádět data do podoby, kterou konkrétní aplikace potřebují zpracovat. Funguje jako "překladatel" dat aby různé systémy mohly data správně interpretovat. Na této vrstvě se data připravují pro přenos mezi systémy při odesílání (např. komprese, šifrování) nebo se dekódují a dekomprimují, pokud byly přijaty. Jejím úkolem je řešit datové formáty, kódování znaků a kompresi/dekompresi, aby aplikační vrstva mohla pracovat s univerzálně srozumitelnými daty. [4]

3.2.3 Relační vrstva

Relační vrstva má za úkol navazovat, spravovat a ukončovat komunikační relace mezi aplikacemi na různých zařízeních. Zajišťuje řízení dialogu, což znamená, že spravuje, která ze zúčastněných stran má v daném okamžiku právo vysílat data. Dále zjišťuje dostupnost přenosu, například zda je možné použít full-duplex (současný obousměrný přenos), half-duplex (střídavý obousměrný přenos) nebo simplex (jednosměrný přenos). Také zajišťuje synchronizaci datových toků a možnost obnovení spojení při případném přerušení. Zodpovídá také za řádné ukončení již nepotřebných spojení. [4]

3.2.4 Transportní vrstva

Transportní vrstva je zodpovědná za spolehlivý přenos dat a za zajištění kvality doručení mezi aplikacemi na zdrojovém a cílovém zařízení. Primárním úkolem této vrstvy je segmentace dat, tedy rozdělení dat z vyšších vrstev na menší segmenty pro efektivní přenos, a jejich následné sestavení na cílové straně. Zajišťuje také řízení toku dat, aby nedocházelo k přetížení přijímajícího zařízení, a provádí detekci a opravu chyb, včetně opakovaného přenosu ztracených segmentů. Tato vrstva nabízí dva základní klíčové protokoly. Transmission Control Protocol (TCP) zajišťuje spolehlivý přenos dat s kontrolou chyb a doručení. User Datagram Protocol (UDP) poskytuje rychlejší, ale nespolehlivý přenos bez navazování spojení a kontroly doručení dat. [4]

3.2.5 Síťová vrstva

Hlavním cílem síťové vrstvy je logické adresování a směrování datových paketů po síti k cílovému zařízení, bez ohledu na to, zda se zařízení nachází ve stejné lokální síti nebo v jiné vzdálené síti. Je zodpovědná za nalezení optimální cesty pro datové pakety od zdroje k cíli napříč sítěmi. Na této vrstvě se pracuje s Internetovým Protokolem (IP), který definuje logické adresy (IP adresy) pro jednoznačnou identifikaci zařízení. Nejčastěji na této vrstvě pracují směrovače (routery), jejichž primární funkcí je přeposílat datové pakety mezi různými síťovými segmenty do rozlehlé sítě Internetu (WAN). [4]

3.2.6 Spojová vrstva

Spojová vrstva (často také linková vrstva) má za úkol zajistit spolehlivé spojení mezi dvěma přímo připojenými zařízeními v rámci stejného síťového segmentu. Základní formou datové jednotky na této vrstvě je rámec (frame). Tato vrstva zajišťuje rámcování (rozdělení bitového proudu na logické rámce), řízení přístupu k přenosovému médiu a také detekci chyb v rámcích a jejich případné opravy či opakované vysílání. K identifikaci zařízení na této vrstvě se používají MAC (Media Access Control) adresy, které jsou jedinečné pro každou síťovou kartu. Na této vrstvě pracují síťové komponenty jako přepínače (switche), které inteligentně přeposílají rámce mezi zařízeními v lokální síti na základě cílových MAC adres. [4]

3.2.7 Fyzická vrstva

Fyzická vrstva je nejnižší vrstva v rámci referenčního modelu ISO/OSI. Je zodpovědná za fyzické spojení mezi dvěma zařízeními a za přenos jednotlivých bitů po fyzickém přenosovém médiu. Tato vrstva pracuje s bity, kdy je uspořádává do bitového proudu (bit stream) a vysílá je ve formě elektrických impulzů po metalickém kabelu, pomocí světelných impulzů v optickém kabelu, nebo jako rádiové vlny v bezdrátových sítích. Definice této vrstvy zahrnuje specifikace pro typy kabelů, konektory, napětí, datové rychlosti, frekvence a fyzické topologie sítě. Na této vrstvě pracují síťové komponenty jako opakovače (repeatery), které zesilují signál, a rozbočovače (huby), které jednoduše kopírují příchozí signál na všechny ostatní porty. [4]

3.3 TCP/IP

Referenční model TCP/IP (Transmission Control Protocol/Internet Protocol) je soubor komunikačních protokolů, které tvoří základní stavební kameny pro fungování internetu a většiny moderních počítačových sítí. Na rozdíl od referenčního modelu ISO/OSI, který slouží

primárně jako teoretický rámec, je model TCP/IP reálně implementovaným a široce využívaným standardem. Jeho vývoj začal v 70. letech 20. století v rámci projektu ARPANET a oficiální plné nasazení s přepnutím ARPANETu na protokoly TCP/IP proběhlo 1. ledna 1983.[5]

Obrázek 3: TCP/IP Model. Zdroj: [Vlastní Zpracování]

3.3.1 Aplikační vrstva

Nejvyšší vrstva modelu představuje kombinaci aplikační, prezentační a relační vrstvy modelu OSI. Obsahuje protokoly, které poskytují síťové služby přímo uživatelským aplikacím a umožňují komunikaci mezi nimi. Příkladem jsou protokoly jako HTTP/HTTPS, FTP, SMTP, DNS a SSH. [5]

3.3.2 Transportní vrstva

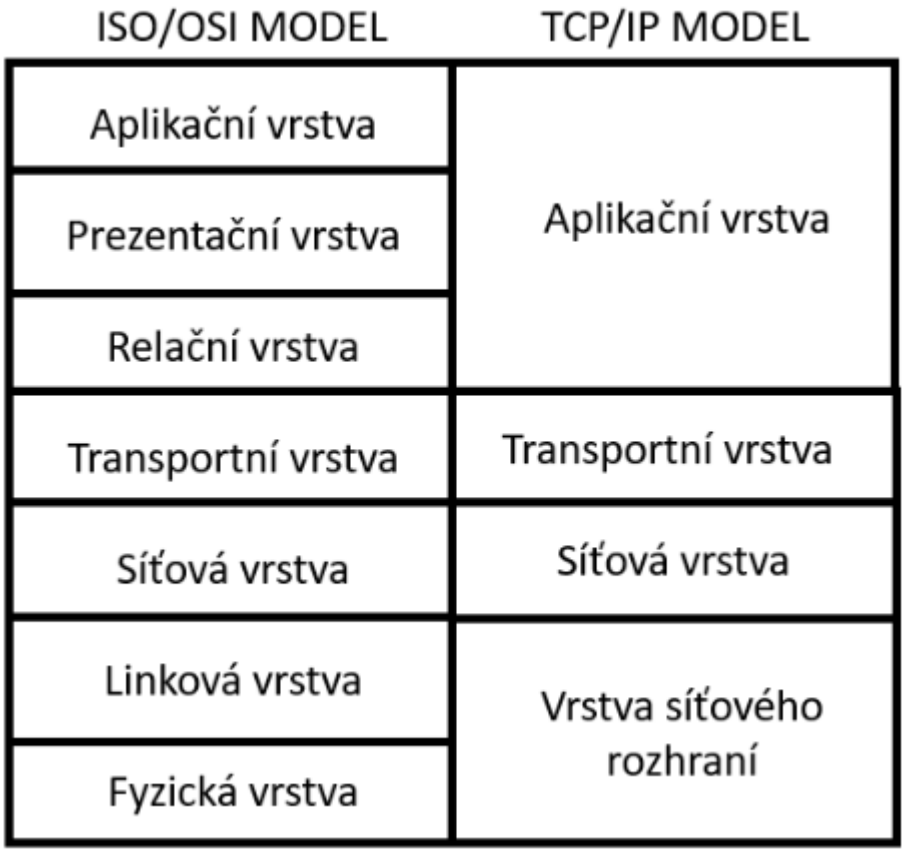
Vrstva je velmi podobná transportní vrstvě modelu OSI. Zajišťuje spolehlivý (TCP) nebo nespolehlivý (UDP) přenos dat mezi aplikacemi. Stará se o segmentaci dat, řízení toku a kontrolu chyb. Transmission Control Protocol (TCP) poskytuje spolehlivý přenos s kontrolou doručení, zatímco User Datagram Protocol (UDP) nabízí rychlý přenos bez potvrzení o doručení dat. [5]

3.3.3 Síťová vrstva

Tato vrstva je ekvivalentem síťové vrstvy v modelu OSI. Jejím hlavním úkolem je logické adresování a směrování datových paketů (IP datagramů) mezi různými sítěmi, aby dorazily z odesílajícího zařízení na správné cílové zařízení. Klíčovým protokolem této vrstvy je Internet Protocol (IP), který definuje IP adresy a je základem pro směrování. [5]

3.3.4 Vrstva síťového rozhraní

Tato vrstva sdružuje funkce fyzické a linkové (spojové) vrstvy z modelu OSI. Je zodpovědná za veškeré aspekty fyzického přenosu dat po síťovém médiu a za správu přístupu k tomuto médiu, včetně hardwarových specifikací a ovladačů. Zde pracují standardy jako Ethernet a Wi-Fi. [5]



Obrázek 4: ISO/OSI a TCP/IP model. Zdroj: [Vlastní Zpracování]

3.4 Ethernet

Ethernet je síťová technologie, která definuje jak hardwarové specifikace fyzického zařízení, tak i pravidla a protokoly pro přenos dat v síti. Je založena na sadě standardů definovaných IEEE (Institute of Electrical and Electronics Engineers) pod označením IEEE

802.3. Ethernet se vyskytuje nejběžněji v LAN sítí, kde slouží k propojení zařízení pomocí fyzických kabelů. [6]

3.4.1 Koaxiální kabel

Koaxiální kabel je typ elektrického kabelu, který se skládá z centrálního vodiče obklopeného izolací, stíněním a vnějším pláštěm. Tato konstrukce je optimalizována pro minimalizaci elektromagnetického rušení. Koaxiální kabely byly původně široce využívány pro přenos televizního a telefonního signálu a také pro anténní systémy. V oblasti počítačových sítí se historicky uplatnily v raných Ethernetových sítích. V současné době se v domácnostech používají především pro připojení kabelové televize a pro poskytování internetového připojení prostřednictvím kabelových modemů. V novějších zástavbách jsou však koaxiální kabely stále častěji nahrazovány optickými vlákny. [7]

3.4.2 Kroucená dvojlinka

Kroucená dvojlinka je v současnosti nejrozšířenější typ kabelu pro Ethernetové sítě. Skládá se z několika párů izolovaných vodičů, které jsou vzájemně zkrouceny, což výrazně snižuje elektromagnetické rušení. Rozlišujeme nestíněnou variantu UTP (Unshielded Twisted Pair), která je nejběžnější pro domácí použití, a stíněnou variantu STP (Shielded Twisted Pair), poskytující lepší ochranu proti rušení. Kabely se dělí do kategorií, které určují jejich maximální přenosovou rychlost a frekvenci, přičemž se připojují pomocí konektorů RJ-45. Kroucená dvojlinka je v domácích sítích preferovaným médiem pro kabelové propojení díky své cenové dostupnosti, snadné instalaci a schopnosti dosahovat vysokých rychlostí, jako je Gigabit Ethernet. [8]

3.4.3 Optické vlákno

Optické vlákno je moderní přenosové médium, které pro přenos dat využívá světelné impulsy namísto elektrických signálů. Skládá se z velmi tenkých skleněných nebo plastových vláken. Hlavními výhodami optických vláken jsou extrémně vysoká přenosová rychlost, imunita vůči elektromagnetickému rušení a schopnost přenášet data na velké vzdálenosti. I přes vyšší cenu a složitější instalaci se optické vlákno stává standardem pro přívod vysokorychlostního internetu do domácností kde nahrazuje starší technologie. [8]

3.5 Wi-Fi

Wi-Fi (Wireless-Fidelity) je bezdrátová technologie která umožňuje zařízením komunikovat a sdílet data bez potřeby fyzických kabelů. Je založena na sadě standardů IEEE 802.11, které definují specifikace pro bezdrátovou komunikaci v pásmech rádiových frekvencí, nejčastěji 2,4 GHz a 5 GHz, a nově i 6 GHz. [10]

3.5.1 Wi-Fi standardy

Vývoj standardů Wi-Fi neustále zvyšuje dostupné přenosové rychlosti a zlepšuje efektivitu komunikace. Mezi důležité verze patří IEEE 802.11n (Wi-Fi 4), které zavedlo technologii MIMO, a IEEE 802.11ac (Wi-Fi 5), optimalizované pro pásmo 5 GHz a nabízející gigabitové rychlosti. IEEE 802.11ax (Wi-Fi 6/6E), je zaměřená na zlepšení výkonu v hustě obsazených prostředích a pro velký počet připojených zařízení. Nejnovější standard IEEE 802.11be (Wi-Fi 7), oficiálně vydaný v roce 2024, přináší revoluční novinku MLO (Multi-Link Operation), která umožňuje zařízením používat více frekvencí současně, čímž výrazně zvyšuje výkon a propustnost sítě. Plánovaný standard Wi-Fi 8 (802.11bn) má teoretický rok vydání 2028. [10]

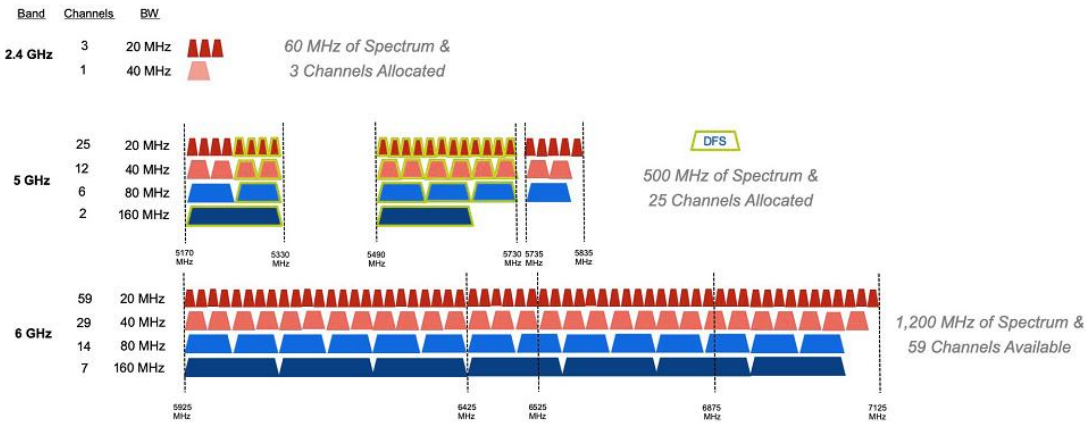
Označení	Standard	Rok vydání	Frekvence (v GHz)
Wi-Fi 0	802.11	1997	2.4
Wi-Fi 1	802.11b	1999	2.4
Wi-Fi 2	802.11a	1999	5
Wi-Fi 3	802.11g	2003	2.4
Wi-Fi 4	802.11n	2009	2.4, 5
Wi-Fi 5	802.11ac	2013	5
Wi-Fi 6	802.11ax	2019	2.4, 5
Wi-Fi 7	802.11be	2024	2.4, 5, 6
Wi-Fi 8	802.11bn	(2028)	2.4, 5, 6

Tabulka 1: Wi-Fi standardy. [9]

3.5.2 Frekvence

Frekvence jsou klíčovým faktorem pro fungování Wi-Fi. Určují, jak jsou rádiové vlny využívány pro přenos dat. Wi-Fi funguje na třech hlavních frekvenčních pásmech: 2,4 GHz, 5 GHz a 6 GHz. Každé z těchto pásem má vyhrazené kanály, které se používají pro přenos dat. Pásmo 2,4 GHz nabízí větší dosah signálu, ale má omezenější kapacitu a může být náchylné

k rušení, jelikož je sdíleno s jinými zařízeními, jako jsou mikrovlnné trouby nebo Bluetooth. V tomto pásmu jsou k dispozici pouze 3 kanály, které se mohou překrývat, což zvyšuje riziko interferencí. Pásmo 5 GHz poskytuje vyšší rychlost přenosu dat a je méně náchylné k interferencím, ale má kratší dosah. Tato frekvence má více než 20 kanálů, což umožňuje lepší rozdělení přenosového spektra a menší riziko rušení. Nejnovější pásmo 6 GHz, využívané Wi-Fi 6E a Wi-Fi 7, nabízí ještě větší šířku pásma a nižší latenci, což zajišťuje lepší rychlost přenosu dat a také poskytuje nové kanály, které jsou méně přeplněné. Výběr frekvence závisí na uživatelských potřebách a okolí. Pro delší dosah je lepší 2,4 GHz, pro rychlost a stabilitu v blízkosti routeru je ideální 5 GHz nebo 6 GHz. [10]



Obrázek 5: Frekvenční kanály. [10]

3.5.3 Zabezpečení Wi-Fi

Zabezpečení Wi-Fi je klíčové pro ochranu bezdrátové sítě před neoprávněným přístupem a krádeží dat. Dříve používaný protokol WEP (Wired Equivalent Privacy) byl nahrazen bezpečnějšími metodami, kterými jsou WPA (Wi-Fi Protected Access) a WPA2, jež využívají silné šifrování AES (Advanced Encryption Standard). Nejrozšířenějším současným standardem je WPA2. Nejnovějším standardem, představeným v roce 2018, je WPA3. Ten nabízí pokročilejší ochranu díky protokolu SAE (Simultaneous Authentication of Equals) pro silnější ověřování a vylepšenému šifrování, které zvyšuje odolnost vůči moderním typům útoků a zajišťuje lepší soukromí i v otevřených Wi-Fi sítích. [11]

3.6 Zařízení v počítačové síti

Počítačová síť je vždy tvořena spojením fyzického hardwaru. Tato zařízení umožňují komunikaci mezi počítači a přístup k internetu, čímž zajišťují plynulý chod veškerého síťového provozu. Bez těchto základních komponent by fungování počítačové sítě nebylo možné. [12]

3.6.1 Směrovač (Router)

Směrovač je klíčové síťové zařízení, které primárně operuje na síťové vrstvě modelu OSI. Jeho hlavní funkcí je propojování různých počítačových sítí a efektivní směrování datových paketů mezi nimi. Při přijetí paketu router analyzuje jeho cílovou IP adresu a na základě svých směrovacích tabulek určí optimální cestu, kudy má paket pokračovat. V domácích sítích router představuje hlavní bod, který propojuje lokální síť s internetem (přesněji se sítí internetového poskytovatele). Často navíc také poskytuje funkcionalitu bezdrátového přístupového bodu pro vysílání Wi-Fi signálu. [12]

3.6.2 Přepínač (Switch)

Přepínač je síťové zařízení operující na linkové vrstvě modelu OSI. Jeho hlavním úkolem je propojování více zařízení v rámci jedné lokální sítě. Přepínač data rozesílá inteligentně, a to pomocí identifikace MAC adres připojených zařízení. Během provozu si přepínač postupně učí MAC adresy zařízení připojených k jeho portům a ukládá si je do své CAM (Content Addressable Memory) tabulky. Při přijetí datového rámce zkontroluje jeho cílovou MAC adresu a pošle rámec pouze na konkrétní port, ke kterému je dané cílové zařízení připojeno, čímž zvyšuje efektivitu sítě. [12]

3.6.3 Modem

Modem (zkratka pro modulátor-demodulátor) je síťové zařízení, které slouží k převodu digitálních signálů z počítače nebo lokální sítě na analogové signály pro přenos po různých typech přenosových médií (např. koaxiální kabely, telefonní linky) a naopak. Jeho hlavní úlohou je zajistit konektivitu mezi lokální sítí a sítí poskytovatele internetových služeb pro domácnosti s analogovým vstupem. [12]

3.6.4 Zesilovač (Repeater)

Zesilovač je síťové zařízení, které pracuje na fyzické vrstvě modelu OSI. Jeho úkolem je rozšířit dosah signálu do lokací, kam by se primární signál již nedostal. Toho dosahuje tak, že přijme původní signál, zesílí ho a opětovně vyšle dál do sítě. Zesilovače jsou běžné například v bezdrátových Wi-Fi sítích, kde pomáhají překonat překážky a rozšířit pokrytí. [12]

3.6.5 Rozbočovač (Hub)

Rozbočovač je jednoduché síťové zařízení operující na fyzické vrstvě modelu OSI. Jeho úkolem je propojení více zařízení v rámci lokální sítě. Na rozdíl od přepínačů se nejedná

o inteligentní zařízení. Data, která hub přijme na jednom ze svých portů, odešle na všechny ostatní připojené porty, bez ohledu na cílové zařízení. Tento princip sdílené sběrnice snižuje efektivitu sítě a je náchylný ke kolizím, proto byly rozbočovače v moderních sítích nahrazeny přepínači. [12]

3.7 Základní funkce v počítačových sítích

Každá počítačová síť pro své správné fungování obsahuje sadu základních protokolů a funkcí, které zajišťují její efektivní běh. Tyto protokoly a funkce se starají o to, jak se data v síti přenášejí, adresují a zabezpečují. Bez těchto klíčových mechanismů by spolehlivá a bezpečná komunikace mezi zařízeními v síti nebyla možná.

3.7.1 IP Adresa

IP (Internet Protocol) adresa je unikátní číselný identifikátor každého zařízení připojeného k počítačové síti, které používá internetový protokol pro komunikaci v dané síti. Jejím účelem je identifikovat zařízení pro správné směrování datových paketů v síti. V současnosti se používají dva hlavní standardy internetového protokolu:

- IPv4 - Starší, avšak stále dominantní protokol v počítačových sítích. Jedná se o 32bitovou adresu skládající se ze čtyř oktetů (číslic oddělených tečkami). Celkový počet adres je 2^{32}, což činí přibližně 4,3 miliardy adres. Tento počet je v dnešní době již nedostačující, což vedlo k zavedení mechanismů jako je NAT (Network Address Translation). Pro lokální (privátní) sítě jsou organizací IANA (Internet Assigned Numbers Authority) rezervovány tři adresní rozsahy: 192.168.0.0/16, 172.16.0.0/12 a 10.0.0.0/8. [13]
- IPv6 - Novější verze protokolu, navržená k řešení nedostatku IPv4 adres. Jedná se o 128bitovou adresaci, zapisovanou v šestnáctkovém (hexadecimálním) formátu, rozdělených do osmi segmentů obsahujících čtyři hexadecimální znaky. Celkový počet adres je 2^{128}, což představuje prakticky nevyčerpatelný zdroj adres. IPv6 poskytuje také další vylepšení pro efektivnější směrování a bezpečnost. Pro lokální (privátní) sítě je rezervován adresní rozsah fd00::/8. [13]

3.7.2 MAC Adresa

MAC (Media Access Control) adresa je unikátní fyzický identifikátor přiřazený každému síťovému rozhraní (například síťové kartě). Operuje na spojové vrstvě (vrstva 2) modelu OSI. Na rozdíl od logických IP adres je MAC adresa obvykle neměnná a vypálená přímo do

hardwaru síťového adaptéru výrobcem. Jde o 48bitové číslo, které je nejčastěji zapisováno v šestnáctkovém (hexadecimálním) formátu, rozdělené do šesti dvojic oddělených pomlčkami nebo dvojtečkami. První polovina adresy (první tři dvojice) identifikuje výrobce zařízení (OUI – Organizationally Unique Identifier), zatímco druhá polovina je unikátní pro konkrétní zařízení od daného výrobce. [14]

3.7.3 DHCP

DHCP (Dynamic Host Configuration Protocol) je síťový protokol určený pro automatickou distribuci síťové konfigurace zařízením připojeným k síti. Jeho hlavní funkcí je dynamické přidělování IP adres, ale také automaticky poskytuje další klíčové parametry, jako je maska podsítě, adresa výchozí brány a adresy DNS serverů. Díky DHCP je výrazně zjednodušena a automatizována správa sítě pro administrátory, jelikož odstraňuje nutnost manuálního nastavení síťových parametrů pro každé zařízení. To vede ke snížení chyb a efektivnějšímu fungování sítě, což je obzvláště výhodné v dynamických prostředích, kde se zařízení často připojují a odpojují. [15]

3.7.4 DNS

DNS (Domain Name System) má za hlavní cíl překládat lidsky čitelná doménová jména na strojově čitelné IP adresy. Díky tomu výrazně usnadňuje práci s internetem, protože uživatelé si pamatují názvy namísto složitých číselných adres. DNS systém je často nazýván také „telefonní seznam internetu“. DNS servery udržují distribuované databáze, ve kterých jsou uloženy tyto mapování. Když se uživatel pokusí navštívit webovou stránku, jeho zařízení odešle dotaz na DNS server, který vrátí odpovídající IP adresu. Mezi nejznámější veřejné DNS servery patří ty od Googlu (8.8.8.8, 8.8.4.4) nebo Cloudflare (1.1.1.1), které nabízejí vysokou rychlost a spolehlivost. [16]

3.7.5 Firewall

Firewall je klíčový systém síťové bezpečnosti, který pomáhá chránit síť pomocí souboru definovaných pravidel. Jeho hlavní funkcí je monitorování a řízení příchozího a odchozího síťového provozu. Na základě specifických bezpečnostních pravidel pak firewall rozhoduje, které datové pakety mohou projít a co se s nimi stane. Funguje jako "bariéra" mezi vaší důvěryhodnou sítí (například domácí lokální sítí) a nedůvěryhodnou sítí, jako je internet, čímž chrání před neoprávněným přístupem a kybernetickými hrozbami. [17]

3.7.6 NAT

NAT (Network Address Translation) je metoda, která umožňuje překlad IP adres uvnitř síťových paketů při jejich průchodu směrovacím zařízením. Jejím hlavním účelem je mapování adres jednoho IP adresního prostoru do druhého. To je nejčastěji využíváno k tomu, aby více zařízení v rámci privátní lokální sítě (LAN) mohlo sdílet jednu veřejnou IP adresu pro přístup do internetu. [18]

3.8 Zabezpečení sítí z pohledu uživatele

Zabezpečení počítačové sítě je komplexní proces, který vyžaduje úsilí nejen ze strany správců síťových zařízení, ale také ze strany samotných uživatelů a jejich koncových zařízení. Ačkoliv moderní síťové prvky disponují pokročilými bezpečnostními funkcemi, slabé místo se často nachází na úrovni uživatele nebo jeho počítače. Proto je klíčové, aby si každý uživatel byl vědom rizik a aktivně přispíval k ochraně sítě prostřednictvím správných návyků a používání vhodného softwaru.

3.8.1 Antivirus

Antivirový program představuje základní kámen digitální ochrany každého počítače. Jeho hlavním úkolem je detekce, prevence a odstranění škodlivého softwaru, jako jsou viry, trojské koně, spyware nebo ransomware.

V dnešní době pro uživatele s operačním systémem Windows plně postačuje integrovaný antivirový program Windows Defender, který je předinstalovaný a automaticky monitoruje stažené soubory i běžící procesy na pozadí. Doporučuje se také pravidelně spouštět celkové skenování systému. Kromě systémových řešení existují i různé placené či volně dostupné alternativy. Před instalací jakéhokoli antivirového programu je vhodné provést průzkum trhu a ověřit jeho reputaci.

Uživatelé operačních systémů macOS, iOS a Android mají rovněž k dispozici integrované bezpečnostní mechanismy a základní ochranu, která ve většině případů pro běžné použití postačuje. Počítače s operačním systémem Linux obvykle nebývají primárním cílem masových virových útoků, a proto na nich antivirový program není standardně součástí instalace, i když existují i pro tuto platformu.

3.8.2 Aktualizace

Pravidelné aktualizace systému a softwaru jsou nedílnou součástí komplexního zabezpečení počítače proti hrozbám. Výrobci softwaru a operačních systémů neustále objevují a opravují bezpečnostní zranitelnosti, které by mohly být zneužity útočníky. Tyto opravy jsou distribuovány formou aktualizací a záplat.

Je proto zásadní používat programy, které jsou stále v aktivní podpoře a dostávají pravidelné bezpečnostní aktualizace. Používání zastaralého softwaru, jehož podpora již skončila, vystavuje počítač a celou síť zbytečnému riziku, jelikož nalezené zranitelnosti již nejsou opravovány. Uživatelé by měli mít zapnuté automatické aktualizace a věnovat pozornost upozorněním na dostupné záplaty.

3.9 Standardní domácí síť

Nelze jednoznačně definovat univerzální podobu běžné počítačové sítě, jelikož existuje řada variant a řešení v závislosti na typu internetové přípojky a preferencích uživatele. Nicméně, typická domácí síť je obvykle postavena na hvězdicové topologii, kde centrální uzel, kterým je nejčastěji modem či router, zajišťuje propojení všech připojených zařízení a přístup k internetu.

Primární bod připojení k internetu je zajištěn zařízením, které uživatelům poskytuje poskytovatel internetových služeb (ISP). V případě koaxiálního kabelu je dodáván modem, který slouží jako centrum pro přístup k internetu. U domácností s optickou přípojkou bývá obvykle dodáván převodník signálu, jako je optický síťový terminál (ONT) nebo optická síťová jednotka (ONU), který konvertuje optický signál na signál pro metalické kabely. Pokud se jedná o přímý přívod Ethernetu do domu, pak je obvykle k dispozici rovnou vývod prostřednictvím portu RJ-45.

Většina zařízení dodávaných poskytovatelem internetu pro domácnosti je integrovaná brána, která v sobě kombinuje funkce modemu, směrovače a bezdrátového přístupového bodu Wi-Fi. Tato zařízení slouží jako hlavní centrální bod. Často však nabízejí omezené možnosti pokročilé konfigurace pro uživatele a nemusí vždy disponovat optimálním výkonem. U domácností s vlastním síťovým zařízením je obvykle k modemu připojen uživatelský router,

přičemž modem od poskytovatele funguje v režimu přeposílání dat na uživatelské zařízení, a stará se pouze o zprostředkování datového toku.

3.10 Shrnutí

Optimální počítačová síť v domácím prostředí nespočívá pouze ve vysoké rychlosti připojení k internetu. S rostoucím počtem bezpečnostních hrozeb v digitálním světě se stává zásadním, aby síť představovala ucelený soubor bezpečnostních opatření, vysokou spolehlivost a efektivní výkon. Uživatelé by měli aktivně dbát na zásady kybernetické bezpečnosti, jako je obezřetnost při stahování obsahu a důsledné zabezpečení svých zařízení. V rámci správné konfigurace sítě je klíčové, aby nastavení a zabezpečení bylo provedeno s ohledem na maximální ochranu dat a zajištění stability výkonu, přičemž by nemělo dojít k nepřiměřenému omezení komfortu uživatelů. Bezpečná a efektivní síť je výsledkem komplexního přístupu v dodržování pravidel a implementaci vhodných ochranných mechanismů. Na základě teoretických poznatků a praktických doporučení lze konstatovat, že pro dosažení optimální domácí sítě je nezbytné prostudovat možnosti základního nastavení a zabezpečení a zvážit pořízení vlastního síťového zařízení. Takové zařízení uživateli poskytuje rozšířené možnosti konfigurace a zabezpečení, a zároveň mu umožňuje mít lepší přehled o síťovém provozu a větší kontrolu nad nastavením.

4 Vlastní práce

Kapitola vlastní práce se zaměřuje na technickou specifikaci, výběr vhodných hardwarových prvků a jejich následnou konfiguraci pro vytvoření zabezpečené domácí sítě. Cílem je nahradit standardní řešení dodávané poskytovatelem pokročilejší síťovou architekturou, která umožní efektivní správu provozu a vyšší míru zabezpečení.

4.1 Modelový scénář a požadavky

Tato kapitola definuje výchozí stav a technické požadavky na novou síťovou infrastrukturu. Popisuje parametry internetové přípojky, omezení stávajícího hardwaru poskytovatele a specifika prostředí, která determinují výběr vlastních síťových prvků. Cílem je navrhnout řešení, které eliminuje rušení, zajistí stabilitu pro klíčová zařízení a umožní pokročilou správu provozu včetně oddělené sítě pro hosty.

4.1.1 Specifikace internetového připojení

Konektivita je zajištěna širokopásmovou přípojkou společnosti Vodafone na bázi technologie DOCSIS, využívající koaxiální vedení kabelové televize. Z principu technologie se jedná o sdílené přenosové médium v rámci dané lokality, kde může v době špičky docházet k agregaci provozu a mírnému kolísání dostupné kapacity. Přípojka je v bytové jednotce zakončena standardní účastnickou zásuvkou, do které je připojen modem dodaný poskytovatelem.

4.1.2 ISP Modem

Koncovým zařízením poskytovatele je modem Vodafone Station, model TG3442VF od firmy Arris. V továrním nastavení funguje jako integrovaná brána zahrnující funkce routeru a Wi-Fi vysílání, což je pro účely pokročilé správy sítě nedostačující. Jeho administrativní rozhraní neumožňuje detailní konfiguraci firewallu. Z tohoto důvodu bude modem přepnut do režimu síťového mostu. Tím dojde k deaktivaci směrovacích funkcí, NAT a Wi-Fi na straně modemu. Zařízení bude sloužit pouze jako transparentní převodník, který předává veřejnou IP adresu přímo na WAN rozhraní vlastního routeru, čímž se eliminuje problém dvojitého překladu adres.

4.1.3 Prostředí a topologie sítě

Návrh síťové topologie reflektuje specifika starší bytové jednotky v husté městské zástavbě, která se vyznačuje vysokou mírou rušení od okolních bezdrátových sítí. Pro zajištění

spolehlivého přenosu dat je proto nezbytné nasazení moderního standardu Wi-Fi 6, který dokáže v takto zarušeném prostředí pracovat efektivněji. Z hlediska fyzické topologie jsou dva stolní počítače připojeny ethernetovým kabelem přímo k centrálnímu routeru, zatímco ostatní zařízení budou obsluhována bezdrátově. Součástí návrhu je rovněž vytvoření izolované sítě pro hosty. V síti také není žádná potřeba statických adres.

4.2 Průzkum trhu

Na trhu domácích síťových zařízení dominují značky jako TP-Link, ASUS či Ubiquiti, přičemž každá z nich cílí na odlišný segment uživatelů.

Značka TP-Link je typická svou cenovou dostupností a orientací na běžné spotřebitele, čemuž odpovídá důraz na snadnou instalaci. Ačkoliv jejich zařízení nabízejí solidní hardware za nízkou cenu, firmware je často uzavřený a neposkytuje detailní možnosti konfigurace. U novějších modelů se navíc objevuje trend přesouvat pokročilé bezpečnostní funkce za platební bránu v rámci měsíčního předplatného, což v dlouhodobém horizontu zvyšuje náklady na provoz.

Na opačném pólu stojí řešení od společnosti Ubiquiti, které se řadí do kategorie „prosumer“ (profesionální spotřebitel). Tato zařízení nabízejí vynikající centrální správu a design, avšak jejich pořizovací cena je výrazně vyšší. Pro plnou funkcionalitu navíc často vyžadují běh softwarového kontroléru nebo zakoupení dalšího hardwarového prvku, což pro běžnou domácnost představuje zbytečnou finanční i technickou zátěž.

Specifickou skupinou jsou zařízení značky ASUS, která jsou často marketingově cílena na hráče počítačových her. Tyto routery sice disponují výkonným hardwarem, ale jejich vysoká cena je často navyšována designovými prvky, jako třeba RGB podsvícení, a specifickými herními funkcemi, které pro stabilitu a bezpečnost běžné sítě nemají reálný přínos. Možnosti pokročilé síťové konfigurace zde často ustupují uživatelsky přívětivému, ale omezenému grafickému rozhraní.

Pro potřeby modelového scénáře, který vyžaduje maximální konfigurovatelnost, transparentnost nastavení, nulové skryté poplatky a výborný poměr cena/výkon, bylo proto zvoleno zařízení od společnosti MikroTik. To nabízí funkce podnikové sféry za cenu srovnatelnou s levnějšími domácími routery.

4.2.1 Specifikace MikroTik hAP ax²

Pro realizaci modelového scénáře byl vybrán konkrétní model hAP ax² (kódové označení C52iG-5HaxD2HaxD-TC). Jedná se o moderní přístupový bod, který plně podporuje bezdrátový standard Wi-Fi 6. Zařízení umožňuje souběžný provoz v pásmech 2,4 GHz i 5 GHz, čímž zajišťuje zpětnou kompatibilitu i vysokou rychlost pro nová zařízení. Z hlediska fyzické konektivity disponuje pěti gigabitovými ethernetovými porty s konektory RJ-45, což umožňuje plné využití rychlosti internetové přípojky. Klíčovou vlastností je operační systém RouterOS, na kterém zařízení běží. Tento systém nabízí plně konfigurovatelné prostředí, včetně pokročilého firewallu a správy sítě. [19]

Obrázek 6: hAP ax². Zdroj: MikroTik.com [19]

4.3 Konfigurace zařízení

Tato kapitola představuje praktický postup zprovoznění navržené síťové infrastruktury. Z důvodu zajištění bezpečnosti a minimalizace výpadků služeb je postup realizace zvolen tak, že nejprve proběhne kompletní konfigurace nového routeru v izolovaném prostředí. Teprve po nastavení lokální sítě, zabezpečení bezdrátových rozhraní a aplikaci firewallových pravidel

dojde k úpravě modemu poskytovatele a jeho finálnímu přepnutí do režimu mostu. Tento přístup zaručuje, že v okamžiku připojení k veřejné síti je již vnitřní síť plně chráněna.

4.3.1 Připojení k routeru a prvotní nastavení

Pro zahájení konfigurace je nutné provést fyzické propojení zařízení. Ethernetový kabel z modemu poskytovatele zapojíme do portu 1 (označen jako Internet/PoE in), čímž zajistíme přístup k síti. Počítač, ze kterého bude probíhat správa, připojíme kabelem do libovolného volného LAN portu.

Samotná konfigurace je realizována prostřednictvím aplikace WinBox, což je proprietární nástroj společnosti MikroTik určený pro správu systému RouterOS. Po spuštění aplikace využijeme funkci vyhledání sousedů a k routeru se připojíme prostřednictvím jeho MAC adresy. Tento způsob komunikace probíhá na 2. vrstvě modelu ISO/OSI, což zaručuje stabilní spojení i v případě změn IP adres nebo firewall pravidel během konfigurace.

Po úspěšném přihlášení je nezbytné odstranit přednastavenou konfiguraci od výrobce, která není pro modelový scénář vhodná. V nabídce System → Reset Configuration zvolíme možnost „No Default Configuration“. Tímto krokem je zařízení uvedeno do zcela čistého stavu bez jakýchkoliv pravidel, kterým je výchozí bod pro vlastní zabezpečený návrh.

```
/system/reset-configuration no-defaults=yes
```

4.3.2 Vytvoření uživatele a nastavení hesla.

Po resetu do továrního nastavení je kritickým bezpečnostním krokem správa přístupových údajů. Výchozí účet „admin“ nedisponuje heslem, což představuje značné bezpečnostní riziko. Prvním krokem je proto vytvoření nového administrativního účtu se silným heslem, které by se mělo skládat z kombinace velkých a malých písmen, číslic a speciálních znaků a následná deaktivace původního systémového účtu. V prostředí terminálu nejprve vytvoříme nového uživatele a přiřadíme mu plná práva. Následně zakážeme výchozí účet.

```
/user add group=full name=NewUser
/user set admin disabled=yes
```

4.3.3 Nastavení identity routeru

Pro jednoznačnou identifikaci zařízení v síti je vhodné nastavit unikátní název routeru.

```
/system identity set name=Router
```

4.3.4 Nastavení WAN rozhraní (DHCP Client)

Aby měl router přístup k internetu, který je nutný pro následné aktualizace, je třeba aktivovat službu DHCP klienta na vstupním rozhraní. V sekci IP → DHCP Client vytvoříme novou instanci pro rozhraní ether1. V nastavení ponecháme aktivní volby Use Peer DNS a Use Peer NTP, což zajistí automatické převzetí adres DNS serverů a synchronizaci času ze sítě poskytovatele. V této fázi router obdrží IP adresu od modemu, který zatím funguje ve standardním režimu, což pro stažení aktualizací postačuje.

```
/ip dhcp-client add interface=ether1
```

4.3.5 Aktualizace systému RouterOS

Z bezpečnostních důvodů je kritické, aby zařízení pracovalo s nejnovější verzí operačního systému. Aktualizace opravuje známé bezpečnostní zranitelnosti a optimalizuje výkon systému. Proces se vyvolá v nabídce System → Packages → Check for Updates. Po ověření dostupnosti nové verze zvolíme možnost Download&Install. Router stáhne potřebné balíčky a automaticky se restartuje, čímž je připraven na finální konfiguraci vnitřní sítě.

```
/system/package/update set channel=stable
/system/package/update install
```

4.3.6 Nastavení domácí Wi-Fi

V továrním nastavení disponuje router dvěma fyzickými bezdrátovými rozhraními. Pro lepší orientaci v konfiguraci je vhodné tato rozhraní nejprve přejmenovat podle frekvenčního pásma, ve kterém operují.

```
/interface/wifi set wifi1 name=2.4Ghz
/interface/wifi set wifi2 name=5Ghz
```

Následně přistoupíme ke konfiguraci samotné domácí sítě. Moderním přístupem je nastavení shodného identifikátoru sítě (SSID) pro obě pásma. Koncová zařízení si tak mohou sama vybírat vhodnější frekvenci podle síly signálu a schopností hardwaru.

Pro pásmo 2,4 GHz využijeme standard 802.11ax, který je zpětně kompatibilní se staršími zařízeními. Šířku kanálu nastavíme na 20/40 MHz, což je kompromis mezi rychlostí a odolností proti rušení. Frekvenční rozsah omezíme na standardní evropské kanály (2412–2484 MHz), přičemž router automaticky zvolí nejméně zarušený kanál.

Pro pásmo 5 GHz rovněž využijeme standard 802.11ax (5ghz-ax). Zde můžeme povolit širší kanály (až 80 MHz), což výrazně zvýší přenosovou rychlost.

Klíčovým prvkem je volba šifrování. Použijeme hybridní režim WPA2-PSK + WPA3-PSK. WPA3 poskytuje vyšší bezpečnost, zatímco WPA2 zajistí, že se připojí i starší elektronika. Zásadním krokem je deaktivace funkce WPS (Wi-Fi Protected Setup). Tato technologie, původně zamýšlená pro snadné připojení tlačítkem, obsahuje kritickou zranitelnost v metodě PIN. Útočník může pomocí útoku hrubou silou tento PIN v řádu hodin uhodnout a získat tak přístup do sítě bez znalosti hesla.

```
/interface/wifi add name=HomeNetwork master-interface=2.4Ghz
configuration.ssid=Wi-Fi_Home channel.band=2ghz-ax channel.width=20/40mhz
channel.frequency=2412-2484 security.authentication-types=wpa2-psk,wpa3-psk
security.wps=disable security.passphrase=Password disabled=no

/interface/wifi add name=HomeNetwork5Ghz master-interface=5Ghz
configuration.ssid=Wi-Fi_Home channel.band=5ghz-ax channel.width=20/40mhz
channel.frequency=2300-7300 security.authentication-types=wpa2-psk,wpa3-psk
security.wps=disable security.passphrase=Password disabled=no
```

4.3.7 Nastavení sítě pro hosty

Součástí bezpečnostní politiky je vytvoření izolované sítě pro návštěvy. Tím zajistíme, že cizí zařízení získají přístup k internetu, ale nebudou moci komunikovat s vnitřními zařízeními v domácnosti.

Technicky je toto řešení realizováno vytvořením virtuálního přístupového bodu nad fyzickým rozhraním. Pro síť hostů bylo zvoleno pouze pásmo 2,4 GHz. Důvodem je fakt, že návštěvy zpravidla nevyžadují maximální přenosové rychlosti, ale ocení spíše stabilitu signálu a lepší průchodnost překážkami, kterou toto pásmo nabízí. Pásmo 5 GHz tak zůstane vyhrazeno výhradně pro domácí provoz.

V konfiguraci je opět použito zabezpečení WPA2 a WPA3 a funkce WPS je deaktivována. Důležitým parametrem je zde „datapath.client-isolation=yes“ která zabrání vzájemné komunikaci mezi hosty.

```
/interface/wifi add name=GuestNetwork master-interface=2.4Ghz
configuration.ssid=Wi-Fi_Guests channel.band=2ghz-ax channel.width=20/40mhz
channel.frequency=2440-3000 security.authentication-types=wpa2-psk,wpa3-psk
security.wps=disable datapath.client-isolation=yes security.passphrase=Password
disabled=no
```

4.3.8 Nastavení síťového mostu

Pro zajištění vzájemné komunikace mezi zařízeními připojenými kabelem a bezdrátově je nutné vytvořit softwarový most. Tento prvek spojuje jednotlivá fyzická rozhraní na 2. vrstvě modelu ISO/OSI do jednoho logického segmentu. V praxi to znamená, že se router chová jako virtuální přepínač, což umožňuje transparentní přenos dat mezi počítači na kabelu a telefony na Wi-Fi pro tisk i sdílení souborů v síti.

```
/interface/bridge add name=LanBridge
```

Následně do tohoto mostu přiřadíme všechna rozhraní, která mají být součástí privátní domácí sítě. Jedná se o fyzické porty ether2 až ether5 a bezdrátová rozhraní 2.4GHz a 5GHz. Z bezpečnostních důvodů zde není nastaven WAN port ether1 ani virtuální síť pro hosty, která musí zůstat izolována.

```
/interface/bridge/port add bridge=LanBridge interface=ether2
/interface/bridge/port add bridge=LanBridge interface=ether3
/interface/bridge/port add bridge=LanBridge interface=ether4
/interface/bridge/port add bridge=LanBridge interface=ether5
/interface/bridge/port add bridge=LanBridge interface=2.4Ghz
/interface/bridge/port add bridge=LanBridge interface=5Ghz
```

Aby mohla v takto vytvořeném segmentu probíhat komunikace a směrování do internetu, je nutné přiřadit mostu IP adresu. Tato adresa bude sloužit jako výchozí brána pro všechna koncová zařízení v domácnosti. Zvolený rozsah adres 192.168.10.0 s maskou podsítě /24 poskytuje kapacitu 254 využitelných adres, což je pro domácí prostředí s dostatečnou rezervou vyhovující.

```
/ip/address add address=192.168.10.1/24 interface=LanBridge
```

4.3.9 Nastavení LAN DHCP

Aby se koncová zařízení mohla k síti připojovat automaticky bez nutnosti manuálního zadávání síťových parametrů na každém klientovi, je nezbytné na routeru zprovoznit službu DHCP.

Prvním krokem je definice IP Poolu, což je rozsah adres, které je server oprávněn dynamicky přidělovat. Vzhledem k dříve zvolené masce sítě /24 vyčleníme rozsah od .2 do .254 (adresa .1 je již obsazena routerem a slouží jako brána).

```
/ip/pool/ add name=LanPool ranges=192.168.10.2-192.168.10.254
```

Následně vytvoříme samotnou instanci DHCP serveru a navážeme ji na rozhraní síťového mostu LanBridge. Tím zajistíme, že požadavky na přidělení adresy přicházející jak z ethernetových portů, tak z bezdrátové sítě Wi-Fi, budou centrálně obslouženy jedním serverem.

```
/ip/dhcp-server/ add name=LanDHCP address-pool=LanPool interface=LanBridge
```

Samotné přidělení IP adresy však pro plnou funkčnost nestačí. Aby měli klienti přístup k internetu, musí jim DHCP server distribuovat také informaci o výchozí bráně. V systému RouterOS se tento parametr definuje v podsekci Networks. Jako bránu nastavíme adresu 192.168.10.1.

```
/ip/dhcp-server/network/ add address=192.168.10.0/24 gateway=192.168.10.1
```

4.3.10 Konfigurace DHCP pro síť hostů

Konfigurace adresace pro oddělenou síť hostů probíhá podobně jako u hlavní sítě, avšak s rozdílnými parametry sítě, které zajistí logickou separaci provozu.

Nejprve je nutné přiřadit virtuálnímu rozhraní GuestNetwork vlastní IP adresu, která bude sloužit jako brána. Pro tento segment zvolíme rozsah 192.168.20.0. Vzhledem k tomu, že se nepředpokládá připojení velkého počtu návštěvníků současně, je zbytečné plýtvat adresním prostorem. Využijeme proto masku podsítě /27, která nám poskytne celkem 32 IP adres, z toho 30 využitelných pro hosty a router.

```
/ip/address add address=192.168.20.1/27 interface=GuestNetwork
```

Následně definujeme IP Pool pro tento rozsah a spustíme samostatnou instanci DHCP serveru vázanou výhradně na rozhraní pro hosty.

```
/ip/pool add name=GuestPool ranges=192.168.20.2-192.168.20.30

/ip/dhcp-server add name=GuestDHCP address-pool=GuestPool
interface=GuestNetwork

/ip/dhcp-server/network add address=192.168.20.0/27 gateway=192.168.20.1
```

4.3.11 Nastavení firewall pravidel

Pro zabezpečení routeru a vnitřní sítě před útoky z internetu využijeme firewall. Konfigurace vychází z bezpečnostního principu „co není výslovně povoleno, je zakázáno“.

Pravidla jsou rozdělena do dvou částí. Řetězec Input řídí provoz směřující přímo do routeru. Zde je nutné povolit plný přístup pro správu pouze z vnitřní sítě. Pro síť hostů však musíme udělit výjimku a povolit nezbytné síťové služby DNS a DHCP. Tím zajistíme, že hosté získají IP adresu a mohou překládat doménová jména, ale firewall jim zabrání v přístupu k přihlašovacímu rozhraní routeru. Veškerý ostatní provoz, zejména z internetu, je nekompromisně zahazován.

Řetězec Forward řídí provoz procházející skrz router. Zde povolíme odchozí komunikaci pro domácí zařízení i hosty směrem do WAN rozhraní (ether1). Díky tomu, že pravidla specifikují pouze odchozí směr do internetu a na konci řetězce je pravidlo DROP, dojde k efektivnímu zablokování jakékoliv komunikace mezi sítí hostů a privátní domácí sítí.

Klíčovým prvkem pro výkon je práce se stavy spojení. Na začátek pravidel vždy umisťujeme pravidlo accept established, related. To zajistí, že router nebude muset zkoumat každý paket zvlášť, ale automaticky propustí ty, které patří k již navázané a schválené komunikaci.

```
/ip/firewall/filter add action=accept chain=input connection-state=established,related
/ip/firewall/filter add action=accept chain=forward connection-state=established,related
/ip/firewall/filter add action=accept chain=input in-interface=LanBridge
/ip/firewall/filter add action=accept chain=forward connection-state=new in-
interface=LanBridge out-interface=ether1
```

```
/ip firewall filter add action=accept chain=input in-interface=GuestNetwork protocol=udp dst-port=53,67
/ip firewall filter add action=accept chain=input in-interface=GuestNetwork protocol=tcp dst-port=53
/ip/firewall/filter add action=accept chain=forward connection-state=new in-interface=GuestNetwork out-interface=ether1
/ip/firewall/filter add action=drop chain=input
/ip/firewall/filter add action=drop chain=forward
```

Nedílnou součástí je také konfigurace NAT. Protože vnitřní sítě používají privátní adresní rozsahy, které nejsou v internetu směrovatelné, je nutné na odchozím rozhraní aktivovat funkci maškarády (Masquerade). Ta má za cíl dynamický překlad IP adres vnitřních zařízení na veřejnou IP adresu routeru.

```
/ip/firewall/nat add chain=srcnat out-interface=ether1 action=masquerade
```

4.3.12 Vypnutí nepotřebných služeb

Pro zajištění maximální bezpečnosti sítě je nutné minimalizovat možnosti připojení k routeru. Prvním krokem je deaktivace nepotřebných služeb, které systém RouterOS ve výchozím stavu nabízí. Jedná se především o webové rozhraní, FTP, Telnet a API. Ponecháme aktivní pouze službu WinBox pro správu.

```
/ip/service/ disable api,api-ssl,telnet,ssh,www,www-ssl,ftp
```

Dále je nutné zabezpečit přístup na 2. vrstvě, tedy správu pomocí připojení přes MAC adresy. Tento způsob připojení je velmi užitečný v případě chyby v konfiguraci IP, ale představuje riziko, pokud by byl dostupný z Wi-Fi sítě pro hosty nebo z portu WAN. Vytvoříme proto seznam rozhraní (Interface List) s názvem LanList, do kterého vložíme pouze náš bezpečný LanBridge. Následně omezíme služby MAC Serveru tak, aby naslouchaly výhradně na rozhraních v tomto seznamu.

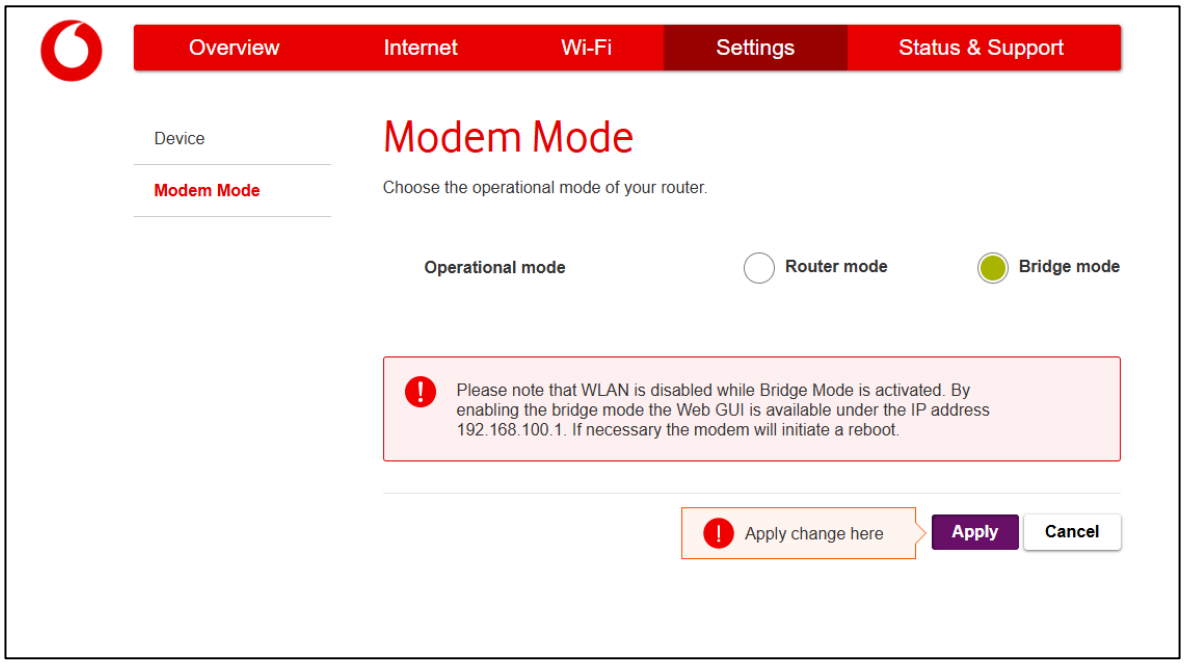
```
/interface list add name=LanList
/interface list member add interface=LanBridge list=LanList
/tool mac-server set allowed-interface-list=LanList
/tool mac-server mac-winbox set allowed-interface-list=LanList
/tool mac-server ping set enabled=no
```

4.3.13 Konfigurace modemu

Posledním krokem realizace je úprava konfigurace koncového zařízení od poskytovatele. Cílem je přepnutí modemu z výchozího režimu směrovače (Router mode) do režimu mostu (Bridge mode).

Připojíme se k modemu prostřednictvím webového prohlížeče na výchozí adrese 192.168.0.1. V administračním rozhraní přejdeme do sekce Settings → Modem Mode. Zvolíme možnost Bridge Mode a potvrdíme nastavení.

Následně dojde k restartu modemu, který trvá několik minut. V tomto režimu modem vypne svou vlastní Wi-Fi část, deaktivuje funkce firewallu a routeru a stane se z něj transparentní převodník signálu z koaxiálního kabelu na Ethernet.



Obrázek 7: Vodafone nastavení. Zdroj: [Vlastní Zpracování]

5 Výsledky a diskuse

Nasazení vlastního síťového prvku od společnosti MikroTik do domácího prostředí přineslo zásadní kvalitativní posun v oblasti správy, výkonu a bezpečnosti sítě oproti standardnímu řešení dodávanému poskytovatelem internetu. Realizace potvrdila, že přechod na vlastní řešení je proveditelný i v domácích podmínkách a přináší benefity, které převyšují počáteční investici do hardwaru i časovou náročnost konfigurace.

5.1 Bezpečnostní limity a minimalizace rizik

Je nezbytné zdůraznit, že žádná počítačová síť není zcela imunní vůči útokům. Kybernetické hrozby se neustále vyvíjejí a absolutní bezpečnost je v dynamickém prostředí internetu nedosažitelný ideál. Cílem návrhu proto nebylo vytvoření neprůstřelné bariéry, ale maximální možné snížení rizika napadení.

Zatímco modem od poskytovatele funguje často jako uzavřený systém, do jehož procesů uživatel nevidí a nemůže efektivně ovlivnit pravidla firewallu, vlastní řešení postavené na systému RouterOS umožňuje plnou kontrolu nad provozem. Díky důsledné izolaci sítě pro hosty, striktním pravidlům firewallu a vypnutí nepotřebných služeb se podařilo eliminovat většinu běžných zranitelností, kterým jsou standardní domácí routery vystaveny.

5.2 Konfigurovatelnost a nezávislost na poskytovateli

Nejvýznamnějším přínosem vlastního zařízení je úplná kontrola nad síťovým provozem. Standardní modemy často disponují pouze omezeným rozhraním, které uživateli často dovoluje změnit pouze název Wi-Fi a heslo.

Nasazením routeru MikroTik došlo k odstranění závislosti na limitovaném hardwaru operátora. Systém RouterOS poskytuje pokročilé nástroje pro detailní analýzu datových toků, řízení šířky pásma a diagnostiku, což umožňuje řešit případné problémy v síti v reálném čase. Vlastní zařízení navíc zajišťuje dlouhodobou softwarovou podporu a pravidelné bezpečnostní aktualizace, což bývá u zařízení pronajímaných od operátorů často problematické.

5.3 Náročnost a proveditelnost implementace

Ačkoliv se systém MikroTik může na první pohled jevit jako složitý a určený výhradně pro experty, praktická realizace ukázala, že nastavení je teoreticky velmi přímočaré a logické. Pokud se postupuje systematicky je konfigurace zvládnutelná i pro poučeného uživatele.

Systém nespoléhá na skryté automatické funkce, které by prováděly nastavení bez vědomí uživatele, ale vyžaduje přesnou definici každého kroku. Tato transparentnost je ve výsledku výhodou, protože správce přesně ví, jak se router chová. Modelový scénář tak prokázal, že vlastní síťové prvky mají své opodstatnění i v moderní domácnosti a jejich konfigurace nepředstavuje nepřekonatelnou překážku.

5.4 Měření rychlosti a latence

Pro objektivní posouzení přenosových rychlostí a latence připojení byla provedena série srovnávacích měření. Cílem bylo porovnat výkonnost modemu poskytovatele a nově nasazeného routeru MikroTik.

5.4.1 Metodika měření

K testování propustnosti sítě byl využit měřicí nástroj Ookla Speedtest [20]. Aby byla zachována maximální konzistence výsledků a eliminován vliv vnějšího trasování v internetu, byl pro všechna měření fixně zvolen měřicí server Vodafone CZ (Prague). Měření probíhala v režimu více paralelních spojení, což umožňuje naplno saturovat kapacitu linky.

Testování obou zařízení probíhalo za totožných podmínek, ze stejných vzdáleností a fyzických překážek. Smluvní rychlost internetové přípojky u poskytovatele je stanovena na 500 Mb/s pro stahování a 50 Mb/s pro nahrávání.

K testování propustnosti byla využita klientská zařízení zastupující různé typy připojení a technologické standardy. Referenční měření probíhalo na stolním počítači připojeném přímo k routeru pomocí metalického kabelu. Bezdrátové připojení bylo následně testováno na dvou odlišných zařízeních. Na stolním počítači, který je osazen moderní bezdrátovou kartou s podporou standardu Wi-Fi 6 a technologie 2x2 MIMO, a pro srovnání výkonu starší elektroniky také na mobilním telefonu, jehož hardwarovým maximem je podpora předchozího standardu Wi-Fi 5.

5.4.2 Výsledky měření

Následující tabulka shrnuje naměřené hodnoty datové propustnosti a latence v klidovém stavu i pod zátěží při stahování (DL) a nahrávání (UL). U bezdrátových testů je rovněž orientačně uvedena síla přijímaného signálu v dBm.

Klientské zařízení	Připojení	Parametry Vodafone Modemu	Parametry MikroTik zařízení
Stolní PC	Kabel (Ethernet)	Rychlost: 503,7 / 50,3 Mbps Ping (Klid/DL/UL): 9 / 22 / 6 ms	Rychlost: 504,0 / 50,3 Mbps Ping (Klid/DL/UL): 9 / 37 / 7 ms
Stolní PC (Wi-Fi 6 klient)	Wi-Fi 5 GHz -65dBm	Rychlost: 355,6 / 50,3 Mbps Ping (Klid/DL/UL): 12 / 47 / 8 ms	Rychlost: 120,8 / 50,3 Mbps Ping (Klid/DL/UL): 10 / 50 / 12 ms
Stolní PC (Wi-Fi 6 klient)	Wi-Fi 2,4 GHz -65dBm	Rychlost: 45,0 / 40,3 Mbps Ping (Klid/DL/UL): 34 / 60 / 12 ms	Rychlost: 164,3 / 50,3 Mbps Ping (Klid/DL/UL): 10 / 50 / 9 ms
Mobilní telefon (Wi-Fi 5 klient)	Wi-Fi 5 GHz -45 dBm	Rychlost: 268,0 / 50,4 Mbps Ping (Klid/DL/UL): 11 / 86 / 9 ms	Rychlost: 275,0 / 50,4 Mbps Ping (Klid/DL/UL): 9 / 78 / 8 ms
Mobilní telefon (Wi-Fi 5 klient)	Wi-Fi 2,4 GHz -65 dBm	Rychlost: 28,2 / 31,3 Mbps Ping (Klid/DL/UL): 14 / 256 / 413 ms	Rychlost: 48,5 / 46,6 Mbps Ping (Klid/DL/UL): 13 / 214 / 63 ms

Tabulka 2: Výsledky měření. Zdroj: [Vlastní Zpracování]

5.4.3 Zhodnocení měření

Z naměřených hodnot vyplývá, že obě zařízení bez potíží dosahují limitů internetové přípojky při použití metalického kabelu. Zásadní rozdíly se však projevily v bezdrátovém přenosu.

Modem Vodafone Station prokázal v pásmu 5 GHz vysoký hrubý vysílací výkon, což pravděpodobně pramení z větších fyzických rozměrů zařízení a dimenzování interních antén, díky čemuž dosáhl vyšších špičkových rychlostí stahování u moderních klientů. Naopak v zarušenějším pásmu 2,4 GHz se naplno projevila technologická převaha standardu Wi-Fi 6 na routeru MikroTik. U klienta s kompatibilní síťovou kartou došlo k masivnímu nárůstu rychlosti stahování z původních 45 Mb/s na více než 164 Mb/s.

Nejdůležitějším zjištěním celého měření je však rozdíl ve stabilitě latence pod zátěží. Samotná vysoká propustnost v pásmu 5 GHz u modemu poskytovatele ztrácí na významu ve chvíli, kdy je síť zatížena odchozím provozem. Jak se ukázalo při měření staršího klienta na frekvenci 2,4 GHz, latence u zařízení Vodafone Station extrémně vzrostla, což v praxi způsobuje zasekávání služeb citlivých na odezvu u všech ostatních uživatelů v síti. Router MikroTik díky efektivnímu zpracování paketů a pokročilému řízení datových front udržel i pod maximální zátěží stabilní a násobně nižší odezvu. Měření tak potvrdilo, že hrubá rychlost modemu operátora je vykoupena nižší stabilitou, zatímco vlastní zařízení poskytuje mnohem konzistentnější a spolehlivější uživatelský zážitek.

6 Závěr

Tato práce se zabývala komplexním návrhem, realizací a zabezpečením počítačové sítě v domácím prostředí. Hlavním motivem bylo vytvořit spolehlivou, stabilní a bezpečnou domácí síťovou infrastrukturu, která překoná omezení standardních zařízení běžně dodávaných poskytovateli internetového připojení.

V teoretické části byly definovány klíčové pojmy a popsány základní principy fungování počítačových sítí. Pozornost byla věnována referenčním modelům ISO/OSI a TCP/IP, specifikaci síťových prvků, moderním standardům bezdrátové komunikace Wi-Fi a základním bezpečnostním mechanismům. Tyto teoretické poznatky posloužily jako podklad pro následnou praktickou realizaci.

V praktické části byl na základě definovaného modelového scénáře a provedeného průzkumu trhu vybrán jako centrální prvek sítě router MikroTik hAP ax². Toto zařízení díky operačnímu systému RouterOS nabízí plnou konfigurovatelnost a detailní správu síťového provozu. Samotná konfigurace byla provedena systematicky od základního síťového nastavení až po pokročilé bezpečnostní restrikce. Byla implementována striktní pravidla firewallu, vytvořena logicky izolovaná bezdrátová síť pro hosty a samotný bezdrátový přenos byl zabezpečen standardem WPA3. Původní modem od poskytovatele byl následně přepnut do režimu síťového mostu, čímž mu byla ponechána pouze role transparentního převodníku signálu.

Ověření vlastností nového řešení proběhlo formou srovnávacího měření mezi původním modemem a nově nasazeným routerem. Ačkoliv obě zařízení dokázala naplno saturovat kapacitu internetové přípojky při kabelovém připojení, v bezdrátovém přenosu se ukázaly podstatné rozdíly. Nasazení standardu Wi-Fi 6 přineslo u kompatibilního zařízení v zarušeném frekvenčním pásmu 2,4 GHz více než trojnásobné zrychlení datového přenosu.

Nejvýznamnějším zjištěním celého testování však bylo diametrální zlepšení stability sítě pod zátěží. Zatímco původní řešení od poskytovatele trpělo výrazným zvýšením latence při plném vytížení, zařízení MikroTik díky efektivnímu zpracování síťového provozu udrželo stabilní a nízkou odezvu.

Měření a následné zhodnocení tak v praxi potvrdilo, že hrubá přenosová rychlost není jedinou metrikou kvality a že stabilita latence je pro plynulý chod moderní domácnosti naprosto kritická. Práce na konkrétním případu ukázala, že nahrazení základního zařízení od operátora pokročilejším síťovým prvkem přináší uživateli nejen vyšší míru zabezpečení a plnou kontrolu nad vlastním síťovým provozem, ale také prokazatelně stabilnější a spolehlivější uživatelský zážitek.

7 Seznam použitých zdrojů

[1] *Lekce 1 - Sítě - Typy používaných sítí*. Online. 2023. Dostupné z: https://www.itnetwork.cz/site/zaklady/site-typy-pouzivanych-siti. [cit. 2025-07-28].

[2] *Types of Network Topology*. Online. 2025. Dostupné z: https://www.geeksforgeeks.org/computer-networks/types-of-network-topology/. [cit. 2025-07-28].

[3] *What Is Network Topology? Best Guide to Types and Diagrams*. Online. 2019. Dostupné z: https://www.dnsstuff.com/what-is-network-topology. [cit. 2025-07-25].

[4] *What is the OSI model? The 7 layers of OSI explained*. Online. 2025. Dostupné z: https://www.techtarget.com/searchnetworking/definition/OSI. [cit. 2025-07-28].

[5] *TCP/IP Model*. Online. 2025. Dostupné z: https://www.geeksforgeeks.org/computer-networks/tcp-ip-model/. [cit. 2025-07-28].

[6] *What is Ethernet?* Online. 2025. Dostupné z: https://www.geeksforgeeks.org/computer-networks/what-is-ethernet/. [cit. 2025-07-28].

[7] *Koaxiální kabely pro televizní příjem: co byste měli vědět a jaké jsou nejlepší?* Online. Dostupné z: https://www.mtlcable.cz/kabely-koaxialni-jake-pouzivat_d14848.html. [cit. 2025-07-28].

[8] *Types of network cables*. Online. Dostupné z: https://amorserv.com/insights/types-of-network-cables. [cit. 2025-07-28].

[9] *IEEE 802.11*. Online. 2021, 2025. Dostupné z: https://cs.wikipedia.org/wiki/IEEE_802.11. [cit. 2025-07-28].

[10] *What frequency band* does *Wi-Fi 6E use?* Online. 2020. Dostupné z: https://www.everythingrf.com/community/what-frequency-band-does-wi-fi-6e-use. [cit. 2025-07-28].

[11] *What is WPA3 vs. WPA2?* Online. Dostupné z: https://www.portnox.com/cybersecurity-101/wpa3/. [cit. 2025-07-28].

[12] *Network Devices*. Online. 2025. Dostupné z: https://www.geeksforgeeks.org/computer-networks/network-devices-hub-repeater-bridge-switch-router-gateways/. [cit. 2025-07-28].

[13] *What Is An IP Address? How Does It Work?* Online. Dostupné z: https://www.fortinet.com/resources/cyberglossary/what-is-ip-address. [cit. 2025-07-28].

[14] *What is MAC Address?* Online. 2024. Dostupné z: https://www.geeksforgeeks.org/computer-networks/mac-address-in-computer-network/. [cit. 2025-07-28].

[15] *Dynamic Host Configuration Protocol (DHCP)*. Online. 2025. Dostupné z: https://www.geeksforgeeks.org/computer-networks/dynamic-host-configuration-protocol-dhcp/. [cit. 2025-07-28].

[16] *Domain Name System (DNS)*. Online. 2025. Dostupné z: https://www.geeksforgeeks.org/computer-networks/domain-name-system-dns-in-application-layer/. [cit. 2025-07-28].

[17] *Introduction of Firewall in Computer Network*. Online. 2025. Dostupné z: https://www.geeksforgeeks.org/computer-networks/introduction-of-firewall-in-computer-network/. [cit. 2025-07-28].

[18] *Network Address Translation (NAT)*. Online. 2025. Dostupné z: https://www.geeksforgeeks.org/computer-networks/network-address-translation-nat/. [cit. 2025-07-28].

[19] *HAP ax²*. Online. Dostupné z: https://mikrotik.com/product/hap_ax2. [cit. 2026-01-14].
[20] *Speedtest by Ookla - The Global Broadband Speed Test*. Online. 2006. Dostupné z: https://www.speedtest.net/. [cit. 2026-02-20].

Seznam obrázků a tabulek

7.1 Seznam obrázků

Obrázek 1: Topologie sítí. Zdroj: dnsstuff.com [3] 16
Obrázek 2: ISO/OSI model. Zdroj: [Vlastní Zpracování] 17
Obrázek 3: TCP/IP Model. Zdroj: [Vlastní Zpracování] 20
Obrázek 4: ISO/OSI a TCP/IP model. Zdroj: [Vlastní Zpracování] 21
Obrázek 5: Frekvenční kanály. [10] 24
Obrázek 6: hAP ax². Zdroj: MikroTik.com [19] 33
Obrázek 7: Vodafone nastavení. Zdroj: [Vlastní Zpracování] 41

7.2 Seznam tabulek

Tabulka 1: Wi-Fi standardy. [9] 23
Tabulka 2: Výsledky měření. Zdroj: [Vlastní Zpracování] 44