

DELTA – Střední škola informatiky a ekonomie, s.r.o.
Ke Kamenci 151, Pardubice

NÁVRH DOMÁCÍ SÍTĚ

Tojšl Jakub

4.B

Informační technologie 18-20-M/01

2023 / 2024

Prohlašuji, že jsem maturitní projekt vypracoval(a) samostatně, výhradně s použitím uvedené literatury.

V Pardubicích 28.03.2024

(vlastnoruční podpis)

Zadání maturitního projektu z informatických předmětů

Jméno a příjmení: *Jakub Tojšl*
Školní rok: *2023/2024*
Třída: *4.B*
Obor: *Informační technologie 18-20-M/01*

Téma práce: *Návrh domácí sítě*
Vedoucí práce: *Ing. Zdeněk Drvota*

Způsob zpracování, cíle práce, pokyny k obsahu a rozsahu práce:

Maturitní projekt se zaměřuje na návrh a implementaci sítě pro domácnost, zahrnuje analýzu rozložení místností a rozmístění uživatelských zařízení. Na základě toho budou navrženy kabeláže, umístění síťových prvků a parametry hardwaru, které odpovídají potřebám uživatelů. Konkrétní typy a značky síťových zařízení budou vybrány s ohledem na cenovou rozvahu a provedena jejich konfigurace. Ideálně se na reálném kusu sítě provede ověření a monitoring, přičemž v teoretické části práce budou popsány principy a technologie.

Stručný časový harmonogram (s daty a konkretizovanými úkoly):

Září	Studium principů a technologií, potřeb uživatelů a výběr parametrů hardwaru.
Říjen	Návrh kabeláže a umístění síťových prvků.
Listopad	Výběr konkrétních zařízení a sestavení cenové rozvahy na základě aktuální nabídky.
Prosinec	Připojení k internetu a návrh adresování
Leden	Ověření sítě
Únor	Kompletace projektu a dokumentace
Březen	Dokončení a odevzdání práce

Poděkování

Rád bych poděkoval vedoucímu mé práce Ing. Zdeňku Drvotovi za vedení a konzultaci mého projektu a cenné rady při zpracování projektu. Také bych chtěl poděkovat přátelům a rodině za podporu.

Obsah

1	Úvod	6
2	Postup.....	6
3	Teorie.....	7
3.1	Domácí síť	7
3.2	Topologie sítě.....	7
3.3	Zařízení v síti	8
3.4	Wi-Fi	9
3.5	Rušení wifi signálu.....	9
3.6	Zabezpečení	10
3.7	Šifrování	10
3.8	Filtrování MAC adres.....	10
3.9	NAT – Network Address Translation	11
3.10	Adresace.....	12
3.11	Routing.....	13
3.12	Záložní zdroj.....	15
	Druhy a parametry UPS	15
4	Návrh bytového domu.....	17
4.1	Návrh síťových kabelů a rozvržení síťových zařízení.....	19
4.2	Zařízení.....	20
4.3	Seznam síťových zařízení	21
4.3.1	Porovnání hlavních parametrů zařízení.....	25

1 Úvod

V dnešní době, kdy se internetová konektivita stala nedílnou součástí života, je domácí síť klíčovým prvkem pro plynulé fungování moderní domácnosti. Maturitní projekt se zaměřuje na individuální řešení, které splní specifické požadavky dané domácnosti a zároveň zajistí optimální propojení všech zařízení.

Maturitní projekt se zaměřuje na návrh a implementaci sítě pro domácnost, zahrnuje analýzu rozložení místností a rozmístění uživatelských zařízení. Na základě toho budou navrženy kabeláže, umístění síťových prvků a parametry hardwaru, které odpovídají potřebám uživatelů. Konkrétní typy a značky síťových zařízení budou vybrány s ohledem na cenovou rozvahu a provedena jejich konfigurace. Ideálně se na reálném kusu sítě provede ověření a monitoring, přičemž v teoretické části práce budou popsány principy a technologie.

2 Postup

Během zpracování projektu jsem začal obecným průzkumem domácích sítí, abych získal přehled o běžných technologiích a řešeních v této oblasti. Během tohoto průzkumu jsem zjišťoval různé typy domácích sítí, jejich topologie a základní principy fungování.

Po získání obecných znalostí jsem se zaměřil na studium konkrétních technologií, které jsou nezbytné pro navrhování a implementaci domácí sítě. To zahrnovalo například topologie sítě, rozdíly mezi protokoly IPv4 a IPv6, adresaci, síťové prvky jako NAT a další klíčové koncepty.

S nabytými znalostmi jsem přistoupil k návrhu konkrétního plánu pro domácí síť v daném bytě. To zahrnovalo určení optimálního umístění zařízení a umístění kabeláže pro dosažení co nejlepšího pokrytí signálem a minimalizaci rušení. Zároveň jsem navrhl vhodný druh připojení k internetu v souladu s potřebami uživatelů a dostupnými možnostmi poskytovatelů.

Dalším krokem byl výběr konkrétních síťových zařízení, které budou použity v navrhované domácí síti. Pro usnadnění rozhodování jsem rozdělil dostupné možnosti do tří cenových kategorií, přičemž jsem zohlednil jak požadavky na výkon a funkce, tak i finanční možnosti klienta. Tento proces výběru zařízení byl proveden s důkladným zvážením, abych zajistil optimální kombinaci kvality, výkonu a ceny pro navrhovanou domácí síť.

3 Teorie

3.1 Domácí síť

Domácí síť je lokální síť využívaná v domácnostech pro účely propojení různých zařízení a spojení internetem. Domácí sítě mohou být jednoduché, s několika zařízeními, nebo složité, s mnoha připojenými zařízeními a pokročilými funkcemi. Důležité je zajistit, aby síť byla bezpečná, spolehlivá a dobře spravována, aby uživatelé mohli plně využívat přínosy propojeného světa. [1]

3.2 Topologie sítě

Počítačové sítě mohou mít různé topologie, nejběžnější je hvězdicová topologie, kde všechna zařízení jsou připojena k centrálnímu routeru. Další možné topologie jsou níže. V tomto konkrétním návrhu je použito takzvané smíšené zapojení neboli mesh.

Běžné typy topologií:

Hvězdicová topologie: V hvězdicové topologii jsou všechny síťové prvky připojeny k centrálnímu zařízení, obvykle routeru. Tato topologie je snadno instalovatelná a spravovatelná, ale může být náchylná k výpadkům, pokud centrální zařízení selže.

Kruhová topologie: V kruhové topologii jsou všechny síťové prvky propojeny do kruhu. Každý prvek odesílá data svému sousedovi v kruhu. Tato topologie je odolnější vůči výpadkům než hvězdicová topologie, ale může být obtížnější ji instalovat a spravovat.

Sběrníková topologie: V sběrníkové topologii jsou všechny síťové prvky připojeny k jedinému kabelu. Data se odesílají po kabelu ve všech směrech a každý prvek přijímá data, která jsou pro něj určena. Tato topologie je snadno instalovatelná, ale může být náchylná ke kolizím dat.

Smíšená topologie: Smíšená topologie je kombinací dvou nebo více topologií. Například síť může mít hvězdicovou topologii pro připojení počítačů k switchům a kruhovou topologii pro propojení switchů dohromady.

Výběr topologie:

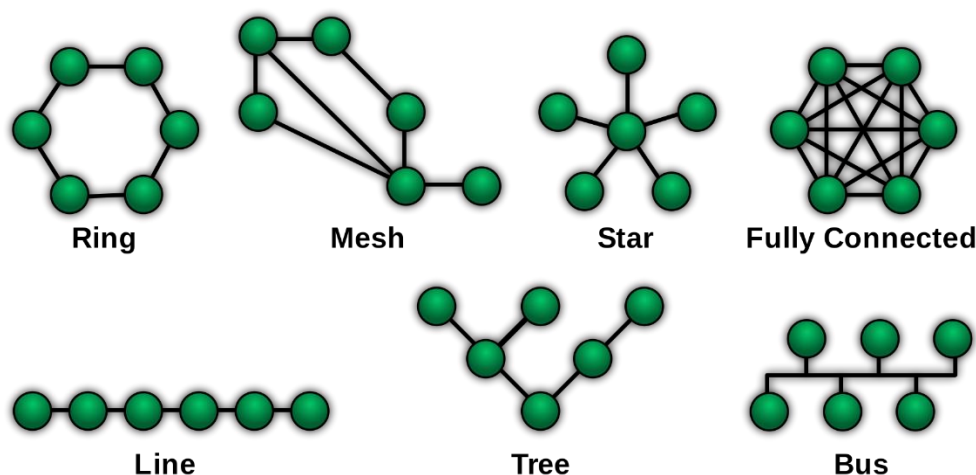
Při výběru topologie sítě je důležité zvážit několik faktorů, jako je počet síťových prvků, požadovaná úroveň výkonu a odolnosti vůči výpadkům.

V domácích sítích:

V domácích sítích se nejčastěji používá hvězdicová topologie. Tato topologie je snadno instalovatelná a spravovatelná a pro většinu domácností je dostatečně výkonná.

V podnikových sítích:

V podnikových sítích se používají různé topologie v závislosti na specifických požadavcích sítě. Velké sítě mohou používat smíšené topologie, které kombinují různé typy topologií pro dosažení optimálního výkonu a odolnosti vůči výpadkům. [2]



Obrázek 1

3.3 Zařízení v síti

Domácí síť může obsahovat různá zařízení, jako jsou počítače, chytré telefony, tablety, tiskárny, televize a další. Tato zařízení jsou připojena k síti pomocí kabelů (Ethernet) nebo bezdrátově (Wi-Fi).

Router

Router je klíčovým prvkem domácí sítě, slouží k propojení sítě s internetem. Také mezi sebou může propojovat zařízení, aniž by musel poskytovat přístup k internetu. Router také může poskytovat další funkce, jako je bezpečnostní firewall nebo DHCP server.

Při výběru routeru do domácí sítě, je dobré zohlednit hlavní parametry, jako je rychlost přenosu dat, která určuje nejvyšší rychlost, jakou mohou vaše zařízení v síti komunikovat mezi sebou a s internetem. Dalším důležitým aspektem jsou technologie implementované v routeru, například podpora standardů Wi-Fi pro lepší, rychlejší a stabilnější bezdrátové připojení. Také je třeba vzít v úvahu počet portů, zda pro domácnost stačí připojení zařízení pouze do routeru, bez nutnosti dalších rozšíření, nebo bude potřeba rozšíření kapacity portů v podobě switchu.

Pro dosažení nejlepšího výkonu Wi-Fi sítě, je důležité dobré umístění routeru. V případě použití jednoho routeru, se musí zvolit místo, aby co nejlépe pokrylo celý prostor bytu. Lepší řešení pro náročnější využití je zapojení takzvaného mesh Wi-Fi systému, který je použit i v tomto konkrétním návrhu domácnosti. Naopak je doporučeno vyhnout se umístění routeru v blízkosti kovových předmětů, mikrovlnných troub a podobných zařízení, které by mohly rušit signál routeru. Neposlední věcí pro zajištění dobrého výkonu Wi-Fi routeru, je pravidelná aktualizace firmwaru a také zvolení vhodného kanálu.

3.4 Wi-Fi

V dnešní době se stala Wi-Fi nedílnou součástí téměř každé domácnosti. Umožňuje připojení zařízení, bez použití kabelů. Návrh a konfigurace optimální Wi-Fi sítě je klíčová pro zajištění bezproblémového a spolehlivého internetového připojení pro všechny uživatele v domácnosti.

Hlavní typy Wi-Fi standardů:

Wi-Fi 4 (802.11n): Starší standard, stále běžný, ale s nižšími rychlostmi a horší propustností.

Wi-Fi 5 (802.11ac): Novější standard s podstatně vyššími rychlostmi a lepší propustností pro více zařízení.

Wi-Fi 6 (802.11ax) Nejnovější standart s mnohonásobně vyšší přenosovou rychlostí a stabilitou signálu.

Pásmo a frekvence

Wi-Fi síť funguje ve dvou pásmech - 2,4 GHz, běžnější pásmo s větším dosahem, ale náchylnější k rušení z okolních zařízení a nižší přenosovou rychlostí.

Druhé pásmo 5 GHz, méně rušené pásmo s vyššími rychlostmi, ale s kratším dosahem.

V rámci obou pásem existují také různé kanály, které se liší frekvencí. Pro optimální výkon je důležité zvolit kanál s nízkým rušením. Přehled frekvencí okolních Wi-Fi sítí se dá například zjistit pomocí mobilních aplikací. [3]

3.5 Rušení wifi signálu

Rušení Wi-Fi signálu může způsobovat mnoho různých fyzických překážek, elektronických zařízení nebo sousedních wifi sítí.

Routery vysílají na svých kanálech (frekvencích) a pro svou správnou funkci musí tuto frekvenci v okolí používat jako jediní (frekvence musí být volná). Pokud na sebe narazí např. dva sousedské routery a mají nastaven stejný kanál (ať už v rámci jednoho domu nebo dvou sousedů), nastane kolize (rušení) výrazně degradující kvalitu spojení.

Problémem staršího 2.4 GHz pásma je překrývání kanálů. Pro Evropu bylo těchto kanálů určeno 13 na frekvenci 2,4 GHz, ovšem ty nepřekrývající už jsou pouze 3. Pokud je router nastaven na šířku kanálu 40 MHz, pak už volný kanál prakticky nenajde. 40 MHz je vhodné používat pouze, pokud není v okolí žádné rušení.

V pásmu 5 GHz má každý 20 MHz kanál má svůj vlastní prostor a k rušení tak dochází daleko méně.

Řešení pro bytové domy s vyšším množstvím bezdrátových sítí jsou duální routery (dual-band), tyto routery vysílají jak v pásmu 2.4 GHz, tak i v novějším pásmu 5 GHz. Využití 5 GHz pásma má menší průstupnost a kvůli tomu nedochází k tak silnému šíření signálů do vedlejších bytů. [4]

3.6 Zabezpečení

Zabezpečení sítě je velmi důležitou částí, jak domácí, tak firemní sítě. Například přes nezabezpečený router může útočník proniknout do naší sítě, napadat počítače, získat přístup k IP adresám a důležitým datům a ohrozit další zařízení, které jsou do sítě připojeny. Základním pravidlem je zvolit kvalitní heslo, dobré heslo by mělo mít minimálně 8 znaků a měla by se v něm střídát malá a velká písmena, číslice a další znaky.

3.7 Šifrování

Šifrování je velmi důležitým bodem pro zabezpečení Wi-Fi sítě, značně snižuje pravděpodobnost úspěšného nabezení do sítě. Řada routerů nabízí ve výchozím nastavení šifrování WEP (Wired Equivalent Privacy), to ale už v dnešní době není považováno za příliš spolehlivé. Lepší varianta je použití WPA (Wi-Fi Protected Access) nebo ideálně WPA2. Šifrování typu WPA2 zajistí, že se k Wi-Fi síti nedostane nikdo bez znalosti hesla.

3.8 Filtrování MAC adres

Adresa MAC (Media Access Control) je zjednodušeně řečeno jedinečné identifikační číslo síťového zařízení. Funkce filtrování MAC adres může zajistit, aby k Wi-Fi síti měla přístup jen určitá zařízení, díky tomu se dá zvýšit zabezpečení sítě. Kdykoliv se síť pokusí připojit jiné zařízení, router mu odepře přístup. Filtrování MAC adres v nastavení routeru má dvě možné

varianty, povolení přístupu specifickým adresám, nebo naopak odepření přístupu konkrétním adresám. Avšak filtrování MAC adres může mít také nevýhodu v tom, že znesnadňuje připojení nových zařízení k domácí Wi-Fi, například při návštěvě.

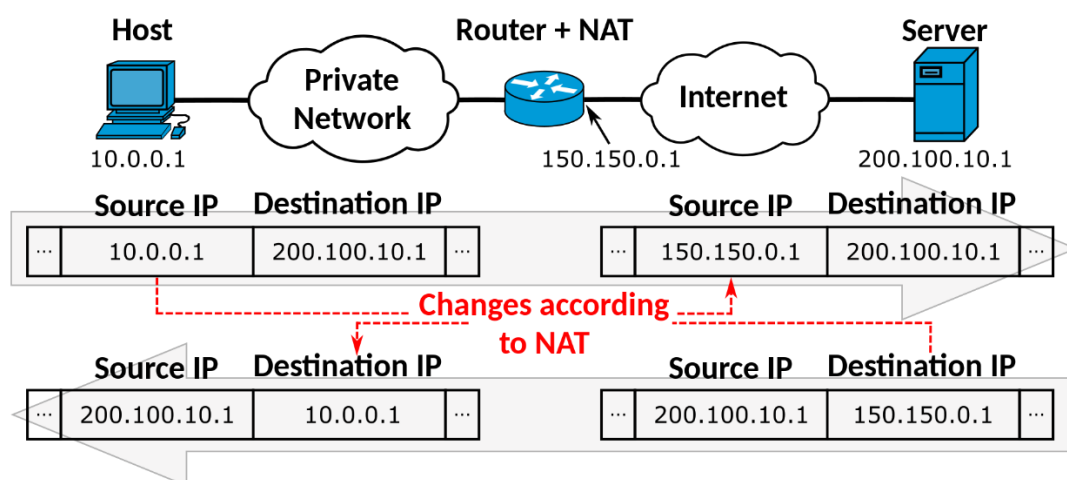
3.9 NAT – Network Address Translation

Pro komunikaci mezi sítěmi se používá typicky Router nebo Firewall. Metoda směrování (routing), mění L2 hlavičku MAC adresy, nikoliv IP adresy paketů. Veřejné IP adresy se směrují v rámci internetu, ale pro interní neveřejné síťové rozsahy je potřeba použít metodu překladu adres (NAT). NAT nahrazuje zdrojovou nebo cílovou IP adresu a udržuje tabulku spojení pro správné směrování odpovědí.

Dva základní typy NAT:

Source NAT (SNAT) - mění zdrojovou IP adresu, typicky při komunikaci z LAN do internetu, řada neveřejných adres se mění na jednu z veřejného rozsahu.

Destination NAT (DNAT) - mění cílovou IP adresu, použije veřejnou adresu a komunikaci na ní předá na interní neveřejnou adresu serveru.[5]



Obrázek 2 NAT [online]. In: . [cit. 2024-03-03]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/thumb/c/c7/NAT_Concept-en.svg/1920px-NAT_Concept-en.svg.png

Firewall

Firewall je klíčová součást síťové bezpečnosti, která slouží k regulaci a monitorování síťového provozu. Standardně je veškerá komunikace mezi sítěmi blokována a teprve na základě definovaných pravidel je specifická komunikace povolena.

Firewall Policy, pravidla pro Firewall, zajišťují propouštění jednotlivých paketů. Kromě základního blokování a povolování paketů může firewall provádět i další bezpečnostní kontroly, například analyzovat obsah paketů a hledat různé viry, malware nebo phishingové útoky. Díky těmto vlastnostem je firewall důležitým nástrojem pro ochranu počítačů a sítí před neoprávněným přístupem a kybernetickými útoky. [6]

3.10 Adresace

IP adresa reprezentuje identifikaci zařízení v počítačové síti a využívá IP protokol. V IPv4 má adresa délku 32 bitů (4 byte) a je zapisována pomocí tečkově oddělené notace. Tedy formou čtyř oktetů, z nichž každý obsahuje dekadickou hodnotu jednoho bytu. Příkladem je adresa 193.222.5.15. IP protokol existuje již dlouhou dobu a stále se vyvíjí; zaměříme se na běžné modifikace v dnešních sítích, které jsou popsány v RFC dokumentech.

Adresa IP může nabývat hodnot od 0.0.0.0 do 255.255.255.255 (teoreticky, ne všechny adresy jsou v praxi použitelné), což je rozsah adres pro IP síť a internet. I když jsou adresy zapisovány v desítkové soustavě, veškerá komunikace je optimalizována pro zpracování binární soustavou v počítačích. Pro výpočty adres je tedy nutné mít povědomí o binární aritmetice.

IPv4

Internet Protocol version 4 (IPv4) je čtvrtá verze internetových protokolů a je široce používána od svého vzniku v roce 1983. Jedná se o numerický systém, který využívá 32bitové adresy k identifikaci jednotlivých zařízení připojených k internetu. Jedna IPv4 adresa má tvar čtyř skupin čísel od 0 do 255, oddělených tečkami, například 192.168.0.1.

IPv6

Internet Protocol version 6 (IPv6) je nejnovější verze internetových protokolů, vytvořená jako odpověď na rostoucí vyčerpání adres IPv4. Tento protokol využívá 128bitový systém, což umožňuje vytvoření mnohem většího množství unikátních adres. IPv6 adresa se skládá z osmi skupin čtyř hexadecimálních číslic, oddělených dvojtečkami, například 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Hlavním rozdílem mezi IPv4 a IPv6 je počet možných adres. Zatímco IPv4 umožňuje vytvořit přibližně 4,3 miliardy unikátních adres, IPv6 jich umožňuje vytvořit až 3.4×10^{38} . Toto je obrovský skok vpřed, který umožňuje připojení mnohem většího počtu zařízení k internetu.

Další významný rozdíl je v zabezpečení. IPv6 byl navržen tak, aby poskytoval lepší zabezpečení než jeho předchůdce. To je díky vestavěné podpoře pro IPsec (Internet Protocol Security), který poskytuje autentizaci, důvěrnost a integritu dat.

Maska sítě

IP adresa se skládá z několika částí. Základními prvky jsou prefix identifikující síť a adresa uzlu v rámci této sítě. V dřívějších modelech classful sítí byl prefix určen pevně podle třídy, do které adresa patřila. V moderních classless sítích lze prefix definovat pomocí masky podsítě. Alternativně lze adresu rozdělit do tří částí: adresy sítě, adresy podsítě a adresy uzlu. Adresa sítě je stanovena třídou IP adresy, zatímco adresa podsítě je rozdílem mezi maskou a třídou. [7]

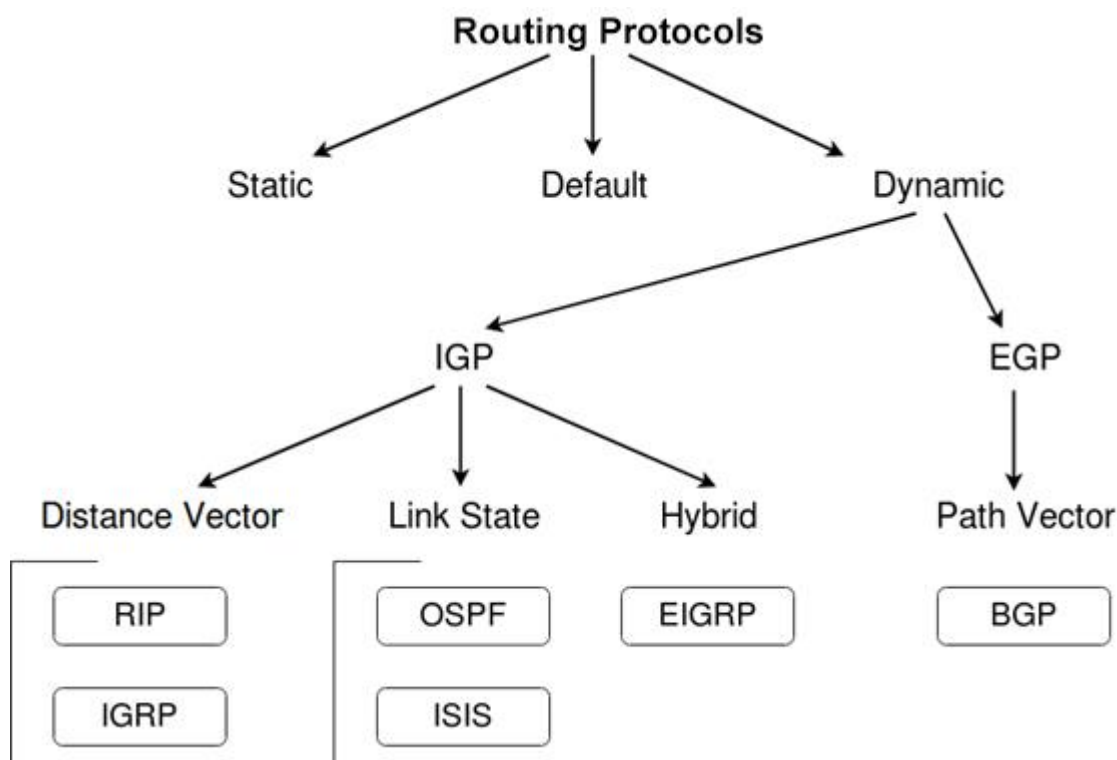
3.11 Routing

Routování je zásadní proces, který umožňuje směrování datových paketů mezi různými síťovými uzly. Když počítač nebo jiné síťové zařízení odesílá data, routování se používá k rozhodnutí, kterou cestou by měla tato data putovat k jejich cíli.

Síťová vrstva modelu OSI je zodpovědná za poskytování logických adres, které směrovače používají k výběru nejlepší cesty pro směrování paketů. Na této vrstvě se používají dva typy paketů:

Datové pakety - Uživatelská data jsou přenášena v inter-síti pomocí těchto datových paketů. Směrované protokoly jsou ty, které podporují takový datový provoz. Příklady směrovaných protokolů jsou IPv4, IPv6 a AppleTalk.

Aktualizace směrnic - Informace o sítích připojených ke všem směrovačům jsou aktualizovány u sousedních směrovačů prostřednictvím paketů aktualizace směrnic. Směrovací protokoly jsou ty, které jsou za jejich odesílání zodpovědné. Příklady směrovacích protokolů jsou RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol) a OSPF (Open Shortest Path First).



Obrázek 3 [online]. In: . [cit. 2024-03-03]. Dostupné z: <https://media.geeksforgeeks.org/wp-content/uploads/Routing-Protocols.png>

Statické směrování: Trasy jsou ručně nastaveny správcem sítě a nemění se dynamicky podle změn v síťové topologii. Nejvhodnější pro malé sítě s málo frekventovanými změnami topologie.

Dynamické směrování: Trasy jsou automaticky aktualizovány podle změn v síťové topologii. Nejvhodnější pro velké, složité sítě s frekventovanými změnami topologie. Zahrnuje v sobě různé typy dynamických směrovacích protokolů:

3.11.1 Typy směrovaných protokolů:

Interior gateway protocol (IGP): Tyto směrovací protokoly se používají v rámci autonomního systému, například OSPF (Open Shortest Path First) a IS-IS (Intermediate System to Intermediate System).

Exterior gateway protocol (EGP): Tyto směrovací protokoly se používají mezi autonomními systémy, například BGP (Border Gateway Protocol).

Protokoly vzdálenostního vektoru: Tyto protokoly určují nejlepší cestu k cíli na základě vzdálenosti, například Routing Information Protocol (RIP) a Routing Information Protocol v2 (RIPv2).

Protokoly podle stavu spojení: Tyto protokoly udržují mapu celé sítě, včetně informací o všech spojeních a jejich stavech, například OSPF a IS-IS.

Hlavní použití směrovaných protokolů:

Směrované protokoly poskytují způsob propojení různých sítí a umožňují výměnu dat mezi nimi.

Výběr trasy: Směrované protokoly pomáhají směrovačům určit nejlepší cestu pro doručení dat na základě různých faktorů.

Škálovatelnost: Směrované protokoly umožňují dynamický růst sítě bez ruční rekonfigurace jednotlivých směrovačů.

Vyvažování zátěže: Směrované protokoly mohou rovnoměrně distribuovat zátěž síťového provozu přes různé cesty, čímž zlepšují výkonnost a spolehlivost sítě.

Odolnost vůči poruchám: Směrované protokoly mohou detekovat poruchy sítě a přesměrovávat provoz na alternativní cesty, udržují konektivitu i při výpadku sítě.

Bezpečnost: Směrované protokoly mohou být využity k prosazování bezpečnostních politik sítě. [8] [9]

3.12 Záložní zdroj

Záložní zdroj UPS (uninterruptible power supply) slouží pro zajištění napájení důležitých zařízení v případě neočekávaného výpadku proudu. Slouží také jako přepětová ochrana hardwaru proti napětovým špičkám rozvodných sítí. Záložní zdroje UPS nabízí výkon až 4 500 W a skvěle se hodí do malých firem nebo kanceláře.

Druhy a parametry UPS

Existuje několik druhů UPS, které se liší v jejich funkcionalitě a účinnosti v ochraně před výpadky elektrické energie.

Offline

Nejjednodušší varianta, která se aktivuje pouze při výpadku elektrické energie, kdy rychle přepne na záložní baterie a poskytuje potřebnou energii k zajištění provozu zařízení. Tyto zdroje jsou vhodné především pro domácnosti a sítě s nižší potřebou energie.

Line-Interactive

Tento typ UPS dokáže dynamicky regulovat napětí a reagovat na výkyvy v síti. Díky této schopnosti nedochází k rychlému vybití baterie a poskytuje stabilní energii. Line-Interactive UPS jsou vhodné pro náročnější domácnosti nebo menší firmy.

Online

Nejvýkonnější a zároveň nejdražší řešení druh UPS. Tyto zdroje jsou v provozu nepřetržitě 24 hodin denně a dobíjejí baterie kontinuálně. Díky okamžité reakci na výkyvy napětí poskytují maximální ochranu před výpadky elektrické energie. Online UPS jsou ideální pro větší firmy, které vyžadují nejlepší a nejefektivnější ochranu dat.

Další parametry UPS

Kapacita akumulátorů je dalším klíčovým faktorem při výběru UPS. Zajímavostí je, že při maximální zátěži je provozní doba přibližně $5\times$ nižší než při výdeji polovičního množství energie. Proto se vždy doporučuje zakoupit výrobek s vyšší kapacitou, než je zapotřebí, pro prodloužení doby fungování přístrojů. Dražší UPS umožňují připojení přídatných baterií, které prodlužují výdrž zdroje, tato možnost je častěji využívána ve firemním prostředí.

Životnost akumulátorů. Standardně se očekává životnost tři let, avšak neustálé přebíjení může snížit tuto hodnotu.

Velký vliv na funkčnost záložních zdrojů má i výkon. Podle množství energie, které je potřeba pro zachování klíčových přístrojů v domácnosti nebo firmě. Tento parametr je většinou udáván ve dvou jednotkách, VA – Voltampér a W – Watt. Činný výkon ve W bývá až o 60 % nižší než výkon uváděný ve VA. Standardně se pro konverzi zdánlivého na činný výkon využívá vzorec $VA = W \times 1,6$. Nejlépe by měl výkon UPS být až o třetinu vyšší, než kolik energie je potřeba.

Záložní doba určuje, jak dlouho bude UPS schopna poskytovat energii po výpadku. V domácích kancelářích může být dostatečná doba kolem 1 minuty, zatímco v firemním prostředí je žádoucí mít záložní dobu přesahující 10 minut. Doba zálohy se odvíjí od množství energie, které je potřeba pro chod zařízení.

Typ a počet zásuvek jsou rovněž důležitými hledisky při výběru UPS. Moderní modely mohou obsahovat USB porty nebo prostory pro připojení mobilních telefonů či routerů, což zvyšuje jejich univerzálnost a praktičnost. Při nákupu je důležité dbát na kompatibilitu zásuvek se standardem používaným ve vaší lokalitě. [7]

4 Návrh bytového domu

Dispozice bytu

3+KK: Klasický bytový dům s 3 pokoji a kuchyňským koutem

90 m²: Celková užitná plocha bytu

Internetové připojení

FTTH (Fiber To The Home): Optické vlákno až do bytu, zajišťující nejvyšší možnou rychlost a stabilitu internetového připojení.

Pevný optický gigabit internet: Symetrická gigabitová rychlost pro stahování i odesílání dat, ideální pro online hraní, streamování videa a práci s velkými soubory.

Síťová kabeláž

70 m síťových kabelů: Dostatečná délka kabelů pro pokrytí celého bytu s rezervou.

CAT5E / CAT6A: Síťové kabely s dostatečnou rychlostí pro gigabitové internetové připojení.

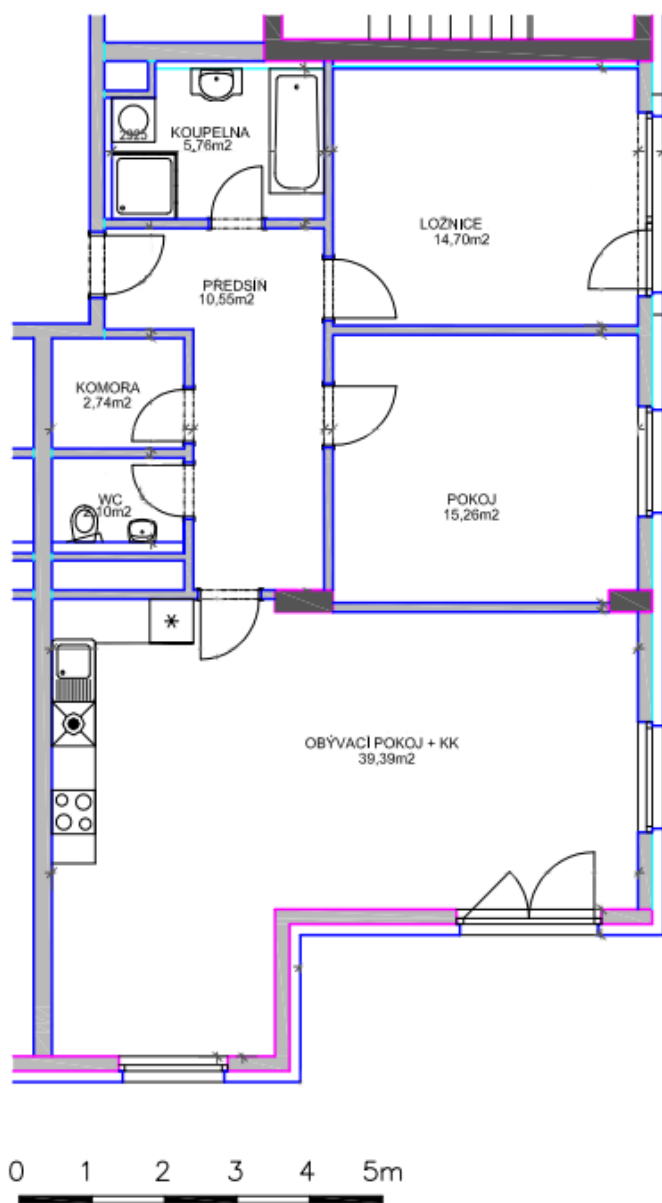
Cena kabeláže od 700 Kč; cena se liší v závislosti na typu kabelu.

Rozvod síťové infrastruktury

Rozvodová místnost: Centrální umístění pro rozvod síťového kabelu do všech místností.

Vyvedeno 8 zásuvek RJ45: Vhodné rozmístění zásuvek do každé místnosti v podobě dvou konektorů v každém vývodu.

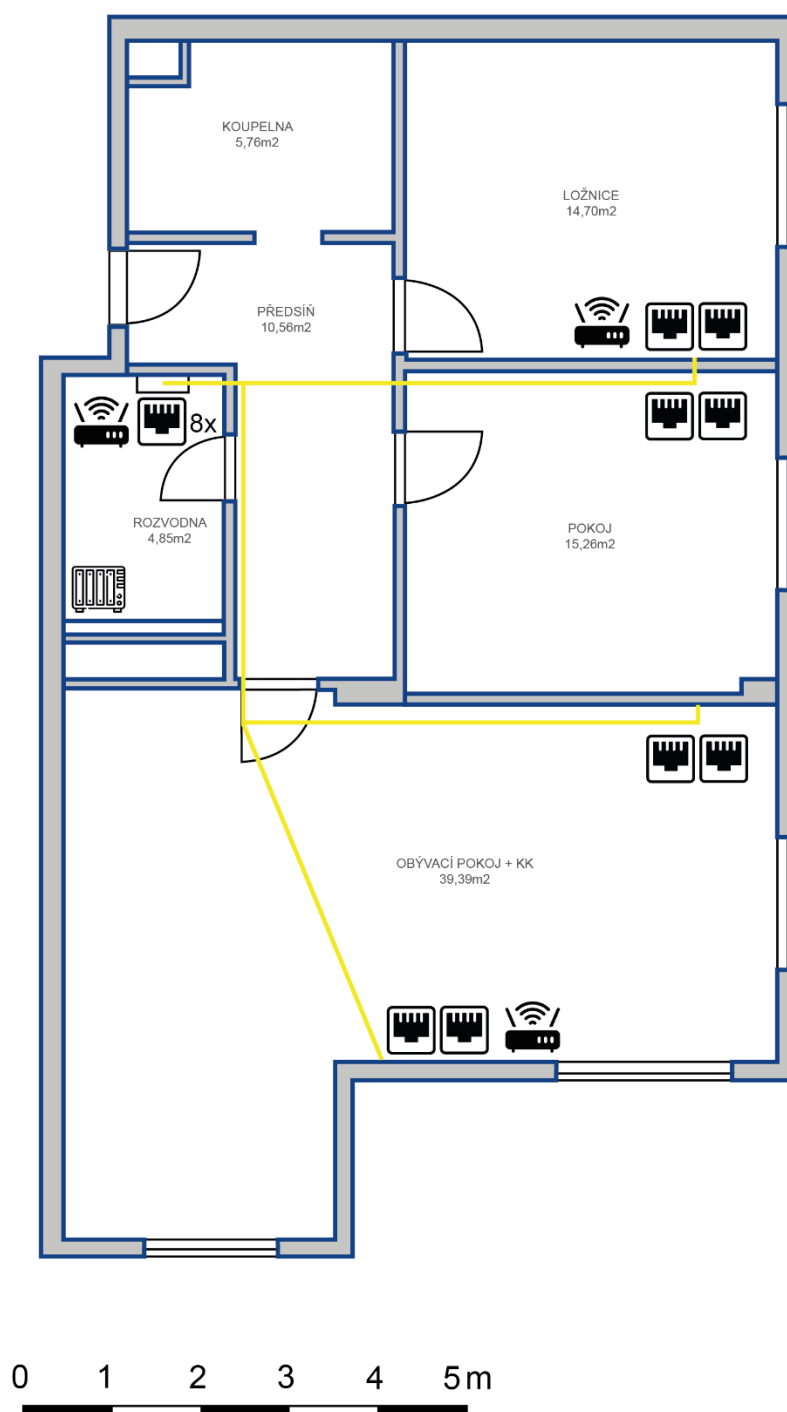
Vedení kabeláže pod podlahou, podle moderních standardů.



M 1:90

Obrázek 4 Návrh bytu

4.1 Návrh síťových kabelů a rozvržení síťových zařízení



M 1:90

Obrázek 5 Návrh kabeláže

4.2 Zařízení

V následující kapitole je výběr konkrétních síťových zařízení. Zařízení rozdělena do tří cenových kategorií – cenově dostupná a nejprodávanější zařízení, střední třída zařízení a zařízení pro náročnější využití. Konkrétní příklady zařízení jsou vybrané z eshopu Alza.cz, který byl vybrán, jako příklad dostupného prodejce s širokou nabídkou síťových zařízení.

Ceny a dostupnost

Ceny síťových zařízení se značně liší v závislosti na jejich funkcích a výkonu.

Cenově dostupná: Zahrnuje síťová zařízení v ceně do 2 000 Kč a NAS do 4 500 Kč. Vhodná pro nenáročné uživatele s malým počtem zařízení v síti.

Střední cenová kategorie: Zahrnuje síťová zařízení v ceně do 8 500 Kč a NAS do 9 500 Kč. Nabízí dobrou kombinaci funkcí a ceny i pro náročnější domácnosti.

Vyšší třída: Zahrnuje síťová zařízení v ceně do 29 000 Kč a NAS do 30 000 Kč. Určena pro náročné uživatele, domácnosti s velkým počtem zařízení a specifickými požadavky.

4.3 Seznam síťových zařízení

Cenově dostupné / nejprodávanější zařízení

Router:

2 kusy - mesh

TP-Link Archer AX23

WiFi 6

Pásmo - Dual-Band (2,4 + 5 GHz)

Rychlost 2,4 GHz - 574 Mb/s

Rychlost 5 GHz - 1201 Mb/s

Přenosová rychlost portů 1 Gbit

Cena - 1500 Kč (3000 Kč)

<https://www.alza.cz/tp-link-archer-ax23-wifi6-router-d6700765.htm>

Switch:

TP-Link TL-SG105

5× RJ-45

QoS

Přepínací kapacita 10 Gb/s

Přenosová rychlost LAN portů 1 Gbit

Cena - 560 Kč

<https://www.alza.cz/tp-link-tl-sg105-d389663.htm>

NAS:

Synology DS124

1x HDD WD Red Plus 4TB

Cena - 4 500 Kč + HDD 2 500 Kč

<https://www.alza.cz/wd-red-plus-4tb-d7587417.htm>

<https://www.alza.cz/synology-ds124-d7863821.htm#popis>

Střední třída

Router:

TP-Link Deco X50(3-pack)

Mesh

WiFi 6

Pásmo - Dual-band (2.4 GHz + 5 GHz)

Rychlost na 2,4 GHz 574 Mb/s

Rychlost na 5 GHz 2402 Mb/s

IPv6 Ready

Cena - 7500 Kč

<https://www.alza.cz/tp-link-deco-x503-pack-d7269421.htm>

Switch:

TP-Link TL-SG1016D

16× RJ-45

Přepínací kapacita 32 Gb/s

Přenosová rychlost LAN portů 1 Gbit

Cena - 1 700 Kč

<https://www.alza.cz/tp-link-tl-sg1016d-d185071.htm>

NAS

Cena - 9700 Kč

Pro náročnější využití

Router:

TP-Link Deco XE75 Pro(3-pack)

Mesh

WiFi 6E

Pásmo - Tri-band (2.4 GHz + 5 GHz + 6GHz)

Rychlost 2,4 GHz - 574 Mb/s

Rychlost 5 GHz - 2402 Mb/s

Rychlost 6 GHz - 2402 Mb/s

Porty - 1× 2.5 Gbps + 2× Gigabit

IPv6 Ready

Cena - 18500 Kč

<https://www.alza.cz/tp-link-deco-xe75-pro-3-pack-wifi-6e-mesh-system-2-5gbit-port-d7566107.htm>

Switch:

Ubiquiti USW-24-POE Gen2

24× RJ-45

Přepínací kapacita 52 Gb/s

Přenosová rychlost LAN portů 1 Gbit

Cena - 9900 Kč

<https://www.alza.cz/ubiquiti-usw-24-poe-gen2-d6333766.htm>

NAS

Synology DS1621+

<https://www.alza.cz/synology-ds1621-d6295529.htm>

Kapacita disků - 6x

4.3.1 Porovnání hlavních parametrů zařízení

Router

	TP-Link Archer AX23	TP-Link Deco X50	TP-Link Deco XE75 Pro
Cena (kus)	1 500 Kč	2 500 Kč	6 000 Kč
Wi-Fi	6	6	6E
Rychlost 2,4GHz	574 Mb/s	574 Mb/s	574 Mb/s
Rychlost 5GHz	1 201 Mb/s	2 402 Mb/s	2 402 Mb/s

Switch

	TP-Link TL-SG105	TP-Link TL-SG1016D	Ubiquiti USW-24-POE
Cena	560 Kč	7 500 Kč	9 900 Kč
RJ45	5x	16x	24x
Přepínací kapacita	10 Gb/s	32 Gb/s	52 Gb/s

NAS

	Synology DS124	Synology DS224+	Synology DS1621+
Cena	4 700 Kč	9 700 Kč	26 300 Kč
Pozice pro disk	1x	2x	6x
Rychlost čtení	113 MB/s	226 MB/s	2 317 MB/s
Rychlost zápisu	113 MB/s	225 MB/s	1 128 MB/s
RAM	1 GB	2 GB	4 GB
Procesor	Realtek RTD1619B	Intel Celeron J4125	Ryzen V1500B
Spotřeba (1H provozu)	11 W	14,7 W	51,22 W

Závěr

Návrh a implementace domácí sítě představuje komplexní proces, který vyžaduje důkladné porozumění nejen technickým, ale i uživatelským potřebám. Během zpracování maturitního projektu jsem se zaměřil na výzkum technologií a návrh, který měl za cíl zajistit optimální návrh moderní domácí sítě.

V průběhu projektu jsem získal hlubší znalosti o různých provedeních nejen domácích sítí a klíčových technologiích, které jsou důležité pro úspěšný návrh domácí sítě. Zároveň jsem se seznámil s procesem výběru vhodného hardwaru a výběru dle určených cenových kategorií a konfigurací síťových zařízení. Navržená síť splňuje požadavky moderní sítě pro domácnost v každodenním užívání. Projekt mi také pomohly lépe porozumět současným technologiím a jejich praktickým aplikacím v domácím prostředí.

Zdroje

- [1] Jak si vytvořit domácí síť. [online]. In: DSL.cz. [cit. 2023-10-22]. Dostupné z: <https://www.dsl.cz/jak-na-to/jak-si-vytvorit-domaci-sit>
- [2] Topologie sítě. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-03-24]. Dostupné z: https://cs.wikipedia.org/wiki/Topologie_s%C3%ADt%C3%AD
- [3] Wi-Fi. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2024-03-24]. Dostupné z: <https://cs.wikipedia.org/wiki/Wi-Fi>
- [4] Rušení Wi-Fi routerů." [online]. In: JMnet.cz. [cit. 2023-10-22]. Dostupné z: <https://www.jmnet.cz/ruseni-wifi-routeru>
- [5] Grygárek, R. [Cit. 2024-02-25].NAT. [online]. VSB - Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky, Katedra počítačových systémů. Dostupné z: <https://www.cs.vsb.cz/grygarek/TPS/projekty/0405Z/NAT/Nat.htm>.
- [6] FortiGate Firewall - Politiky, NAT, Load Balancing, Debug." [online]. In: Samuraj-cz.com. [cit. 2023-10-22]. Dostupné z: <https://www.samuraj-cz.com/clanek/fortigate-firewall-politiky-nat-load-balancing-debug/>
- [7] *Adresovani v IP sitich* [online]. [cit. 2024-03-26]. Dostupné z: <https://www.samuraj-cz.com/clanek/adresovani-v-ip-sitich/>
- [8] GeeksforGeeks. Dostupné z: <https://www.geeksforgeeks.org/routing-v-s-routed-protocols-in-computer-network/>. [Cit. 2024-02-25].
- [9] Samuraj-cz.com [Cit. 2024-02-25].TCP/IP Routing - Směrování. [online]. Samuraj-cz.com. Dostupné z: <https://www.samuraj-cz.com/clanek/tcpip-routing-smerovani/>.
- [9] ARecenze.cz. [Cit. 2024-02-25].Záložní zdroje. [online]. ARecenze.cz. Dostupné z: <https://www.arecenze.cz/zalozni-zdroje/>.
- T-Mobile Czech Republic. [Cit. 2024-02-25]. IPv6. [online]. T-Mobile Czech Republic. Dostupné z: <https://www.t-mobile.cz/ipv6>.
- Home Networking - The Basics." [online]. In: . [cit. 2023-10-22]. Dostupné z: <https://www.youtube.com/playlist?list=PLABF0jOixZlvmByLSjzTW9QKtsrjHU0Cz>
- ChatGPT 3.5* [online]. [cit. 2024-03-26]. Dostupné z: <https://chat.openai.com/>
- Google Gemini* [online]. [cit. 2024-03-26]. Dostupné z: <https://gemini.google.com/>

Obrázek 1 Přehled topologií počítačových sítí [online]. In: . [cit. 2024-03-03]. Dostupné z: <https://commons.wikimedia.org/wiki/File:NetworkTopologies.svg#/media/Soubor:NetworkTopologies.svg>

Obrázek 2 NAT [online]. In: . [cit. 2024-03-03]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/thumb/c/c7/NAT_Concept-en.svg/1920px-NAT_Concept-en.svg.png

Obrázek 3 Routing protocols [online]. In: . [cit. 2024-03-03]. Dostupné z: <https://media.geeksforgeeks.org/wp-content/uploads/Routing-Protocols.png>

Seznam použitých obrázků

Obrázek 1 Přehled topologií počítačových sítí	8
Obrázek 2 NAT	11
Obrázek 3 Routing protocols	14