Vyšší odborná škola, Střední průmyslová škola a Střední odborná škola

služeb a cestovního ruchu, Varnsdorf, příspěvková organizace

**Návrh LAN propojených domácností**

Adam Steinert

**2022/23**

**NÁVRH LAN PROPOJENÝCH DOMÁCNOSTÍ**

Obsah

[1 Úvod 1](#_Toc128345500)

[2 cíl práce 3](#_Toc128345501)

[3 počítačové sítě 4](#_Toc128345502)

[3.1 Rozvoj bezdrátových počítačových sítí 4](#_Toc128345503)

[3.2 Spojování počítačových sítí – internetworking 5](#_Toc128345504)

[3.2.1 OSI model 5](#_Toc128345505)

[3.2.2 Opakovač (repeater) 6](#_Toc128345506)

[3.2.3 Můstek (bridge) 6](#_Toc128345507)

[3.2.4 směrovač (Router) 7](#_Toc128345508)

[3.2.5 Brána (gateway) 8](#_Toc128345509)

[3.3 typy sítí 8](#_Toc128345510)

[3.3.1 LAN 9](#_Toc128345511)

[3.3.2 MAN 9](#_Toc128345512)

[3.3.3 PAN 9](#_Toc128345513)

[3.4 Bezdrátová komunikace 9](#_Toc128345514)

[3.4.1 přenosové techniky 9](#_Toc128345515)

[3.5 Přehled bezdrátové rádiové technologie 10](#_Toc128345516)

[3.5.1 Frekvence 10](#_Toc128345517)

[3.5.2 Hlavní normy radiokomunikačních bezdrátových sítí 11](#_Toc128345518)

[3.5.3 Topologie bezdratové sítě 12](#_Toc128345519)

[3.6 Hardwarové vybavení bezdrátových sítí 14](#_Toc128345520)

[3.6.1 Přístupový bod (Access point) 14](#_Toc128345521)

[3.6.2 Bezdrátový opakovač (repeater) 16](#_Toc128345522)

[3.6.3 WiFi Síťového adaptéru 16](#_Toc128345523)

[3.6.4 Antény 17](#_Toc128345524)

[4 Správa sítí 19](#_Toc128345525)

[4.1 Možnosti konfigurace přístupových bodů 19](#_Toc128345526)

[4.2 Přístup na internet 19](#_Toc128345527)

[4.3 DHCP server 19](#_Toc128345528)

[4.4 Veřejné a privátní IP adresy 19](#_Toc128345529)

[4.5 Firewall 20](#_Toc128345530)

[4.6 demilitarizovaná zóna 20](#_Toc128345531)

[4.7 Přesměrování portů 21](#_Toc128345532)

[4.8 Filtrování 21](#_Toc128345533)

[4.9 VPN (Virtual Private Network) 21](#_Toc128345534)

[4.10 DNS (Domain Name Systém) 21](#_Toc128345535)

[5 Bezpečnost sítí 22](#_Toc128345536)

[5.1 šifrování 22](#_Toc128345537)

[5.1.1 WEP (Wired Equivalent Privacy) 22](#_Toc128345538)

[5.1.2 WPA (WiFi Protected Access) 22](#_Toc128345539)

[5.1.3 AES 23](#_Toc128345540)

[5.2 Autentizace 23](#_Toc128345541)

[5.2.1 Open – system 23](#_Toc128345542)

[5.2.2 Shared – key 23](#_Toc128345543)

[5.2.3 Filtrování adres 24](#_Toc128345544)

[5.3 Základní kroky k zabezpečení WiFi sítě 24](#_Toc128345545)

[6 Návrh konkrétního bezdrátového propojení 25](#_Toc128345546)

[6.1 Volba média pro přenos dat 25](#_Toc128345547)

[6.2 Škodlivost Wi-Fi 27](#_Toc128345548)

[6.3 použitá zařízení k propojení 29](#_Toc128345549)

[6.4 Propustnost sítě 31](#_Toc128345550)

[6.5 Oblast pokrytí 31](#_Toc128345551)

[6.5.1 Vzdálenost nemovitostí a pokrytí signálem 2. nemovitosti. 34](#_Toc128345552)

[6.6 Mobilita 36](#_Toc128345553)

[6.7 Uživatelé 37](#_Toc128345554)

[6.8 Logika síťového plánování 40](#_Toc128345555)

[6.9 Bezpečnost 40](#_Toc128345556)

[6.10 Vliv prostředí 40](#_Toc128345557)

[6.11 Finanční rozpočet – spotřeba energie, porovnávání cen poskytovatelů internetu a cena při změně přenosového média 43](#_Toc128345558)

[6.12 Monitoring stavu sítě 45](#_Toc128345559)

[6.12.1 Monitoring stavu sítě pomocí programu LANState 45](#_Toc128345560)

[6.12.2 Monitoring stavu sítě pomocí programu Algorius Net Viewer 47](#_Toc128345561)

[7 Správa a konfigurace aktivních prvků 50](#_Toc128345562)

[7.1 Zyxel 50](#_Toc128345563)

[7.2 Spoj 52](#_Toc128345564)

[7.3 3\_doma\_1 53](#_Toc128345565)

[7.4 4\_doma\_2 53](#_Toc128345566)

[7.5 5\_powerline 54](#_Toc128345567)

[8 Závěr 55](#_Toc128345568)

# Úvod

V začátcích využívání výpočetní techniky, kdy počítače byly velké a drahé a měly relativně omezenou kapacitu paměti RAM, docházelo k nejnutnější výměně dat prostřednictvím transportu sekundárního paměťového média (děrné pásky, děrných štítků, cívek s magnetickou páskou i kazet s diskovými kotouči). Později, když se počítače více rozšířily, se tento způsob komunikace ukázal jako nedostatečný. S pokrokem počítačové technologie docházelo stále častěji k tomu, že bylo více terminálů současně obsluhováno jedním procesorem. Byly vyvinuty techniky, umožňující připojit terminály na větší vzdálenosti prostřednictvím pevných linek i komutovaných telefonních linek. Centrální procesor bylo nevýhodné zatěžovat prací, spojenou s udržováním takovéto komunikace. Proto byly přidány front-end procesory pro tuto práci, hlavně procesor dostával pak čistá data ke zpracování.

Jednoduchá pravidla a o protokoly, realizující propojení u těchto homogenních systémů, byla většinou realizována hardwareově. Vzájemné propojení systémů od různých výrobců bylo takřka nemožné – byly zde odlišnosti počínaje mechanickými (konektor, kabel) a elektrickými parametry přes formáty dat, kódování, rychlosti přenosu, druhy přenosu atd. Majitelé výpočetních systémů se tak stali životně závislými na vývoji toho producenta výpočetní techniky, kterého si zvolili. S vývojem prvních integrovaných obvodů se výpočetní systémy stávaly menší, levnější a byly využívány na více odděleních u podniků. Zpravidla šlo o systémy od různých výrobců, specializované pro přesně určenou činnost. Jejich vzájemné propojení ovšem bylo zapotřebí. Rovněž výpočetní techniku v kancelářích a domovech bylo zapotřebí uschopnit ke komunikaci. K umožnění vzájemné komunikace vyvinuli výrobci techniku propojování vzájemně nezávisle, např. Digital vyvinul DECnet a IBM vyvinula SNA. Tak byla umožněna komunikace v relativně homogenním prostředí systémů a emulátorů jednoho výrobce, ale překročit hranice mezi výrobci stále nebylo možné.

Podpora pro vývoj protokolů a hardware, které by umožnily dobrou spolupráci sítí různých výrobců, přišla v USA v roce 1960 od vlády. Bylo zapotřebí sítě, vzájemně spojující počítačovou výbavu různých institucí (vládních, výzkumných, univerzit i obranných). Koncem šedesátých let byla první síť tohoto druhu, síť s přepínáním paketů ARPANET spuštěna (ARPANET – Advanced Research Projects Agency NETwork). Tato síť se v průběhu let sedmdesátých rozrostla, pokračovaly práce na protokolech skupiny TCP/IP, vznikla celosvětová síť Internet. Komerční implementace sítí s přepojováním paketů brzy následovaly.

S nástupem osobních počítačů jako kvalitativně nového způsobu využití výpočetní techniky četní výrobci těžili z možnosti realizovat homogenní lokální síť počítačů, připojených stejným způsobem. Dnes však nabývá velkého významu spojování různých lokálních sítí do větších celků a budování heterogenních sítí. Tyto lokální sítě se také napojují na rozsáhlejší firemní sítě, případně sítě globálního charakteru. To je umožněno existencí síťových standardů, užívaných shodně oběma výrobci zařízení, jež spolu komunikují, nebo standardizovaného způsobu připojování k rozsáhlejší síti.  
Některé síťové specifikace, jako Ethernet fy. Xerox, byly prověřeny spojováním produktů různých výrobců, řada jiných má přidány schopnosti napojení na odlišné typy sítí.

# Cíl práce

Tato práce se zabývá návrhem, správou, zabezpečením a konfigurací konkrétního bezdrátového propojení dvou domácností (dvou nemovitostí), za účelem sdílení internetového připojení, dat a tiskáren. Bezdrátový spoj je založen na normách IEEE 802.11, neboli WiFi (Wireless Fidelity). V teoretické část popíši krátkou historii vývoje bezdrátových sítí, následuje stručný popis normy IEEE 802.11. Dále je uveden přehled aktivních a pasivních prvků WiFi sítě, správa a konfigurace WiFi sítí a jejich zabezpečení. Závěrem v praktické části popíši vytvoření konkrétního bezdrátového spoje mezi nemovitostmi a jeho konfiguraci.

Teoretická část

# počítačové sítě

Sít' je spojením určitého hardwaru, softwaru a kabelů, které společně umožňují vzájemnou komunikaci různých počítačových zařízení. Pokud jsou počítače propojené s dalšími počítači a sdílejí společné prostředky, označujeme tuto skupinu počítačů jako počítačovou síť. Přitom není podstatné, zda jde o prostředky softwarové či hardwarové. Počítače mohou sdílet například data, zprávy, tiskárny, datové disky a další hardwarové zařízení.

## Rozvoj bezdrátových počítačových sítí

V sedmdesátých letech vznikla velká řada sítí s velkou rozlohou, srovnatelnou s rozlohou státu, kontinentu i sítí celosvětových. Pokud taková síť patří jedné organizaci a propojuje prakticky všechna její oddělení nebo pobočky, bývá nazývána "enterprise network". Pokud síť překračuje rámec komerční, vládní nebo jiné organizace či státu, nazývá se globální. Tehdy jde vždy o (někdy složitou) soustavu nestejnorodých sítí. Moderní sítě zakrývají síťový charakter uživateli, takže jsou z uživatelského hlediska jednoduché k používání.

Bezdrátové sítě se začali používat po roce 1992 s přenosovými rychlostmi, které byly, v porovnání rychlosti se současnými bezdrátovými sítěmi, velmi pomalé. Velkým problémem bylo, že nebyla jakákoliv standardizace bezdrátové komunikace. Výrobci si vyráběli vlastní bezdrátová zařízení, která byla vzájemně nekompatibilní.  
V roce 1997 byl schválen standard pro bezdrátové sítě IEEE 802.11 označován jako WiFi (Wireless Fidelity). Zavedením standardu došlo k velkému rozvoji tohoto odvětví. Vzájemnou kompatibilitou zařízení, došlo ke konkurenci mezi výrobci, a tím ke snížení pořizovacích nákladů na nákup a rozšiřování WiFi sítí.

Bezdrátové sítě normy 802.11 jsou jen částí skupiny sítí označovaných termínem WLAN (Wireless Local Area Network), které využívají přenosové medium radiové vlny, jež také využívá například televizní a rádiové vysílání. K jejich provozování je nutné, aby provozovatel měl licenci vydávanou patřičným regulačním úřadem. Každý vlastník licence dostává od regulátora přiděleno svoje frekvenční pásmo, na kterém může provozovat vysílaní. Bezdrátové sítě 802.11 využívají bezlicenční pásmo 2,4 GHz a 5 GHz.

Mezi zásadní výhodu WiFi sítí je především možnost snadno vytvořit počítačovou síť bez nutnosti pokládky kabelů. Příznivé ceny vedly k tomu, že uživatelé začali budovat velmi rozsáhlé komunitní sítě (např. VDFFREE, Výběžek.NET a podobné), pomocí nichž je možné sdílet data, hrát hry, a především sdílet širokopásmové připojení k internetu.

## Spojování počítačových sítí – internetworking

Pokud může být vývoj v počítačové technice po roce 1980 charakterizován propojováním počítačů do sítí, lze vývoj po roce 1990 zhodnotit jako spojování sítí počítačů do sousítí (internetworks). Zařízení, jež spojuje sítě, může být buď repeater (opakovač), bridge (můstek), router (směrovač) nebo gateway (brána). Správný název závisí na úrovni, které vrstvy OSI modelu zařízení pracuje. Tak na úrovni vrstvy fyzické pracuje repeater, na úrovni vrstvy linkové pracuje bridge, na úrovni vrstvy síťové pracuje router. Pracuje-li zařízení na úrovni jakékoli vyšší vrstvy než síťové, užívá se názvu gateway.

### OSI model

Open System Interconnection neboli propojování otevřených systémů) je standardem v počítačových sítích, vydanou normou standardizační organizací ISO v roce 1979. Model se skládá ze sedmi vrstev. Pro naši potřebu nás budou zajímat hlavně první tři vrstvy.

#### Fyzická vrstva (Phisic layer)

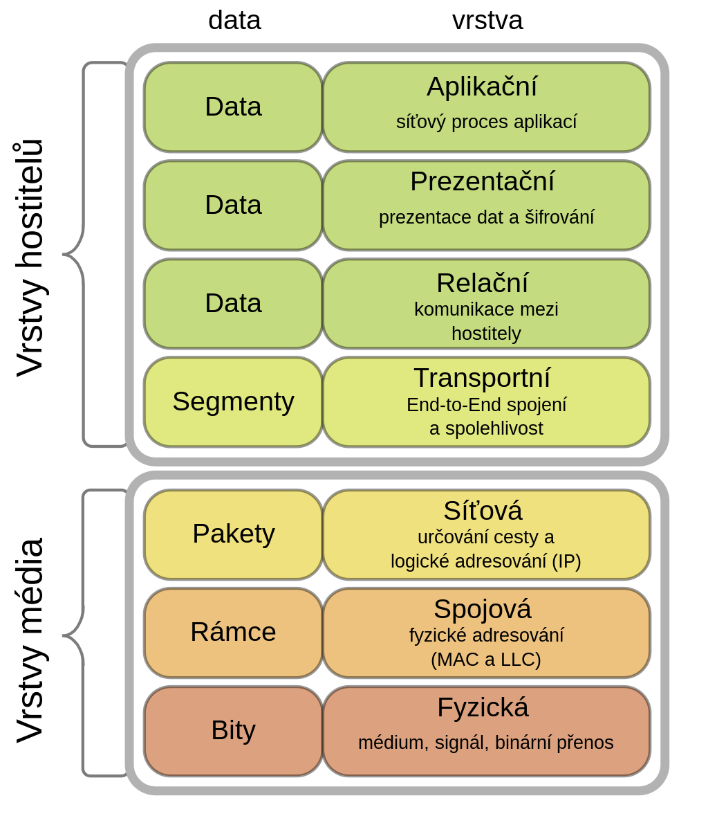
**n**ejnižší vrstva která zprostředkovává fyzický přenos dat v podobě bitů mezi odesílatelem a příjemcem. Řeší se zde především technické parametry, jako jsou elektrické signály definující 0 a 1, typy konektorů, druhy kabelů apod. Zabývá se také kódováním, modulací a synchronizací přenosu dat. Vyšší, spojové (linkové), vrstvě nabízí služby typu „přijmi bit“ a „odešli bit“ a musí zajistit, aby byl vyslaný jedničkový bit přijmut také jako jedničkový, nikoli nulový.

#### linková vrstva (Data link layer)

**t**ato vrstva bývá také označována jako **spojová** nebo **vrstva datového spoje**. Linková vrstva se stará o komunikaci mezi dvěma nebo více uzly, které spojuje stejný datový spoj. Funkce linkové vrstvy je zahájena nejčastěji přijetím dat z vyšší vrstvy. Z těchto dat vytvoří rámce, které dle potřeby seřadí, přiřadí jim MAC adresy a odešle fyzické vrstvě.

#### Síťová vrstva (Network layer)

**j**estliže vrstva spojová (linková) přenášela data jen u přímého spojení, vrstva síťová využívá tzv. směrování k přenášení dat dále než k sousedním uzlům. Data jsou zde členěna do tzv. **packetů**. Na rozdíl od rámců složených ze záhlaví, dat a patičky využívajících tzv. MAC adresu odesílatele a příjemce je packet blok dat s hlavičkou na úrovni síťové a vyšší vrstvy a jako adresy jsou zde používány IP adresy obou koncových účastníků a také informace o potvrzování nebo o řízení toku.



### Opakovač (repeater)

Překoná-li číslicový nebo analogový signál, nesoucí data, určitou vzdálenost, nutně se zvětší jeho zkreslení, či šumové pozadí a zmenší se jeho úroveň. Tím se ztěžuje možnost na přijímací straně správně interpretovat data. Zesílení signálu pomocí zesilovače příliš nepomůže, neboť se sice zvětší úroveň signálu, ale zůstává zkreslení a šum.

Repeater obnovuje kvalitu datového signálu. Neprovádí žádnou změnu ani NEZKOUMÁ obsah přenášených rámců. Provádí pouze reprodukci signálu. Proto říkáme, že pracuje na úrovni fyzické vrstvy.

Data, která opouštějí repeater, jsou přesnou kopií původního signálu, ale s lepšími elektrickými a časovými parametry. Teoreticky by počet repeaterů v cestě signálu mohl být neomezený, prakticky však tento počet bývá omezen.

### Můstek (bridge)

Bridge spojuje dva síťové segmenty na úrovní linkové vrstvy. Bridge zkoumá totiž FYZICKÉ ADRESY, přenášené v rámcích. Poté rozhoduje, zda rámec předá do následujícího segmentu na základě znalosti fyzických adres.

Protože vlastní bridge redukují neužitečné obsazení média, je výhodné je použít k rozdělení velmi zatížené sítě na menší segmenty. Za předpokladu, že větší část přenosů probíhá v rámci segmentů a nikoli mezi nimi, lze tak významnou část přenosové kapacity znovu získat.

Uvažujme například síť s několika sty stanic. Jak příslušná firma roste, zvětšují se i požadavky na síť a zatížení sítě přesáhne maximum. Síť již nepostačuje svou přenosovou kapacitou a práce na ní je zdlouhavá a obtížná. Tehdy může přijít ke slovu bridge, spojující segmenty v různých poschodích, o nichž je známo, že největší hustoty přenosu jsou v rámci nich. Tímto řešením můžeme dosáhnout dobrého provozu sítě.

Činnost bridge je následující:

- Přijetí všech dat ze segmentu A.

- Vypuštění všech paketů, jejichž příjemce je také na segmentu A.

- Vyslání všech zbývajících paketů do příslušných segmentů.

- Stejnou činnost opakovat pro data na jiných připojených segmentech.

Existují dva typy bridge: transparentní (někdy nazývané rozpínající se strom —spanning tree, nebo učící se – learning bridge) a se zdrojovým směrováním – source routing.  
Transparentní bridge nevyžadují žádné počáteční naprogramování. Během provozu se "naučí" umístění jednotlivých stanic na segmentech tím, že zkoumají adresu odesílatele a pamatují si, ze kterého segmentu paket přišel. Za provozu potom ignorují pakety, jež přišly ze segmentu, o němž vědí, že příjemce je na tomtéž segmentu. Ostatní pakety potom pošlou do správného segmentu.

Bridge se zdrojovým směrováním se používají u IBM sítí. Princip spočívá v tom, že celá cesta od zdroje k příjemci je již obsažena v paketu, zaznamenaná tam přímo odesilatelem. Činnost bridge je proto velmi jednoduchá. Na základě odpovědi na vyslané "průzkumné" pakety tak příslušnou cestu sestaví sám odesilatel.

### Směrovač (Router)

Routery pracují na úrovní síťové vrstvy. Mají proto přístup k informacím této vrstvy. Obvykle se na této úrovni pracuje s tzv. LOGICKÝMI ADRESAMI, jež se obecně (v praxi většinou) liší od adres fyzických. Logickou adresu tehdy přidělují správci sítě, zatímco fyzické adresy jsou většinou dány výrobci hardware. Přidělení logických adres lze tedy provést podle logiky uspořádání soustavy sítí.

Když routery posílají data přes sousítí, využívají logické adresy namísto fyzických. Dělení sousítí podle logických síťových adres se nazývá subnetting, jednotlivé díly pak podsítě (subnets). Podsítě nemusí být totožné s jednotlivými fyzickými segmenty.

Routery využívají jeden nebo více směrovacích algoritmů (routing algorithms) ke zjištění nejvhodnějšího dalšího směru paketů. Cesty mohou být vypočítávány v reálném čase (dynamicky), takže výběry cest se neustále přizpůsobují měnícím se podmínkám v síti. Dynamické směrovací algoritmy se liší faktory (metrikou), které uvažují pro optimální výběr cesty. Např. lze jako kritérium brát počet přeskoků (hops) neboli počet routerů, které je ještě třeba překonat na cestě k cíli. Jiný faktor může být doba přenosu (transit time). Moderní směrovací algoritmy uvažují více faktorů, každý s určitou váhou. Váhy může v některých případech upravovat správce sítě.

Jak je snad již patrno, routery typicky spotřebují pro svou činnost více strojového času než bridge. Výsledkem je pak menší propustnost routeru. Na druhé straně je způsob výběru cesty dokonalejší než u bridge. Existují i další rozdíly. Obecně nelze říci, zda je výhodnější bridge nebo router, rozhodnutí záleží na konkrétní situaci.  
Mnohé moderní routery jsou ve skutečnosti broutery. Jsou to routery, jež mají rovněž schopnosti bridge. Protože směrovací algoritmy jsou různé pro různé protokoly síťové vrstvy, podporují tyto routery většinu rozšířených protokolů síťové vrstvy včetně příslušných směrovacích algoritmů. Pokud do takového brouteru dorazí paket neznámého (nepodporovaného) protokolu, nedojde k jeho likvidací, ale zachází se s ním stejně, jako v bridge běžného typu.

Naopak někteří výrobci bridge nabízejí o něco "inteligentnější" bridge, jejichž chování má prvky routeru. Nejde ale o skutečné routery, neboť zacházejí pouze s daty linkové vrstvy. Velmi podstatným rysem routeru je také to, že síťová vrstva je nejnižší vrstva, na jejíž úrovní lze spojovat rozdílné hardwarové síťové platformy. Jinak řečeno, chceme-li spojit například sítě Ethernet, Arcnet a sériovou linku, můžeme to provést pomocí routeru, ale nikoliv bridgem.

### Brána (gateway)

V případě, že chceme propojit vzájemně odlišné sítě, jež se liší i v protokolu síťové vrstvy, popřípadě vyšších vrstev, nemůžeme provést propojení na úrovni síťové vrstvy. Spojovací zařízení, nazývané gateway, musí předávat data mezi nekompatibilními implementacemi protokolů, formátů dat atd. Gateway může být realizována buď jako "černá skříňka", jež se zapojuje mezi spojované sítě, nebo pomocí desky a programového vybavení, určených pro instalaci do stávajícího počítače. Tento druhý typ gateway může být buď vyhrazený (počítač je zcela zaměstnán funkcí gateway) nebo nevyhrazený.

## Typy sítí

Počítačové sítě můžeme rozdělit z více hledisek. Jedním z nich je rozdělení dle rozlehlosti a účelu, a to na sítě LAN, MAN, WAN a PAN.

### LAN

Dnešní moderní sítě LAN (Local Area Network – Lokální sítě) propojují širokou škálu počítačů a dalších zařízení. Jednotlivé LAN sítě se pak navzájem propojují do větších celků. Přenosové rychlosti LAN sítí se pohybují od desítek Mbit/s až po jednotky Gbit/s. Mezi LAN sítě patří například Ethernet, Fast Ethernet, Gigabit, bezdrátové sítě a jiné.

### MAN

MAN (Metropolitan Area Network) je označení pro metropolitní sítě. Propojují lokální sítě v městské zástavbě, slouží pro přenos dat, hlasu a obrazu. Spojují počítače na vzdálenost řádově jednotek až desítek km. Přenosová rychlost bývá vysoká a vychází z rychlostí LAN sítí.

### PAN

PAN (Personal Area Network) neboli osobní síť se označuje síť, která je tvořena propojením osobních elektronických zařízení, jakou jsou například mobilní telefony, PDA, notebooky a další. Rychlost PAN sítí zpravidla nepřekračuje jednotky Mbit/s. Pro tyto sítě je důležitější odolnost proti rušení, nízká spotřeba a snadná konfigurovatelnost. Mezi PAN sítě řadíme například Bluetooth nebo IrDA.

## Bezdrátová komunikace

Je to spojení dvou zařízení jiným způsobem, než mechanicky (kabelem). Většina bezdrátových sítí používá kabely k propojení bezdrátových komponent, částí svých segmentů a kabelové sítě. Takovéto kombinované sítě se také nazývají hybridní sítě.

### přenosové techniky

Pro přenos dat se u bezdrátových sítí využívají různé metody komunikace

#### Infračervené záření, IrDA

IrDA (Infrared Data Association) je technologie umožňující snadnou komunikaci mobilních zařízení na krátkou vzdálenost. Používá se například pro komunikaci mezi mobilními telefony, palmtopy atp. Komunikace pomocí IrDA vyžaduje přímou viditelnost, dosah je cca 1 metr a přenosové rychlosti se pohybují od 2,4 Kbit/s až 16 Mbit/s.

#### Laser

Pro komunikaci pomocí laseru se využívá dvousměrných teleskopů s rychlými transceivery, které mohou dosahovat rychlost až 2,5 GB/s. Je nutná přímá viditelnost mezi optickými jednotkami. Spojení není ohroženo deštěm ani sněžením, problém však nastává za mlhy.

#### Bluetooth

Bluetooth je bezdrátová radiokomunikační technologie pracující ve frekvenčním pásmu 2,4 GHz. Technologie Bluetooth spadá do kategorie osobních počítačových sítí PAN. Existuje několik verzí, které se liší dosahem a rychlostí přenosu. Datová propustnost se pohybuje kolem 1 Mbit/s a ve verzi Bluetooth 2.0 ERD má trojnásobek přenosové rychlosti. Bluetooth je určena především k bezdrátovému propojení počítače s jinými periferními zařízeními jako jsou například mobilní telefony, PDA atp.

#### Rádiové frekvence

Technologie založené na komunikaci pomocí radiových vln. Patří mezi nejrozšířenější a nejvíce využívané. Většina rádiových přenosů může probíhat na vzdáleností několika stovek až tisíce metrů a není omezena přímou viditelností.

## Přehled bezdrátové rádiové technologie

### Frekvence

Bezdrátové sítě využívající radiové viny pracují ve stanovených frekvencích. Používání radiofrekvenčních pásem však podléhá regulaci ze strany státních úřadů. V případě České republiky tato regulace podléhá ČTU (Český telekomunikační úřad). Většina vysílacího spektra podléhá licencím. Z tohoto důvodu musí WiFi sítě využívat jednoho ze dvou nelicencovaných pásem:

2,4 GHz v pásmu 2,412-2,472 GHz (1-13 kanálů, Evropa mimo Francii a Španělska)  
5 GHz v pásmu 5,15-5,725 GHz (1–79 (75) kanálů, Evropa)

Pásmo 5 GHz je velmi nepřehledné, má několik subpásem, které mají rozdílnou regulaci jak v Americe, tak v Evropě.

### Hlavní normy radiokomunikačních bezdrátových sítí

#### IEEE 802.11

The Institute of Electrical and Electronics Engineers (IEEE) sdružuje přes 350   
000 elektroinženýrů a informatiků v cca 150 zemích všech světadílů. Tato organizace vyvíjí a schvaluje normy pro širokou řadu počítačových technologií. Skupiny expertů navrhují nové normy, podle kterých pak výrobci vyvíjejí své výrobky. Číslo 802 slouží pro označení všech síťových norem, další číslo označuje podskupinu síťových norem (například číslo .11 slouží pro označení norem pro bezdrátové sítě).

Přijetím první normy s označením IEEE 802.11 se jednalo o radiovou normu pracující v pásmu 2,4 GHz s maximální propustností 2 Mbit/s. Norma byla dále zmodernizovaná a dostala označení 802.11 High Rate a dosahovala přenosových rychlostí až 11 Mbit/s. V roce 1999 došlo k dalšímu přejmenování této normy na 802.11b. Dále vznikla další norma s označením 802.11a, která přinesla vyšší rychlosti, odlišnou metodu rozprostřeného spektra a pracovala ve frekvenčním pásmu 5 GHz. V roce 2002 přibyla další norma 802.11g. IEEE schválilo poté další normu v oblasti bezdrátových lokálních sítí. Nejednalo se o čtvrtý typ, ale o doplněk ke specifikaci 802.11a určenou pro použití v Evropě.

##### 802.11b

Norma IEEE 802.11b je v podstatě vylepšená původní norma IEEE 802.11. O rychlé rozšíření této normy se postarala firma Apple Computer, která jako první zavedla dostupné výrobky založené na této normě. V roce 1997 ji uvedla pod názvem Air-Port. Sada se skládala z bezdrátového přístupového bodu a PC karty pro notebooky Macintosh. Díky tomu se technologie bezdrátových sítí značně zpopularizovala a rozšířila mezi širokou veřejnost. V dnešní době patří norma IEEE 802.11b stále mezi nejvíce rozšířené především z hlediska dostupnosti zařízení založených na této normě a oblíbeností mezi uživateli. Sítě založené na normě 802.11b pracují s maximální přenosovou rychlostí 11 Mbit/s.

##### 802.11a

Norma IEEE 802.11a byla schválena brzy po normě 802.11b v roce 1999. Práce na této normě začali sice jíž dříve, ale vyžádali si delší čas vzhledem ke složitějšímu přenosu na fyzické vrstvě. Norma pracuje na frekvenčním pásmu 5 GHz, teoretická přenosová rychlost je 54 Mbit/s. Výhodou této normy je, že využívá pásmo 5 GHz, které nabízí na rozdíl od často přeplněného pásma 2,4 GHz větší šířku a poskytuje více kanálů pro bezdrátovou komunikaci.

##### 802.11g

Norma IEEE 802.11g byla schválena v roce 2002. Maximální rychlost bezdrátových sítí založených na této normě je 54 Mbit/s. Pracuje ve frekvenčním pásmu 2,4 GHz. Další důležitou vlastností je zpětná kompatibilita s rozšířenou normou 802.11b.

##### 802.11n

Norma 802.11n přinesla revoluční zvýšení přenosových rychlostí. Cílem normy 802.11n je nabídnout uživatelům rychlosti dosahující minimálně 100 Mbit/s, v ideálním případě až 600 Mbit/s. Tohoto nárůstu přenosových rychlostí se dosáhne využitím více antén a změnou kódovacích schémat MAC protokolů.

### Topologie bezdratové sítě

Termín topologie se používá pro označení základního uspořádání sítě. Jedná se především o fyzické uspořádání počítačů a dalších komponent v síti. Zaměříme se na WiFi topologii.

WiFi sítě lze nastavit dvěma základními způsoby:

* IBBS (Independent Basic Service Set) — klienti se připojují mezi sebou navzájem
* BSS/ESS (Basic Service Set / Extended Service Set) — klienti se připojují k centrálnímu přístupovému bodu

#### IBBS (independent Basic Service Set), Ad-hoc sítě

IBBS též označován jako režim ad-hoc. Pracuje v režimu peer-to-peer to znamená, že ke své činnosti nepotřebuje přístupový bod. Tento režim je vhodný zejména pro dočasné propojení počítačů nebo pro sítě, jež obsahují malý počet bezdrátových klientů.

Původně byl režim ad-hoc určen pro rozsáhlé sítě s neúplnou viditelností, kde by každý uzel fungoval jako klient a zároveň jako směrovač předávající pakety dalším uzlům v síti. Tato myšlenka se ale příliš neujala a sítě v režimu ad-hoc se mnohem častěji používají jako dočasná náhrada rozbočovače (např. konference atp.). V tomto režimu stačí počítače pouze zapnout a propojit s kolegy. Nevýhodou tohoto řešení je slabá bezpečnost tohoto uspořádání.

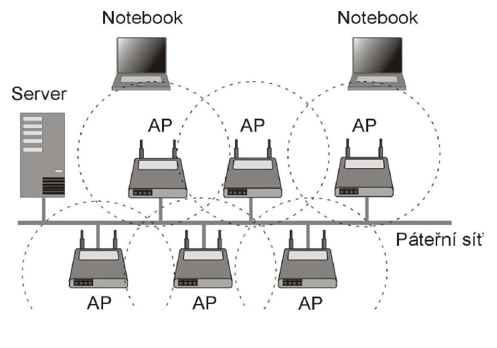
Obsah obrázku text, elektronika, interiér, počítač

Popis byl vytvořen automaticky

#### BBS (Basic Service Set) / ESS (Extended Service Set), infrastrukturní sítě

BSS (Basic Service Set) je základní soubor služeb pro sítě sestávající se ze zařízení, která jsou všechna ve vzájemném dosahu nebo v dosahu jednoho přístupového bodu.  
ESS (Extended Service Set) sítě s rozšířeným souborem služeb umožňují překrývání většího počtu přístupových bodů, což značně rozšiřuje dosah jedné sítě.  
BSS/ESS přístupové body fungují v rámci ESS jako mosty mezi sítěmi BSS, které tvoří ESS, přičemž umožňují každé stanici v síti komunikovat s jakoukoliv jinou stanicí a dále umožňují mobilním stanicím pohyb mezi segmenty dané sítě. Všechny přístupové body musí být nastaveny jako členové jedné sítě (tj. mají stejný název sítě, stejné bezpečnostní nastavení atp.). Každý přístupový bod komunikuje na jiném kanálu z důvodů rušení mezi přístupovými body. Toto uspořádání umožňuje mobilní stanici, která se dostane mimo dosah svého přístupového bodu jeho nové automatické přidružení k jinému přístupovému bodu, který je v dosahu stanice. Při návrhu sítě je vhodné umístit jednotlivé přístupové body tak, aby se jejich oblasti pokrytí překrývaly, čímž se zabrání mezerám v přístupu pro pohybující se stanice.

Pro společnou práci přístupových bodů je nutné, aby podporovaly protokol vzájemné komunikace přístupových bodů IAPP (Inter Access Point Protocol). Protokol zajišťuje, aby všechny přístupové body v ESS věděly o všech stanicích připojených k ostatním přístupovým bodům.



## Hardwarové vybavení bezdrátových sítí

### Přístupový bod (Access point)

Obsah obrázku text

Popis byl vytvořen automatickyPřístupový bod nebo také AP (Access Point) zajišťuje přístup bezdrátových zařízení k lokální síti, přístup na internet, most mezi bezdrátovými zařízeními a kabelovými sítěmi atd.

Většina přístupových bodů jsou malé skřínky s jednou či více anténami. Bez ohledu na design jsou všechny z hlediska své vnitřní struktury stejné. Každý přístupový bod obsahuje minimálně jeden rádio přijímač/vysílač pracující na frekvenci podle norem 802.11, programové vybavení pro řízení přístupového bodu a bezdrátové sítě (firmware) a porty pro připojení přístupového bodu ke kabelové sítí (LAN port) a k internetu (WAN port). Další nezbytnou součástí přístupových bodů je anténa, která je interní nebo externí.

Obsah obrázku text, elektronika

Popis byl vytvořen automaticky

#### Komunikační porty

Přístupové body zpravidla obsahují ethernetový WAN port pro širokopásmové připojení na internet ať už přes kabelový nebo DSL modem. Dále obsahují několik LAN portů k připojení lokální sítě. K LAN portům lze připojit rozbočovač (HUB), který může být také nahrazen přepínačem (Switch). LAN porty přístupových bodů jsou zpravidla přepínanými porty.

#### Antény

Součástí přístupových bodů je jedna nebo dvě malé antény, které umožňují spolehlivou komunikaci zařízení v řádu několika desítek metrů. Většina přístupových bodů také obsahuje port pro připojení externí antény pro zvětšení dosahu. Připojením výkonné externí antény lze dosah WiFi sítě zvětšit na stovky metrů, v extrémních případech až na několik kilometrů.

#### Důležité vlastnosti přístupových bodů

* Administrace příjmů
* Firewall
* Šifrování WEP/WPA/WPA2
* DHCP/NAT

Bližší popis vlastností přístupových bodů v následujících kapitolách

### Bezdrátový opakovač (repeater)

Bezdrátový opakovač přijímá bezdrátový signál od zdroje, provádí jeho zesílení a dále ho vysílá do cílového místa. Opakovače se používají v případech, kdy je potřeba rozšířit oblast pokrytí bezdrátové sítě.

### WiFi Síťového adaptéru

Každý síťový adaptér obsahuje radiostanici a konektor který odpovídá jednomu I/O portu daného počítače. Často síťové adaptéry obsahují malou anténu pro zvýšení dosahu nebo konektor pro připojení externí antény.

#### Součásti síťového adaptéru

Každý síťový adaptér obsahuje radiostanici a konektor který odpovídá jednomu I/O portu daného počítače. Často síťové adaptéry obsahují malou anténu pro zvýšení dosahu nebo konektor pro připojení externí antény.

#### Druhy síťových adaptérů

##### PCMCIA karty

Přenosné počítače mohou obsahovat jeden nebo více PCMCIA slotů pro PC karty Type II. Většina WiFi radiostanic jsou karty typu Type II slučitelné s Card Bus, což je 32bitová verze PCMCIA.

Výhody PCMCIA síťových adaptérů jsou v jejich snadné instalaci, kompaktních rozměrech, kompatibilitě a v neposlední řadě také v ceně těchto zařízení. Použití je implicitně pro notebooky a jiná přenositelná zařízení vybavená PCMCIA slotem.

##### PCI síťové adaptéry

Jsou určeny především pro stolní PC, komunikace probíhá přes PCI sběrnici. Výhodou těchto zařízení je, že s nimi lze vybavit téměř jakýkoliv stolní počítač PC. Většina z nich má výstup pro externí anténu pomocí reverzního SMA konektoru. V dnešní době čím dál více výrobců integruje WiFi síťové adaptéry do základních desek. WiFi adaptér se tak stává standardním vybavením PC.

##### USB síťové adaptéry

Jsou WiFi adaptéry, které se připojují k počítači přes USB sběrnici, kterým je vybaven každý stolní počítač i notebook. Díky tomu jsou USB adaptéry nejflexibilnějším druhem adaptéru, pomocí něhož se může počítač připojit do WiFi sítě. Nevýhodou USB adaptérů je, že v naprosté většině nejsou vybaveny žádným konektorem pro připojení externí antény. Své uplatnění USB adaptéry nacházejí při použití v kancelářském a domácím prostředí, kde je dobře dostupný signál bezdrátové sítě.

Obsah obrázku text

Popis byl vytvořen automaticky

### Antény

Základní funkcí antén je, že zvyšují dosah a pokrytí WiFi sítí. Jednou z nejdůležitějších věcí, které je nutné v souvislosti s anténami chápat je, že antény nezesilují signál. Slouží pouze k tomu, že vyzařovanou energii zaostřují do určitého směru.

Některé síťové adaptéry a přístupové bodů se dodávají s malou anténou nebo s vestavěnou a tím jsou často velmi slabé. Někteří výrobci notebooku dodávají počítače s integrovanou anténou, která je uložena v těle notebooku nejčastěji uvnitř LCD displeje, což z části eliminuje nevýhody slabých antén dodávaných se síťovými adaptéry.

Pak jsou zde přístupové body a síťové adaptéry podporující připojení externí antény, která nahrazuje antény dodávané výrobci těchto zařízení jako součást balení. To umožňuje zvýšit dosah přístupových bodů až na několik kilometrů při vhodném umístění antény ([např. na](http://např.na) střeše).

#### Charakteristické vlastnosti společné pro všechny typy antén

* Šířka frekvenčního pásma (bandwidth) - jedná se o frekvenční pásmo (např. 2,4GHz pro normy 802.11b/g/n a 5GHz pro normu 802.11ac), kdy každá anténa je díky své velikosti a typu vhodná pro konkrétní frekvenci.
* Zisk (gain) - popisuje stupeň směrovosti antény. Směrové antény směřující signál přímočaře mají větší zisk než antény, které distribuují signál v širším diagramu. Zisk se měří v decibelech (dB).
* Vyzařovací diagram (radiation pattern) - slouží pro označení diagramu vyzařovaní antén v prostoru. Směrové antény provádějí modulaci lineárně ve směru zaměření antény, naopak všesměrové antény pokrývají kruhový prostor.
* Úhel vyzařování (beam width) - úhel vyzařování se vyjadřuje ve stupních a vztahuje se obvykle k vodorovné rovině. Úhel vyzařovaní lze použít pro výpočet oblasti pokrytí signálem.
* Polarizace (polarization) - elektromagnetické vlny lze vysílat buď s vertikální nebo s horizontální polarizací. Polarizace antén mezi vysílačem a přijímačem musí být stejná, aby se předešlo vytváření signálového šumu a ztrátám anténního zisku.

#### Typy antén

Výběr antény závisí na jejím použití. Na výběr jsou jak malé antény vhodné zejména k notebookům, tak velké antény určené pro montáž na střechy. Výběr antény je vždy určitým kompromisem mezi oblastí jejího pokrytí a sílou signálů.

##### Všesměrové antény

Jak už název těchto antén napovídá všesměrové antény vyzařují signál všemi směry. Obvykle jsou tyto antény sloupcového tvaru a umísťují se ve vertikální poloze. Výhodou těchto antén je, že pokrývají velkou oblast a jsou vhodné tam, kde jsou zařízení rozprostřena v kruhovém prostoru. Čím větší zisk má všesměrová anténa, tím plošší signál vyzařuje. Nevýhodou tohoto typu antén je, že v bezprostřední blízkosti a pod úrovní této antény se nalézá mrtvé místo.

##### Sektorové antény

Jsou obdobou všesměrových antén. Narozdíl od nich je jejich úhel vyzařování maximálně 180 stupňů. Jelikož jsou sektorové antény směrovější, dosahují také většího zisku a jsou méně citlivé na šum než všesměrové antény. Sektorové antény jsou vhodné tam, kde všechna zařízení leží v jednom směru.

##### Panelové antény

Jsou ploché antény s pevnou konstrukcí. Podobně jako ostatní směrové antény jsou i tyto vysoce směrové a hodí se k propojení dvou přístupových bodů.

##### Parabolické antény

Jsou ploché antény s pevnou konstrukcí. Podobně jako ostatní směrové antény jsou i tyto vysoce směrové a hodí se k propojení dvou přístupových bodů.

# Správa sítí

## Možnosti konfigurace přístupových bodů

* Klientský software – používá se zpravidla pro platformu Windows, bývá zpracován formou tzv. „wizardů", neboli průvodců, kteří provedou uživatele kompletní instalací krok za krokem.
* SNMP (Simple Network Management Protocol) - označuje síťový protokol a standard zpřístupňující dohodnuté postupy, pravidla a architekturu pro management sítě TCP/IP a jejich síťových prvků. Vyžaduje základní znalosti terminologie a je méně uživatelsky přátelský oproti klientskému softwaru.
* Webové rozhraní – patří mezi nejrozšířenější způsoby konfigurace přístupových bodů. Webový prohlížeč, který je standardní součástí každého operačního systému, umožňuje snadnou konfiguraci a správu přístupového bodu.

## Přístup na internet

Přístupový bod umožňuje sdílení přístupu na internet. Způsoby, jakými se přístupový bod autorizuje a konfiguruje připojení do sítě internet jsou:

* Automatické získání IP Adresy. Přístupový bod si vyžádá od serveru IP adresu a tu si
* Statická IP adresa. Poskytovatel internetového připojení Vám přidělí permanentní veřejnou IP adresu. Většinou je placená.

## DHCP server

DHCP server poskytuje počítačům připojeným ať už bezdrátově nebo kabelem přístup na síť přes TCP/IP protokol. Každému počítači na síti přiřazuje IP adresu, která slouží k jeho identifikaci. IP adresy přiděluje dynamicky (při každém připojení počítače do sítě) nebo staticky (permanentně přidělená IP adresa). V kombinaci s překladem síťových adres NAT (Network Address Translation), který umožňuje, aby několik počítačů sdílelo jednu veřejnou IP adresu. Všechny počítače připojené do sítě tak mohou využívat jednu veřejnou IP adresu přiřazenou od poskytovatele.

## Veřejné a privátní IP adresy

Veřejné IP adresy přiděluje poskytovatel a slouží k jednoznačné identifikaci na internetu (vnější sít'). Privátní IP adresy se používají k identifikaci počítače v lokální síti (vnitřní síť) a nejsou na internetu rozpoznávány. Pokud chceme sdílet připojení k internetu, musíme za jednu veřejnou IP adresu, kterou obdržíme od ISP schovat lokální síť. Ke sdílení veřejné IP adresy slouží směrovací funkce přístupového bodu NAT. DHCP server přiřadí každému počítači v lokální síti privátní IP adresu a sám se připojí na internet pomocí veřejné IP adresy. Přístupový bod tak předává internetové pakety počítačům na lokální síti. Všechny počítače jsou pak připojeny přes jednu veřejnou IP adresu.

## Firewall

Firewall chrání počítač před vnějším napadením a nežádoucím průnikům do sítě z internetu. Tuto činnost vykonává blokováním prostředků, které využívají specifické internetové a síťové aplikace.

Internetové aplikace (např. elektronická pošta, web, FTP atd.) používají pro komunikaci takzvané komunikační porty. Každá aplikace pro svoji komunikaci má přiřazena čísla portů, které používá pro svojí komunikaci. Každý port je očíslován (např. webový prohlížeč používá port 80, FTP (File Transfer Protocol) používá port 21 atd.

Jestliže je port na počítači otevřen může s ním navázat komunikaci kdokoliv, kdo zná IP adresu daného počítače. Buď prostřednictvím aplikace k tomuto účelu určené (např. v případě portu 80 to je webový prohlížeč) nebo pomocí speciálního softwaru, který umí detekovat otevřené porty. Případný útočník může prostřednictvím těchto nástrojů do počítače proniknout.

Firewall umožňuje zablokovat všechny nestandardní porty, které uživatel nepotřebuje, a tak chránit počítače před nežádoucími návštěvníky. Také umožňuje nastavit přístup na určité porty jen z určitých portů.

Firewall přístupového bodu chrání síť proti průnikům z internetu prostřednictvím blokování komunikace, která přichází z portu WAN (vnější síť). Počítače, které jsou připojeny za tímto firewallem tedy na lokální síti (vnitřní síť) jsou chráněny prostřednictvím tohoto firewallu proti průnikům z internetu, ale komunikace na úrovni lokální sítě (vnitřní síť) probíhá bez omezení.

Firewall přístupového bodů neobsahuje tolik funkcí jako softwarový firewall.

## Demilitarizovaná zóna

Demilitarizovaná zóna umožňuje, aby počítač ve vnitřní síti byl viditelný a přístupný z internetu bez ochrany firewallu. V tomto nastavení bude přístupový bod směřovat veškerou komunikaci na počítač v DMZ bez kontroly a omezení. Toto nastavení se používá při provozu webových či e-mailových serverů. Většina přístupových bodů podporuje pouze jeden počítač v DMZ.

## Přesměrování portů

Přesměrování portů (Port forwarding) představuje možnost, jak na vnitřní síti provozovat služby dostupné z internetu. Přesměrování portů umožní vybrat jeden nebo více počítačů a jeden nebo více specifických portů, které budou k dispozici pro vnější síť (internet), zatímco zbývající část vnitřní sítě zůstane chráněna. Počítač, na který je provoz přesměrován, musí mít nastavenou statickou IP adresu. Přesměrování portu využívají například on-line hry, IP telefonie, P2P klienti a mnoho dalších podobných aplikací.

## Filtrování

Řada přístupových bodů nabízí možnost filtrování služeb a přístupu na internet. Filtry umožňují blokování určitých serverů, omezení přístupu na základě klíčových slov nebo zdrojové domény, omezit přístup na internet v určitých hodinách a také na určité porty.

## VPN (Virtual Private Network)

VPN umožňuje počítačům připojeným k internetu bezpečně přistupovat k prostředkům privátní (vnitřní) sítě. K privátní síti přistupují počítače prostřednictvím nedůvěryhodné transportní sítě nejčastěji internetu, přičemž dochází k šifrování všech dat přenášených ze vzdáleného počítače na privátní síť. Tato služba umožňuje, aby například zaměstnanci využívali privátní firemní sít', když se nacházejí mimo kancelář. VPN zajišťuje větší bezpečnost přenášených dat než bezpečnostní mechanismy normy 802.11. Existuje celá řada protokolů VPN mezi nejpoužívanější patří protokoly PPTP a L2TP, především z důvodu podpory operačního systému Windows. Je nutné si ověřit u správce VPN sítě, jaký druh přístupu podporuje.

## DNS (Domain Name Systém)

DNS je protokol, který jménům domén, která jsou snadno zapamatovatelná pro lidi, přiřazuje IP adresy, kterým zase rozumí počítače. Napíšeme-li do prohlížeče adresu nějaké stránky (např. www.google.cz), musí počítač nejprve zjistit, na jaké IP adrese nalezne server, který požadovanou stránku obsahuje. První dotaz je směrován na kořenový DNS server, zda zná IP adresu serveru. Ten ji sice nezná, ale ví, který server zná IP adresu serverů v doméně .cz. Postupným dotazováním nakonec počítač vyhledávanou IP adresu získá a spojí se s www serverem na vyhledané adrese, kde stáhne obsah stránky k zobrazení. Avšak pokud by dotazování probíhalo vždy celé, bylo by to zbytečně zdlouhavé. Proto se počítač rovnou dotáže vyrovnávacího DNS serveru, zda se již někdo dotazoval na stejnou adresu. Celý proces trvá velmi rychle.

## Cisco Packet Tracer

Cisco Packet Tracer je software simulátor sítě, který umožňuje uživatelům vytvářet, konfigurovat, testovat a vizualizovat různé sítě. Tento software je navržen tak, aby byl přístupný pro učitele, studenty a profesionály, kteří se učí o síťových technologiích a potřebují prostředí pro praktické cvičení.

Cisco Packet Tracer obsahuje různé síťové prvky, jako jsou směrovače, přepínače, koncové zařízení a další, které mohou být umístěny a propojeny pomocí grafického rozhraní. Uživatelé mohou také konfigurovat různé parametry těchto síťových prvků, jako jsou IP adresy, protokoly a další.

Další výhodou Cisco Packet Tracer je, že umožňuje uživatelům simulovat různé scénáře a testovat, jak se sítě chovají v různých situacích. Software také umožňuje uživatelům vytvářet vlastní laboratoře a projekty, které mohou sdílet s ostatními uživateli.

Celkově lze říci, že Cisco Packet Tracer je užitečný nástroj pro výuku a trénink síťových technologií a umožňuje uživatelům prakticky experimentovat s různými síťovými scénáři.



# Bezpečnost sítí

Bezdrátová sít' má oproti kabelovým sítím jednu bezpečnostní nevýhodu, vycházející z principu komunikace těchto sítí. Na rozdíl od kabelových sítí na to, aby někdo mohl odposlouchávat komunikaci v bezdrátové síti stačí, aby zachytil vysílaný signál.

Pomocí dalších nástrojů nebo programů volně dostupných na internetu může útočník snadno zachytávat hesla a další citlivá data.

Mezi další bezpečnostní rizika bezdrátových sítí patří zabránění neautorizovanému přístupu do sítě.

Bezpečnost bezdrátových sítí lze rozdělit do dvou hlavních skupin:

* Šifrování – zabezpečení přenášených dat proti odposlechnutí.
* Autentizace – zabezpečení proti neoprávněným přístupům.

## Šifrování

### WEP (Wired Equivalent Privacy)

Většina bezdrátových sítí pro své zabezpečení používá WEP. Jedná se o standard zajišťující bezpečnost bezdrátové sítě na úrovni radiové části. To znamená na úroveň přístupového bodu, za ním již bezpečnost není zajišťována a musí být realizována jinými prostředky (např. HTTPS, SSH, VPN).

I přestože protokol WEP má řadu zranitelných míst, která výrazně omezují jeho schopnost chránit přenášená data, představuje WEP základní zabezpečení pro bezdrátové sítě nepřenášející důležitý obsah.

### WPA (WiFi Protected Access)

WPA je nový bezpečnostní mechanismus ratifikovaný WiFi Aliancí. Původně byl WPA vyvíjen jako bezpečnostní norma 802.11i. Bylo nutné však co nejdříve vydat nový bezpečnostní protokol, a tak došlo k tornu, že se vzalo to, co už bylo hotovo v normě 802.11i a vznikl WPA, který je v podstatě podmnožinou normy 802.11i. WPA lze implementovat prostřednictvím aktualizace firmwaru a softwaru. Obsahuje nástroje šifrování TKIP (Tempoval Key Integrity Protocol) a řízení přístupu (802.1x).

TKIP využívá stejného algoritmu šifrování jako WEP, používá standardně 128 bitový klíč a dočasné dynamické klíče, které pomocí automatického mechanismu mění každých 10 000 paketů. Dále TKIP obsahuje vylepšenou funkci kontroly integrity MIC (Massage integrity Code) a vylepšená pravidla generování inicializačního vektoru včetně sekvenčních pravidel.

WPA představuje řešení všech známých problémů protokolu WEP.

### AES

AES (Advanced Encryption Standard) nabízí různé režimy činností, ve specifikaci 802.11i používá čítačový režim s protokolem CBM-MAC (Cipher Block Chaining ­Message Authentication Code) obvykle označovaný jako AES-CCMP (AES-Counter Mode CBC-MAC Protocol), který zajišťuje šifrování. CBC-MAC pak zajišťuje autentizaci a integritu dat.

AES šifra pracuje se symetrickým klíčem, což znamená, že text šifruje i dešifruje stejným sdíleným tajným klíčem, ale na rozdíl od šifry RC4 pracuje s bloky o velikosti 128 bitů a bývá také označována jako bloková šifra. Celý vstupní text se rozdělí na 128 bitové bloky. Ty se postupně XORují se 128 bitovým pokaždé nově generovaným výstupem AES tak dlouho, dokud není celá zpráva zašifrována. Nakonec se čítač vynuluje a XORuje se hodnota MIC, která se přidává na konec rámce.

CCPM obsahuje algoritmus MIC, zajištující ověření, že nedošlo k modifikaci přenášených dat. Výpočet MIC je založen na hlavičkových hodnotách vycházející z inicializačního vektoru a z dalších hlavičkových informací ve 128 bitových blocích a počítá se přes jednotlivé bloky až na konec zprávy, kde se vypočte konečná hodnota.  
Výsledkem je mnohem silnější šifra, která má však zvýšené nároky na výkon. Z tohoto důvodu vyžaduje AES nový hardware a není tudíž zpětně kompatibilní s první generací bezdrátových zařízení.

## Autentizace

### Open – system

Tato metoda autentizace spočívá v tom, že přístupový bod přijme klientské zařízení na základě údajů, které mu poskytne, aniž by je ověřoval. Klient posílá svojí identifikaci v podobě SSID (Service Set Identifier). U přístupových bodů se doporučuje SSID vypnout, a to z toho důvodu, že přístupový bod, který SSID vysílá, může každá stanice přijmout a použít pro neoprávněný přistup do sítě.

### Shared – key

Autentizace se sdíleným klíčem. Princip této autentizace je, že každé zařízení, které chce přistupovat do sítě, se musí prokázat přístupovým klíčem. Přístupový bod ověří platnost tohoto klíče a pak zařízení autentizuje. Ověření probíhá tak, že přístupový bod odešle náhodné číslo, bezdrátový klient toto číslo zakóduje algoritmem RC4 s pomocí přístupového klíče a odešle zpět přístupovému bodu, který je dekóduje. Pokud se dekódované číslo rovná odeslanému číslu, je klient autentizován.

Standard 802.11 vyžaduje, aby každé zařízení s implementovaným WEP zabezpečením bylo také schopno užívat autentizaci se sdíleným klíčem.

### Filtrování adres

Autentizace založená na filtrování MAC adres spočívá v tom, že administrátor sítě může pro každý přístupový bod zadat seznam MAC adres, jimž je povolen přístup do bezdrátové sítě. MAC adresa je unikátní adresa každého síťového zařízení a slouží k jeho jednoznačné identifikaci.

Existují i jiné varianty založené na autentizaci pomocí MAC adres. Například lze vytvořit seznam MAC adres, kterým je naopak přistup do sítě zakázán, omezit přístup časově nebo umožnit používat jen určitou šířku pásma atp.

Problém autentizace pomocí filtrace MAC adres je, že MAC adresa jako jednoznačný identifikátor je uložena v programovatelné paměti, lze ji tudíž měnit a tím obejít filtrování. Z tohoto důvodu se také více prosazuje používání seznamů MAC adres, které mají přístup do sítě povolen než naopak. Je obtížnější pro případné útočníky zjistit MAC adresu, která má přistup do sítě povolen než si náhodně upravit MAC adresu, která má přístup do sítě zakázán.

## Základní kroky k zabezpečení WiFi sítě

* + Aktualizace firmware – pravidelnou aktualizací firmwaru lze odstranit řadu bezpečnostních problémů. Firmware lze stáhnout z domovských stránek výrobce přístupového bodu.
  + WEP/WPA/ WPA2 – aktivujte minimálně WEP šifrování. Pokud je to možné přejděte na vyšší bezpečnostní normu.
  + SSID – zrušte vysílání SSID, mnoho přístupových bodů umožňuje vypnout SSID broadcast, tím se docílí toho, že většina WiFi zařízení síť neuvidí.
  + Filtrace MAC adres – filtrace MAC adres je poměrně dobrá metoda k zvýšení zabezpečení sítě, doporučuje se vytvořit seznam MAC adres s povoleným přístupem než naopak.
  + Firewall - pomocí firewallu oddělte přístup z vnitřní sítě do internetu.
  + VPN - pokud je to možné, používejte přístupové body s podporou IPSec, které mohou zajišťovat bezpečný tunel mezi přístupovým bodem a koncovým uživatelem.
  + Access point - zajistěte přístup k administraci přístupového bodu heslem a často toto heslo měňte.

Praktická část

# Návrh konkrétního bezdrátového propojení

Při plánování a návrhu propojení LAN sítí, jsem si nejdříve ujasnil požadavky tohoto propojení:

## Volba média pro přenos dat

přenos dat se v počítačových sítích (a samozřejmě nejen zde) děje pomocí vlnění a používají se primárně tři přenosová média:

* + metalické kabely – přenos pomocí elektrického potenciálu
  + optické kabely – přenos pomocí světla
  + vzduch (vzduchoprázdno) – bezdrátový přenos, např. WiFi

Bezdrátový přenos jsem popsal výše, a proto krátce popíši první dvě kategorie, které by připadaly v úvahu při vytvoření propojení a rozvodech v nemovitostech.

U metalických kabelů se zmíním pouze o kroucené dvojlince.Kroucená dvojlinka (Twisted Pair), používá se zkratka TP, je tvořena čtyřmi páry vodičů, které jsou po celé délce pravidelným způsobem zkroucené. Zlepšují se tím elektromagnetické vlastnosti kabelu, minimalizují se přeslechy a omezuje vyzařování elektromagnetického záření. Každý vodič má ochrannou izolaci a všechny vodiče jsou společně zabaleny do pláště. Jsou k dispozici různé kategorie kabeláže, definující minimální parametry, které jsou kladeny na kabely. Určuje různé úrovně výkonu, co se týče šířky pásma signálu, útlumu a přeslechů. Obecně čím vyšší kategorie, tím podporuje vyšší přenosové rychlosti. Nejrozšířenější **kategorií je Cat5e**, pro FastEthernet (využívá dva páry) a GigabitEthernet (využívá všechny čtyři páry) zakončené konektorem RJ45.

Optický kabel (Optical Fiber Cable) je tvořen jedním nebo více optickými vlákny (optical fiber), která přenáší světelný paprsek od zdroje k cíli s co nejmenší ztrátou. Optické vlákno obsahuje jádro (core), které má tloušťku 9 nebo 50 nebo 62,5 µm, tvořené oxidem křemičitým. A obložení z jiného druhu skla, které má nižší index lomu, takže se signál odráží zpět, o tloušťce 0,125 mm. Pak následuje primární ochrana a tloušťka je 0,25 mm. Optická vlákna sdružujeme do optických kabelů a přidáváme řadu ochranných vrstev (často PVC), podle toho, do jakého prostředí jsou určeny. Jako u metalických kabelů existují kategorie optických vláken. Vždy je podporována určitá standardní přenosová rychlost na danou minimální vzdálenost (třeba MMF vždy podporuje FastEthernet alespoň na 2 km), ale funguje i vyšší rychlost na vzdálenost kratší.

Single-mode Optical Fiber (označení OS)

U SMF vláken se udává maximální koeficient útlumu v dB na km a znamená pokles signálu na jeden kilometr:

* + OS1 – útlum 1 dB/km
  + OS2 – útlum 0,4 dB/km

Multi-mode Optical Fiber (označení OM)

U MMF vláken se udává minimální modální šířka pásma, tedy jeho kapacita v MHz na vzdálenost jednoho kilometru:

* + OM1 - jádro 62,5 µm, šířka pásma 200 MHz-km při 850 nm (pro 1300 nm je vyšší), běžně se používá pro FastEthernet na vzdálenost 2 km
  + OM2 - jádro 50 µm, šířka pásma 500 MHz-km při 850 nm, běžně se používá pro GigabitEthernet na vzdálenost 550 m
  + OM3 - jádro 50 µm, šířka pásma 2000 MHz-km při 850 nm, běžně se používá pro 10GigabitEthernet na vzdálenost 300 m, přechází se z LED na VCSEL lasery
  + OM4 - jádro 50 µm, šířka pásma 3500 MHz-km při 850 nm, nejnovější standard podporuje 40 a 100GigabitEthernet na vzdálenost 150 m, optimalizováno pro laser

Výhody a nevýhody:

* + metalické kabely
* relativně levné a méně náchylné k poškození (poloměr ohybu 2-3cm)
* běžné standardy jsou pro vzdálenosti do 100m (bez aktivního prvku, počítá se 90m kabelový rozvod a na každé straně dva konektory a patch kabel 5m)
* podporuje napájení po datovém kabelu (Power over Ethernet, IEEE 802.3af PoE 15,4W, IEEE 802.3at PoE+ 30W)
* náchylné k elektromagnetickému rušení (EMI), i když se provádí různé stínění
* rychlosti dnes běžně do 10Gbps

optické kabely (Optical Fiber Cables)

* dražší kabely (i celá technologie) a náročnější pro manipulaci (poloměr ohybu 8 cm)
* pro dlouhé vzdálenosti (záleží na typu, ale možno i 100km, s dalšími technologiemi jde i o sotvky km)
* imunní vůči elektromagnetickému rušení – EMI
* nižší zpoždění (latence) a možné větší přenosové rychlosti (dnes 100Gbps na jednom vlákně)
* menší energetická náročnost

Když jsem vzal v potaz výše uvedené výhody a nevýhody, včetně bezdrátového přenosu, rozhodl jsem se pro bezdrátový spoj pomocí bezdrátové technologie WiFi, která je na vytvoření spoje časově nejméně náročná (výkopové práce při pokládce chráničky kabelu) a z nižších finančních nákladů. Jelikož většina zařízení v domácnostech jsou přenosná, nebylo nutné vytvářet rozvody po nemovitostech.

## Škodlivost Wi-Fi

Naší životní součástí se staly Wi-Fi sítě, které jsou všude kolem nás a vytváří obavy, jestli to není pro naše zdraví škodlivé.

Někteří lidé tvrdí, že jsou velmi náchylní na přítomnost bezdrátového Wi-Fi signálu a cítí díky němu lehkou až silnou nevolnost, trpí na bolesti hlavy a migrény.

Mnozí z těchto jedinců proto z obav před Wi-Fi prchají do lesů a routerů, kteří signál šíří, se bojí natolik, že se k nim raději ani nepřibližují. Jejich protipólem pak jsou lidé, kteří tvrdí, že internetový signál je pro člověka zcela neškodný a na jejich zdraví nemá žádný vliv.

Názor skupiny lidí, která tvrdí, že Wi-Fi sítě jsou bezpečné.

Před několika lety Mezinárodní agentura pro výzkum rakoviny [rozhodla](https://www.iarc.who.int/wp-content/uploads/2018/07/pr208_E.pdf) o zařazení Wi-Fi sítě do rizikové třídy 2B. Znamená to, že riziko vzniku karcinogenních onemocnění, působení Wi-Fi je zhruba stejně nebezpečné, jako účinky plastových obalů pro naše potraviny, konzumace nakládané zeleniny, nebo pití kávy. Pro představu je například intenzita Wi-Fi signálu až 100 000násobně nižší než intenzita běžné mikrovlnné trouby.

Důkazů o nebezpečnosti Wi-Fi je velmi málo a vědci jakýkoli negativní vliv vylučují. Zákonné limity zaručují, že mikrovlnné pole nemůže mít žádné škodlivé zdravotní účinky. Takže se nemusíme bát, Wi-Fi nic nedělá, člověku neškodí. Ostatně i světová zdravotnická organizace [dospěla](https://www.iarc.who.int/wp-content/uploads/2018/07/pr208_E.pdf) k závěru, že pokud vás pobolívá hlava, je problém třeba hledat jinde, než ve Wi-Fi signálu.

Druhá skupina lidí zastává názor, že Wi-Fi signál je škodlivý.

Zastávají názor, že nové bezdrátové technologie užívají mikrovlnných pulsů (radiace), obdobných těm, jaké používají radary a tím nejde o klasické radiové vlny. Vědci, jako dr. Johansson z Karolinského institutu ve Švédsku, zjistili, že mikrovlnné záření nízké úrovně způsobuje změny kůže. Na jaře roku 2007 vyzval Sir William Stewart, ředitel britského úřadu na ochranu zdraví, k oficiální revizi používání této technologie ve školách. Německá vláda doporučuje, aby se lidé vystavovali záření z Wi-Fi jen na „nejnižší možnou míru“ a raději používali „konvenční kabelové připojení“. Ve frankfurtských školách je již tato technologie zakázána. Evropská agentura životního prostředí v témže roce navrhla, aby zdravotní úřady doporučily omezovat vystavení vlivu Wi-Fi zejména citlivé skupiny, jako jsou děti. Knihovny ve Francii odstraňují Wi-Fi z důvodu obav jak vědecké komunity, tak zaměstnanců a vedení. Školní správa ve Vancouveru vydala v lednu 2005 rozhodnutí, které zakazuje stavbu mobilních antén v dosahu 300 m od školních zařízení. Palm Beach na Floridě, Los Angeles v Kalifornii a Nový Zéland zakázaly antény mobilních telefonů v blízkosti škol z obav o bezpečnost. Je jasné, že pokud nechceme antény v blízkosti škol, nechceme je ani uvnitř škol v podobě Wi-Fi!

Většina zjištění uváděla jako příčinu potíží především vysílače pro mobilní telefony a mobily samotné, ale dnes už víme, že (Wi-Fi) routery jsou ještě nebezpečnější, protože jsou umístěny uvnitř budov. Soudí se, že 3 % obyvatel velkých aglomerací jsou již těžce postižena a dalších 35 % má mírnější symptomy. Dlouhodobé vystavení tomuto mikrovlnnému záření zřejmě souvisí s individuální citlivostí, a proto je nezbytné, aby jeho působení na děti (Wi-Fi a mobilní telefony) bylo co nejvíce minimalizováno. Bezdrátový počítač (Wi-Fi) vystavuje záření celou horní část těla, a pokud ho máme na klíně, jsou ozářeny i reproduktivní orgány.

Lékaři už dokonce tuhle nemoc, kterou zatím trpí jen pár procent lidí, vystavených nějaké formě vysokých elektromagnetických frekvencí, pojmenovali. Co konkrétně toto záření podle jejich zjištění způsobuje? Zvýšenou propustnost mozkové krevní bariéry, zvýšený únik kalcia, nárůst rakoviny a poškození DNA, vytváření stresových proteinů a poškození nervů. Vystavení této energii je spojováno se změnami v krevních buňkách u školních dětí, dětskou leukémií, oslabením motorických funkcí, zhoršením reakčního času a paměti, bolestmi hlavy, závratěmi, únavou, slabostí a nespavostí. Další symptomy této dnes již nemoci (EHS) jsou problémy se spánkem, únava, bolesti, nevolnost, problémy s kůží, očima a ušima (tinnitus), závratě atd.

Tato technologie je ještě poměrně mladá, a tak teprve v budoucnu uvidíme, která skupina lidí měla větší pravdu.

Jak jsem to řešil v mém návrhu propojení dvou domácností? Celý rozvaděč umístěný na půdě první domácnosti, který je osazen VDSL modemem a Wi-Fi routerem zabezpečující spojení druhé domácnosti, je připojen do elektrické sítě přes dálkově ovládanou zásuvku WS101 s dosahem 100 m a do druhé zásuvky v prvním patře je připojen Wi-Fi router, který pokrývá toto patro. Tato zásuvka WS101 umožňuje současně ovládat až čtyři zařízení jednou klíčenkou, a naopak jedno připojené zařízení do přijímače (zásuvky) lze ovládat až osmi různými vysílači (klíčenkami). Funkce zásuvky jsou buď zapnutí a vypnutí jedním tlačítkem, zapnutí jedním tlačítkem a vypnutí druhým tlačítkem anebo zapnutí jedním tlačítkem následné časování a automatické vypnutí. Tímto je možné v noci zabezpečit „elektromagnetický“ klid a také kdykoliv to je nutné, restartovat na dálku tyto zařízení.

## Cisco packet tracer

Ukázka návrhu propojení v programu Cisco packet tracer

## Použitá zařízení k propojení

k tomuto propojení jsem použil následující zařízení, která vyhovovala přijatelnému finančnímu rozpočtu a dostatečné přenosové rychlosti:

**Obsah obrázku text, směrovač

Popis byl vytvořen automatickyTP-Link TL-WA901ND**

Přístupový bod s podporou moderních bezdrátových standardů IEEE 802.11 b/g/n (11/54/450 Mb/s) ve frekvenčním rozsahu 2,4 - 2,4835 GHz s maximálním vysílacím výkonem 20dBm. Na zařízení je pouze jeden ethernet port 10/100 Mbit/s (RJ-45) pro připojení k předchozímu prvku ve struktuře sítě. O výstupní výkon se starají 3 odnímatelné antény s konektorem R-SMA a výkonem každé antény 4 dBi. Antény lze odpojit a připojit výkonnější. K dispozici je 64/128bitové WEP a WPA/WPA2 šifrování. Nastavit lze bezdrátové módy AP, client, repeater a AP + bridge. Cena 1.029 Kč.

**Obsah obrázku text

Popis byl vytvořen automatickyJPA-18 Duplex – sektorová anténa 2,4 GHz**

Pro pokrytí jen určité lokace v daném směru na krátkou vzdálenost jsem zvolil sektorovou anténu, která je pro tyto podmínky nejvhodnější. Snadno tak pokryjeme pouze určitou oblast a nemusíme se obávat, že signálem budeme zarušovat místa, která leží mimo zvolený úhel. Tato anténa pracuje ve frekvenčním pásmu 2,4 GHz. Parametry antény jsou – zisk 18 dBi, vyzařovací úhel 45° v horizontální polarizaci a 35° ve vertikální. Anténu jsem umístil na budovu 1. domácnosti. Cena 1.239 Kč.

Obsah obrázku exteriér, budova, obloha, strom

Popis byl vytvořen automaticky

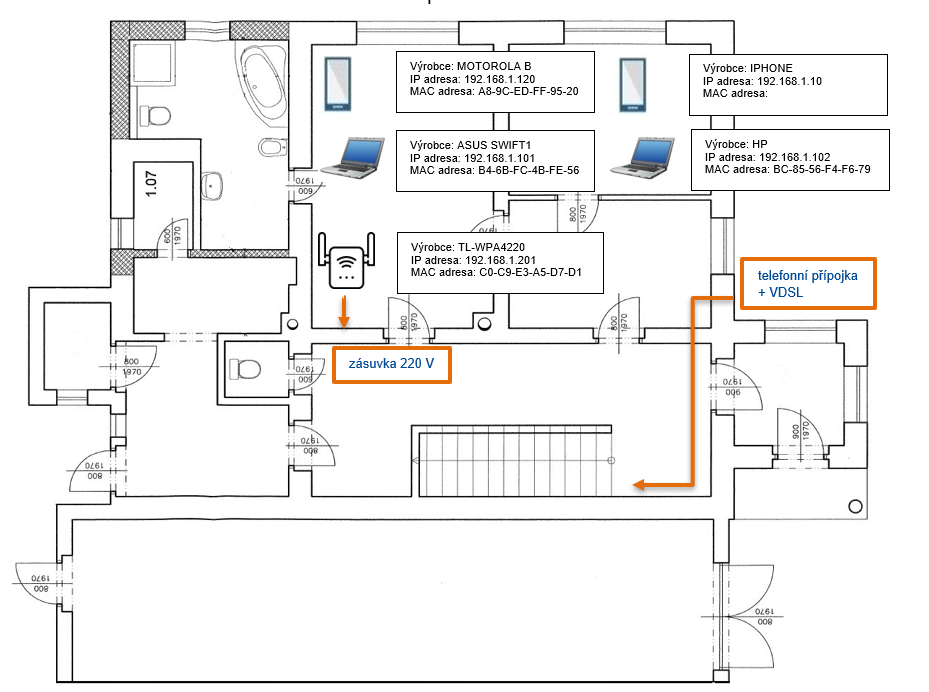
## Propustnost sítě

požadavky na propustnost sítě patřily mezi základní. Pro využití maximální propustností jsem využil zařízení podporující normu 802.11n, výše uvedený WiFi router TP-Link TL-WA901ND. Koncové body měly různé normy 802.11b, 802.11g a 802.11n a frekvenci 2,4 GHz. Jeho nastavení popíši níže.

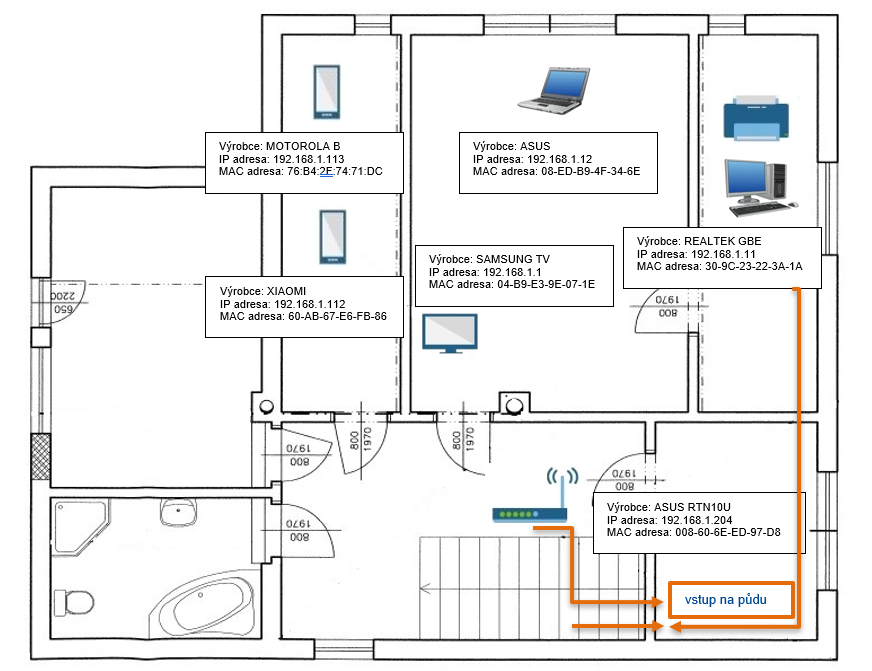
## Oblast pokrytí

požadavky na pokrytí byly důležité při plánování tohoto spoje. Vytvořil jsem orientační plán se zakreslením rozmístění používaných zařízení pro vnitřní pokrytí a náhled venkovního pokrytí.

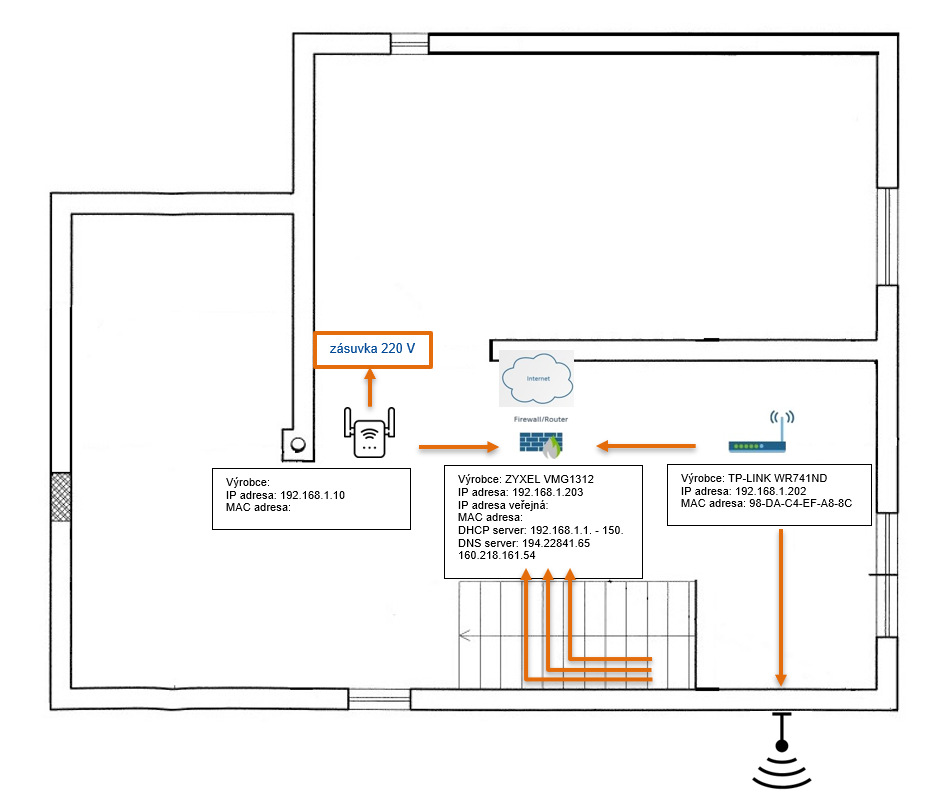
**1. domácnost s internetovým připojením a sektorovou anténou**



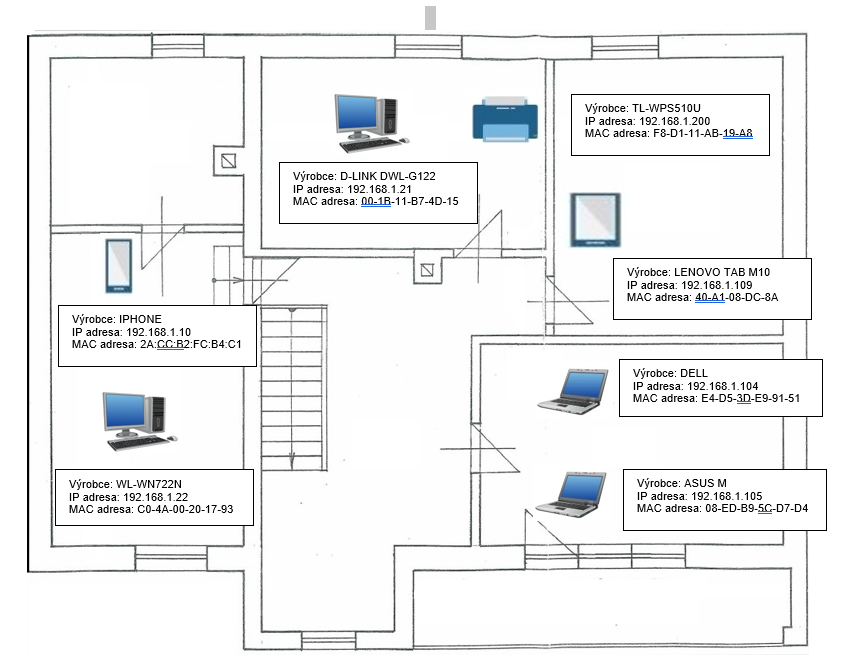
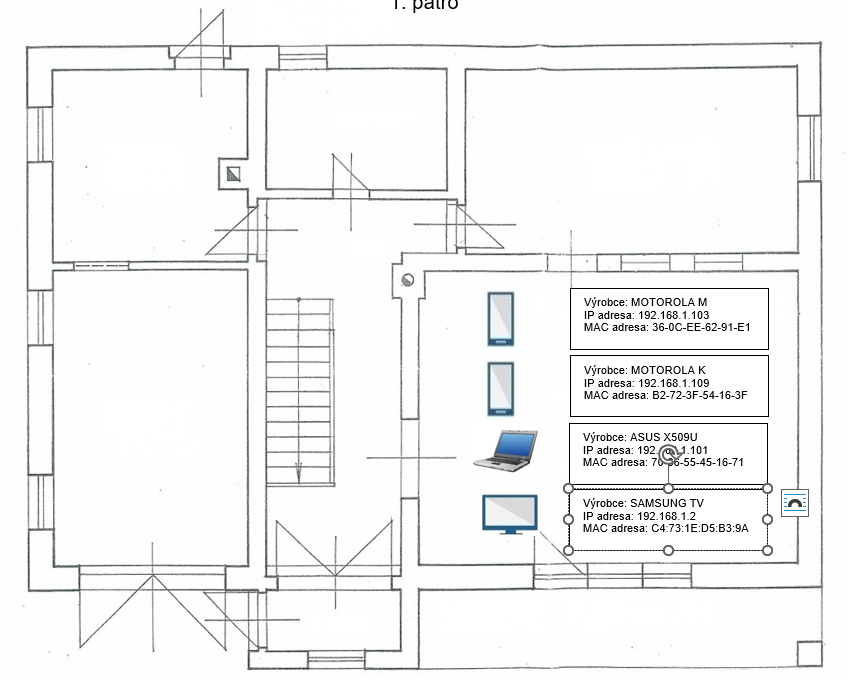
přízemí



1. patro

****

půda

****

**2. domácnost**

přízemí

1.patro

### Vzdálenost nemovitostí a pokrytí signálem 2. nemovitosti.

Z následujících obrázků je patrné, že na vzdálenosti 30 metrů od vysílající sektorové antény je signál po celé ploše druhé nemovitosti rovnoměrně rozprostřen. Anténa je správně natočena. Dokonce naměřená rychlost za zadní stěnou druhé nemovitostí je 9 Mb/s, což značí, že díky sektorové anténě a šířce kanálu 40 MHz je možné prostoupení signálem přes celou budovu.

Obsah obrázku text, zařízení, metr, ovládací panel

Popis byl vytvořen automatickyObsah obrázku text

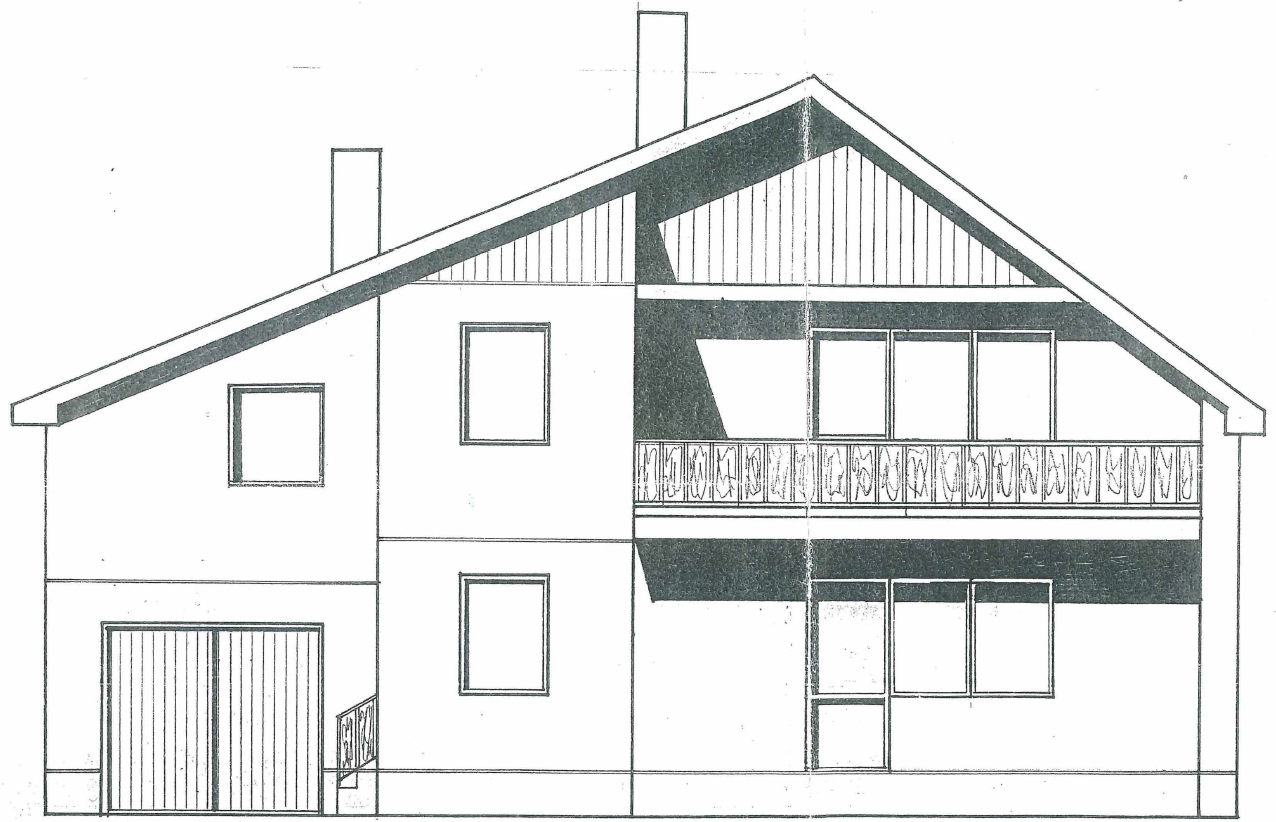
Popis byl vytvořen automaticky

30 metrů

Obsah obrázku text, zařízení, metr, černá

Popis byl vytvořen automatickyObsah obrázku text, zařízení, metr, indikátor

Popis byl vytvořen automatickyObsah obrázku text, zařízení, metr, indikátor

Popis byl vytvořen automaticky

## Mobilita

zajistit mobilitu používaných zařízení, aby se překrýval signál mezi přístupovými body. V celém návrhu je počítáno s třemi přístupovými body (čtvrtý je využit velmi zřídka, jedná se o vykrytí zahrady 2. domácnosti), které se nacházejí v   
1. domácnosti. První AP (výše zmíněné zařízení TP-Link TL-WA901ND) se nachází v půdním prostoru 1. domácnosti, který vykrývá pomocí sektorové antény celý objekt 2. domácnosti a zřídka čtvrtý přístupový bod, který je nakonfigurován jako repeater. Druhý AP je v prvním patře 1. domácnosti. Zde je použito následující zařízení:

Obsah obrázku text

Popis byl vytvořen automaticky**ASUS RT-N10U**

Bezdrátový router pro bezdrátové sítě se standardem IEEE 802.11 b/g/n s rychlostí přenosu až 150Mbps ve frekvenčním rozsahu 2,4 - 2,4835 GHz, s porty 1xWAN a 4xLAN (RJ-45) 10/100 Mbit/s a možností šifrování 64bitová/128bitová WEP, WPA, WPA2. K dispozici je USB port pro připojení tiskárny a síťového disku. O výstupní výkon se stará jedna 5 dBi odnímatelná anténa. Nastavit lze bezdrátové módy AP, client, repeater a AP + bridge s možností filtrování MAC adres. Cena 699 Kč.

Třetí AP se nachází v přízemí 1. domácnosti, kde bylo použito zařízení nazývané WiFi range extender a je spojený přes elektrické rozvody do půdního prostoru:

Obsah obrázku text, elektronika, projektor

Popis byl vytvořen automaticky**TL-WPA4220 KIT**

Sada TP-LINK TL-WPA4220 obsahuje dvojici zařízení pro rozšíření stávajícího internetového připojení do jakékoliv místnosti v domě pomocí elektrické sítě. **Nastavení i obsluha jsou velmi jednoduché,** stačí zapojit do zásuvky, připojit datový kabel RJ45 ze stávajícího internetového připojení a přes webové rozhraní nastavit komunikaci a šifrování. S powerline opakovačem AV600 je možné dosáhnout bezdrátové přenosové rychlosti **až 300 Mb/s** ve frekvenčním rozsahu 2,4 GHz standardem IEEE 802.11 b/g/n s šifrováním 64/128bitové WPA/WPA-PSK, WPA2/WPA2-PSK. P**řes rozvod elektrické sítě** až do vzdálenosti 300 m s rychlostí **až 600 Mb/s a šifrováním 128bit AES.**

Cena 1.549 Kč.

## Uživatelé

počet uživatelů a jejich nároky na používaní sítě byl důležitý parametr v případě sdílení širokopásmového internetu. Především pak nároky uživatelů na rychlost, odezvu a agregaci sdíleného internetu. V obou domácnostech je celkem sedm osob, které datově nenáročně využívají internetové spojení, přístup k síťové tiskárně (print serveru) a sdílení dat mezi počítači. Byla zde použita následující zařízení:

**Obsah obrázku text, elektronika

Popis byl vytvořen automatickyZyXEL VMG1312-B30B**

Modem ZyXEL VMG1312-B umožňuje připojení k internetu portem RJ-11 jak pomocí staršího standardu ADSL2+ (příchozí rychlost 24 Mb/s a odchozí 1,3 Mb/s), tak moderního VDSL2 (100/45 Mb/s). Dále obsahuje jeden USB 2.0 port vyhrazený pro volitelný 3G modem, který může sloužit jako flexibilní záloha v případě výpadku VDSL sítě. Dále jsou zde 4x RJ45 LAN porty o rychlosti 10/100 Mbit/s a 2x2 interní antény pro bezdrátovou komunikaci standardem IEEE 802.11 b/g/n s šifrováním 64/128bitové WPA/WPA-PSK a WPA2/WPA2-PSK a rychlostí až 300 Mb/s ve frekvenčním rozsahu 2,4 GHz. Dále umožňuje filtrování MAC adres a nastavení QoS, aby nedocházelo k zahlcení sítě a tím ke snížení kvality síťových služeb. Pomocí QoS se může např. nastavit maximální nebo minimální [přenosové pásmo](https://cs.wikipedia.org/w/index.php?title=P%C5%99enosov%C3%A9_p%C3%A1smo&action=edit&redlink=1) pro určitá data, prohlásit některý provoz za prioritní nebo rozdělit provoz do kategorií podle nastavených parametrů. Toto zařízení jsem použil jednak jako gateway, firewall a switch. WiFi komunikace je vypnutá, z důvodu zbytečného rušení a zatížení bezdrátového pásma komunikace. Jsou zde využívány čtyři porty RJ45 pro připojení jednoho počítače v 1. patře, kam nebyl problém svést UTP kabel CAT5e, dále pro propojení AP, který pomocí sektorové antény zabezpečuje pokrytí druhé domácnosti, pro propojení extenderu do přízemí 1. domácnosti a AP pro pokrytí prvního patra 1. domácnosti. Poskytovatelem je O2 o rychlost stahování 50Mb/s a odesílání 5Mb/s (resp. 60/10 Mb/s). Cena 1.199, - Kč (koupě mimo O2).

**TP-LINK TL-WPS510U**

Obsah obrázku elektronika

Popis byl vytvořen automaticky

Bezdrátový tiskový server, který zabezpečí síťový přístup uživatelů k tiskárně, která není prioritně určená pro síťový tisk. Tímto řešením se ušetřilo značné množství investic za novou síťovou tiskárnu. Tento model je vybavený jedním USB portem pro připojení tiskárny a WiFi odnímatelnou anténou s podporou normy IEEE 802.11 b/g (až 54 Mb/s). Při bezdrátovém přenosu jsou data šifrována těmito způsoby: WEP, WPA-PSK, WPA2-PSK (TKIP, AES). Cena 1.516 Kč.

Výše uvedený tiskový server je využit na připojení laserové tiskárny do lan sítě v 1. patře 2. domácnosti a jeho nedostačující anténa s malým dosahem je nahrazena výkonnější anténou:

**W-STAR WStar101 2,4GHz 10dBi RSMA**



Všesměrová prutová anténa použitá ke zvýšení pokrytí signálem WiFi v pásmu 2,4 GHz, ziskem 10 dBi a vyzařovací úhel 360° v horizontální polarizaci a 20° ve vertikální. Cena 167 Kč.

## Logika síťového plánování

byla navržena hierarchie přidělování IP adres uživatelům prostřednictvím DHCP serveru a DNS serveru běžícím na VDSL modemu. Nastavil jsem směrování provozu a rozhodl, jak bude vhodné používat DHCP server, případně s jakým nastavením. Dále jsem naplánoval, která zařízení budou používat statickou IP adresu, jelikož není vhodné, aby adresu přiděloval DHCP server. Jedná se o zařízení jako jsou televize, tiskový server a přístupové body. Nastavení DHCP serveru popíši v bodě Správa a konfigurace aktivních prvků.

## Bezpečnost

bylo bráno v úvahu zabezpečení sítě, především pak autentizace přihlášení klientských stanic a mobilních telefonů pomocí šifrování. Naplánoval jsme uzavřenou síť s uzavřeným přístupem do ní. Nastavení popíši v bodě Správa a konfigurace aktivních prvků.

## Vliv prostředí

posoudil jsme vliv prostředí a překážek pro zajištění dostatečného a stabilního internetového spojení. Zjistil jsem a proměřil ostatní WiFi sítě v dané lokalitě, abych se vyhnul vzájemnému rušení s ostatními bezdrátovými sítěmi.

Obsah obrázku text, monitor, obrazovka, televizor

Popis byl vytvořen automatickyObsah obrázku text, zařízení, obrazovka, černá

Popis byl vytvořen automatickyMěření jsem prováděl pomocí mobilního zařízení Xiaomi s parametry WiFi 802.11 a/b/g/n.

Venkovní měření okolních sítí a rychlosti pod anténou 1. domácnosti.

Obsah obrázku text, zařízení, černá, obrazovka

Popis byl vytvořen automaticky**Obsah obrázku text, monitor, obrazovka, snímek obrazovky

Popis byl vytvořen automaticky**

Obsah obrázku text, monitor, obrazovka, zařízení

Popis byl vytvořen automatickyMěření okolních sítí a rychlosti v přízemí 2. nemovitosti.

Stabilita WiFi signálu.

## Finanční rozpočet – spotřeba energie, porovnávání cen poskytovatelů internetu a cena při změně přenosového média

**spotřeba energie** – při používání použitých zařízení celého návrhu a při průměrné ceně 8500 Kč/MWh:

TP-Link TL-WA901ND - 5,8 W – za rok 432,- Kč

TL-WR841N - 8 W – za rok 596,-

Zyxel VMG1312-B - 10,4 W – za rok 775,- Kč

TL-WPS510U - 2,5 W – za rok 186,- Kč

TL-WPA4220 Kit - 7,6 W – za rok 566,-

ASUS RT-N10U - 12 W – za rok 893,-

Celkové náklady na energii jsou 3.448, - Kč.

**porovnání cen poskytovatelů internetu** – toto porovnání je pouze orientační, protože mohu zhodnotit jen DSL technologii, která je použita pro přístup k internetu v tomto návrhu propojení, jelikož všichni poskytovatelé této technologie využívají stejnou kabeláž od firmy Cetin. Skutečná rychlost je závislá na vzdálenosti od ústředny a jaké aktivní prvky jsou v ústředně používány. Dále v porovnání nabídek pro připojení vzduchem musím předpokládat, že nebude přístupový bod ovlivněn vzdáleností a viditelností.

O2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| technologie | název tarif | měsíční paušál | rychlost v Mb/s (upload/download) | cena zřízení |
| DSL | O2 stříbrný | 549,- | 50/5 | 3312,- |
| DSL | O2 zlatý | 649,- | 100/10 | 5940,- |
| 5G | O2 stříbrný | 549,- | 50/5 | 5940,- |
| 5G | O2 zlatý | 649,- | 100/10 | 5940,- |

výběžek.net

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| technologie | název tarif | měsíční paušál | rychlost v Mb/s (upload/download) | cena zřízení |
| DSL | DSL 50/10 | 499,- | 50/10 | 1900,- |
| DSL | DSL 100/20 | 599,- | 100/20 | 2600,- |
| 5G | RD60 standard | 399,- | 50/10 | 1900,- |
| 5G | RD60 premium | 499,- | 70/15 | 2600,- |

Artemis NET

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| technologie | název tarif | měsíční paušál | rychlost v Mb/s (upload/download) | cena zřízení |
| DSL | DSL 30/15 | 450,- | 30/15 | zdarma |
| --- | --- | --- | --- | --- |
| 5G | Opti | 360,- | 20/10 | zdarma |
| 5G | Extra | 600,- | 40/40 | zdarma |

Interdata

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| technologie | název tarif | měsíční paušál | rychlost v Mb/s (upload/download) | cena zřízení  závazek na 12 měsíců |
| --- | --- | --- | --- | --- |
| 5G | G1 Home 6/2 | 385,- | 6/2 | 1499,- |
| 5G | G1 Home 8/2 | 426,- | 8/2 | 1499,- |
| 5G | G1 Home 10/4 | 496,- | 10/4  (15/6 slabé vytížení) | 1499,- |

Výsledkem porovnání poskytovatelů vychází nejlépe výběžek.net.

**cena při změně přenosového média** –při realizaci návrhu byla použita bezdrátová technologie WiFi k propojení obou nemovitostí. Kdyby bylo spojení vytvořeno pomocí optického či metalického kabelu, nebudu brát v úvahu náklady na výkopové práce, byla by cena navýšena o ceny následujících komponentů:

|  |  |  |
| --- | --- | --- |
| **Název** | **Délka** | **Cena** |
| optický kabel – Ubiquiti Fiber Cable 200 | 60m | 2800,- |
| chránička HDPE pro optický kabel 40mm | 60m | 4096,- |
| TP-Link MC200CM – převodník z optiky na TP | - | 2x 736,- |
| Datacom CAT5e, UTP | 75m | 1375,- |

Celková cena realizace pomocí optického kabelu by se navýšila o 8368,- a TP kabelem o 5471,- Kč.

## Monitoring stavu sítě

### Monitoring stavu sítě pomocí programu LANState

10–Strike LANState je nástroj pro síťový monitoring. Umožňuje sledovat aktuální stav sítě pomocí grafické mapy, skenovat síť a zjišťovat topologii, organizovat centrum monitorování zařízení, spravovat a přistupovat k hostitelům rychleji pomocí mapy.

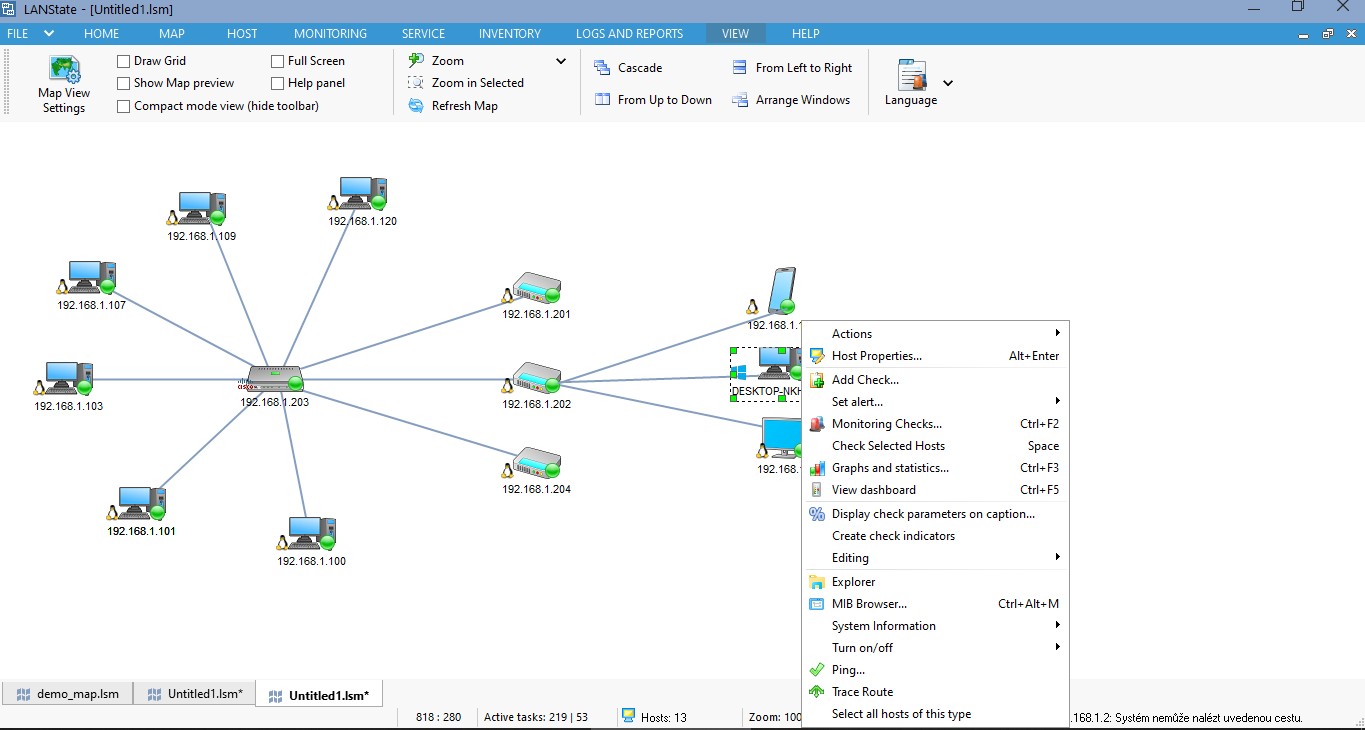
Dále monitorovat různé prvky a atributy (přepínače – switche, UPS, senzory, napájení apod.), získávat notifikace formou e-mailu nebo SMS, v neposlední řadě nechybí možnost analýzy grafů a trendů.

Cena software - 100 hostů (1 host = jedna ikona zařízení na síťové mapě) – 4965,- Kč

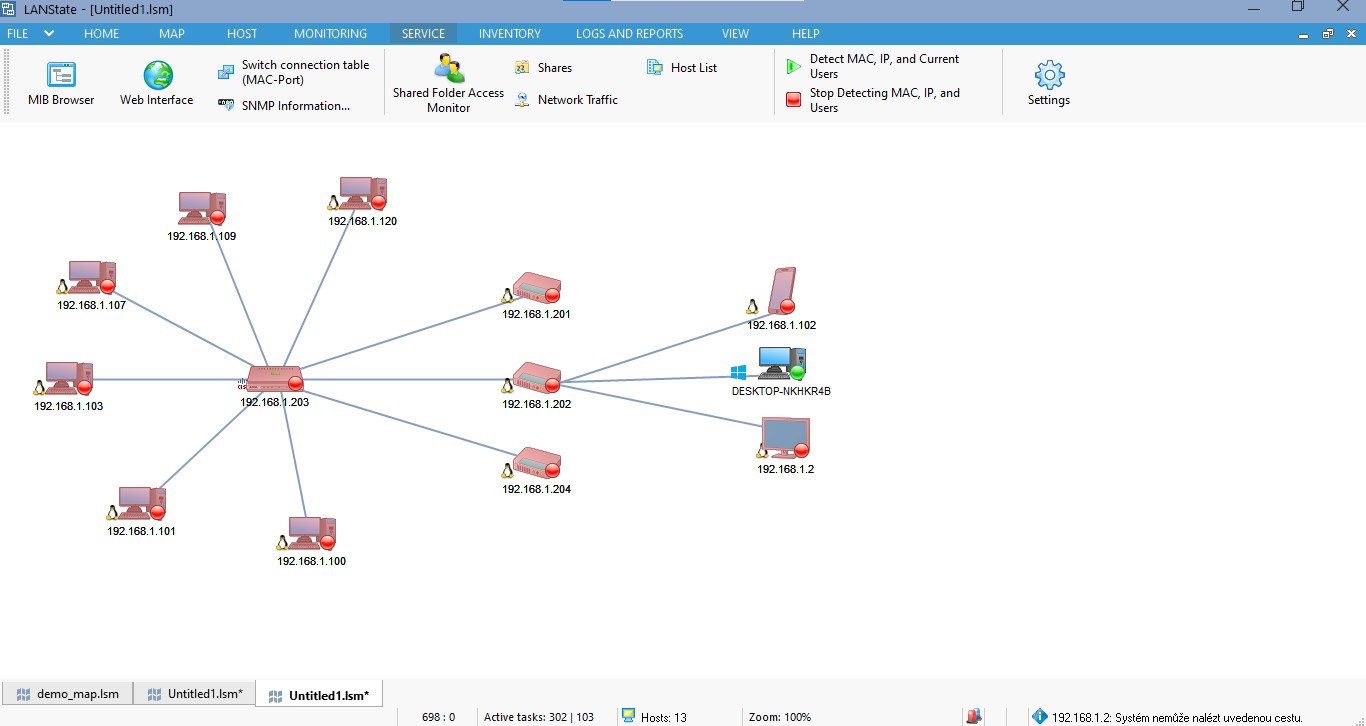
Ukázkové screenshoty z realizovaného návrhu:

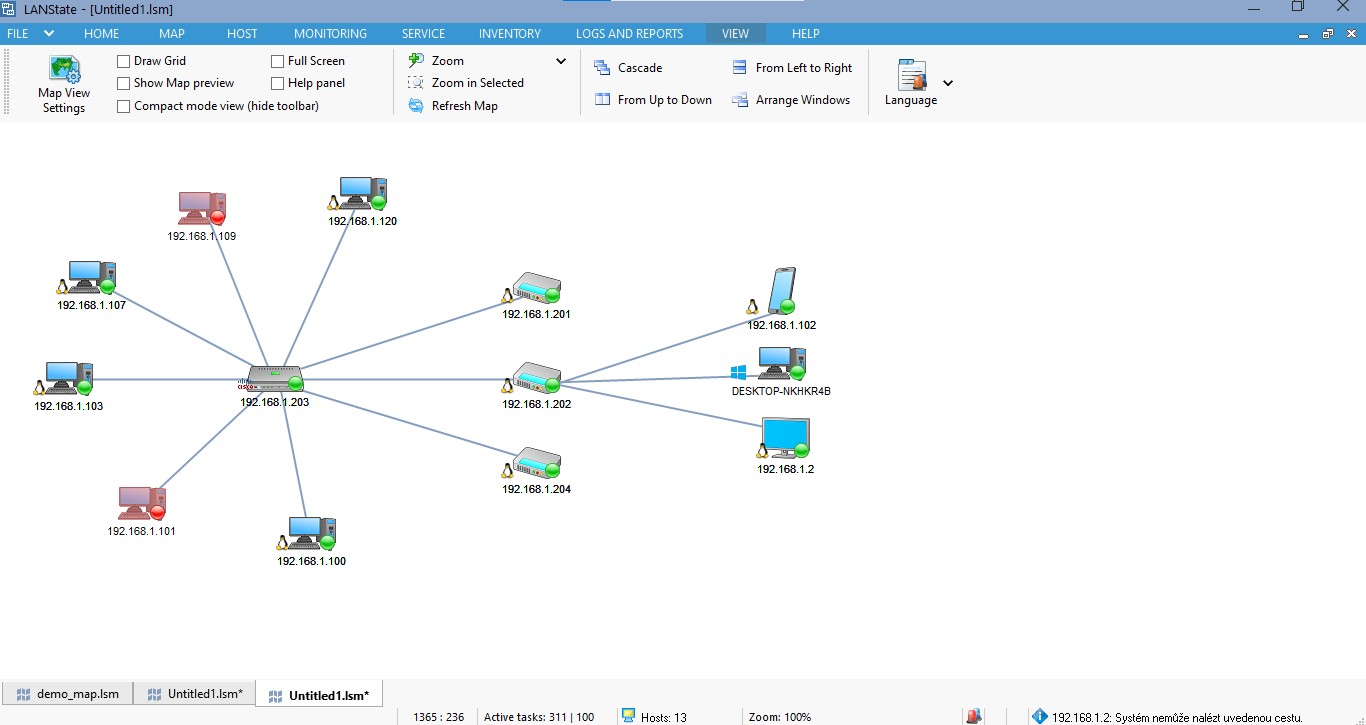
Obsah obrázku text

Popis byl vytvořen automatickyVytvoření nové mapy – automatické. Jestliže program nenalezne zařízení, lze jej doplnit manuálně (např. právě vypnuté).



Každé zařízení lze po otevření nabídky testovat a konfigurovat.

Příklad odpojení bezdrátové sítě PC, kterým sledujeme síť.



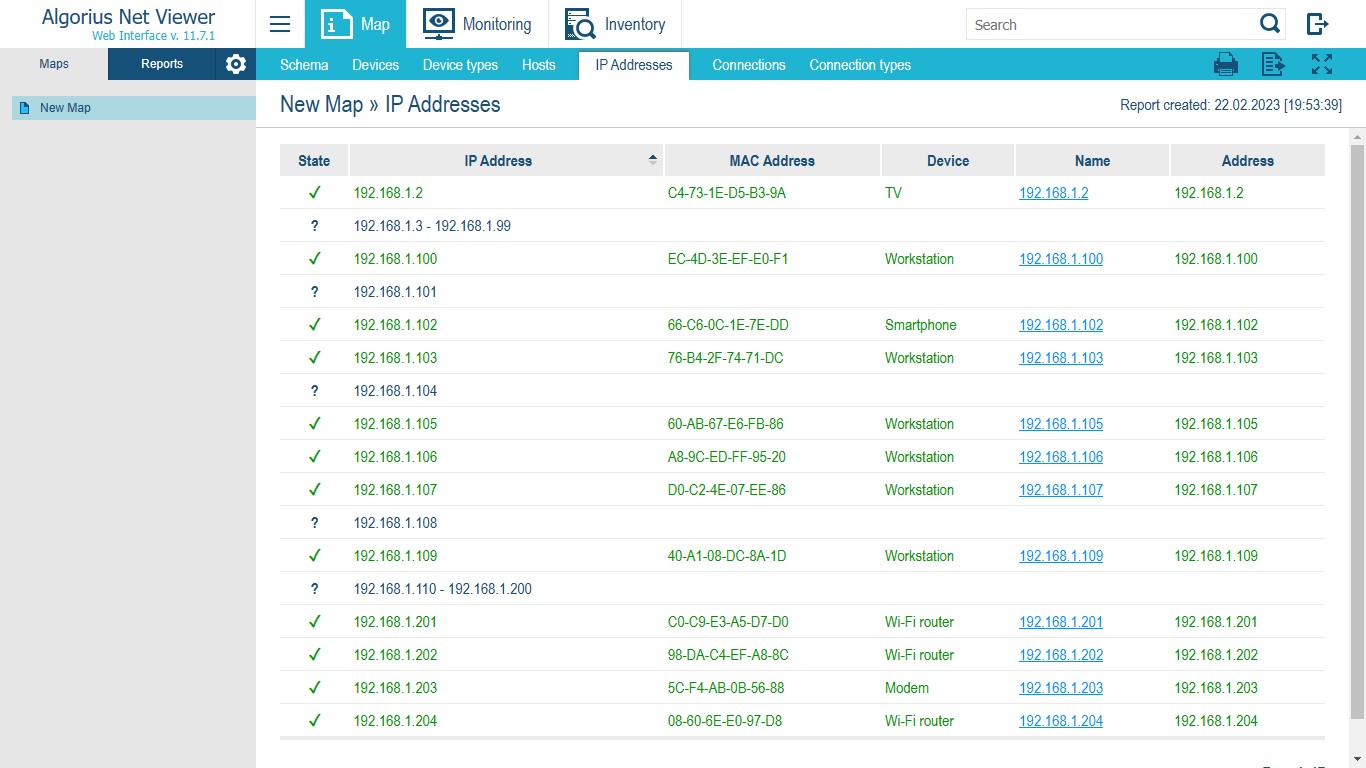
Příklad ukázky online PC a offline PC.

### Monitoring stavu sítě pomocí programu Algorius Net Viewer

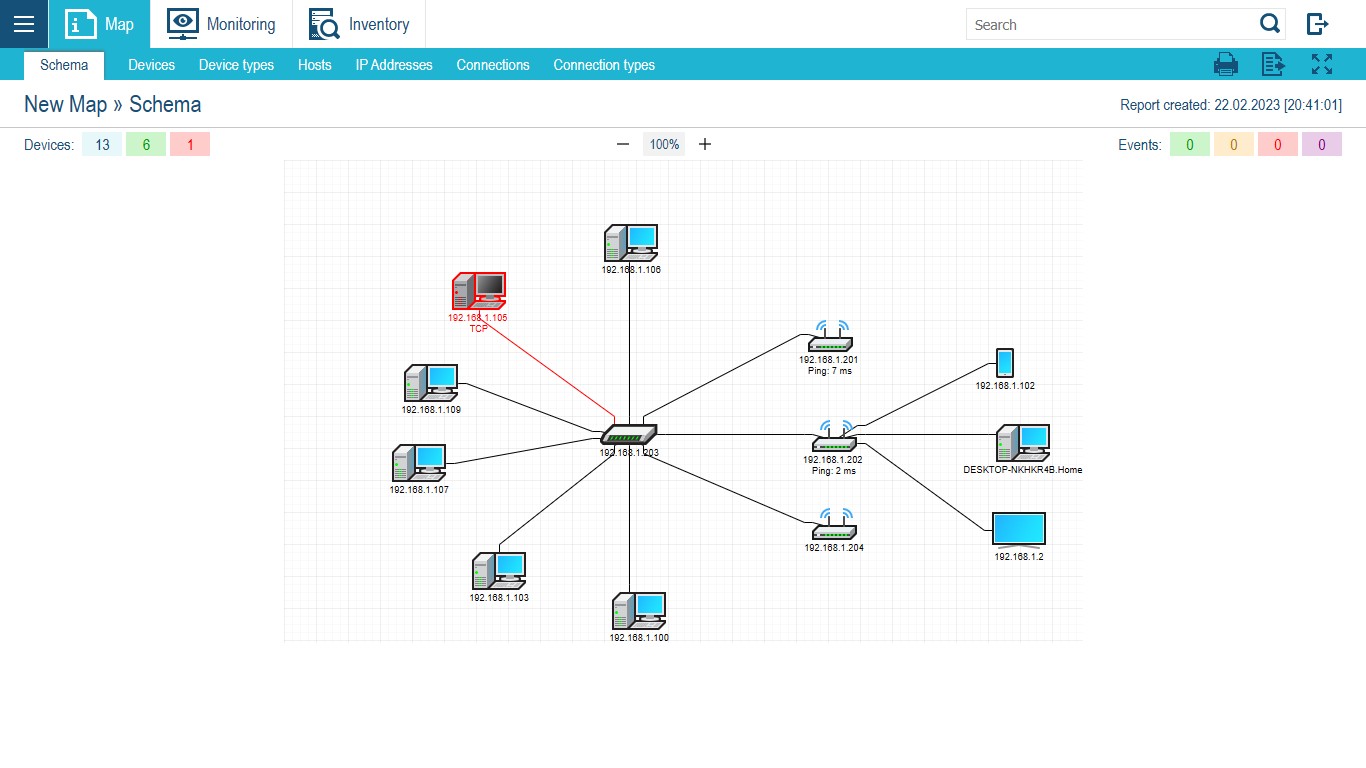
Algorius Net Viewer je software pro vizualizaci, monitoring, administraci a inventarizaci počítačové sítě jakékoli úrovně. Umožňuje řízení služeb, serverů a ostatních síťových zařízení, sledovat jejich stavy přes SNMP, WMI či jiné protokoly. Podporuje notifikace odesílané na Telegram, Skype, přes SMS či skrze jiné kanály.

Poradí si s generováním reportů, logů a diagramů. Slouží také pro přístup k síťovým mapám a real-timovému monitoringu. Pro každou instanci je schopen monitorovat více než 100 tisíc zařízení.

Cena software - 100 hostů (1 host = jedna ikona zařízení na síťové mapě) – 4140,- Kč

Ukázkové screenshoty z realizovaného návrhu:

Mapa IP adres na Web serveru aplikace.

Mapa zařízeních na Web serveru aplikace.

Obsah obrázku stůl

Popis byl vytvořen automatickyUkázka monitoringu.

# Správa a konfigurace aktivních prvků

## Zyxel

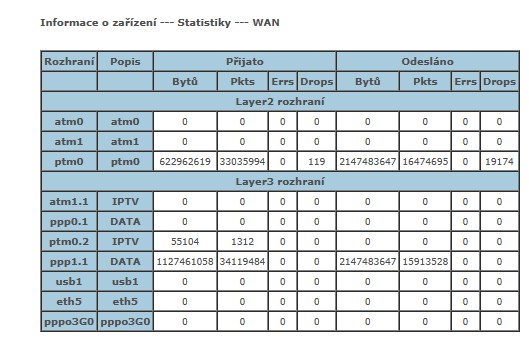
Lan statistika\_5

Info\_1

Info\_2

Diagnostika\_6

DHCP\_3

****

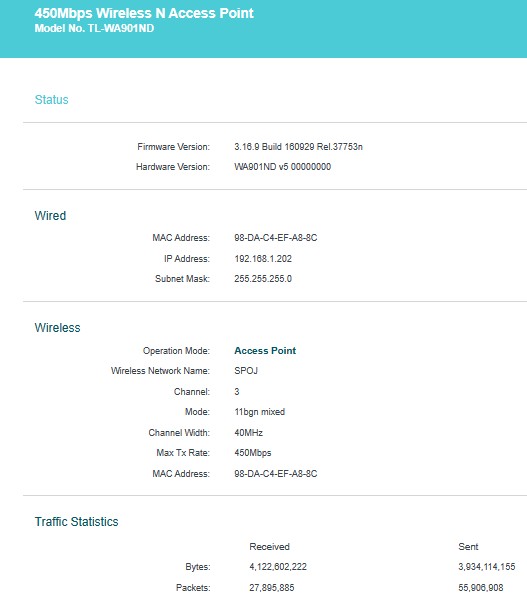
Wan statistika\_4

## Spoj

Monitor propustnosti – stahování filmů\_6

Monitor – stahovaní flimů\_5

Lan\_2



Zabezpečení\_4

Wifi nastavení\_3

Status\_1

Nutná změna hesla\_7

## 3\_doma\_1

Info\_1

## 4\_doma\_2



Nastavení wifi\_2

Info\_1

## 5\_powerline

Info\_1

# Závěr

Cílem mé práce byl návrh propojení dvou domácností, kdy tento návrh jsem realizoval v domácnosti, v které bydlím, a tudíž jsem mohl z praxe popsat výhody, nevýhody a provést skutečná měření.

Bezdrátové sítě jsou v dnešní době jedním z nejrychleji se rozvíjejícím odvětvím. Prostřednictvím bezdrátové technologie je možné provozovat počítačové sítě i z míst, kde to dříve bylo nemyslitelné. Oproti klasickým sítím nabízejí bezdrátové sítě výhody jako je mobilita, nižší náklady na budování a vyšší efektivnost.

Ve svém návrhu propojení jsem použil klasické „drátové“ prvky stejně jako bezdrátové. Snahou bylo dodržet požadavky majitelů domácností, technické možnosti s co nejnižšími náklady. Hlavním požadavkem bylo neprovádění stavebních úprav nemovitostí, průrazů mezi podlažími a instalování rozvodných žlabů – lišt pro vedení metalických kabelů. Tento požadavek byl téměř splněn, ale přesto bylo nutné použít metalických rozvodů mezi aktivními prvky, aby nedocházelo k zbytečnému zarušení přenosového pásma bezdrátových aktivních prvků.

Samotný návrh obsahuje nákres topologie sítě, kde jsou zakresleny koncová zařízení (PC, mobily, printserver atd.), stejně tak jako použité aktivní síťové prvky s konkrétním nastavením. Z nákresů je patrné, že ve většině případů jsou připojená zařízení mobilní a nebylo by tedy výhodnější realizovat připojení tažením kabelů v lištách, i když přenos po kabelu je výhodnější co se týče spolehlivosti a rychlosti.

Při budování sítě byly použity bezdrátové prvky s frekvenčním pásmem 2,4 MHz pro normy 802.11 b/g/n z důvodu technického vybavení koncových zařízeních. V budoucnu bude na zvážení, zda provést výměnu aktivních prvků, které budou v duálním frekvenčním pásmu 2,4 MHz a 5 GHz. To se samozřejmě bude týkat i výměny sektorové antény, která pokrývá druhou nemovitost. Dále je na zvážení, zda nenavýšit rychlost připojení internetu ze současné rychlosti 50/5 Mb/s (na VDSL modemu je nastaveno 60/10 Mb/s) od poskytovatele O2 anebo změnit poskytovatele.

Celý realizovaný návrh je plně funkční a pro uživatele dostačující.