Česká zemědělská univerzita v Praze

Technická fakulta

Analýza a srovnání standardů 802.11 pro WiFi zařízení

Bakalářská práce

Vedoucí bakalářské práce: Ing. Zdeněk Votruba, Ph.D.

Autor práce: Martin Šustr

PRAHA 2019

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Martin Šustr

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Analýza a srovnání standardů 802.11 pro WiFi zařízení

Název anglicky

Analysis and comparison of 802.11 standards for WiFi devices

Cíle práce

Cílem práce je analyzovat a porovnat technické a provozní parametry standardů 802.11 užívaných v současných WiFi zařízeních. Definovat doporučení pro provoz u jednotlivých tříd a definice klíčových parametrů. V závěru provézt shrnutí pro koncového uživatele včetně predikce dalšího vývoje v oblasti

Metodika

1. Úvod
2. Cíl práce
3. Metodika
4. Rozbor jednotlivých standardů 802.11
5. Výběr a podrobný popis aktuálně využívaných skupin
6. Souhrn provozních a technologických parametrů
7. Doporučení pro provoz
8. Očekávaný vývoj a zhodnocení

Doporučený rozsah práce

30 až 40 stran textu včetně obrázků, grafů a tabulek

Klíčová slova

počítačová síť, WiFi

Doporučené zdroje informací

HORÁK, J.: Vytváříme domácí bezdrátovou síť, COMPUTER PRESS, 2011
James F. Kurose, Keith W. Ross: Počítačové sítě, CPress, 2014, 3. vydání
KERŠLÁGER, M. – HORÁK, J. Počítačové sítě pro začínající správce. Brno: Computer Press, 2003. ISBN 80-7226-876-7.
Wendell, O., Rus, H., Naren, M.:Směrování a přepínání sítí, CPress, 2009, ISBN:978-80-251-2520-5
Zandl, P.:Bezdrátové sítě WiFi Praktický průvodce, COMPUTER PRESS, 2003

Předběžný termín obhajoby

2018/19 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 16. 10. 2018

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 16. 10. 2018

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 13. 03. 2019

Čestné prohlášení

„Prohlašuji, že jsem bakalářskou práci na téma: Analýza a srovnání standardů 802.11 pro Wi-Fi zařízení vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.“

V Praze: ....

Martin Šustr

Poděkování

Děkuji svému vedoucímu práce Ing. Zdeňkovi Votrubovi, Ph.D. za pomoc s výběrem tématu a za cenné rady při zpracovávání práce.

Abstrakt: Tato práce je zaměřena na problematiku bezdrátových přenosů dat a bezdrátových sítí. Začátek práce pojednává o principu přenosu signálu, protokolu TCP/IP, struktuře bezdrátových sítí a způsobech modulace signálů. Další část se zabývá podrobným popisem standardů IEEE 802.11 a jejich porovnáním. V neposlední řadě se práce zaměřuje na bezpečnost bezdrátových sítí. Závěr práce pojednává o potencionálním směru rozvoje bezdrátových sítí.

Klíčová slova: IEEE 802.11; WLAN; bezdrátová síť; bezpečnost; Wi-Fi

Analysis and comparison of 802.11 standards for WiFi devices

Summary: This thesis is focused on wireless transmission of data and wireless networks. The beginning of the thesis is about principle of signal transmission, TCP/IP protocol, structure of wireless networks and methods of signal modulation. The next part is focused on detailed description of IEEE 802.11 standards and their comparison. Last but not least, the thesis is focused on the security of wireless networks. The conclusion deals with the potential direction of wireless network development.

Key words: IEEE 802.11; WLAN; wireless network; security; Wi-Fi

Obsah

1 Úvod

Přenos dat je realizován buď pevným nebo bezdrátovým způsobem. Pevný přenos je realizován pomocí fyzického média, většinou buď metalických nebo optických kabelů. Tento typ přenosu má své výhody, ale i spoustu nevýhod. Mezi výhody pevného spojení patří zpravidla větší rychlost a stabilita připojení nebo bezpečnost sítě. Ovšem tyto výhody už jsou v dnešní době téměř zanedbatelné, vzhledem k tomu, že spousta moderních bezdrátových sítí může dosahovat rychlostí přes 1Gbit/s a zabezpečení je téměř srovnatelné s tím fyzickým.

Trend bezdrátových sítí v posledních několika letech doslova explodoval. Jedním z příkladů může být například poměr mobilních telefonů oproti pevným telefonům. V minulosti byl pevný telefon prakticky součást domácnosti, dnes už je téměř raritou. Bezdrátová technologie se nachází ve spoustě zařízení (notebooky, chytré telefony, tablety, síťové karty do stolních počítačů, ...). Z tohoto důvodu lze zachytit bezdrátový signál na téměř každém rohu. Hlavní výhodou bezdrátových technologií je jejich flexibilita, signál se dostane i na místa, kam by se kabel natahoval velice obtížně.

Velice populární řešení bezdrátových sítí je technologie Wi-Fi. Wi-Fi je založena na standardech IEEE 802.11 a je spravována skupinou Wi-Fi Alliance, která určuje, které technologie a standardy odpovídají normě. Jednou z velkých výhod této technologie je její cenová dostupnost. Díky tomu Wi-Fi nachází využití jak ve velkých firmách, tak v malých domácnostech. Využití této technologie poskytuje řadu výhod, ve firmách může Wi-Fi usnadnit mobilitu pracovníků nebo v domácnostech může zvýšit pohodlí uživatele.

Velice důležitým parametrem bezdrátových sítí je jejich bezpečnost. Bezdrátový signál se může šířit přes různé zdi či překážky, proto je velice snadné podcenit bezpečnost bezdrátového přenosu. Bez příslušných zabezpečení není pro útočníka těžké signál zachytit a zneužít. V lepším případě se nezvaný host jen připojí a svou přítomností nám snižuje bandwidth, v horším případě nám může ukrást nebo vymazat důležitá data.

2 Cíl práce

Jedním z cílů této práce je popis základních principů funkcí bezdrátových sítí a jejich rozdělení. Dalším cílem je posouzení a porovnání provozních parametrů standardů IEEE 802.11, které se využívají v současných Wi-Fi zařízeních. Klíčovým výsledkem práce je podat uživateli bezdrátové sítě kompletní přehled o užívaných standardech a rozdílech mezi nimi. Práce v neposlední řadě pojednává také o zabezpečení bezdrátových sítí.

2.1 Metodika

Práce je rozdělena do několika částí. První část se zabývá základním popisem principu bezdrátové komunikace a rozdělením bezdrátových sítí. Stěžejní část práce je zaměřena na popis jednotlivých standardů IEEE 802.11 a jejich hodnocení. Závěrečná část práce se zabývá bezpečností bezdrátových přenosů.

3 Bezdrátové sítě

3.1 Historie bezdrátových přenosů

Historie bezdrátových sítí jde ruku v ruce s historií bezdrátových přenosů. Bez objevů technologií jako je rádio, by bezdrátové sítě pravděpodobně vůbec neexistovaly. [15]

V roce 1888 německý fyzik Heinrich Rudolf Hertz vytvořil první rádiovou vlnu. V roce 1894 se začaly rádiové vlny využívat jako forma komunikace. K přijímání rádiových vln ve formě signálu byly využity telegrafní dráty. Tímto objevem se otevřely dveře technologiím jako jsou televize nebo rozhlas. Italský vynálezce Marchese Guglielmo Marconi pak rozšířil rádius vysílání rádiových vln na tři kilometry a tím se stal takzvaný „otec rádia". Během několika dalších let se bezdrátová komunikace rozvinula tak, že v roce 1902 už Marconi mohl posílat signál přes celý Atlantský oceán. [15]

V roce 1971 na Havajské univerzitě skupina výzkumníků vedena Normanem Abramsonem vytvořila první lokální bezdrátovou síť s názvem ALOHAnet. Tato síť se skládala ze sedmi počítačů, které komunikovaly mezi sebou. V roce 1991 začal institut elektrotechnických a elektronických inženýrů diskutovat o standardizaci. [15]

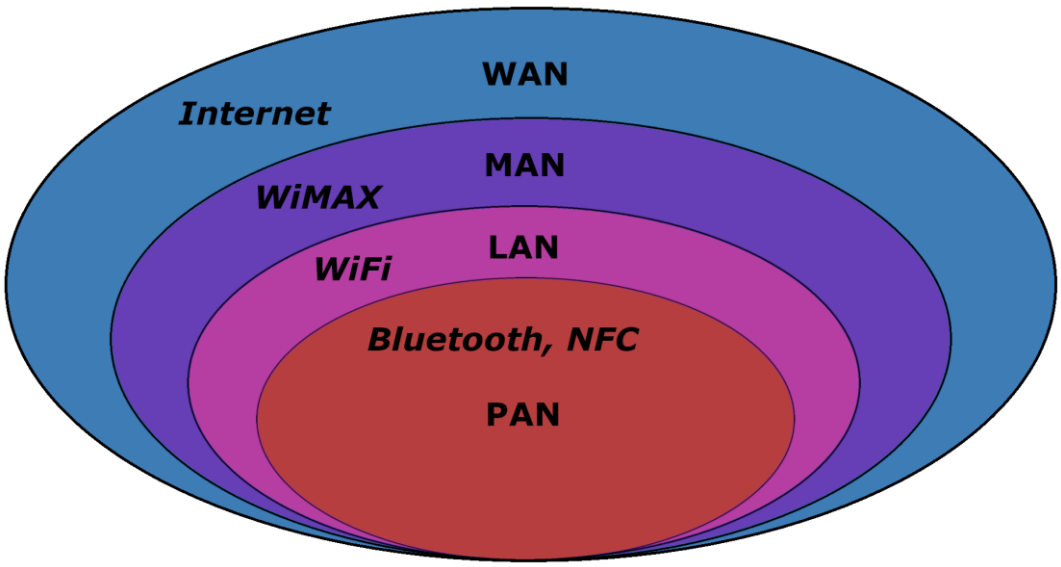
3.2 Co je to bezdrátová síť?

Bezdrátová síť zajišťuje vzájemnou komunikaci a sdílení informací u jednotlivých přístrojů jako třeba počítač, tiskárna nebo mobilní telefon pomocí bezdrátového spojení, tedy bez použití fyzických kabelů.

Nicméně bezdrátová síť nepřenáší informace jen tak vzduchem, ale pomocí takzvaného přenosového média. Typ nosného média záleží na tom, na co je daný signál modulován. Typů bezdrátových médií je několik, například zvukové vlny, které využívá třeba ultrazvuk. Dalším příkladem může být světlo, využívané u infračerveného záření nebo laseru. Zdaleka nejpoužívanější je ale přenos pomocí rádiových vln. [2]

Sítě, které využívají přenos rádiových vln se mohou dělit několika způsoby. Nejtypičtější rozdělení je podle velikosti. Velikost sítě může být vyjádřena buď geografickou rozlohou, kterou zaujímají nebo počtem zařízení v dané síti. Mezi nejmenší sítě se řadí PAN, tyto sítě jsou zaměřeny na jednoho člověka v malém okruhu, většinou kolem deseti metrů. Do této skupiny patří také Bluetooth nebo NFC. Dalším stupněm dle velikosti sítě jsou sítě LAN, tyto sítě pokrývají celkem malé geografické území, většinou domácnosti nebo malé firmy. Hlavní technologií, kterou využívají tyto sítě je Wi-Fi. O něco větší síť se nazývá MAN, tato síť pokrývá většinou oblast města. Sítě MAN využívají především technologii WiMax (IEEE 802.16), dají se také pochopit jako Wi-Fi pro venkovní sítě s velkým dosahem. Největší sítě se nazývají WAN, jedná se o síť, která pokrývá region, stát nebo kontinent. Nejznámější příklad sítě WAN je internet. Na obrázku 1 je znázorněno rozdělení sítí dle velikosti. [2]

Obrázek 1: Rozdělení sítí dle velikosti [vlastní]

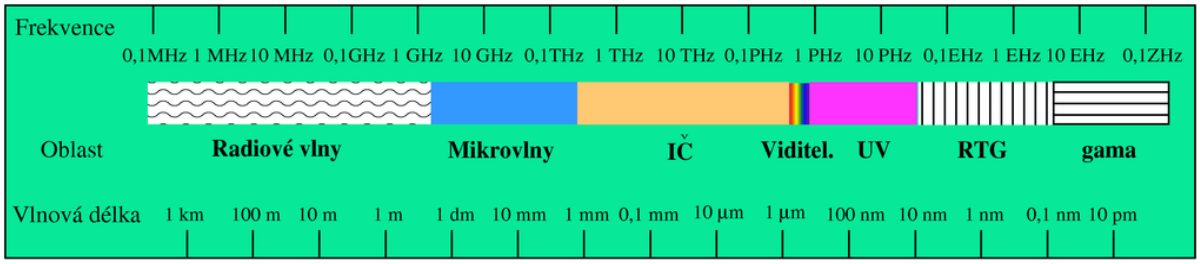


Další možnost rozdělení bezdrátových sítí může být například dle mobility. Tato kategorie se dělí na mobilní sítě a fixní sítě. Mobilní sítě i při celkem rychlém pohybu neztratí signál, mezi tyto sítě patří především mobilní sítě WAN, například GPRS, EDGE nebo LTE. U fixních sítí mohou klientská zařízení při rychlejším pohybu ztrácet signál. Nejběžnější fixní síť je Wi-Fi. [2]

3.3 Elektromagnetické spektrum

Elektromagnetické vlny pokrývají širokou škálu frekvencí a vlnových délek, tato škála se nazývá elektromagnetické spektrum. Pravidlem je, že čím delší je vlnová délka, tím menší je frekvence. Na obrázku 2 je znázorněn plynulý přechod mezi jednotlivými segmenty elektromagnetického spektra. Bezdrátové sítě využívají elektromagnetické spektrum jako hlavní přenosové médium. Jsou různé typy bezdrátových sítí, které využívají různé části tohoto spektra. [46]

Obrázek 2: Elektromagnetické spektrum [49]



3.4 Frekvence

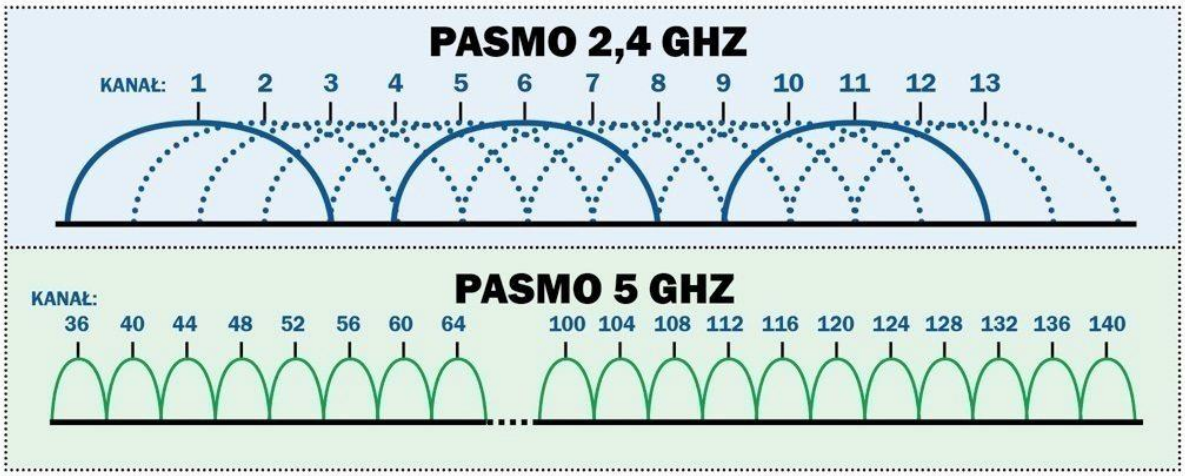
Frekvenční pásmo se dělí na licencované a nelicencované. Ovšem jen málo sítí využívá licencované pásmo. Důvodem asi bude to, že pokud chce uživatel využívat licencované pásmo, musí individuálně žádat o povolení vysílat v daném pásmu a v dotyčné oblasti. Dále pak, vysílání v tomto pásmu bývá velice často zpoplatněno. Na druhou stranu tato pásma mají právní ochranu proti rušení nebo proti zneužití neoprávněným uživatelem. Díky tomu lze částečně garantovat i kvalitu služeb. Naopak v nelicencovaném pásmu může vysílat prakticky každý bez jakéhokoli oprávnění. Ovšem samozřejmě i u tohoto pásma jsou definována generická pravidla, která by měl každý dodržovat. Bohužel proti rušení u tohoto pásma není žádná právní ochrana. V České republice spravuje frekvenční pásma Český telekomunikační úřad (ČTÚ). [2]

Tabulka 1: Výhody a nevýhody frekvenčních pásem [vlastní]

	Licencované frekvenční pásmo	Nelicencované frekvenční pásmo
Přístupnost	Individuální oprávnění pro uživatele	Všeobecné oprávnění (bez žádosti)
Poplatek	Většinou zpoplatněno	Bez poplatku za frekvenci
Právní ochrana	Právní ochrana proti rušení	Bez právní ochrany proti rušení
Kvalita služeb	Částečná garance kvality služeb	Bez garance kvality služeb

Správně zvolená vysílací frekvence hraje klíčovou roli ve výsledné rychlosti, dosahu a celkové kvalitě vysílaného signálu. V základu platí, že čím vyšší frekvence, tím větší přenosová rychlost a čím nižší frekvence, tím vyšší dosah. Většina Wi-Fi zařízení využívá k provozu buď frekvenci 2,4Ghz nebo 5Ghz a vysílá v nelicencovaném pásmu. Hlavní nevýhodou pásma 2,4Ghz je, že má jen 13 kanálů, které se navzájem překrývají, takže jsou prakticky využitelné jen 3. Další nevýhodou pásma 2,4Ghz je, že ho nevyužívají jen Wi-Fi, ale i některé domácí spotřebiče jako třeba mikrovlnné trouby, tudíž je velice náchylné k rušení. Pokud se v blízkosti nachází spotřebiče způsobující rušení a zároveň je kladen důraz na dobrou prostupnost sítě, upřednostňuje se pásmo 5Ghz. Je-li prioritou dosah signálu, prostupnost překážkami, je dobré zvolit pásmo 2,4Ghz.

Obrázek 3: Porovnání pásem 2,4Ghz a 5Ghz [50]



3.5 Protokol TCP/IP

Protokol TCP/IP je v současné době chápan jako standard pro komunikaci počítačových sítí. Jedná se o sadu komunikačních protokolů používaných k propojení síťových zařízení na internetu. Tento komunikační protokol lze využít i

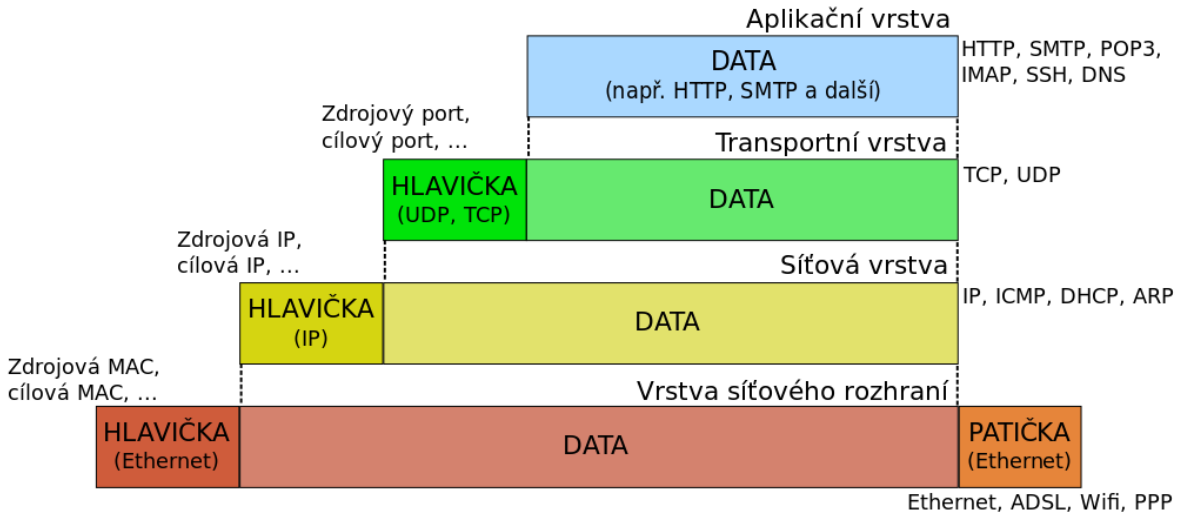
v soukromé síti jako intranet nebo extranet. Velkou výhodou tohoto protokolu je, že ho nevlastní žádná společnost, díky tomu lze sadu internetových protokolů jednoduše upravit. Je kompatibilní se všemi operačními systémy, takže může komunikovat s jakýmkoliv jiným systémem. [13]

TCP/IP definuje způsob, jakým jsou data vyměňována prostřednictvím internetu. Určuje, jakým způsobem mají být data rozdělena na pakety. Ty jsou dále adresovány, přenášeny, směrovány a přijímány. Tento protokol vyžaduje malý centrální management, který je navržen tak, aby byla síť spolehlivá a schopna se automaticky obnovit v případě, že selže nějaký prvek sítě. [13]

TCP/IP se skládá z dvou hlavních protokolů. TCP se v první řadě stará o to, jak mohou aplikace vytvořit komunikační kanály po síti. Dalším úkolem TCP je spravovat, jak jsou data rozdělena do menších paketů před jejich přenesením a znovu je po dokončení přenosu sestavit. Úlohou IP je adresace, směrování každého paketu a ověření, zda dosáhl správného cíle. [13]

Vzhledem ke složitosti síťové komunikace, je protokol TPC/IP rozdělen do vrstev. Přenos informací je přesně definován, každá vrstva využívá služeb nižších vrstev a poskytuje služby vrstvám vyšším. Na obrázku 4 je znázorněno zapouzdření dat do jednotlivých vrstev.

Obrázek 4: Zapouzdření dat v sítí TCP/IP [51]



3.5.1 Aplikační vrstva

Tato vrstva se zabývá poskytováním síťových služeb aplikacím. Existuje mnoho aplikačních síťových procesů a protokolů, které pracují na této vrstvě. K nejznámějším protokolům patří například HTTP, SMTP, POP3, IMAP, SSH, DNS. [2]

3.5.2 Transportní vrstva

Tato vrstva je nadřazena aplikační vrstvě a zabývá se přenosem dat. Využívá dva protokoly, mezi kterými si aplikace mohou libovolně vybrat. První protokol UDP je méně spolehlivý a neposkytuje žádnou garanci doručení dat. Po odeslání dat neprovede žádnou kontrolu, jestli byla data bezpečně přijata. Na druhou stranu je protokol UDP výrazně rychlejší. Druhý protokol TCP je považován za spolehlivý a zaručuje, že byla data v pořádku doručena. [2]

3.5.3 Síťová vrstva

Primárním úkolem této vrstvy je hledání cesty pro pakety. Cestu nehledá pouze mezi přímými sousedy, ale mezi všemi uzly v síti. Cílem je najít cestu, která poskytne co nejrychlejší přenos dat. Po nalezení vhodné cesty zajistí přenos paketů přes vybrané uzly v cestě. Hlavním protokolem, který tato vrstva využívá, je protokol IP. Může ale využívat i jiné, jako třeba ICMP, DHCP nebo ARP. [2]

3.5.4 Vrstva síťového rozhraní

Jedná se o nejnižší úroveň protokolu TCP/IP. Provádí funkce jako zapouzdření paketů do rámců pro přenos, mapování IP adres na hardwarové adresy MAC a použití protokolů pro fyzický přenos. Do této vrstvy se řadí například Ethernet, Wi-Fi, ADSL. [2]

3.6 Základní prvky bezdrátové sítě

3.6.1 Bezdrátový hostitel

Pojem bezdrátový hostitel se dá chápat jako zařízení, které se stará o funkci aplikací. Bezdrátovým hostitelem může být například stolní počítač, notebook, tablet nebo chytrý telefon. Bezdrátové hostitele lze dělit na mobilní a nemobilní. [3]

3.6.2 Základní stanice

Základní stanice je zodpovědná za přijímání a odesílání dat od bezdrátového hostitele, který je připojen k této stanici. Základní stanice je také zodpovědná za koordinaci přenosů mezi více bezdrátovými hostiteli, se kterými je asociována. Základní stanice může být například mobilní věž nebo v případu standardu IEEE 802.11 přístupový bod (AP). [3]

3.6.3 Bezdrátové linky

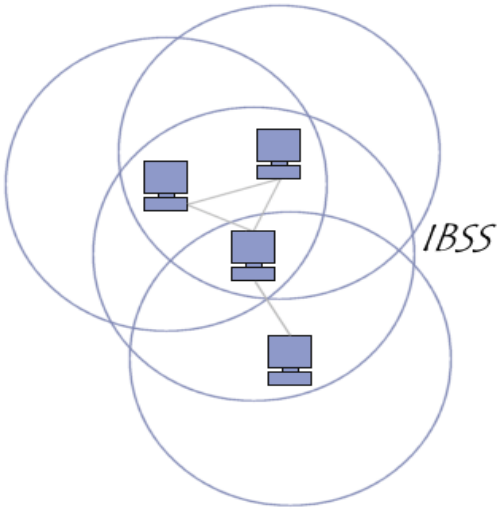
Bezdrátovou linku lze pochopit jako přípojku hostitele k základní stanici nebo k jinému hostiteli. Různé technologie bezdrátových spojení mají různé parametry jako přenosové rychlosti nebo oblast pokrytí. [3]

3.7 Struktura bezdrátové sítě

3.7.1 IBSS neboli Ad-Hoc sítě

Jedná se o nejjednodušší řešení ze všech sítí IEEE 802.11 v tom, že není vyžadována síťová infrastruktura, na obrázku 5 lze vidět strukturu této sítě. Hlavní výhodou sítě IBSS je, že neexistuje žádné hlavní zařízení. Všechna zařízení mají stejný stav a mohou komunikovat s jakýmkoliv jiným zařízením. U tohoto tytu sítí je však hlavní problém se zabezpečením přenosu. Takový typ připojení se většinou využívá jen jako dočasný, pokud všechna zařízení opustí síť, tak síť zanikne. [1]

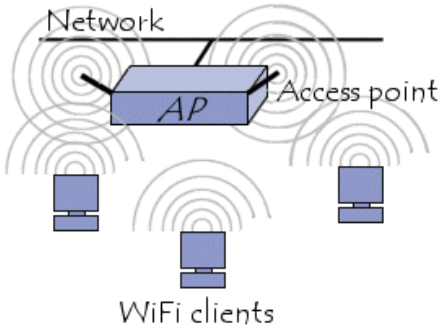
Obrázek 5 : IBSS síť [52]



3.7.2 BSS neboli infrastrukturní sítě

V tomto režimu je jedna stanice vysílač, obvykle hardware zvaný Access Point (AP), funguje jako brána mezi bezdrátovou a kabelovou sítí. Na obrázku 6 je vidět strukturu této sítě. Před tím, než se zařízení připojí k sítí, se připojí k AP, který umožňuje průchod paketů mezi bezdrátovým klientem a drátovou sítí, až po ověření bezdrátového klienta. [3]

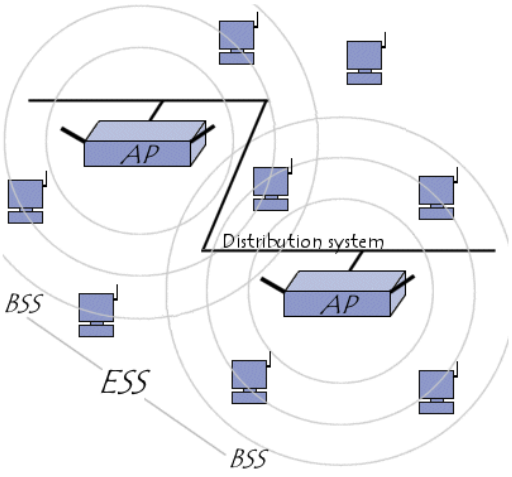
Obrázek 6: BSS síť [52]



3.7.3 ESS neboli rozšířené mesh sítě

ESS nachází využití tam, kde je třeba pokrýt větší prostory Wi-Fi signálem. Jedná se o několik propojených AP (neboli BSS), takzvaným distribučním systémem. Struktura této sítě je znázorněna na obrázku 7. Pod pojmem distribuční systém je možno si představit například kabel nebo bezdrátové propojení dvou Access Pointů. [3]

Obrázek 7: ESS síť [52]



3.8 Způsoby modulace

3.8.1 FHSS

Tato technologie se využívala hlavně pro vojenské účely. V průběhu 80. let byla tato technologie uvolněna pro civilní užití. Přenos signálu probíhá na rozprostřeném spektru. To znamená, že při přenosu bitů přeskakuje mezi několika frekvencemi.[1]

3.8.2 DSSS

DSSS je technikou rozptýleného spektra, při které je původní datový signál vynásoben pseudonáhodným rozšiřovacím kódem. Tento kód má vyšší bitrate, což vede k širokopásmovému kódovanému signálu. DSSS chrání před rušivými signály a činí signál méně nápadný. Pokud kód není znám, tak může i zabezpečovat přenos. Z těchto důvodů byl DSSS velice populární u armády, kde byl i poprvé využit. Využívá ho původní 802.11 standard a 802.11b standard. [1]

3.8.3 OFDM

Jedná se o digitální modulaci signálu, ve které je jeden datový tok rozdělen do několika samostatných úzkopásmových kanálů s různými frekvencemi pro snížení rušení. Původní bity datových proudů, které by byly v konvenčním jednokanálovém schématu vysílány postupně jsou vysílány paralelně, několik najednou v oddělených kanálech, ale při nižších rychlostech. [41]

Výhody [41]

- **Odolnost vůči selektivnímu úniku** – Tato výhoda souvisí s použitím více sub-kanálů, pokud je v jednom sub-kanálu signál narušen díky rušení, je možné vhodným kódováním (např. FEC) tuto chybu opravit.
    - Pod pojmem únik je možno si představit kolísání intenzity vlny na přijímací straně.
- **Velká účinnost spektra** – Díky využití překrývajících se nosičů využívá efektivně dostupné spektrum.

    - Spektrální účinnost je poměr přenosové rychlosti a šířky kmitočtového pásma.

- **Snížení mezisymbolové interference ISI** – Při zachování stejné přenosové rychlosti a při zvýšení počtu sub-kanálů je možné snížit modulační rychlost v jednotlivých sub-kanálech, to zapříčiní prodloužení doby symbolového stavu.

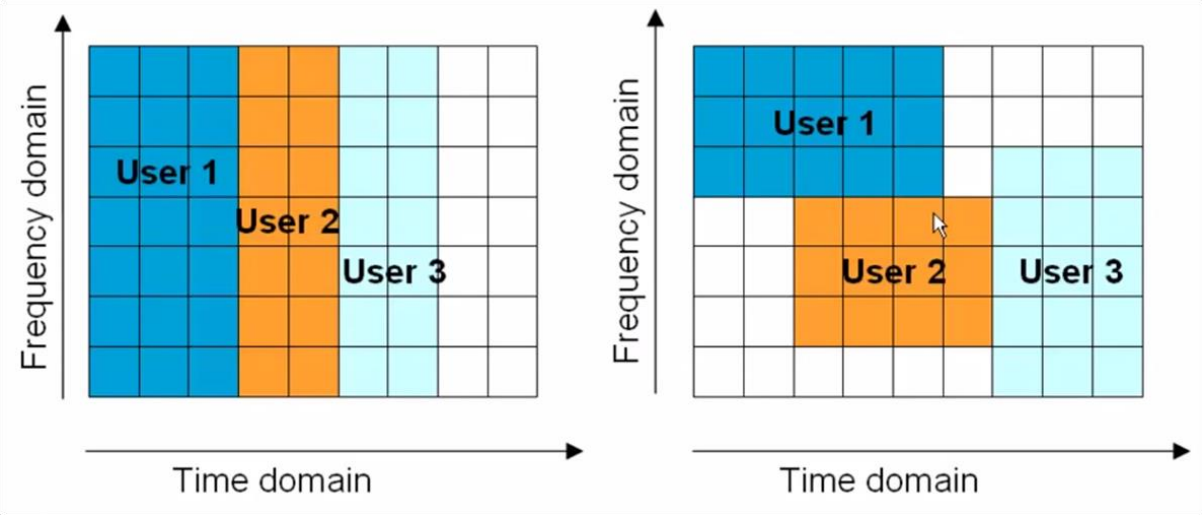
Nevýhody [41]

- **Nutnost dodržovat vzdálenost mezi sub-kanály** – Sub-kanály se nachází blízko od sebe. V případě, že bude vzdálenost sub-kanálů kolísat, mohou vznikat nežádoucí jevy ICI nebo ISI.
- **Vysoký poměr špiček signálu k průměrnému výkonu** – Stává se, že některé amplitudy výrazně převýší průměrnou hodnotu signálu, proto zesilovače na přijímací straně musí mít velký dynamický rozsah.

3.8.4 OFDMA

Jedná se o rozšíření populární architektury OFDM. Hlavním rozdílem mezi OFDM a OFDMA je, že u OFDM přiřazuje uživatele jen k časové doméně a OFDMA přiřazuje uživatele k časové i frekvenční doméně. Někteří uživatelé mohou mít lepší kvalitu připojení na určitém pásmu, tak jim ho OFDMA přiřadí. Na obrázku 8 je možné vidět rozdíl mezi OFDM a OFDMA. [20]

Obrázek 8: Rozdíl mezi OFDM a OFDMA [20]



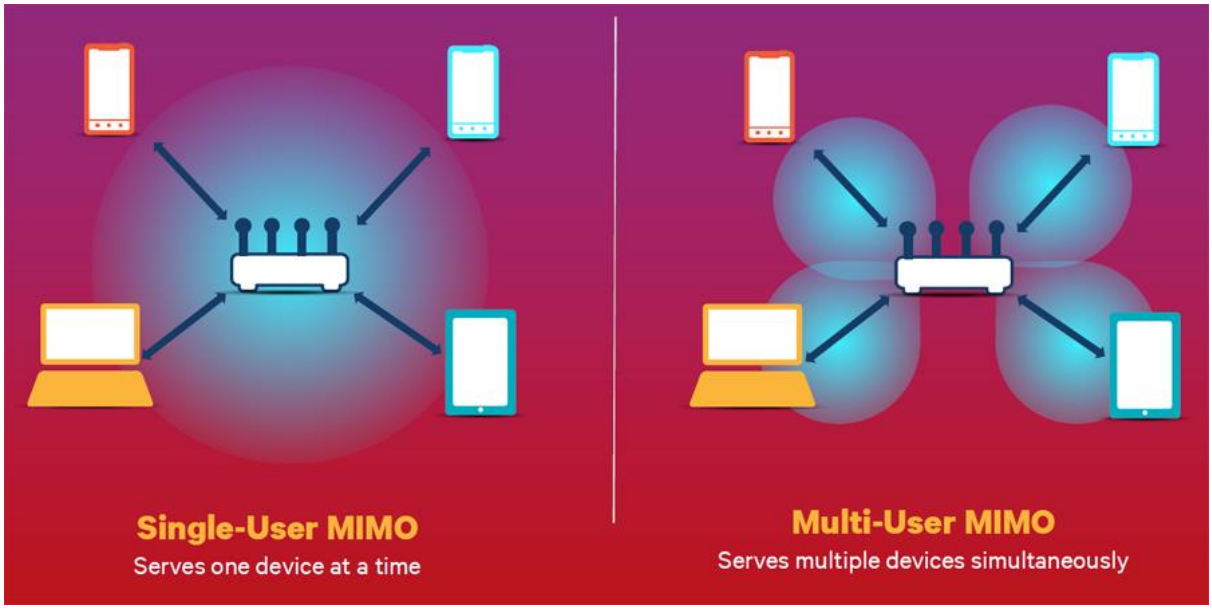
3.8.5 MIMO

MIMO je bezdrátová technologie, která je schopna přenášet více dat najednou pomocí využití více vysílačů a přijímačů. Technologie MIMO využívá jev zvaný multipath. Multipath zajišťuje díky různým odrazům od zdí nebo od různých objektů, že se přenášená informace k přijímací anténě dostane z několika různých úhlů a lehce rozdílných časů. Tento jev v minulosti způsoboval rušení a tím zpomaloval bezdrátové signály, ovšem při technologii MIMO je využit tak, že podstatně zvyšuje výkon sítí. MIMO funguje na frekvencích 2,4Ghz i 5Ghz. [45]

3.8.6 MU-MIMO

Technologie MU-MIMO byla vytvořena, aby zlepšila dostupnost signálu v prostředích, kde se připojuje k bezdrátové síti více uživatelů. Klasicky, pokud se k routeru připojí více uživatelů, tak obslouží prvního, zatímco ostatní čekají až na ně přijde řada. Díky této vlastnosti se síť lehce může přetížit, pokud se připojí hodně uživatelů. Systém MU-MIMO se stará o to, že poskytuje data více uživatelům najednou, aniž by se router přetížil. Na obrázku 9 je možné vidět rozdíl v přenosu dat mezi systémy MIMO a MU-MIMO. [39]

Obrázek 9: Rozdíl mezi MIMO a MU-MIMO [39]



4 Rozdělení bezdrátových sítí

4.1 Optická bezdrátová komunikace

OWC umožňuje bezdrátové připojení pomocí infračerveného, viditelného nebo ultrafialového pásma. Nabízí nám vysokou šířku pásma, nízké náklady a provoz v neregulovaném spektru. S těmito výhodami může být OWC dobrá alternativa k ostatním bezdrátovým technologiím. U budoucích bezdrátových sítí se považuje za možnou technologii, která bude řešit problémy s přetížením spektra a celkově zvýší kapacitu bezdrátové sítě. [17]

4.1.1 Komunikace viditelným světlem (VLC)

Tato technologie využívá světelné LED diody, které pulzují velmi vysokou rychlostí a tím pádem téměř neovlivňují osvětlení nebo lidské oko. Tento typ komunikace může mít širokou škálu uplatnění, jako například osobní nebo lokální bezdrátové sítě. [17]

4.1.2 Komunikace infračerveným světlem (IR)

Tento typ komunikace se využívá na krátké až střední vzdálenosti. Existují dva režimy, ve kterých tato komunikace funguje, takzvaný LOS a difuzní režim. Pokud pracuje v LOS režimu, nesmí být mezi vysílačem a přijímačem žádné překážky a dosah je většinou limitován do jednoho metru. Příkladem využití tohoto režimu může být například infraport u starých mobilních telefonů. Pokud pracuje v difuzním režimu, tak na sebe vysílač a přijímač nemusí přímo vidět. Ovšem i u tohoto režimu jsou určité limitace, signál se přenáší na bázi odrazu, takže přesto, že na sebe prvky nemusí přímo vidět, musí být zpravidla ve stejné místnosti, protože signál neprochází skrz překážky. Příkladem toho režimu může být například ovladač k televizi. [18]

4.1.3 Komunikace ultrafialovým světlem (UV)

Tato komunikace probíhá v takzvaném hlubokém UV pásmu, díky tomu je sluneční záření téměř zanedbatelné. Komunikace UV světlem umožňuje takzvanou NLOS komunikaci ve venkovním prostředí na krátkou vzdálenost, což znamená, že na sebe zařízení nemusí přímo vidět. [19]

4.2 Rádiové bezdrátové sítě

Rádiové bezdrátové sítě jsou nejběžnější typ bezdrátových sítí. Přenosové médium jsou rádiové vlny, které se nachází mezi 3kHz a 300 GHz v elektromagnetickém spektru.

4.2.1 Bluetooth (IEEE 802.15.1)

Bluetooth je bezdrátová komunikační technologie krátkého dosahu. Umožňuje přenos dat do vzdálenosti kolem 10 metrů. Bluetooth, stejně jako některé jiné bezdrátové technologie, využívá k provozu frekvenci 2,4Ghz. Oproti Wi-Fi má nižší výkon, tudíž je méně náchylný na rušení, ale na druhou stranu nedosahuje takových rychlostí přenosu. Tato technologie se nejčastěji vyskytuje v mobilních telefonech, ale existují i externí Bluetooth zařízení na připojení k počítači. Tuto technologii lze využít například při přenosu souborů mezi dvěma zařízeními nebo spárování mobilního telefonu s inteligentními hodinkami. [6]

4.2.2 ZigBee (IEEE 802.15.4)

ZigBee je technologie pro sítě PAN. Na rozdíl od technologií jako Bluetooth nebo Wi-Fi, neužívá komunikaci point to point, ale jednotlivé prvky sítě komunikují navzájem mezi sebou a fungují jako meshová síť. Tato technologie se nejčastěji využívá v chytrých domech. [1]

4.2.3 NFC

NFC je technologie, která umožňuje v bezprostřední blízkosti komunikovat bez potřeby připojení k internetu. NFC čip funguje jako jedna část bezdrátového spojení, jakmile je aktivován jiným čipem, umožňuje přenášet malé množství dat. Zařízení musí být od sebe maximálně 4 centimetry. K propojení není potřeba žádného párovacího kódu, protože čipy běží na velmi malém množství výkonu.

Velká výhoda, oproti ostatním typům bezdrátové komunikace, je velká energická účinnost. Často se vyskytuje v mobilních telefonech nebo na tiskárnách. Velice populární využití NFC čipu v dnešní době je na bezkontaktní platby mobilním telefonem. [5]

4.2.4 WiMAX (IEEE 802.16)

WiMAX je bezdrátová technologie využívaná na velkou vzdálenost, nejčastěji u sítí typu MAN. Tato technologie byla navrhována se záměrem vytvořit alternativu standardního kabelového připojení. Existují dvě základní formy této technologie, vysílací stanice, které jsou instalovány poskytovateli internetu a přijímače, které jsou součástí klientských zařízení. Výhoda této technologie je její flexibilita, není třeba na dané místo natahovat kabel. Nevýhodou je, že čím dál je uživatel od vysílače, tím pomalejší je jeho připojení. Někteří lidé si o této technologii myslí, že je to „lepší forma Wi-Fi", což není pravda, v základu jsou sice technologie podobné, ale každá je určená na něco jiného. Jedním z důvodů, proč WiMAX nenahrazuje Wi-Fi hotspoty je ten, že jsou na jeho provoz potřeba mnohem vyšší náklady. [1]

4.2.5 Wi-Fi (IEEE 802.11)

Wi-Fi je technologie, která umožňuje připojení různých zařízení k internetu bez použití fyzických kabelů. Wi-Fi je jeden z nejrozšířenějších typů bezdrátového přenosu. Při procházce po městě je možné zachytit několik různých signálů, jak už osobních, tak různých veřejných, vysílaných podniky jako služba zákazníkům. Signál je vysílaný pomocí zařízení nazývaného Access Point. Rozsah signálů se může lišit podle toho, jak dobrý má vysílač, ale většinou se pohybuje kolem 35 metrů. Přijímač Wi-Fi signálů je dnes integrovaný téměř v každém zařízení, jak v mobilních telefonech, tabletech či noteboocích. Někdy se využívá i síťová karta do stolních počítačů k přijímání Wi-Fi signálu. Jedním z hlavních důvodů popularity Wi-Fi je její cenová dostupnost, koupi vysílače si může dovolit téměř každý. [6]

4.2.6 Mobilní sítě

Vzhledem k tomu, že mobilní síť na telefonování je přítomná téměř po celém světě, začaly se tyto sítě rozvíjet, aby kromě hlasové komunikace podporovaly i přístup k internetu. Tento typ připojení by měl zajišťovat dostačující rychlost a hlavně velkou mobilitu, což znamená, že by měl poskytovat poměrně kvalitní signál i při poměrně rychlém pohybu, jako třeba jízdě vlakem či autem. [3]

2G

Tato síť byla vytvořena v roce 1991, s jejím nástupem umožnila první datové služby, jako SMS a MMS. Jednalo se o první mobilní digitální typ signálu. Dosahovala maximální rychlosti 50kbit/s. [10]

GPRS

Tato síť se běžně začala užívat v roce 2000. Zkratka, kterou je možné vidět při připojení k síti je „G". Tato technologie dosahovala maximální rychlost až 114kbit/s. [10]

EDGE

Tato síť se začala využívat v roce 2003. Při připojení k této síti se na displeji může ukázat zkratka „E". Maximální rychlost této sítě se pohybovala kolem 217kbit/s. [10]

3G

Tato síť byla prvně zapojena do provozu v roce 2001 v Japonsku. Díky rozšířenému využití a vývoji chytrých telefonů se jedná o jednu z nejznámějších sítí. Jednalo se o první mobilní síť, která umožnila používání mobilního internetu, jak je znám dnes. Maximální rychlost této sítě se pohybovala kolem 384kbit/s. [10]

HSPA

Standard HSPA je založen na stejné technologii jako 3G. Tato síť se začala nasazovat do provozu v roce 2010. Při připojení k této síti je možné vidět zkratku „H“ na displeji. Tato síť dosahovala rychlosti až 7,2Mbit /s. Díky této rychlosti se dalo pohodlně dívat na videa na YouTube či poslouchat streamovanou hudbu například na Spotify. [10]

HSPA+

Na zařízeních, které jsou připojené k této síti, je možné vidět zkratku H+. Tato technologie byla vydána několikrát, pokaždé se zvýšila její rychlost, při posledním vydání dosahovala rychlosti až 168 Mbit/s. [10]

LTE

Tato síť navazuje na předešlou 3G síť, ovšem operátoři ji dost často inzerují jako 4G. Ve skutečnosti tuto síť lze chápat jako krok mezi 3G a 4G, tedy 3,5G. Teoreticky může dosahovat rychlosti stahování až 172,8 Mbit/s a rychlosti uploadu až 57,6Mbit/s. [1] Česká republika je již touto sítí pokryta z 99%. [11]

4G

Jedná se o čtvrtou generaci širokopásmové mobilní sítě. Tato síť by měla dosahovat teoretické rychlosti až 1Gbit/s, ovšem tuto rychlost téměř nelze využít díky FUP limitům nastavených operátory. [1]

5G

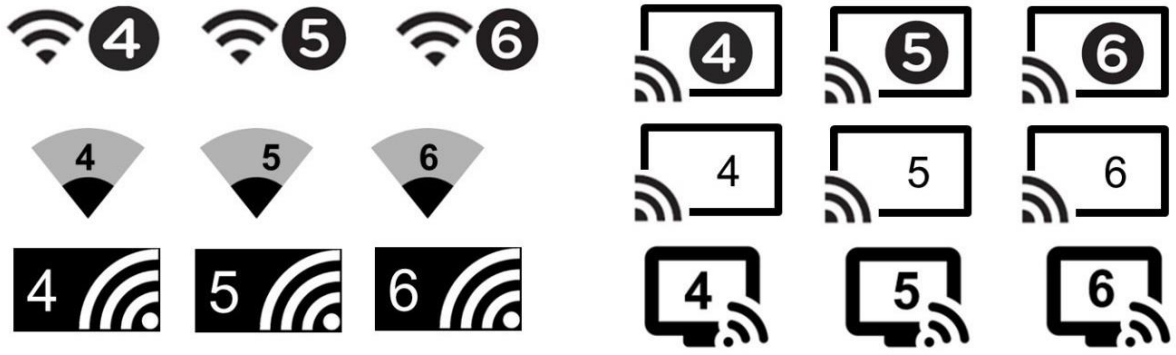
Jedná se o pátou generaci připojení k mobilnímu internetu, která nabízí výrazně rychlejší připojení než předchozí generace. Očekávaná doba spuštění těchto sítí by měla být do roku 2020. Teoretická rychlost této sítě by mohla dosahovat až 20Gbit/s. Ovšem hlavním zaměřením této generace není rychlost, ale vytvoření síťové architektury, která splňuje požadavky internetu věcí. [12]

5 Standardy IEEE 802.11

Standard IEEE 802.11 byl vyvinut institutem elektrotechnického a elektronického inženýrství (IEEE). Jedním z hlavních důvodů standardizace byla vzájemná kompatibilita zařízení od různých výrobců. Standardy se stále rozvíjejí a s tím jejich propustnost, stabilita, rozsah připojení, možnost využití nových frekvencí a spousta dalších parametrů.

Vzhledem k tomu, že názvy standardů nejsou zrovna podle abecedy, se u novějších standardů zavedlo číslování dle generací. Toto číslování zlepšuje přehled o technologiích pro standardní uživatele a u některých zařízení lze na první pohled poznat, kterou technologii využívají. Na obrázku 10 je možné vidět případné značky různých Wi-Fi na uživatelském rozhraní.

Obrázek 10: Značení Wi-Fi na uživatelském rozhraní [53]



5.1 Hlavní Wi-Fi standardy

5.1.1 IEEE 802.11-1997

V roce 1997 schválil IEEE první standard 802.11. Stanovili dvě přenosové rychlosti 1 Mbit/s a 2 Mbit/s na frekvenci 2,4 GHz. Kvůli své pomalé rychlosti nebyl příliš rozšířený. [1]

5.1.2 IEEE 802.11a

Jedná se o první rozšíření standardu 802.11, které bylo schváleno v roce 1999. Tento standard byl spíše rozšířený ve firemním prostředí díky tomu, že na jeho provozování byl potřeba celkem drahý hardware. Dosahuje rychlosti až 54 Mbps na frekvenci 5 GHz. Rozsah signálu 802.11a byl omezen pro použití frekvence 5Ghz, vysílač 802.11a mohl pokrýt ani ne jednu čtvrtinu toho, co 802.11b. Díky využití frekvenčního pásma 5 GHz, je tento standard odolnější vůči rušení.[1]

5.1.3 IEEE 802.11b

Byl uveden a schválen v roce 1999. Tento standard dosáhl velkého komerčního úspěchu. Se standardem 802.11b začaly ve velkém vznikat první domácí Wi-Fi sítě, které dosahovaly v průměru rychlosti okolo 4-5 Mbit/s. Jedná se o rozšíření standardu 802.11, který dosahuje rychlosti až 11Mbit/s. Využívá stejnou frekvenci jako 802.11 2,4 GHz. Vzhledem k tomu, že tento standard využívá pásmo 2,4Ghz, může se setkávat s rušením od jiných domácích produktů, třeba od bezdrátových mobilních telefonů nebo mikrovlnných trub. [1]

5.1.4 IEEE 802.11g

Tento standard je kombinací dobrých vlastností standardu 802.11a a 802.11b, díky tomu se stal převládajícím standardem na celém světě. Standard 802.11g dosahuje rychlosti až 54 Mbit/s na frekvenci 2,4Ghz, což je stejná rychlost jako u standardu 802.11a, ale díky využití frekvence 2,4Ghz dosahuje o dost většího rozsahu. Reálně zařízení s tímto standardem dosahují rychlosti okolo 24-31 Mbit/s. [1]

5.1.5 IEEE 802.11n (Wi-Fi 4)

Tento standard byl schválen v roce 2009. Byl navržen tak, aby nahradil starší standardy 802.11a, 802.11b a 802.11g. Využívá takzvaný systém MIMO, který umožňuje, aby standard zvládl koordinovat více signálů, v případě standardu 802.11n až čtyři najednou. Tento standard může dosahovat rychlosti až 300 Mbit/s a dokáže pracovat v pásmech 2,4Ghz i 5Ghz. Do roku 2014 sloužil jako nejrychlejší Wi-Fi standard, než se schválil standard 802.11ac. [1]

5.1.6 IEEE 802.11ac (Wi-Fi 5)

Jedná se o nástupce standardu 802.11n a o pátou generaci Wi-Fi. Vývoj začal v roce 2011 a na začátku roku 2014 ho formálně schválili. Byl navržen tak, aby fungoval jako „Gigabit Ethernet". Standard 802.11ac nabízí teoretickou datovou rychlost až 3,4Gbit /s. Toho je dosaženo prostřednictvím kombinace bezdrátových signalizačních vylepšení, jako třeba že kanály využívají širší rozsah frekvenčních signálů nebo většího počtu vysílačů (popř. antén), umožňujících díky systému MU-MIMO přenášet více signálů najednou a při připojení více uživatelů najednou, není tak náročný na přetížení. Tento standard využívá pouze pásma 5 GHz. [1]

5.1.7 IEEE 802.11ax (Wi-Fi 6)

Na tomto standardu ještě IEEE pracuje a plánuje jej zveřejnit někdy v průběhu roku 2019. Tento standard by měl být nástupce standardu 802.11ac. Tento standard je také možné najít pod jménem HEW. Na rozdíl od ostatních standardů, kde hlavním cílem bylo zvýšit rychlost přenosu, se tento standard zaměřil především na vyšší efektivitu, výkon a kapacitu. Dále by tento standard měl vyhovovat požadavkům internetu věcí. Přesné parametry tohoto standardu ještě nejsou známé, ale spekuluje se, že by měl dosahovat rychlosti až 11Gbit/s. Další velký plus oproti svému předchůdci je, že kromě pásma 5Ghz dokáže využívat i pásmo 2,4Ghz a dokonce i případně pásma v rozsahu 1-7Ghz. [1]

Tabulka 2: Shrnutí parametrů jednotlivých Wi-Fi standardů [vlastní]

Standard	Frekvence (GHz)	Rychlost (Mbit/s)	Kódování	Rok vydání
IEEE 802.11 (1997)	2,4	2	FHSS, DSSS	1997
IEEE 802.11a	5	54	OFDM	1999
IEEE 802.11b	2,4	11	DSSS	1999
IEEE 802.11g	2,4	54	OFDM	2003
IEEE 802.11n	2.4 a 5	600	OFDM - MIMO	2009
IEEE 802.11ac	5	3400	OFDM - MU-MIMO	2013
IEEE 802.11ax	2.4, 5 a 1-7	10500	OFDMA - MU-MIMO	asi konec 2019

5.2 Ostatní standardy a revize

5.2.1 IEEE 802.11d

Jedná se o doplněk k MAC vrstvě u standardu IEEE 802.11, který podporuje využívání sítí WLAN 802.11 po celém světě. V některých zemích nemohly standardy IEEE 802.11 legálně fungovat, proto tento standard přidává funkce a omezení, aby byly dostupné po celém světě v rámci pravidel těchto zemí. [22]

5.2.2 IEEE 802.11i

Tento standard byl schválen v roce 2004 a dá se chápat jako dodatek do standardu IEEE 802.11. Zdokonaluje šifrovací algoritmus pro bezdrátové sítě, které využívají populární standardy IEEE 802.11a, b, g. Vyžaduje nové protokoly šifrovacích klíčů TKIP a AES, které byly ve své době většinou společností považovány za dostatečnou ochranu. AES ovšem vyžaduje speciální čip, což mohlo znamenat nutný upgrade pro sítě WLAN. [23]

5.2.3 IEEE 802.11h

Tento standard je doplněk do rodiny standardů IEEE 802.11. Hlavním cílem tohoto standardu bylo vyřešení problémů s rušením, které vznikly při využívání technologie 802.11a, zejména u vojenských radarových systémů nebo u nemocničních zařízení. Tento standard využívá převážně dva systémy DFS a TPC. DFS detekuje přítomnost jiných zařízení na daném kanálu, pokud detekuje cizí signál, tak přehodí síť na jiný kanál. TCP snižuje výkon každého vysílače v sítí na úroveň, která sníží riziko rušení z ostatních systémů, ale zachová dobrý výkon sítě. [24]

5.2.4 IEEE 802.11j

Tento standard je speciálně designovaný pro japonský trh, jedná se o dodatek ke standardu IEEE 802.11. Umožňuje provoz WLAN v pásmu 4,9Ghz až 5Ghz, aby vyhovoval japonským předpisům pro provoz rádiových signálů. [25]

5.2.5 IEEE 802.11e

Standard IEEE 802.11e byl schválen roku 2005 a definuje sadu kvality služeb (QoS) pro WLAN pomocí změn na MAC vrstvě. Tento standard je obzvláště důležitý pro funkce, které jsou náročné na zpoždění, jako třeba streamování videa nebo VoIP. [26]

5.2.6 IEEE 802.11-2007

Jedná se o revizi standardu IEEE 802.11. Tato revize sjednotila všech osm doposud vydaných standardů IEEE 802.11. Mimo jiné také vylepšila funkce na MAC a PHY vrstvách. [21]

- IEEE 802.11a – Komunikační standard
- IEEE 802.11b – Komunikační standard
- IEEE 802.11d – Globální dostupnost standardů
- IEEE 802.11g – Vylepšení výkonu sítě
- IEEE 802.11h – Řešení problému s rušením
- IEEE 802.11i – Šifrování bezdrátové komunikace
- IEEE 802.11j – Provoz WLAN v pásmu 4,9 - 5Ghz pro japonský trh
- IEEE 802.11e – Sada kvality služeb pro WLAN

5.2.7 IEEE 802.11k

Standard IEEE 802.11k je dodatek ke standardu IEEE 802.11-2007, který rozšiřuje funkce RRM pro sítě WLAN. Specifikuje doporučení pro optimalizaci údržby a zvýšení výkonu bezdrátových sítí. [27]

5.2.8 IEEE 802.11r

Podobně jako ostatní standardy v této kategorii se jedná o dodatek ke standardu IEEE 802.11-2007. Tento standard zařizuje rychlé a hlavně bezpečné přechody mezi jednotlivými přístupovými body (AP). Protokol se připojí k novému přístupovému bodu ještě než se provede přechod, aby měl čas realizovat bezpečné spojení a minimalizoval dobu výpadku spojení. [28]

5.2.9 IEEE 802.11y

Přidání dodatku IEEE 802.11y ke standardu IEEE 802.11-2007, umožňuje využití mechanismů, které dovolují kooperativní využití pásma 3650Mhz-3700Mhz. Využívá vysílače s vysokým výkonem pro přenos dat. Umožňuje způsob regulace spektra zvaný „light licencing“, klientská zařízení nepotřebují licenci, ale vysílací stanice musí být licencovány. Stanice sdílí zodpovědnost za rušení, pracují spolu, aby mu předcházely. Tento standard byl vyvinut převážně pro USA. [29]

5.2.10 IEEE 802.11w

Tento standard je postaven na standardu IEEE 802.11i. Ovšem standard IEEE 802.11i chrání pouze datové rámce paketu a zanechává řídící rámce bez jakékoliv ochrany nebo ověření. Standard 802.11w se primárně zaměřuje na ochranu řídících rámců. Tento standard se stará o to, aby zprávy chodily z ověřených zdrojů pomocí systému MIC. S tímto standardem přišel i nový šifrovací klíč IGTK, který je využit k ochraně robustních řídících rámců vysílání. [30]

5.2.11 IEEE 802.11p

Jedná se o standard, který umožňuje bezdrátovou komunikaci ve vozidlových prostředích (WAVE). Umožňuje výměnu dat mezi vysokorychlostními vozidly a silniční infrastrukturou. Dopravní komunikační aplikace nemohou tolerovat dlouhé prodlevy při vytváření spojení, je důležité, aby mohly včas komunikovat s ostatními vozidly na silnici. Vzhledem k tomu, že komunikační spojení mezi vozidly vydrží jen krátkou dobu, tento standard nečeká na ověření před výměnou dat, tudíž data se začnou přijímat a odesílat hned po připojení ke komunikačnímu kanálu. Z tohoto důvodu se nemohou využít některé bezpečnostní mechanismy standardu IEEE 802.11, kontrola dat musí být provedena na vyšších vrstvách. [31]

5.2.12 IEEE 802.11z

Tento standard umožňuje přímý přenos dat mezi dvěma bezdrátovými klienty, kteří jsou připojeni ke stejné síti. Obvykle jsou data přenášena mezi klienty přes AP. Standard IEEE 802.11z dovolí klientům vzájemně navázat přímé spojení, zatímco jsou stále připojeni k Access Pointu. Tento mechanismus se nazývá TDLS. Použitím tohoto mechanismu se sníží objem dat přenášených přes AP a tím je zabráněno jeho přetížení. [32]

5.2.13 IEEE 802.11v

Standard 802.11v je dodatek ke standardu IEEE 802.11, poskytuje možnost konfigurace klientských zařízení během připojení k bezdrátové síti. Umožňuje výměnu informací o topologii sítě a o rádio-frekvenčním prostředí, čímž se celkově zvedne kvalita sítě. [33]

5.2.14 IEEE 802.11u

Jedná se o dodatek ke standardu IEEE 802.11, který umožňuje připojení k externím sítím pomocí běžných zařízení, jako třeba chytrých telefonů nebo tabletů. Zařízení, která podporují tento standard využívají technologie zvanou HotSpot 2.0. Díky této technologii uživatelé nemusí manuálně vyhledávat Wi-Fi sítě a zadávat hesla, pokud zařízení detekuje síť s tímto standardem, zařízení se automaticky ověří pomocí karty SIM a připojí se. Tímto způsobem se ulehčí přetížení celulárních sítí, které jsou mnohem náročnější na provoz než Wi-Fi sítě. [34]

5.2.15 IEEE 802.11s

Standard IEEE 802.11s je dodatek ke standardu IEEE 802.11. Je zaměřený na meshové sítě, které nejsou v původním standardu definovány. Standard 802.11s umožňuje bezdrátovým klientům možnost připojení k uzlům bezdrátové sítě a zároveň slouží jako přístupové body. Směrování uzlů v síti je založeno na MAC adrese. To dává bezdrátovým zařízením možnost vidět ostatní uzly a směrovat provoz přes nejbližší uzly v síti. [1]

5.2.16 IEEE 802.11-2012

Jedná se o druhou revizi standardu IEEE 802.11, která podobně jako předchozí revize 802.11-2007 sjednotila doposud vydané dodatky ke standardu IEEE 802.11. [36]

- IEEE 802.11k – Řízení rádiových zdrojů
- IEEE 802.11r – Rychlé přechody mezi sítěmi WLAN
- IEEE 802.11y – Funkce v pásmu 3650Mhz-3700Mhz pro USA
- IEEE 802.11w – Ochrana řídících rámců
- IEEE 802.11n – Vylepšení výkonu sítí
- IEEE 802.11p – Bezdrátová komunikace ve vozidlových prostředích
- IEEE 802.11z – Přímý přenos mezi bezdrátovými klienty
- IEEE 802.11v – Správa bezdrátových sítí
- IEEE 802.11u – Funkce s externími sítěmi
- IEEE 802.11s – Mesh sítě

5.2.17 IEEE 802.11ae

Tento dodatek ke standardu IEEE 802.11 definuje sadu kvality služeb pro řídící rámce (QMF). Bez QFM stanice odesílá všechny řídící rámce přes nejvyšší kategorii přístupu (AC). QFM poskytuje mechanismus, který rozdělí provoz do různých AC. [37]

5.2.18 IEEE 802.11aa

Základní standard IEEE 802.11 nemá moc dobrou podporu vícesměrového vysílání (multicast). Tento dodatek se zabývá tímto problémem a poskytuje možnost spolehlivého vícesměrového vysílání pro bezdrátové sítě WLAN. Multicast je možno považovat za skupinovou komunikaci, kde jsou data přenášena více zařízením současně. Tento standard je zaměřen především na přenosy videa. [1]

5.2.19 IEEE 802.11ad

Tento standard se dá chápat jako dodatek ke standardu IEEE 802.11, aby mohl fungovat v pásmu okolo 60Ghz. Díky využití toho pásma může rychlost přenosu dosahovat rychlosti až 7Gbit/s, ovšem s tím přichází i velká nevýhoda, signály jsou pohlcovány různými překážkami, tudíž se dosah pohybuje okolo 10 metrů. [1]

5.2.20 IEEE 802.11af

Tento standard umožňuje přenos v nevyužitých televizních pásmech (neboli v bílých mezerách). Díky tomuto získal tento standard přezdívku White-Fi. Funguje na frekvencích 470-790 MHz v Evropě a 54-698 MHz v USA. Vzhledem k tomu, že funguje na poměrně nízkých frekvencích, tak dosahuje vyšších vzdáleností než klasické standardy. [1]

5.2.21 IEEE 802.11-2016

Jedná se o třetí revizi standardu IEEE 802.11. V této revizi se zdokonalily existující funkce MAC a PHY vrstev a odebraly se některé zastaralé funkce. Obdobně jako předchozí revize sjednocuje některé doposud vydané standardy. [42]

- IEEE 802.11aa – Podpora vícesměrového vysílání videa
- IEEE 802.11ae – Priority přenosu řídících rámců
- IEEE 802.11ac – Zdokonalený přenosový standard
- IEEE 802.11ad – Vysokorychlostní přenos v pásmech okolo 60 Ghz
- IEEE 802.11af – Přenos v nevyužívaných televizních kanálech

5.2.22 IEEE 802.11ah

Tento standard lze také najít pod názvem HaLow. Změny na PHY a MAC vrstvě umožnily tomuto standardu pracovat v pásmu 900MHz. Díky této nízké frekvenci se signál poměrně lehce šíří přes překážky a dosahuje o dost větších vzdáleností než většina ostatních standardů, maximální dosah se pohybuje okolo jednoho kilometru. Tento standard je také velice energeticky úsporný, toho je dosaženo díky předem nastaveným intervalům probouzení a spánků. Tento standard je ideální pro malé objemy dat, které jsou potřeba poslat na dlouhé vzdálenosti. [1]

5.2.23 IEEE 802.11ai

Standard IEEE 802.11ai poskytuje metody k rychlému navázání spojení (FILS). Bezdrátový klient naváže spojení během prvních 100ms bez výrazného snížení bezpečnosti. Hlavní využití tohoto standardu je možné vidět v místech, kde velké množství uživatelů pravidelně přichází a odchází ze sítě, tedy u sítí využívajících strukturu ESS. [44]

5.2.24 IEEE 802.11aj

Tento standard je modifikace PHY a MAC vrstev standardu IEEE 802.11ad, která umožňuje provoz v Čínském milimetrovém frekvenčním spektru kolem 45Ghz a 60Ghz. [40]

5.2.25 IEEE 802.11aq

Standard IEEE 802.11aq dovoluje zjištění, jaké služby fungují na bezdrátové síti WLAN bez nutnosti připojení k dané bezdrátové síti. Umožňuje uživateli učinit informované rozhodnutí, jestli chce zahájit výměnu informací mezi jeho zařízením a přístupovým bodem. [38]

5.2.26 IEEE 802.11ay

Tento standard zlepšuje vlastnosti standardu IEEE 802.11ad, pomocí různých technických vylepšení. Hlavním důvodem zavedení tohoto standardu byly požadavky kladené na jeho populárního předchůdce, které z technických důvodů nemohly být splněny. Mezi hlavní vylepšení se řadí využití technologie MIMO, lepší zpracování signálu a možnost propojení kanálů pro zvýšení výkonu. [16]

6 Zabezpečení počítačových sítí

Mnoho uživatelů bezdrátových sítí si neuvědomuje, že se signál šíří přes zdi budov či jiné překážky, což je největší problém bezpečnosti bezdrátových sítí. Při využití dobré antény se nezvaný host nebo útočník může velice snadno připojit a to i když vysílač dobrou anténu nemá a je od něj poměrně daleko.

Zabezpečení sítě je velmi důležité téma, které by nikdo neměl podceňovat, jak vlastníci malých domácích sítí, tak velké podniky. Lze jej chápat jako preventivní opatření k ochraně síťové infrastruktury před neoprávněným přístupem, zneužitím, zničením či ukradením dat. Útočníkům se bohužel stále daří nacházet různé bezpečnostní poruchy a slabiny systémů. Z tohoto důvodu se musí stále vyvíjet nová zabezpečení, kterými se tyto chyby opraví. Existuje spousta typů útoků, kterým je nutno se bránit, počínaje viry, červy, DoS, odposlouchávání a mnoho dalších. [4]

6.1 Bezdrátové šifrovací protokoly

Už od počátku bezdrátových sítí bylo jasné, že je potřeba data šifrovat. Problémem šifrování je, že různé typy šifrování se dají různými způsoby obejít, proto je nutné, aby se šifrovací technologie rozvíjely zároveň s rozvojem standardů IEEE 802.11. V dnešní době se do starších zařízení může dostat útočník velice jednoduše, protože starší typy zabezpečení poskytují pouze minimální obranu proti útoku.

6.1.1 WEP

Jedná se o první typ zabezpečení WLAN, který se využíval u standardů IEEE 802.11a a IEEE 802.11b. Byl navržen tak, aby poskytoval ochranu srovnatelnou se standartní kabelovou sítí LAN, která je obecně chráněna mechanickými ochranami (řízený přístup do budovy, atd...). Ovšem tato ochrana měla velké nedostatky a v protokolu se dají zachytit a analyzovat určité části, ze kterých se dal velice lehce získat šifrovací klíč. Mezi další nedostatky patří například to, že klíče se vkládají lokálně a ručně a díky tomu se málokdy mění. Maximální délka klíče mohla být pouze 64 bitů, ovšem reálná délka klíče se pohybovala kolem 40 bitů, tudíž se dá klíč získat pomocí útoku „brute force", zhruba do dvaceti minut. [3]

Systém ověřování WEP

1. Klient odešle žádost o autentizaci k AP
2. AP zašle klientovi takzvanou „výzvu”
3. Klient zašifruje přijatou výzvu svým WEP klíčem a pošle ho zpět
4. AP dešifruje odpověď svým klíčem, pokud se shoduje s odeslanou výzvou, odešle zpět pozitivní odpověď.

6.1.2 WEP2

WEP2 bylo krátce využívané rozšíření svého předchůdce WEP. Hlavním cílem bylo zlepšit bezpečnost bezdrátových přenosů u zařízení, které díky hardwarovým limitacím nepodporovaly lepší protokoly jako WPA nebo WPA2. S příchodem WEP2 se zvedla maximální délka šifrovacího klíče na 128 bitů, což výrazně pomohlo proti útokům brute force. Bohužel nedostatky protokolu WEP šly velice hluboko, proto se vývoj tohoto protokolu zastavil. [14]

6.1.3 WPA

Po prolomení ochrany WEP v roce 2001 začala Wi-Fi Alliance vytvářet nové zabezpečení WPA, které bylo nasazeno v roce 2002. Toto zabezpečení vzniklo při čekání na WPA2. Jádro tohoto mechanismu je podobné jako u WEP, oba musí na začátku a na konci použít stejný šifrovací klíč. Ovšem zatímco WEP využívá u každého autorizovaného systému stejný klíč, WPA využívá protokol TKIP, takže se klíč nedá odposlechnout z nezašifrovaného záhlaví rámce. Další výhodou WPA oproti WEP je, že pro autorizaci uživatelů využívá protokol EAP, kromě autorizování počítačů jen pomocí MAC adresy, využívá i několik dalších metod. [2]

6.1.4 WPA2

V roce 2005 bylo zavedeno novější WPA2, které přineslo kvalitnější šifrování AES a namísto protokolu TKIP začalo využívat protokol CCMP. Šifrování AES bohužel vyžaduje hardwarovou podporu, proto ho nebylo možno využívat u starších zařízení. Od roku 2006 bylo WPA2 povinností pro všechny zařízení, co chtěly certifikaci a logo Wi-Fi. WPA2 bylo prolomeno v roce 2017 útokem KRACK. [2]

6.1.5 WPA3

Po dlouhých čtrnácti letech používání WPA2 začal být potřeba nový standard. Standard WPA3 přidává nové funkce, které WPA2 neposkytoval. WPA3 nahrazuje doposud využívanou autentizační metodu PSK lepší technologií SAE. Díky tomu je síť lépe chráněna i při využití hesla, které nevyhovuje bezpečnostním standardům. WPA3 chrání data uživatelů i přesto, že útočník zná heslo a je sám úspěšně připojen k sítí. [9]

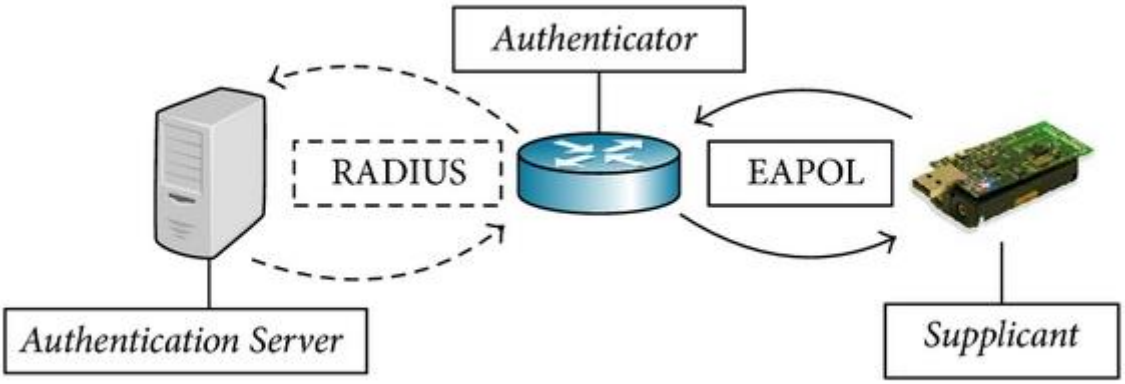
6.2 Autentizace sítí pomocí IEEE 802.1x

Tento standard byl navržen ke zvýšení bezpečnosti lokálních bezdrátových sítí WLAN, které využívají IEEE 802.11 standard. Standard IEEE 802.1x využívá centrální autoritu, u které se uživatelé musí ověřit. Tento standard využívá autentizační protokol EAP, který poskytuje několik různých autentizačních metod, v současné době kolem čtyřiceti. Na obrázku 11 je možné vidět architekturu 802.1x. [8]

Postup autentizace [47]

1. Žadatel odešle požadavek na připojení k přístupovému bodu.
2. Přístupový bod si vyžádá autentizační informace dle EAP protokolu.
3. Klient odešle své autentizační informace dle EAP protokolu.
4. AP přepošle žádost na RADIUS server.
5. RADIUS server pošle přístupovému bodu výzvu s EAP metodami, kterými se musí žadatel ověřit.
6. Přístupový bod přepošle výzvu žadateli.
7. Žadatel odešle odpověď přístupovému bodu, který ji přepošle na RADIUS server
8. Pokud je autentizace úspěšná, tak přístupový bod odblokuje klientovi datový provoz.

Obrázek 11: Architektura IEEE 802.1x [54]



6.3 Provozní zabezpečení: Firewall

Téměř všechny organizace mají svou interní síť připojenou k veřejnému internetu. Z tohoto důvodu může být tato síť ohrožena. Útočník se může pokusit například nasadit do sítě červa, který může například ukrást firemní tajemství nebo namapovat konfiguraci interní sítě a spustit útok DoS.

Firewall lze chápat jako kombinaci hardwaru a software, který izoluje interní síť od internetu, dovoluje některým paketům projít dovnitř do sítě a některé úplně zablokuje. Dovoluje správci sítě řídit přenos paketů mezi venkovním světem a zdroji ve spravované síti.

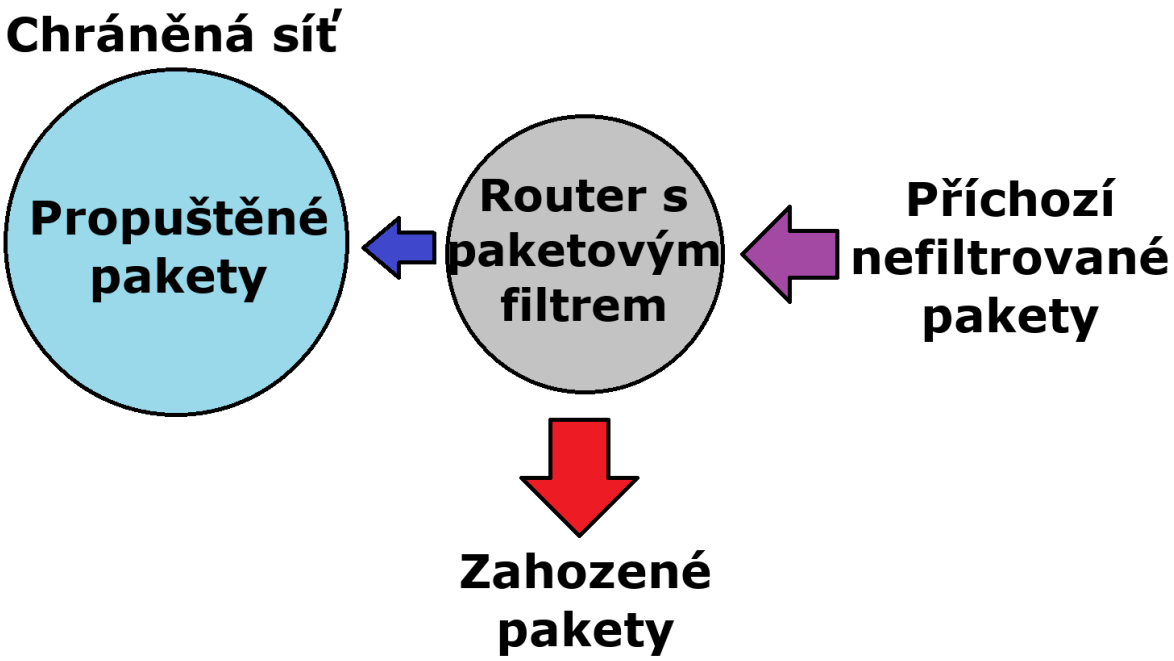
Nastavení a instalace firewallu je velice důležitý krok, na kterém je třeba si dát extra záležet, protože pokud je firewall do sítě nainstalovaný nebo nastavený špatně, dá se velice lehce obejít. Takto nainstalovaný firewall je ve finále horší než nemít žádný, protože poskytuje falešný pocit bezpečí. Firewall by měl být nastaven tak, aby veškerá komunikace s venkovním internetem probíhala přes něj. Větší firmy mohou využít více vrstev firewallu najednou nebo distribuovaný firewall.

Firewall chrání zařízení před různými typy útoků metodou filtrování přenášené komunikace. Filtrace přenášené komunikace případného nezvaného hosta probíhá především na aplikační, síťové nebo transportní vrstvě. [3]

6.3.1 Paketové filtry

Jedná se o nejstarší formu firewallu, funguje na principu tabulky pravidel, kde jsou uvedeny adresy a porty mezi kterými se mohou přenášet pakety. Hlavní výhodou tohoto typu firewallu je jeho vysoká propustnost dat, ovšem nevýhodou je, že útočník může celkem snadno falšovat údaje o původu paketů, tudíž tato metoda není moc bezpečná. Na obrázku 12 je vidět, jak paketový filtr propouští pakety. [3]

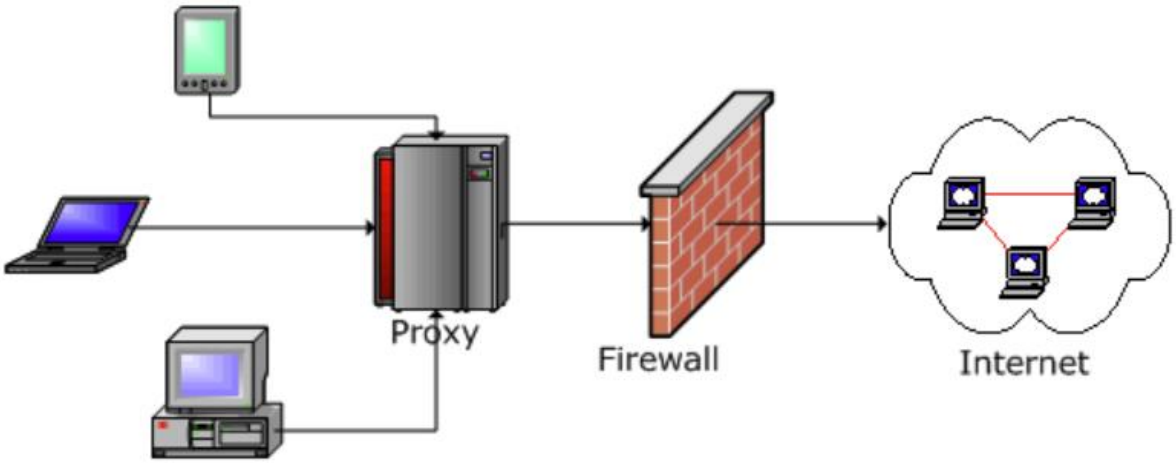
Obrázek 12: Funkce paketového filtru [vlastní]



6.3.2 Aplikační brány (Proxy firewall)

Aplikační brána je program, který běží na firewallu mezi dvěma sítěmi. Když se klient chce připojit k cílové službě, připojí se první k aplikační bráně, která vyjednává s cílovou službou jménem klienta. Tímto se vytvoří dvě spojení, jedno mezi klientem a proxy serverem a jedno mezi proxy serverem a cílovým serverem. Vzhledem k tomu, že veškerá komunikace probíhá přes proxy server, počítače za firewallem jsou skryty a chráněny. Velkou nevýhodou je malá propustnost dat, ale poskytují lepší ochranu než paketové filtry. [3]

Obrázek 13: Architektura aplikační brány [55]



6.3.3 Stavové paketové filtry

Kromě kontroly adresy a portu monitorují také stav aktivních připojení a využívají tyto informace k vyhodnocení, který síťový paket propustit firewallem. Výhodou je velmi vysoká rychlost oproti aplikačním branám a poměrně dobrá bezpečnost oproti standardním paketovým filtrům. Nevýhodou je nižší bezpečnost oproti aplikačním branám. [3]

6.3.4 Stavové paketové filtry s IDS

Kromě funkce standardních stavových paketových filtrů dokáží i částečně jako antivirus dle databáze signatur rozpoznat vzorce útoků a packet nepropustit. Výhodou je velmi vysoká úroveň bezpečnosti při zachování relativně velké propustnosti paketů. [3]

6.3.5 Neuronové firewally

Standardní firewally jsou založeny na sestavě pravidel, na jejichž bázi vyhodnocují přijaté pakety. To znamená, že nemohou udělat nic, co nebylo výslovně nakonfigurováno. Neuronový firewall modeluje svá pravidla pomocí umělé neuronové sítě, což poskytuje možnost větší adaptability a flexibility k měnícím se okolnostem. [56]

7 Závěr

Obliba bezdrátových technologií v posledních několika letech razantně vzrostla. Tato práce stručně popisuje historii bezdrátových přenosů, bez kterých by bezdrátové sítě nemohly existovat. Jedním z hlavních cílů této práce bylo stručně popsat princip, funkce a rozdělení bezdrátových sítí jako takových.

Dále se práce zaměřuje na podrobný popis standardů IEEE 802.11, jejich porovnání, přehled a rozvoj jejich služeb s postupně rostoucími nároky na ně. Práce mimo jiné také pojednává o zabezpečení bezdrátových sítí, které je v dnešní době jejich neoddělitelnou součástí.

Je jasné, že rozvoj populárního standardu IEEE 802.11 se nijak nezpomaluje. Ovšem je nutné se zamyslet nad tím, jestli je tento trend ten správný. Frekvenční pásmo 2,4Ghz je téměř úplně zahlcené a pásmo 5Ghz bude brzo pravděpodobně také. Proto, při budoucím rozvoji tohoto standardu, bude nutné, aby telekomunikační úřad vymezil další frekvenční pásmo. To ovšem není tak jednoduché, protože o další pásmo nemají zájem jen Wi-Fi standardy, ale i třeba mobilní operátoři a další.

Odhadnout cestu, kterou půjde budoucí bezdrátová technologie je velice obtížné. Rozhodně nelze zanedbat ani optickou bezdrátovou komunikaci, která v posledních letech zaznamenala velký pokrok. Hlavní výhodou této možnosti je široké spektrum, které poskytuje.

Rozhodně většina moderních bezdrátových standardů je designována tak, aby splňovala požadavky internetu věcí. Internet věcí rozšiřuje konektivitu internetu i na nestandardní zařízení jako například domácí spotřebiče nebo vozidla. Cílem internetu věcí propojení těchto zařízení přes internet, aby je bylo možné dálkově monitorovat a ovládat.

8 Seznam použité literatury

[1] ROBERTAZZI, Thomas. *Introduction to Computer Networking*. 1. NY, USA: Stony Brook, 2017. ISBN 978-3-319-53102-1.

[2] VAVREČKOVÁ, Šárka. *Počítačová síť a internet*. 1. vyd Opava: Filozoficko-přírodovědecká fakulta v Opavě, Slezská univerzita v Opavě, 2017. ISBN 978-80-7510-245-4.

[3] KUROSE, James F. a Keith W. ROSS. *Computer networking: a top-down approach*. 6th ed. Boston: Pearson, 2013. ISBN 978-0-13-285620-1.

[4] *Inside radio: an attack and defense guide*. New York, NY: Springer Berlin Heidelberg, 2018. ISBN 978-981-10-8446-1

[5] FAULKNER, Cameron. What is NFC? Everything you need to know. Techradar [online]., May 09, 2017 [cit. 2019-03-16]. Dostupné z: https://www.techradar.com/news/what-is-nfc

[6] MILLER, Michael. *Wireless networking: absolute beginner's guide*. Indianapolis, Ind.: Que, c2013. Absolute beginner's guide (Indianapolis, Ind.). ISBN 978-0-7897-5078-5.

[7] TILLMAN, Maggie a Chris HALL. What is ZigBee and why is it important for your smart home?. Pocket lint [online]., 7 January 2019 [cit. 2019-03-16]. Dostupné z: https://www.pocket-lint.com/smart-home/news/129857-what-is-zigbee-and-why-is-it-important-for-your-smart-home

[8] ROUSE, Margaret. 802.1X. *Techtarget* [online]., September 2005 [cit. 2019-03-16]. Dostupné z: https://searchmobilecomputing.techtarget.com/definition/8021X

[9] GEIER, Eric. What is WPA3? And some gotchas to watch out for in this Wi-Fi security upgrade. Networkworld [online]., November 02, 2018 [cit. 2019-03-16]. Dostupné z: https://www.networkworld.com/article/3316567/what-is-wpa3-wi-fi-security-protocol-strengthens-connections.html

[10] PRICE, Dan. TECHNOLOGY EXPLAINED EDGE, 3G, H+, Etc: What Are All These Mobile Networks?. *Makeuseof* [online]., February 15, 2016 [cit. 2019-03-16]. Dostupné z: https://www.makeuseof.com/tag/edge-3g-h-etc-mobile-networks/

[11] VACULÍK, Přemysl. Pokrytí LTE v Česku dosahuje až 99 %. *Dotekomanie* [online]. 2017, 12. února 2017 [cit. 2019-03-16]. Dostupné z: https://dotekomanie.cz/2017/02/pokryti-lte-cesku-dosahuje-az-99-lte/

[12] MOORE, Mike. What is 5G? Everything you need to know. *Techradar* [online]. 15. 03 2019 [cit. 2019-03-16]. Dostupné z: https://www.techradar.com/news/what-is-5g-everything-you-need-to-know

[13] ROUSE, Margaret. TCP/IP (Transmission Control Protocol/Internet Protocol). *Techtarget* [online]. February 2019 [cit. 2019-03-17]. Dostupné z: https://searchnetworking.techtarget.com/definition/TCP-IP

[14] WEP2. *Afterdawn* [online]. [cit. 2019-03-17]. Dostupné z: https://www.afterdawn.com/glossary/term.cfm/wep2

[15] J'D. A Brief History of Wireless Networking. *Techiesupports* [online]. 21 November 2011 [cit. 2019-03-17]. Dostupné z: https://techiesupports.blogspot.com/2011/11/brief-history-of-wireless-networking.html

[16] GHASEMPOUR, Yasaman, Carlos CORDEIRO, Edward W. KNIGHTLY a Claudio R. C. M. DA SILVA. IEEE 802.11ay: Next-Generation 60 GHz Communication for 100 Gb/s Wi-Fi. *IEEE Communications Magazine* [online]. IEEE, 2017, 27 October 2017, (12) [cit. 2019-03-17]. DOI: 10.1109/MCOM.2017.1700393. ISSN 1558-1896. Dostupné z: https://ieeexplore.ieee.org/document/8088544

[17] UYSAL, Murat a Hatef NOURI. Optical wireless communications — An emerging technology. *2014 16th International Conference on Transparent Optical Networks (ICTON)* [online]. Graz, Austria: IEEE, 2014, 6 July 2014 [cit. 2019-03-17]. DOI: 10.1109/ICTON.2014.6876267. ISSN 2161-2064. Dostupné z: https://ieeexplore.ieee.org/document/6876267

[18] CICNAVI. Overview of Infrared (IrDA) and Bluetooth Standards. *Utilizewindows* [online]. 3 December 2011 [cit. 2019-03-17]. Dostupné

z: https://www.utilizewindows.com/overview-of-infrared-irda-and-bluetooth-standards/

[19] ARDAKANI, Maryam, Ali Reza HEIDARPOUR a Murat UYSAL. Non-line-of-sight ultraviolet communications over atmospheric turbulence channels. *2015 4th International Workshop on Optical Wireless Communications (IWOW)* [online]. 2015, 7 September 2015 [cit. 2019-03-17]. DOI: 10.1109/IWOW.2015.7342265. ISSN 978-1-4673-7726-3. Dostupné z: https://ieeexplore.ieee.org/document/7342265

[20] OFDMA. *GTA UFRJ* [online]. [cit. 2019-03-17]. Dostupné z: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2014_2/rafaelreis/ofdma_scfdma.html

[21] *IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements*. 12 June 2007. New York: IEEE, 2007. ISBN 0-7381-5656-6.

[22] IEEE 802.11d-2001. *IEEE standards association* [online]. 2001-06-14 [cit. 2019-03-17]. Dostupné z: https://standards.ieee.org/standard/802_11d-2001.html

[23] ROUSE, Margaret. 802.11i. *Techtarget* [online]. June 2006 [cit. 2019-03-17]. Dostupné z: https://searchmobilecomputing.techtarget.com/definition/80211i

[24] ROUSE, Margaret. 802.11h. *Techtarget* [online]. April 2006 [cit. 2019-03-17]. Dostupné z: https://searchmobilecomputing.techtarget.com/definition/80211h

[25] IEEE 802.11j. *Technopedia: Where Information Technology and Business Meet* [online]. [cit. 2019-03-17]. Dostupné z: https://www.techopedia.com/definition/16647/ieee-80211j

[26] IEEE 802.11e. *Technopedia: Where Information Technology and Business Meet* [online]. [cit. 2019-03-17]. Dostupné z: https://www.techopedia.com/definition/505/ieee-80211e

[27] IEEE 802.11k. *Technopedia: Where Information Technology and Business Meet* [online]. [cit. 2019-03-17]. Dostupné z: https://www.techopedia.com/definition/16176/ieee-80211k

[28] IEEE 802.11r. *Technopedia: Where Information Technology and Business Meet* [online]. [cit. 2019-03-17]. Dostupné z: https://www.techopedia.com/definition/5039/ieee-80211r

[29] IEEE 802.11y. *Telecom ABC* [online]. 2005 [cit. 2019-03-17]. Dostupné z: http://www.telecomabc.com/numbers/80211y.html

[30] SANJI, Ishaan. Configure 802.11w Management Frame Protection on WLC. *Cisco* [online]. May 9, 2018 [cit. 2019-03-17]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212576-configure-802-11w-management-frame-prote.html

[31] *IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments* [online]. 1. Singapore: IEEE [cit. 2019-03-17]. ISBN 978-1-4244-1644-8. Dostupné z: https://ieeexplore.ieee.org/document/4526014

[32] IEEE 802.11z - TDLS. *Telecom ABC* [online]. [cit. 2019-03-17]. Dostupné z: http://www.telecomabc.com/numbers/80211z.html

[33] IEEE 802.11v. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-03-17]. Dostupné z: https://en.wikipedia.org/wiki/IEEE_802.11v

[34] ROUSE, Margaret. 802.11u. *Techtarget* [online]. June 2013 [cit. 2019-03-17]. Dostupné z: https://whatis.techtarget.com/definition/80211u

[35]-ROUSE, Margaret. 802.11s. *Techtarget* [online]. October 2010 [cit. 2019-03-17]. Dostupné z: https://searchmobilecomputing.techtarget.com/definition/80211h

[36] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. New York, NY 10016-5997: IEEE, 2012. ISBN 978-0-7381-7245-3.

[37] *802.11ae-2012: IEEE Standard for Information technology--Telecommunications and information exchange between systems*. 1. New York, NY 10016-5997: IEEE, 2012. ISBN 978-0-7381-7241-5.

[38] What is IEEE 802.11aq?. *Everythingrf* [online]. Sep 20, 2018 [cit. 2019-03-17]. Dostupné z: https://www.everythingrf.com/community/what-is-ieee-802-11aq

[39] GEIER, Eric. 13 things you need to know about MU-MIMO Wi-Fi. *NetworkWorld* [online]. MAY 24, 2016 [cit. 2019-03-17]. Dostupné z: https://www.networkworld.com/article/3256905/mobile-wireless/13-things-you-need-to-know-about-mu-mimo-wi-fi.html

[40] IEEE 802.11aj-2018: EEE Standard for Information Technology--Telecommunications and information exchange between systems Local and metropolitan area networks. *IEEE standards association* [online]. IEEE, 2018-04-18 [cit. 2019-03-17]. Dostupné z: https://standards.ieee.org/standard/802_11aj-2018.html

[41] What is OFDM: Orthogonal Frequency Division Multiplexing. *Electronics notes* [online]. [cit. 2019-03-17]. Dostupné z: https://www.electronics-notes.com/articles/radio/multicarrier-modulation/ofdm-orthogonal-frequency-division-multiplexing-what-is-tutorial-basics.php

[42] MURPHY, Rick. 802.11-2016. *WiTS* [online]. August 12, 2017 [cit. 2019-03-17]. Dostupné z: https://www.wirelesstrainingsolutions.com/802-11-2016/

[43] NITSCHE, Thomas a Carlos CORDEIRO. IEEE 802.11ad: directional 60 GHz communication for multi-Gigabit-per-second Wi-Fi. *IEEE Communications Magazine* [online]. IEEE, 2014, 11 December 2014, (12) [cit. 2019-03-17]. DOI: 10.1109/MCOM.2014.6979964. ISSN 1558-1896. Dostupné z: https://ieeexplore.ieee.org/document/6979964

[44] HWEE ONG, Eng. Performance analysis of fast initial link setup for IEEE 802.11ai WLANs. *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications* [online]. Sydney: IEEE, 2012, 29 November 2012 [cit. 2019-03-17]. DOI: 10.1109/PIMRC.2012.6362543. ISSN 2166-9589. Dostupné z: https://ieeexplore.ieee.org/document/6362543/authors#authors

[45] Learn about Multiple-Input Multiple-Output. *Intel* [online]. 09/06/2017 [cit. 2019-03-17]. Dostupné z: https://www.intel.com/content/www/us/en/support/articles/000005714/network-and-i-o/wireless-networking.html

[46] SATTEL, Sam. Electromagnetic Waves and How They Work. *Autodesk* [online]. [cit. 2019-03-17]. Dostupné z: https://www.autodesk.com/products/eagle/blog/electromagnetic-wireless-electronic-basics/

[47] SNYDER, Joel. What is 802.1X? Everything you need to know about LAN authentication. *Networkworld.* [online]. AUGUST 17, 2010 [cit. 2019-03-17]. Dostupné z: https://www.networkworld.com/article/2216499/wireless-what-is-802-1x.html

[48] DOLEJŠ, Jan. LTE – vše, co potřebujete vědět o nejrychlejším mobilním internetu. *Svetandroida* [online]. 4.7.2017 [cit. 2019-03-17]. Dostupné z: https://www.svetandroida.cz/lte-internet/

[49] Elektromagnetické spektrum. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-03-17]. Dostupné z: https://cs.wikipedia.org/wiki/Elektromagnetick%C3%A9_spektrum

[50] DOLEJŠ, Jan. Jak zjistit, zda váš telefon podporuje 5GHz Wi-Fi síť?. *Svět androida* [online]. 3.1.2019 [cit. 2019-03-17]. Dostupné z: https://www.svetandroida.cz/telefon-podporuje-5ghz-wi-fi-sit/

[51] TCP/IP. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-03-17]. Dostupné z: https://cs.wikipedia.org/wiki/TCP/IP

[52] WiFi Modes of Operation (802.11 or Wi-Fi). *CCM* [online]. [cit. 2019-03-17]. Dostupné z: https://ccm.net/contents/804-wifi-modes-of-operation-802-11-or-wi-fi

[53] TURNER, Mark. Wi-Fi 6 Explained: The Next Generation of Wi-Fi: What Does 802.11ax Bring to the Table?. *Techspot* [online]. December 24, 2018 [cit. 2019-03-18]. Dostupné z: https://www.techspot.com/article/1769-wi-fi-6-explained/

[54] PAWLOWSKI, Marcin Piotr. Schema of IEEE 802.1x secured network architecture. *Researchgate* [online]. Nov 2015 [cit. 2019-03-18]. Dostupné z: https://www.researchgate.net/figure/Schema-of-IEEE-8021X-secured-networks-architecture_fig5_284717130

[55] Firewalls and Proxies Explained. *Postcast server* [online]. [cit. 2019-03-18]. Dostupné z: http://www.postcastserver.com/help/firewalls_and_proxies_explained.aspx

[56] Valentin, Kristian & Maly, Michal. (2013). NETWORK FIREWALL USING ARTIFICIAL NEURAL NETWORKS. Computing and Informatics. 32. 1312-1327.

9 Seznam použitých obrázků

10 Seznam použitých tabulek

11 Seznam použitých zkratek

IEEE	Institute of Electrical and Electronics Engineers
GPRS	General Packet Radio Service
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
HSPA	High speed packet access
FUP	Fair Usage Policy
AP	Access Point
TCP / IP	Transmission Control Protocol / Internet Protokol
HTTP	Hypertext Transfer Protocol
SMTP	Simple Mail Transfer Protocol
POP3	Post Office Protocol 3
IMAP	Internet Message Access Protocol
SSH	Secure Shell
DNS	Domain Name Servers
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
DHCP	Dynamic Host Configuration Protocol
ARP	Address Resolution Protocol
MAC	Medium Access Control
ADSL	Asymmetric digital subscriber line
DoS	Denial of Service
OWC	Optical Wireless Cmmunication

UV	Ultraviolet
IR	Infrared
VLC	Visible Light Communication
NLOS	Non-Line of Sight
LOS	Line of Sight
PHY	Physical Layer
WLAN	Wireless Local Area Network
TKIP	Temporal Key Integrity Protocol
AES	Advanced Encryption Standard
DFS	Dynamic Frequency Selection
TPC	Transmit Power Control
VoIP	Voice over Internet Protokol
RRM	Radio Resource Management
MIC	Message Integrity Check
IGTK	Integrity Group Temporal Key
WAVE	Wireless Access in Vehicular Environments
TDSL	Tunneled Direct Link Setup
QoS	Quality of Service
QMF	Quality of Service for Management frames
AC	Access Category
LTE	Long Term Evolution
LTE-A	Long Term Evolution-Advanced
BSS	Basic Service Set
IBSS	Independent Basic Service Set

ESS	Extended Service Set
EAP	Extensible Authentication Protocol
FILS	Fast Initial Link Setup
IDS	Intrusion Detection System
WPA	Wi-Fi Protected Access
WEP	Wired Equivalent Privacy
CCMP	Counter–Mode CBC MAC Protocol
PSK	Pre-Shared Key
SAE	Simultaneous Authentication of Equals
OFDMA	Orthogonal frequency-division multiple access
FHSS	Frequency Hopping Spread Spectrum
DSSS	Direct Sequence Spread Spectrum
OFDM	Orthogonal Frequency Division Multiplexing
MIMO	Multiple-Input Multiple-Output
MU-MIMO	Multi-User, Multiple-Input Multiple-Output
HEW	High Efficiency Wireless
ICI	Inter-Channel Interference
ISI	Inter-Symbol Interference
FEC	Forward Error Correction
PAN	Personal Area Network
LAN	Local Area Network
MAN	Metropolitan Area Network
WAN	Wide Area Network
NFC	Near-field Communication