Univerzita Pardubice
Dopravní fakulta Jana Pernera

Vytvoření podpory pro výuku počítačových sítí v oblasti bezdrátové komunikace

Bakalářská práce

Autor: Václav Bašta

Vedoucí práce: Mgr. Josef Horálek

Pardubice **květen 2009**

University Pardubice
Jan Perner transport faculty

Creation of Support for Teaching Computer Networks in Area of Wireless Communication

Bachelor work

Author: Václav Bašta

Supervisor: Mgr. Josef Horálek

Pardubice **May 2009**

Prohlášení

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Barchově dne 22. 5. 2009

Václav Bašta

Poděkování

Děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi za veškerou podporu a pomoc při jejím zpracování.

Anotace

Cílem bakalářské práce je seznámení s problematikou bezdrátových sítí, jak z pohledu teoretického, tak praktického využití.

V první části se práce zabývá teorií, která popisuje základní principy bezdrátových sítí, problematiku standardu IEEE 802.11 a jeho vztah k ISO/OSI modelu. V závěru této části se osvětluje samotný pojem Wi-Fi.

V další části je podrobně popsána základní architektura bezdrátových sítí včetně využití základních druhů bezdrátových zařízení a zároveň příkladů z praxe. Poslední kapitola teoretické části práce je zaměřena na popis základních způsobů zabezpečení bezdrátových sítí.

Praktická část práce je zaměřena na problematiku bezdrátových sítí, kterou vysvětluje na modelových příkladech sítí vytvořených pomocí simulátoru počítačových sítí Packet Tracer 5.0. Simulátor je k dispozici všem studentům Cisco Network Academy. U každého modelu je odkaz na teoretickou část, kterou daný příklad využívá a popsáno nastavení všech aktivních síťových prvků. Obtížnost jednotlivých příkladů se postupně zvyšuje, od jednoduchých řešení až po komplexnější návrhy sítí. V modelech je ukázána i problematika zabezpečení bezdrátových sítí.

Práce tak naplňuje i svůj sekundární význam, kterým je vytvořit souhrnný materiál o bezdrátových sítích, pro podporu výuky počítačových sítí na DFJP UPCE.

Klíčová slova

standart 802.11, MAC, CSMA/CA, Wi-Fi, přístupový bod, most, Ad-hoc síť, infrastrukturní síť, WEP, WPA, SSID

Annotation

The main purpose of the Bachelor Thesis is to acquaint with the issue of wireless networks from both the theoretical and practical point of view.

The first part of the Thesis is aimed at a theoretical description of the elementary principles of wireless networks, especially the matter of IEEE 802.11 Standard and its relation to the ISO/OSI Model. The first part is concluded by an explanation of the Wi-Fi conception itself.

The next part of the Thesis describes in detail the fundamental structure of wireless networks and furthermore, includes the usage of their main types and itemizes examples from practice. The last part of the theoretical section is dedicated to the basic methods of securing the wireless networks.

The practical part of the work focuses on explaining the wireless networks on the model examples of particular networks created by Packet Tracer 5.0. Wireless Network Simulator which is available to all students of Cisco Network Academy. Every given model example refers to a specific theoretical method used in it and describes the setting of all the active network components. The complexity of model examples gradually increases from the simple conceptions to the more complicated network designs. In addition, the models also outline the subject of wireless networks security of wireless networks.

Subsequently, the Thesis thus fulfils the intention of creating a comprehensive material about wireless networks to support the teaching of this subject at Jan Perner Transport Faculty, University of Pardubice.

Keywords

standard 802.11, MAC, CSMA/CA, Wi-Fi, access point, Bridge, Ad-hoc network, infrastructure network, WEP, WPA, SSID

Obsah

Úvod

Bezdrátové sítě jsou úzce spjaty s konvenčními sítěmi, metalickými případně optickými. Cíle této práce není popis obou druhů sítí, a proto nebudou vysvětleny některé pojmy. Předpokladem je alespoň základní znalost kurzů CCNA (Cisco Certified Network Associate). V teoretické části práce by měla dostačovat znalost na úrovni kurzu CCNA 1 (Networking Fundamentals). Praktická část s modely sítí je náročnější a proto vychází hlavně u kapitol 5.1 až 5.5 a kapitoly 5.7 ze znalosti kurzu CCNA 2 (Routing Protocols and Concepts) a u modelu v kapitole 5.6 i CCNA 3 (LAN Switching and Wireless).

Teoretická část bakalářské práce, popisuje základní principy bezdrátových sítí, problematiku standardu IEEE 802.11 a jeho vztah k ISO/OSI modelu. Následující kapitola osvětluje samotný pojem Wi-Fi. V další dvou kapitolách je podrobně popsána základní architektura bezdrátových sítí včetně využití základních druhů bezdrátových zařízení a zároveň příkladů z praxe. Poslední kapitola teoretické části práce je zaměřena na základy bezpečnosti bezdrátových sítí.

Praktická část práce vysvětluje problematiku bezdrátových sítí na modelových příkladech sítí vytvořených pomocí simulátoru počítačových sítí Packet Tracer 5.0. Simulátor je k dispozici všem studentům Cisco Network Academy v rámci programu CCNA. Každého model se odkazuje na přesně definovanou teoretickou část, kterou daný příklad využívá. Každý příklad obsahuje popis nastavení všech aktivních síťových prvků. V modelech je také ukázána problematika zabezpečení bezdrátových sítí. Obtížnost jednotlivých příkladů se postupně zvyšuje, od jednoduchých řešení až po komplexnější návrhy sítí, kde je využito i znalostí získaných v kurzech CCNA.

1 Bezdrátové sítě

Bezdrátová komunikace je s námi už odpradávna, z historie tu máme například kouřové signály. Až v posledních dvou desetiletích ale po přenosovém médiu, atmosféře, začínají komunikovat i počítače a vznikají bezdrátové sítě. WLAN, z anglického wireless local area network, doslova bezdrátové místní sítě, zažívají v poslední době nebývalý rozmach a jsou jedním z nejdynamičtěji se rozvíjejících oborů počítačových sítí. Bezdrátová komunikace poskytuje stejné výhody jako tradiční LAN sítě, ale není omezena kabely nebo dráty. Uživateli má možnost volného pohybu při současně neustálé konektivitě k okolní síti.

Tolik stručně k začátku a nyní se již začnu podrobněji věnovat bezdrátovým sítím LAN a s tím souvisejícím standardem IEEE 802.11.

1.1 Bezdrátové spojení

Bezdrátově sítě LAN, stejně jako jejich předchůdce, využívající tzv. křížených dvoulinek nebo optických kabelů, potřebují médium, po kterém bude přenášen signál. Namísto měděných kabelů nebo skleněných vláken je využito infračervené světlo, IR (infrared light), nebo radiová frekvence, RF (radio frequencies). I přes snahu některých výrobců se nakonec stala populárnější RF, hlavně díky několikanásobně většímu dosahu a vyšší datové propustnosti. Bezdrátovou radiovou technologii nevyužívají jen počítačové sítě, ale slouží například i pro mobilní telefonní sítě, radiové sítě Telra nebo pro profesionální datové sítě FWA. Za jejího uživatele můžeme považovat i televizní a rádiové vysílání.

Všechny sítě založené na radiové frekvenci mají jeden společný znak, k jejich provozování musí mít provozovatel licenci vydávanou patřičným regulačním orgánem. Tyto licence mají svoje vyhrazené a přidělené frekvence, na nichž nesmí být nikým jiným vysíláno. Jde o takzvané placené licencované pásmo. Frekvenční pásmo se rozdělilo a licencuje se, protože použitelných radiových frekvencí není nekonečně mnoho.

Protože existuje nespočet zařízení využívajících rádiové frekvence, od antén pro připojení WLAN u notebooku jako např. na obrázku č.1, po mikrovlnou troubu, je pravděpodobně nemyslitelné, aby si každý majitel takového zařízení zažádal o svoji licenci. Proto vzniklo takzvané pásmo ISM neboli pásmo vyhrazené pro průmyslové, vědecké a lékařské potřeby (Industrial Science and Medical). Toto pásmo vymezil pro tyto účely jak americký regulátor FCC (Federal Communications Commission), tak evropský ETSI (European

Telecommunications Standards Institute) v roce 1992, tím prakticky započal rozvoj WLAN až do podoby jak je známe dnes. Česká republika je též členem ETSI a provoz zde vymezuje generální licence ČTÚ VO-R/12/08.2005-34. Bezlicenční pásmo se nachází na frekvencích 900 MHz, 2,4 až 2,48 GHz a 5,1 až 5,8 GHz.

Bezdrátová komunikace, jako předtím řada jiných nových technologií, potřebovala pro svoji životaschopnost a rozvoj definovat společný standard. Toho se ujal mezinárodní standardizační institut IEEE a v roce 1997 byla publikována specifikace standardu bezdrátové sítě pracující v pásmu ISM pod označením 802.11. Za zmínku stojí, že IEEE byl původně akronym pro Institute of Electrical and Electronics Engineers. V současnosti již ale institut expandoval to tolika různých odvětví, že se původní víceslovné označení nepoužívá.

Obrázek č. 1: PCMCIA bezdrátová karta do notebooku [1]

1.2 Standard 802.11

Původní standard 802.11 pracoval na frekvenci 2,4 GHz, s maximální přenosovou rychlostí 2 Mb/s. Tyto hodnoty ale brzo přestaly dostačovat a tak se IEEE začal zabývat dalším vylepšováním. V současnosti je již standardů a dodatků vycházejících z původní 802.11 velmi mnoho. Jejich stručná soupiska je uvedena níže i s krátkým komentářem, plné znění standardu lze získat na adrese http://standards.ieee.org. Podrobněji se zaměřím na z dnešního pohledu nejvýznamnější standardy odvozené od normy 802.11. Budou to normy s písmenným označením a,b,g,n.

Výpis všech standardů 802.11 se stručným komentářem.

- 802.11 - Původní standard pro 1 a 2 Mbit/s rychlost s frekvencí 2.4 GHz (1999)
- 802.11a - Standard podrobně popsán níže

[1] Obrázek převzat z [13]

- 802.11b - Standard podrobně popsán níže
- 802.11c - Bezdrátové přemostění (bridge), obsaženo v IEEE 802.1D standardu (2001)
- 802.11d - Mezinárodní roamingový dodatek (2001)
- 802.11e - Vylepšení QoS včetně dlouhých (burst) paketů (2005)
- 802.11F - Komunikace mezi bezdrátovými přístupovými body (2003)
- 802.11g - Standard podrobně popsán níže
- 802.11h - Správa spektra 802.11a (5 GHz) pro Evropu (2004)
- 802.11i - Vylepšený autentifikační a šifrovací algoritmus (WPA2) (2004)
- 802.11j - Dodatek pro Japonsko; nová frekvenční pásma pro multimedia (2004)
- 802.11k - Vylepšení správy rádio zdrojů pro vysoké frekvence (navazuje na IEEE 802.11j)
- 802.11l - (rezervováno a nebude použito)
- 802.11m - Správa standardu: přenosové metody a drobné úpravy.
- 802.11n - Standard podrobně popsán níže
- 802.11o - (rezervováno a nebude použito)
- 802.11p - Bezdrátový přístup pro pohyblivé prostředí (auta, vlaky, sanitky)
- 802.11q - (rezervováno a nebude použito, aby se nepletlo s 802.1Q)
- 802.11r - Rychlé přesuny mezi přístupovými body (roaming)
- 802.11s - Samoorganizující se bezdrátové sítě. (ESS Mesh Networking)
- 802.11T - Předpověď bezdrátového výkonu - testovací metody
- 802.11u - Spolupráce se sítěmi mimo 802 standardy (například s mobilními sítěmi)
- 802.11v - Správa bezdrátových sítí (konfigurace klientských zařízení během připojení)
- 802.11w - Chráněné servisní rámce
- 802.11x - (rezervováno a nebude použito)
- 802.11y - Pro běh ve frekvenčním pásmu 3650 - 3700 MHz (veřejné pásmo v USA)

802.11F (stažen v březnu 2006) a 802.11T jsou samostatné dokumenty a nejsou to tedy dodatky k IEEE 802.11 standardu, proto obsahují velké písmeno.

1.2.1 802.11a

Varianta 802.11a schválená v roce 1999 specifikovala bezdrátové sítě v dalším nově uvolněném bezlicenčním pásmu 5 GHz o rychlosti až 54 Mb/s. Vysílání v tomto pásmu bylo dlouho zakázáno, ale v současné době je již situace jiná. Ta ale platí pro novější 802.11h, 802.11a neodpovídá platným předpisům ETSI.

802.11a má z dnešního pohledu dva velké nedostatky, které byly vyřešeny až v následujících normách. Je to neodpovídající zabezpečení přenosů a nepřítomnost tzv. kvality služeb QoS (Quality of service). QoS se používá zejména u VoIP a HTTP, kde přerozděluje přidělené datové pásmo. Děje se tak na základě priorit nebo nastavení minimální rychlosti tak, aby například VoIP neměl nežádoucí výpadky v důsledku zahlcení datového pásma velkým přenosem dat přes FTP apod.

V 802.11a byl využit ortogonální frekvenční multiplex s kmitočtovým dělením OFDM (Orthogonal Frequency Division Multiplex) známý též z přenosu signálu v ADSL nebo ve standardu pro digitální televizi DVB-T. Problematika OFDM je podrobněji rozebrána v kapitole 1.5.

Velkou výhodou 802.11a je fakt, že pásmo 5 GHz je daleko méně zarušené než pásmo 2,4 GHz a díky velké šířce tohoto pásma je možno využít více kanálů bez toho, aby docházelo k jejich překrývání.

1.2.2 802.11b

Standard 802.11b z roku 1999 se zrodil o něco dříve než 802.11a, jelikož implementace v pásmu 2,4 GHz, kde se podle něj vysílá, je o něco snazší. Nabízí přenosovou rychlost max. 11 Mb/s. Rychlost se podle specifikací normy může v závislosti na zarušení prostředí dynamicky měnit od 11 Mb/s až k 1 Mb/s. Nedostatky uvedené u 802.11a, QoS a nedostatečná bezpečnost, platí i u této normy. Systémy pracující se standardem 802.11b využívají techniku přímého rozprostřeného spektra DSSS (Direct Sequence Spread Spectrum). Společnost Texas Instruments přišla s paketově binárnírním konvolučním kódováním PBCC (Packet Binary Convolutional Coding), to se ale neprosadilo a proto se již o něm nebudu podrobněji zmiňovat. Problematika DSSS je dále rozebrána v kapitole 1.5.

1.2.3 802.11g

V roce 2003 se objevil v dnešní době zřejmě nejpoužívanější standard 802.11g. Stejně jako 802.11b pracuje v pásmu 2,4 GHz, ovšem nabízí rychlost až 54 Mb/s (podobně jako u 802.11a), což ale na druhou stranu o něco snižuje dosah na cca 30 m. Výhodou je zpětná kompatibilita s 802.11b, která přináší možnost vzájemné spolupráce zařízení obou standardů. Komunikace na úrovni fyzické vrstvy probíhá s využitím OFDM, avšak při komunikaci se zařízeními 802.11b se využívá technologie DSSS. 802.11g obsahuje mechanizmus pro koexistenci 802.11b a 802.11g klientů v jedné síti. Ten se v tomto případě spustí v okamžiku přidružení klienta 802.11b k síti 802.11g. Zajímavé je porovnání 802.11a a g. Ukazuje se, že pokud v síti nejsou klienti 802.11b, je výkonnost sítě 802.11g prakticky shodná s výkonností 802.11a. S přítomností klientů 802.11b se reálná propustnost sítě snižuje až na třetinu (cca 8 Mb/s), což je sice více než u tradiční 802.11b, ale rozhodně ne o mnoho.

1.2.4 802.11n

V současnosti ještě není norma 802.11n oficiálně schválena, mělo by se tak stát v průběhu roku 2009. 802.11n by měla přinést mnoho vylepšení stávajících technologií. Rapidní nárůst přenosových rychlostí, reálně přes 100 Mbit/s a zvýšení dosahu až ke 300 m. K tomuto je ale třeba upravit fyzickou vrstvu a podčást linkové vrstvy, takzvanou Media Access Control (MAC). Bude zde použita také technologie MIMO (Multiple Input – Multiple Output), tzv. technologie chytrých antén, která je jako taková poměrně hodně stará. Přišly s ní již zhruba před více než 40 lety Bellovy laboratoře. Navzdory tomu se ale s jejím využitím v počítačové komunikaci počítá teprve až v tomto standardu. Technika zjednodušeně pracuje na principu vysílání několika datových signálů naráz různými telekomunikačními cestami, avšak v rámci jednoho přenosového kanálu. U přijímače i vysílače se musí samozřejmě počítat s využitím více antén, jejichž přesný počet ale stanoven není. Zařízení pracující na 802.11n se od ostatních již na první pohled liší právě větším počtem antén, jak je patrné na obrázku č. 2.

Obrázek č. 2: Bezdrátový router s podporou technologie MIMO [2]

1.3 Wi-Fi

Wi-Fi (Wireless Fidelity) je obchodní značka Wi-Fi Aliance pro certifikované produkty založené na standartu IEEE 802.11. Wi-Fi Aliance, do roku 2003 známá jako WECA (Wireless Ethernet Compatibility Alliance), je certifikační autorita testující interoperabilitu jednotlivých zařízení hlásících se ke standardu 802.11. Výrobek, který vyhovuje všem testovacím kritériím, dostane propůjčeno logo WiFi, na obrázku č. 3, ujišťující kupujícího o propojitelnosti zařízení označených tímto logem. Zařízení také dostane Wi-fi certifikát, kde se uvádí co vše zařízení splňuje a jaké standardy podporuje. Příklad takového certifikátu je na obrázku č. 4. Wi-Fi je v současnosti podporována většinou operačních systémů, herních konzolí, notebooků, tiskáren a dalším hardwarem.

Obrázek č. 3: Logo Wi-Fi [3]

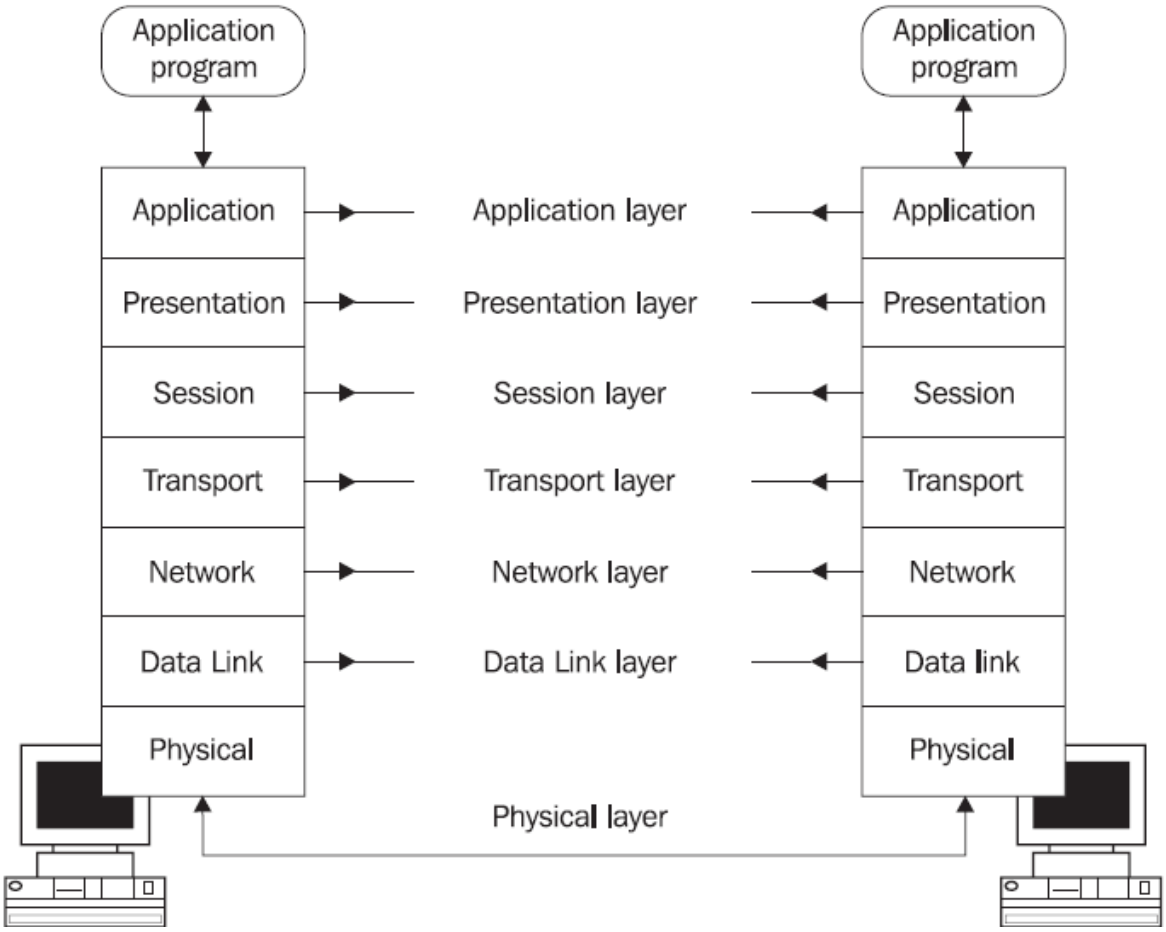
[2] Obrázek převzat z [14]
[3] Obrázek převzat z [15]

Obrázek č. 4: Wi-fi certifikát[4]

1.4 Model ISO/OSI

Bezdrátové sítě, stejně jako ostatní druhy počítačových sítí, jsou postaveny na společném pilíři. Je jím tzv. referenční model ISO/OSI. Byl vypracován organizací ISO (International Standards Organization), jejíž hlavní snahou byla standardizace počítačových sítí nazvaná OSI (Open Systen Interconnection). V roce 1984 byla přijata mezinárodní normu ISO 7498. Norma nespecifikuje realizaci systémů, ale uvádí všeobecné principy sedmivrstvé síťové architektury, jejíž názorné schéma je na obrázku č. 5. Každá ze sedmi vrstev je navržena pro vykonání skupiny jasně definovaných funkcí potřebných pro komunikaci. Pro svou činnost využívá služeb své sousední nižší vrstvy. Své služby pak poskytuje sousední vyšší vrstvě. Některé vrstvy nemusí být aktivní, ale jejích vynechání není dovoleno.

[4] Obrázek převzat z [10]



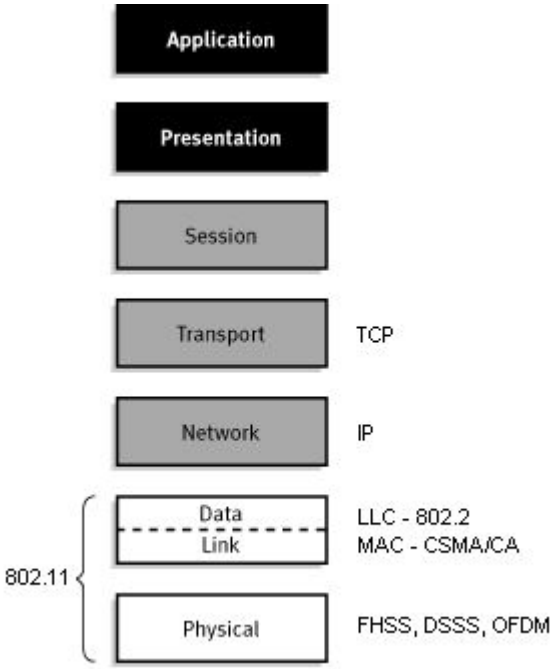
Obrázek č. 5: Referenční model ISO/OSI [5]

Jednotlivé vrstvy ISO/OSI od nejnižší k nejvyšší:

1. Physical layer (fyzická vrstva). Komunikace na nejnižší, hardwarové úrovni. Jde v podstatě o řešení vlastního fyzického spojení.
2. Data-link layer (spojová vrstva). Vrstva zabývající se kódováním a přenosem informací.
3. Network layer (síťová vrstva). Obsluha přenosových tras a zpráv.
4. Transport layer (transportní vrstva). Řízeni doručování informací a kvality přenosu.
5. Session layer (relační vrstva). Udržování a koordinace komunikace.
6. Presentation layer (prezentační vrstva). Formátování, konverze a zobrazení přenesených dat.
7. Application layer (aplikační vrstva). Přenos informací daným prostředím.

[5] Obrázek převzat z [17]

Standard 802.11 je definován pouze na dvou nejnižších vrstvách OSI, na fyzické a spojové a její podčásti MAC (Media Access Control). Všechny ostatní vrstvy nechává standard 802.11 nedotčené. Na obrázku č. 6 je upraven ISO/OSI model pro účely standardu 802.11.



Obrázek č. 6: ISO/OSI model pro 802.11

1.5 Fyzická vrstva

Fyzická vrstva je nejníže položenou vrstvou ISO/OSI modelu. Realizuje se zde vysílání a příjem dat po fyzickém médiu. V našem případě je tím médiem vzduch. V původní normě 802.11 z roku 1997 byly definovány tři typy fyzické vrstvy. Dvě jsou založeny na radiovém přenosu dat, třetí využívá infračerveného světla. Posledně jmenovaný způsob přenosu dat již následníci 802.11, jako například normy 802.11b a 802.11g, nepodporují. Je to hlavně v důsledku nízké přenosové rychlosti, ta dosahuje jen 2 Mbit/s, nemožnosti překlenout překážky a velmi malého dosahu.

V případech radiového přenosu dat je použito techniky rozprostřeného spektra SS (Spread Spectrum). Na vysílači je použita matematická funkce pro rozptýlení síly signálu do širokého frekvenčního bloku a přijímač tento signál následně složí do klasického úzkopásmového signálu, vhodného pro další zpracování.

Jak je již zmíněno výše, původní 802.11 definoval dvě techniky přenosu dat. První je frekvenční přeskakování FHSS (Frequency Hopping Spread Spectrum), druhou technika rozprostírání přímou posloupností DSSS (Direct Sequence Spread Spectrum). Společně se standardem 802.11a v roce 1999 přibyl k těmto dvěma technikám ještě multiplex s kmitočtovým dělením OFDM (Orthogonal Frequency Division Multiplex).

FHSS

Při použití frekvenčního přeskakování je dostupná frekvenční šířka 83,5 MHz v pásmu 2,4 GHz rozdělena na 79 (nebo 75) kanálů po 1 MHz a zbylé 4,5 MHz slouží jako ochrana před sousedním frekvenčním pásmem. Ke změnám kanálů dochází pseudonáhodně. Každých 30 sekund je vystřídáno alespoň 75 kanálů a na každém je vysíláno maximálně po dobu 400 milisekund. Realizace této techniky nedovoluje přesáhnout přenosovou rychlost 2 Mb/s. FHSS dovoluje soužití až 26 systémů v jedné lokalitě bez vzájemného rušení.

.

DSSS

Tato technika využívá 22 MHz široké frekvenční pásmo. DSSS pracuje tak, že každý bit je nahrazen určitou, za použití například Goldova nebo Barkerova kódu (podrobnosti o obou druzích kódování je možné nelézt na [7] a [8]), početnější sekvencí bitů. Této sekvenci, mající pseudonáhodná charakter, se říká chip. Poté je takto rozprostřená přímá posloupnost modulována na nosnou frekvenci a odeslána. Přijímač pak vykoná k získání dat inverzní operaci. Původní standard 802.11 dovoluje rychlosti až 2 Mb/s, standard 802.11b pak až 11 Mb/s. Při DSSS mohou koexistovat jen 3 systémy bez vzájemného rušení. Jen pro zajímavost bych uvedl, že tato technika se používá například i v navigačním systému GPS.

OFDM

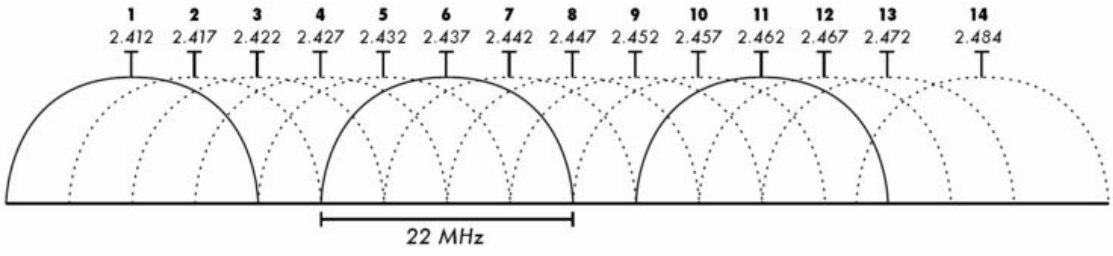
Technologie s ortogonálním frekvenčním multiplexem operuje v pásmu 2,4 GHz i 5 GHz. Může pracovat s kanály širokými 5, 10 a 20 MHz. V kanálu širokého 20 MHz dojde k jeho rozdělení na 52 dílčích kanálů po 300 kHz. Zde slouží 48 pro přenos dat a 6 pro signalizaci a detekci chyb. Výsledná přenosová rychlost je součtem všech dílčích kanálů a dosahuje hodnot až 54Mb/s.

1.5.1 Kanály

802.11 rozděluje pro sebe přiřazené pásmo do velkého množství kanálů podobně jako například televizní nebo radiové vysílání.

V pásmu 2.4 GHz je vyhrazeno 14 kanálů v rozmezí 2,412 - 2,484 GHz. Šířka kanálu je 22 MHz. Vzdálenost mezi kanály je 5 MHz s výjimkou kanálu číslo 14, kde je 12 MHz. Tuto situaci ilustruje obrázku č. 7. Z obrázku je patrné, že v celém pásmu 2,4 GHz se nacházejí pouze tři nepřekrývající se kanály. Počet použitelných kanálů se v různých částech světa liší v závislosti na místní legislativě. Amerika a Kanada má 11 kanálů, Evropa 13 a Japonsko 14. Ucelený přehled je v tabulce č. 1. Pro českou republiku je v pásmu 2,4 GHz definováno 13 kanálů.

Pásmo 5 GHz teoreticky má teoreticky až 201 kanálů. Přehled použitelných kanálů je pro přehlednost uveden v tabulce č. 2. Opět je zde vidět, že dochází k regulacím počtu použitelných kanálů v rámci místních legislativ. Šířka kanálu je 20 MHz. V Japonsku se můžeme setkat i s kanály o šířce 10 MHz.



Obrázek č. 7: Schéma rozdělení pásma 2,4 GHz [6]

Tabulka č. 1 : Přehled použitelných kanálů v pásmu 2,4 GHz

Kanál	Střední frekvence	Severní Amerika	Japonsko	Zbytek světa
1	2412	Ano	Ano	Ano
2	2417	Ano	Ano	Ano
3	2422	Ano	Ano	Ano
4	2427	Ano	Ano	Ano
5	2432	Ano	Ano	Ano
6	2437	Ano	Ano	Ano
7	2442	Ano	Ano	Ano
8	2447	Ano	Ano	Ano
9	2452	Ano	Ano	Ano
10	2457	Ano	Ano	Ano
11	2462	Ano	Ano	Ano
12	2467	Ne	Ano	Ano

[6] Obrázek převzat z [16]

Kanál	Střední frekvence	Severní Amerika	Japonsko	Zbytek světa
13	2472	Ne	Ano	Ano
14	2484	Ne	Jen 802.11b	Ne

Tabulka č. 2: Přehled použitelných kanálů v pásmu 5 GHz

Kanál	Střední frekvence	Spojené státy	Evropa	Japonsko 20MHz	Japonsko 10MHz
7	5035	Ne	Ne	Ne	Ano
8	5040	Ne	Ne	Ne	Ano
9	5045	Ne	Ne	Ne	Ano
11	5055	Ne	Ne	Ne	Ano
12	5060	Ne	Ne	Ne	Ne
16	5080	Ne	Ne	Ne	Ne
34	5170	Ne	Ne	Ne	Ne
36	5180	Ano	Ano	Ano	Ne
38	5190	Ne	Ne	Ne	Ne
40	5200	Ano	Ano	Ano	Ne
42	5210	Ne	Ne	Ne	Ne
44	5220	Ano	Ano	Ano	Ne
46	5230	Ne	Ne	Ne	Ne
48	5240	Ano	Ano	Ano	Ne
52	5260	Ano	Ano	Ano	Ne
56	5280	Ano	Ano	Ano	Ne
60	5300	Ano	Ano	Ano	Ne
64	5320	Ano	Ano	Ano	Ne
100	5500	Ano	Ano	Ano	Ne
104	5520	Ano	Ano	Ano	Ne
108	5540	Ano	Ano	Ano	Ne
112	5560	Ano	Ano	Ano	Ne
116	5580	Ano	Ano	Ano	Ne
120	5600	Ano	Ano	Ano	Ne
124	5620	Ano	Ano	Ano	Ne
128	5640	Ano	Ano	Ano	Ne
132	5660	Ano	Ano	Ano	Ne
136	5680	Ano	Ano	Ano	Ne
140	5700	Ano	Ano	Ano	Ne
149	5745	Ano	Ne	Ne	Ne
153	5765	Ano	Ne	Ne	Ne
157	5785	Ano	Ne	Ne	Ne
161	5805	Ano	Ne	Ne	Ne
165	5825	Ano	Ne	Ne	Ne
183	4915	Ne	Ne	Ne	Ano
184	4920	Ne	Ne	Ano	Ano
185	4925	Ne	Ne	Ne	Ano
187	4935	Ne	Ne	Ne	Ano
188	4940	Ne	Ne	Ano	Ano
189	4945	Ne	Ne	Ne	Ano

Kanál	Střední frekvence	Spojené státy	Evropa	Japonsko 20MHz	Japonsko 10MHz
192	4960	Ne	Ne	Ano	Ne
196	4980	Ne	Ne	Ano	Ne

1.5.2 PMD a PLCP

Fyzická vrstva standardu 802.11 je rozdělena do dvou podvrstev. Vrstva závislá od fyzického média PMD (Physical Medium Dependent) a vrstva protokol konvergence fyzické vrstvy PLCP (Physical Layer Convergence Procedure).

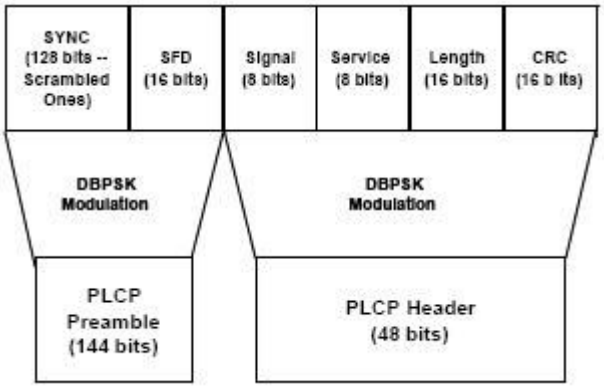
PMD

Tato podvrstva je zodpovědná za samotný tok dat. Stará se o přenos z podvrstvy PLCP pomocí antény vysílače po bezdrátovém prostředí k přijímači.

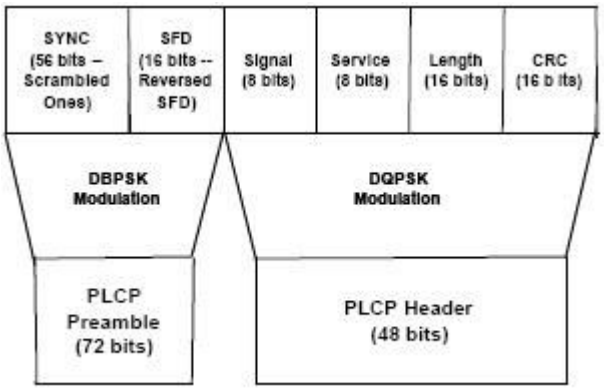
PLCP

PLCP dodává k MAC (Medium Access Control) rámcům vlastní hlavičku. V ní je obsažena informace o metodě modulace, tím je rámec nezávislý na typu fyzické vrstvy. Do hlavičky je přidána i funkce CCA (Clear Channel Assessment), která umožňuje použít pro přenos dat jak radiové spektrum, tak infračervené záření. V této podvrstvě jsou standardem 802.11 definovány dvě varianty preambule, dlouhá a krátká. Všechny systémy splňující standard musí podporovat dlouhou preambuli, krátká preambule je ve standardu určena pro zvýšení propustnosti sítě při přenášení speciálních typů dat, jako například VoIP. Níže je stručně popsána preambule a hlavička PLCP, jednoduchá schémata jsou na obrázku č. 8 a obrázku č. 9.

- PLCP preambule - je tvořena synchronizačním polem o délce 128 bitů pro dlouhé preambuli a 56 bity pro krátkou preambuli. Dále je zde 16-ti bitové pole SFD (Start Frame Delimiter) označující informační začátek každého rámce.
- PLCP hlavička - je dlouhá 48 bitů. Je rozdělena na čtyři části. Prvních 8 bitů je vyhrazeno pro určení přenosové rychlosti datového bloku. Dalších 8 bitů informuje o použitém typu modulace. V tomto poli jsou některé bity vyhrazeny pro budoucí použití. Třetí pole je šestnácti bitové a informuje o délce přenášených dat. Poslední pole má také šestnáct bitů a obsahuje CRC (Cyclic Redundancy Check), tj. kód pro vyloučení chyb.



Obrázek č. 8: PLCP s dlouhou preambulí



Obrázek č. 9: PLCP s krátkou preambulí

1.6 Spojová vrstva

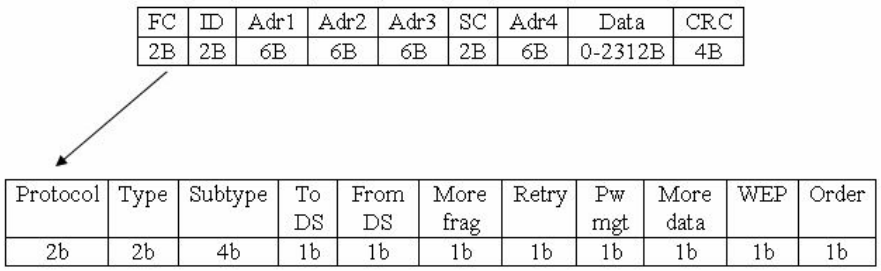
Spojová vrstva je složena ze dvou podvrstev, LLC (Logical Link Control) a MAC (Media Access Control). LLC používá protokol 802.2. Tento protokol je shodný s tím, jenž se používá i v ostatních typech lokálních datových komutací vycházejících ze standardu IEEE 802. V problematice bezdrátových sítí je nejdůležitější součást spojové vrstvy MAC podvrstva, která bude dále podrobněji rozebrána. Ještě před podrobnějším popisem MAC podvrstvy je důležité si říci něco o mezirámcových mezerách IFS (Inter Frame Spacing), které slouží ke koordinaci přístupu k přenosovému médiu. IFS jsou na standardu 802.11 rozděleny do čtyř typů.

1. SIFS (Short interframe space) – používá se například pro ACK, CTS; je nejkratším IFS.
2. PIFS (Point coordination function interframe space) – používá se pro výzvy; má přednost před normálním provozem; je delší než SIFS.

3. DIFS (Distributed coordination function interframe space) – stanice má přístup k médiu v okamžiku, kdy toto bylo volné po dobu delší než trvání DIFS; nejdelší IFS.
4. EIFS (Extended interframe space) – používá se při chybě v přenosu dat; IFS není pevně daný.

1.6.1 MAC

Základem MAC podvrstvy je MAC rámec. Rámec se skládá z hlavičky (MAC header), obsahuje informace o datech, těla (frame body), zde jsou samotná data a kontrolního součtu CRC (Cyclic redundancy check), což je jednoduchá hashovací funkce sloužící k ověření integrity dat. Rámec je znázorněn na obrázku č. 10, ve schématu je vždy uvedeno pole a jeho velikost.



Obrázek č. 10: MAC rámec

Nyní se pokusím podrobněji popsat jednotlivá pole MAC rámce.

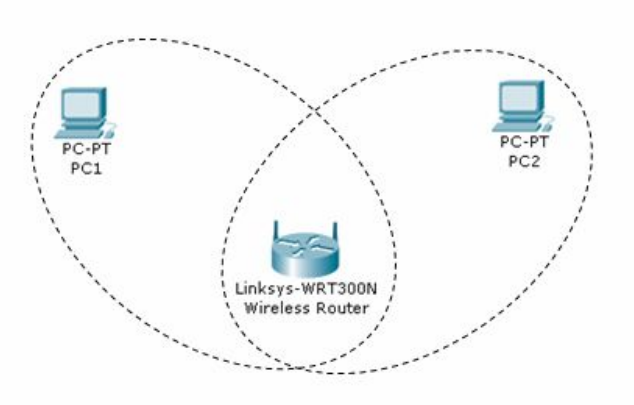
- Frame Control (FC) - informace o přenášeném rámci; jeho struktura je popsána níže
    - Protocol – udává verzi standardu IEEE 802.11.
    - Type – udává obsah rámce: řídící, ovládací a datový.
    - Subtype – dále specifikuje Typ: RTS, CTS, ACK atd.
    - To DS – hodnota 1 v případě, že je rámec zaslán do distribučního systému.
    - From DS - hodnota 1 v případě, že je rámec zaslán z distribučního systému.
    - More fragment (More frag) – hodnota 1 v případě, že byl rámec rozdělen na více samostatně přenesených částí.

- Retry – označuje, zda jde o již jednou vyslaný rámec.
- Power management (Pw mgt) – hodnota 1 v případě, že stanice se bude nacházet stanice po odeslání dat v módu úspory energie.
- More data – oznamuje, že jsou ještě ve vyrovnávací paměti další data k odeslání.
- WEP – hodnota 1 v případě, že je tělo kódováno pomocí WEP algoritmu.
- Order – označuje, zda rámec má být dále zpracováván

- Duration /ID (ID)
  - Station ID je identifikátor stanice používaný pro funkci úspory energie.
  - Duration Value - délka trvání rámce používaná pro výpočet rezervace přenosového média pomocí Network Allocation Vector (NAV)
- Address field (Adr1…adr4) – v závislosti na FC pole obsahují adresy zdroje, cíle, vysílače a přijímače bezdrátového signálu.
- Sequence control – užití při likvidaci duplicitních rámců.

1.6.2 CSMA/CA

Spojová vrstva a její podvrstva MAC je velmi podobná Ehernetu dle standardu 802.3. Na rozdíl od Ethernetu však používá jiný princip přístupu ke sdílenému přenosovému médiu. Ethernet je založen na přístupu poslechu nosné a detekcí kolizí CSMA/CD (Carier Sense Multiple Access - Collision Detection). Tento způsob přenosu dat ale bezdrátové komunikaci ne zcela vyhovuje a proto byl tedy lehce pozměněn. V 802.11 se při přístupu k médiu poslouchá nosná, ale je zde snaha předcházet kolizím, proto tedy CSMA/CA (Carier Sense Multiple Access - Collision Avoidance). Velkým omezením bezdrátových sítí je tzv. problém skrytého uzlu znázorněný na obrázku č. 11. Zjednodušeně jde o to, že stanice, v našem případě PC1, detekuje volné médium a začne komunikovat s bezdrátovým routerem. Druhá stanice, PC2, by také ráda komunikovala s routerem. Začne naslouchat, zjistí, že je přenosové médium je volné a začne vysílat. Nastává ale problém. Přesto, že přenosové médium bylo volné v okolí obou stanic, stanice se navzájem neslyšely, tak router „slyší“ obě stanice a tím pádem zde nastává kolize. PC1 bylo fakticky skrytým uzlem pro PC2 a obráceně.



Obrázek č. 11: Problém skrytého uzlu

Tomuto problému se protokol CSMA/CA snaží předcházet, řeší se to použitím čtyř specifických rámců, RTS (Request to send), CTS (Clear to send), ACK (Acknowledge) a NAV (Network allocation vector). Pokud tedy chce stanice vysílat, naslouchá, zda je médium volné, pokud ano, počká předem daný čas DIFS a pak začne vysílat. Přijímací stanice potvrzuje přijetí packetem ACK. Když nebyl ACK přijat, vysílací stanice pošle data znovu.

Pokud je ale v dosahu cílového zařízení, na obrázku bezdrátový router, více vysílacích stanic, je pro snížení kolizí definován RTS/CTS mechanimus. Vysílací stanice pošle RTS packet, kde je udána i délka vysílání a cílová stanice na to odpoví potvrzujícím CTS packetem, kde je opět dána délka vysílání. CTS packet slyší všechny připojené stanice v dosahu routeru, tedy i ty co jsou skrytým uzlem pro stanici, která hodlá vysílat. Tyto stanice pak po předem danou dobu, tu zjistí z CTS, budou brát médium za obsazené a nebudou vysílat.

2 Topologie sítě

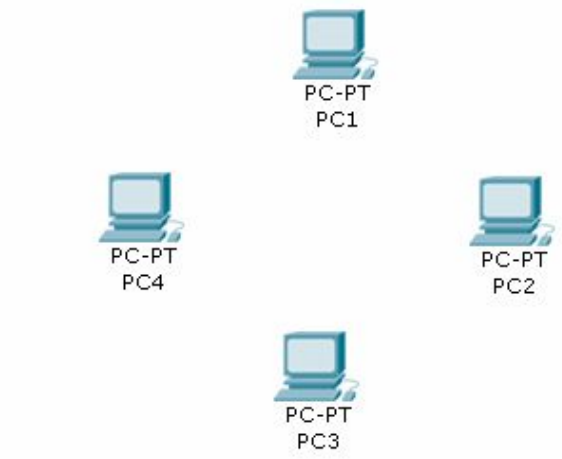
802.11 sítě používají dva druhy topologií. Základní soubor služeb BSS(Basic Service Set) a rozšířený soubor služeb ESS (Extended service area).

2.1 BSS

Zařízení spadající do BSS sítě jsou rozmístěna na území, kde jsou všechna ve vzájemném dosahu. Takovéto území se označuje jako BSA (Basic service area). Podle způsobu komunikace mezi členy skupiny BSA rozeznáváme dva typy sítí, ad-hoc a infrastrukturní sítě.

2.1.1 Ad-hoc síť

Pro ad-hoc sítě je charakteristické, že zařízení spolu komunikují přímo, nepotřebují tedy další prvek, například bezdrátový router. Názorné schéma tohoto druhu sítě je na obrázku č. 12.



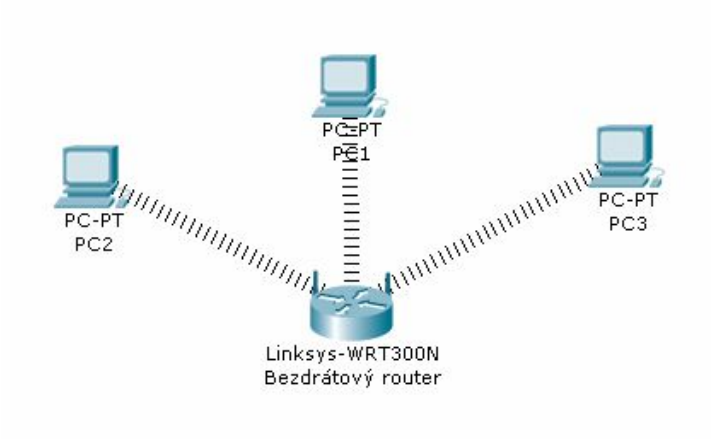
Obrázek č. 12: Ad-hoc síť

Pro komunikaci musí být všechna zařízení ve vzájemném dosahu. Z tohoto důvodu je tato síť velmi omezena prostorově, protože ve členitějším prostředí by se nemusely všechny stanice „vidět“. Její nejčastější použití tedy spočívá v propojení několika málo počítačů, často ze specifického důvodu na omezený čas, například přenos dat. Ad-hoc sítě v poslední době nejsou zdaleka tak oblíbené jako infrastrukturní sítě. Tento druh sítě potřebuje specifické

nastavení na každém zařízení, toto nastavení je pro jinou ad-hoc síť často nepoužitelné. Nemalý vliv na nevelké oblibě ad-hoc sítí má také stále se snižující cena aktivních prvků sítí, jako jsou například bezdrátové routery, Tato zařízení stačí v ideálním případě nastavit jen jednou a díky několikanásobně výkonnější anténě pokryje větší oblast a díky tomu se může připojit více zařízení. Pro případné podrobné nastudování problematiky ad-hoc sítí mohu doporučit knihu [6].

2.1.2 Infrastrukturní síť

Infrastrukturní sítě mají přesně vymezenou infrastrukturu. Základní součástí se zde stává síťový prvek, tzv. přístupový bod AP (access point). AP slouží jako rozhraní mezi drátovou a bezdrátovou sítí. Jednoduché schéma tohoto druhu sítě je na obrázku č. 13.

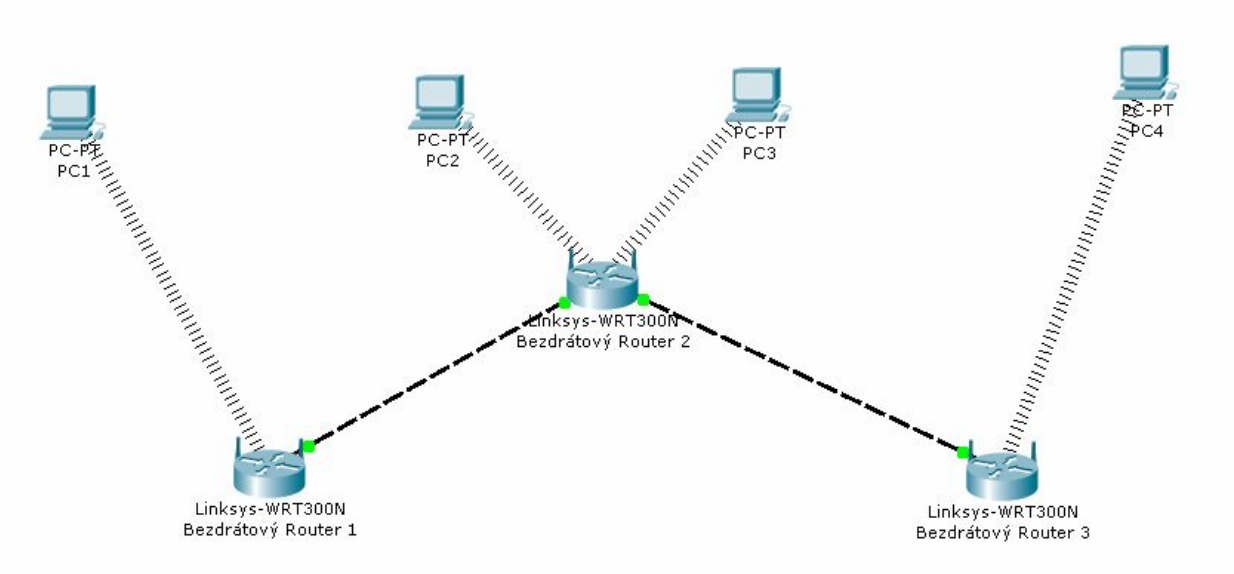


Obrázek č. 13: Infrastrukturní síť

Základní vlastností přístupového bodu je schopnost současně komunikovat se všemi stanicemi, které jsou v oblasti pokrytí signálem. V infrastrukturní síti, na rozdíl od ad-hoc sítě, pokud chce jedna stanice komunikovat s jinou, na obrázku například PC1 a PC2, tyto stanice komunikují přes prostředníka, jímž je přístupový bod, v našem případě bezdrátový router. Užitím přístupového bodu se síť centralizuje. Značně se tím zjednodušuje nastavení a správa sítě. Také lze lépe ošetřit zabezpečení sítě proti případným útokům. Z pohledu koncové stanice je použití také snazší, v případě vhodného nastavení si stačí vybrat příslušnou síť a automaticky se připojit. Z tohoto důvodu se nadále budu věnovat převážně tomuto druhu sítí.

2.2 ESS

Rozšířený soubor služeb ESS (Extended Service Set) je prakticky vzájemné propojení samostatných BSS, tak aby tvořily větší síť a tím pokryly větší oblast. Jednotlivé BSS jsou navzájem propojeny přes tzv. páteřní síť, to je nejčastější ethernetová síť. V ESS pak mohou jednotlivé stanice mezi sebou komunikovat a přecházet i mezi jednotlivými dílčími BSS. Nutnou podmínkou pro „přecházení“ stanic je dostatečný překryv signálu jednotlivých AP. Příklad takové sítě je na obrázku č. 14. Aby tento druh sítě splňoval svůj účel, musí být všechny AP v jedné doméně. Toho lze dosáhnout připojením na stejný rozbočovač nebo přepínač, případně použít technologii VLAN (virtual LAN).



Obrázek č. 14: Rozšířený soubor služeb

3 Bezdrátová zařízení

V současnosti na trhu existuje bezpočet různých bezdrátových zařízení od mnoha desítek výrobců. Zařízení se na první pohled liší tvarem a velikostí, ale všechna jsou postavena na stejném obecném modelu. Zařízení se skládá z řídícího softwaru, tzv. firmware, antény, může jích být i více, viz. například norma 802.11n, mohou být schovány v těle zařízení, a sady portů. Porty slouží pro připojení zařízení k metalické sítí, případně zde může být sériový port pro snazší konfiguraci. O napájení zařízení proudem se stará příslušný konektor. V poslední době lze využít i velmi oblíbenou funkci PoE (power over ethernet), ta využívá napájení přes nepoužívané vodiče kabelu UTP, případně STP. Rozdílem mezi levnými a dražšími přístupovými body je nejen výkonnější radiostanice, ale i propracovanější firmware, který je uživatelsky příjemnější a dovoluje pokročilejší nastavení zařízení.

Bezdrátová zařízení ve WLAN síti mohou zastávat úlohu bezdrátový přístupový bod nebo síťového mostu. V následujících podkapitolách jsou lehce nastíněny jejich základní charakteristiky.

3.1 Access Point

Bezdrátový přístupový bod AP (Access point) slouží pro směrování komunikace mezi klienty navzájem nebo mezi nimi a kabelovou sítí, tou může být například ethernet. AP není schopen k sobě připojit další AP, to zvládá až bridge, o tom je více v následující kapitole. Jednoduché schéma s využitím přístupového bodu je na Obrázek č. 13: Infrastrukturní síť. Access point je velmi často využíván, a proto je v kapitole 5 ukázáno jeho nastavení.

3.2 Bridge

Bridge, česky most, je zařízení sloužící k propojení dvou a více sítí nebo jejich segmentů, které jsou fyzicky nebo logicky odděleny. V současnosti funkci bridge a bezdrátového opakovače nabízí i mnoho přístupových bodů. Při návrhu sítě je důležité uvědomit si, zda je bridge vůbec třeba, není-li výhodnější použití „klasického“ metalického vedení, které je spolehlivější a má také daleko větší datovou propustnost.

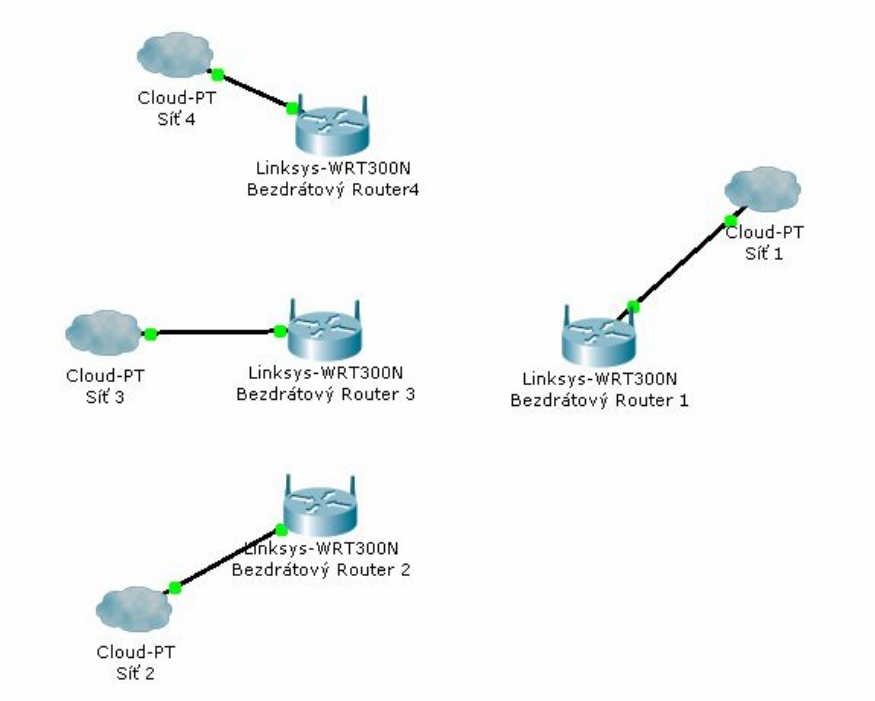
3.2.1 Point to Point

Point to point se využívá k propojení dvou zařízení, každé náležející jedné síti, nebo jejímu segmentu. Častým využitím point to point je v místech, kde by to pomocí kabeláže bylo nevhodné. Příkladem může být propojení vrchních pater dvou výškových budov, nebo užití v místech, kde je například z důvodů památkové ochrany nevhodné umísťovat metalické, případně optické vedení. Point to point je velmi často k nalezení i jako funkce v bezdrátových přístupových bodech. Jednoduché schéma je na obrázku č. 15. Na obrázku je point to point bridgem Bezdrátový router 1 a 2. Ke každému routeru je připojena síť, tou může být například LAN. Jeden router ale také může sloužit pro připojení k Internetu a toto připojení pomocí point to point technologie šířit bezdrátově dál. Drobnou nevýhodou point to point je, že zařízení spolu často nemusí spolupracovat, pokud budou od různých výrobců, proto se doporučuje mít oba bridge od stejné firmy. Příklad užití point to point je ukázán v kapitole 5.4.

Obrázek č. 15: Point to point

3.2.2 Point to Multipoint

Tato funkce je ve svém principu nadstavbou point to point, a proto je velmi podobná. Hlavní rozdíl od point to point představuje možnost propojení více než dvou bezdrátových zařízení. Jednoduché schéma sítě s využitím point to multipoint je na obrázku č. 16. Jedním z častých využití této technologie je například bezdrátová distribuce přístupu na internet. Dále lze point to multipoint použít třeba při bezdrátovém sesíťování většího počtu kanceláří, případně budov. Stejně jako u point to point i zde platí, že všechna zařízení v síti by měla být od jednoho výrobce, je tak zaručen bezproblémový chod sítě.



Obrázek č. 16: Point to multipoint

3.2.3 Bezdrátový opakovač

Bezdrátový opakovač rozšiřuje oblast bezdrátové sítě opakováním signálu. S jeho pomocí tak lze propojit vzdálené AP namísto metalickým vedením pomocí opakovače. Jako využití opakovače se nabízí například propojení dvou vzdálenějších kancelářských sítí, případně dvou budov, kde už by ani bridge svým výkonem nedostačoval.

4 Bezpečnost

Při využití kabelové sítě si lze asi jen těžko představit, že by útočník přišel do budovy nebo kanceláře a bez povšimnutí se připojil do switche nebo routeru. U bezdrátových sítí takové riziko ale reálně existuje. Útočníkovi většinou postačuje notebook s Wi-fi zařízením a pohodlné místo někde na lavičce v parku, případně v autě. Nemusí ani vkročit do budovy, nebo kanceláře, do které se plánuje „připojit“. Bezdrátové sítě vytváří velké bezpečnostní riziko už díky médiu, které využívají pro přenos, vzduch. U WLAN totiž nelze dostatečně přesně omezit prostor kam se bude šířit signál.

Wi-fi sítě je dnes možné chránit různými prvky, některé jsou účinnější, některé nikoliv. V následujících podkapitolách budou ty nejpoužívanější popsány.

4.1 Nejslabší ochranné prvky

Následující ochranné prvky sice nejsou pro cílené útoky velkou překážkou. Dokáží ale ztížit přístup do sítě náhodným, „nevítaným“ uživatelům.

4.1.1 SSID

Každá bezdrátová síť má svůj jedinečný identifikátor, tzv. SSID (Service Set Identifier). Tento identifikátor je vysílán přístupovým bodem v tzv. majákovém rámci (beacon frame). V rámci je parametr SSID skládající se z řetězce ASCII znaků o maximální délce 32 znaků. Všechna bezdrátová zařízení, která se pokusí o vzájemnou komunikaci si mezi sebou tento klíč předávají. V nastavení AP lze zamezit vysílání SSID. Identifikátor se pak v majákovém rámci nevysílá. Bez znalosti tohoto identifikátoru se není možno k síti připojit, taková síť je pak bez užití specializovaného softwaru „neviditelná“.

4.1.2 MAC adresy

Na přístupovém bodu můžeme povolit nebo zakázat daným uživatelům přístup. K tomuto se výborně hodí MAC adresa (Media Access Control address), je to totiž jedinečný, výrobcem přiřazený identifikátor síťového zařízení. Filtrování MAC adres se hodí do sítí, kde jsou připojeni stále stejní klienti, protože se musí adresa zadat ručně do přístupového bodu ještě před připojením klienta.

4.1.3 DHCP server

DHCP (Dynamic Host Configuration Protocol) je protokol sloužící pro automatické přidělování IP adres jednotlivým klientům v síti. Po vypnutí DHCP serveru sice musíme IP adresy nastavit „ručně“, ale zároveň tím ztížíme případné připojení „náhodných kolemjdoucích“. Přístupový bod totiž při připojení nepřidělí zařízení IP adresu.

4.1.4 Jméno a heslo

Každé bezdrátové zařízení má při výrobě nastaveno pro přístup do konfiguračního menu jméno a heslo. Ta jsou pro všechna zařízení daného výrobce stejná. Uživatel by jméno a heslo měl ve vlastním zájmu co nejdříve změnit. Pro útočníka, který by se přihlásil k přístupovému bodu s výrobcem přednastaveným jménem a heslem, není problém si ho zjistit podle typu zařízení. Následně pak pro útočníka není žádný problém se přihlásit do konfiguračního menu a změnit nastavení přístupového bodu dle libosti.

4.2 WEP a WEP2

Zabezpečovací protokol WEP (Wired Equivalent Privacy) byl definován již v prvním standardu 802.11 a byl vymyšlen tak, aby poskytl zabezpečení obdobné jako ve drátových sítích. Kvůli slabému kryptografickému základu tomu tak ale není. Základem je proudová šifrovací metoda RC4 a metoda kontrolního součtu CRC-32. Pro podrobnější informace o RC4 doporučuji [11] a o CRC [9]. RC4 používá tajný klíč o velikosti 40 nebo 104 bitů a 24 bitový inicializační vektor IV. Následně pak vzniká 64bitový WEP nebo 128 bitový WEP, někteří výrobci však podporují i WEP 256 bitový.

S uvedení WEP2 přišlo zesílené 128 bitové šifrování a rozšířil se inicializační vektor. Byl použit u zařízení, na kterých nešel změnit firmware pro používání WPA nebo WPA2.

WEP je v současnosti velmi zranitelnou ochranou, jeho prolomení je za použití speciálního softwaru otázkou několika minut. WEP2 obsahuje stejné bezpečnostní problémy jako WEP, a proto i jeho prolomení v současnosti není problém, pouze zabere o něco více času.

4.3 WPA a WPA2

Vývoj WPA (Wi-Fi Protected Access) byl podnícen vážnými bezpečnostními nedostatky WEP. Tento protokol používá stejný šifrovací algoritmus jako WEP, má 128

bitový klíč a 48 bitový inicializační vektor. Novinkou je dynamicky se měnící klíč TKIP(Temporal Key Integrity Protocol) a vylepšená kontrola integrity dat MIC (Message-Integrity Check) nahrazující CRC. Standard 802.11i je z velké části implementován již ve WPA, kompletní implementace je ale až ve WPA2. Ve WPA2 je použit protokol CCMP (Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol) se silným šifrováním AES (Advanced Encryption Standard). Autentizace se provádí pomocí přednastaveného sdíleného klíče PSK (Pre-shared key) nebo za využití EAP (Extensible Authentication Protocol) pomocí RADIUS (Remote Authentication Dial In User Service) serveru, který vzdáleně ověřuje uživatele.

Pro zabezpečení bezdrátové sítě lze dnes použít v případě starších zařízení WPA-PSK/TKIP, nebo pokud to hardware dovolí, WPA2-PSK/AES. Oba způsoby jsou v současné době dostatečně odolné proti útoku, ale vybírají si za to daň v podobě vyšší hardwarové náročnosti a nutnosti pokročilého nastavení zařízení.

5 Modely sítí

V následující kapitole bude předvedeno na praktických modelech nastavení bezdrátové sítě. Modely budou vytvořeny za využití programu Packet tracer 5.0, který je stažitelný v rámci programu CCNA.

5.1 Základní model

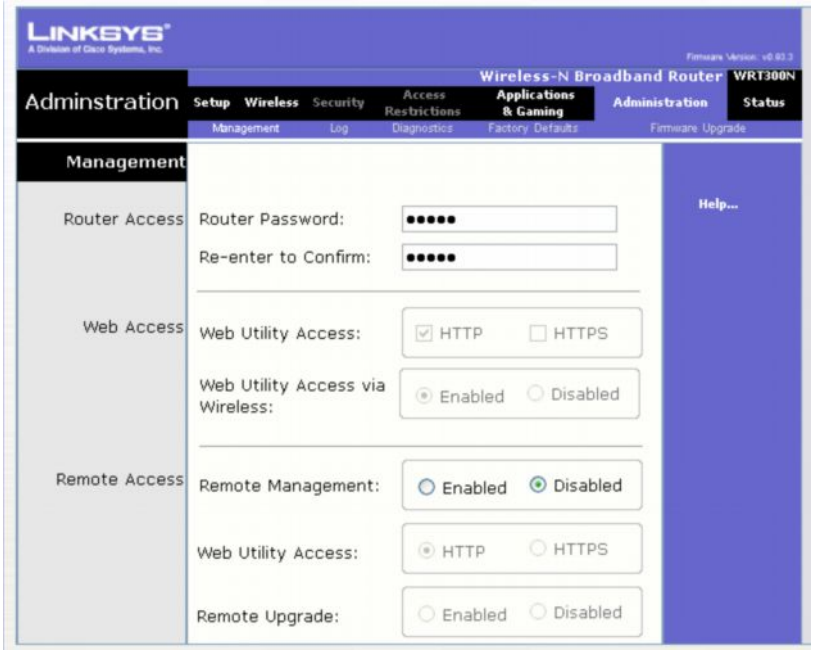
Nejjednodušší model bezdrátové sítě je propojení jednoho AP s jedním PC, případně více PC. V následujících podkapitolách bude toto nastavení ukázáno na modelovém příkladu.

5.1.1 Statická IP

Model, jehož schéma je na obrázku č. 17, se skládá z jednoho uživatele, v našem případě PC 1, a jednoho přístupového bodu, na schématu Wireless Router 1. Je zde využito statických IP adres přiřazovaných bezdrátovým zařízením. Přístupový bod v tomto modelu pracuje dle normy 802.11n, která je popsána v kapitole1.2.4.

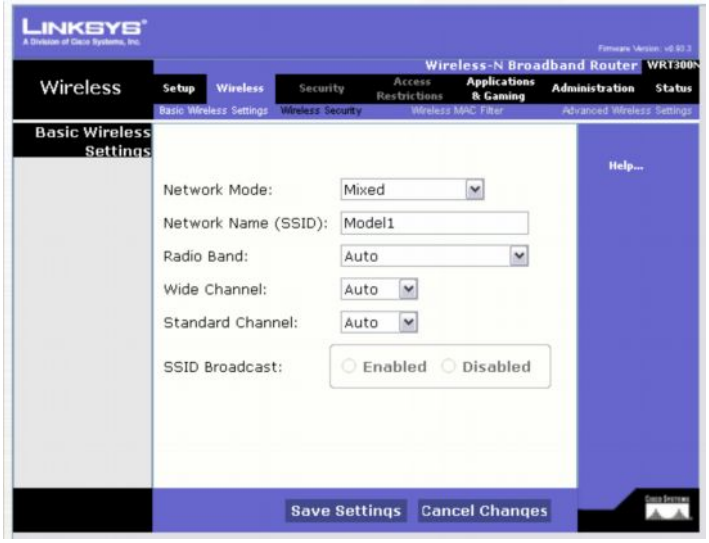
Obrázek č. 17: Model o jednom PC a AP

- Prvním krokem při nastavování přístupového bodu by mělo být změna výrobcem implicitně nastaveného přihlašovacího jména a hesla. V použitém modelu je bezdrátový router Linksys WTR300N, který má jen volbu změny hesla. Na následujícím Obrázek č. 18: Změna hesla je vidět zadávací pole (Router Password) a pole pro ověření (Re-enter to Confirm) zadaného hesla. Další nastavení nás na této záložce v současnosti nemusí zajímat, ale jen pro informaci, je zde ještě nastavení přístupu k webovému rozhraní a možnost nastavení vzdálené zprávy AP.



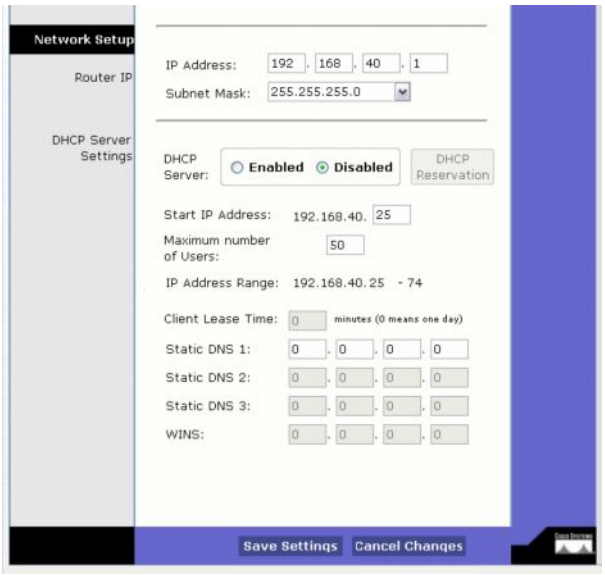
Obrázek č. 18: Změna hesla

- Výhodná při práci se sítí je změna původní SSID na jiné, vhodnější jméno, v modelu je použito jméno Model1. Nastavení je vidět na obrázku č. 19. Další položky menu můžeme nechat v implicitním stavu. Další nastavení není v tomto modelu sítě nutné, ale v případě potřeby je zde ještě možnost upřednostnění použitého standardu, viz kapitola 1.2, změna kanálu, kapitola 1.5.1 a možnost zamezení vysílání SSID, o tom více v kapitole 4.1.1.



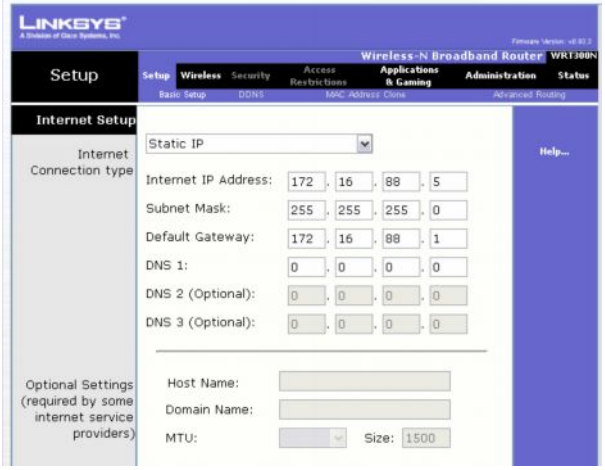
Obrázek č. 19: SSID

- Dalším krokem při užití statické IP adresy je přiřazení adresy k bezdrátovému rozhraní na AP, v modelu je např. použita adresa 192.168.40.1 /24. Nastavení je možno vidět na obrázku č. 20. Nastavení DHCP nás v tomto modelu nemusí zajímat.



Obrázek č. 20: IP adresa

- Nyní se přiřadí IP adresa k rozhraní, ke kterému se připojí okolní metalická síť, nejčastěji to bývá Internet. V našem modelu žádná taková síť není, ale pro názornost je to předem nastaveno. Nastavuje se IP adresa, maska, brána a případně DNS server. Příklad nastavení možno vidět na obrázku č. 21.

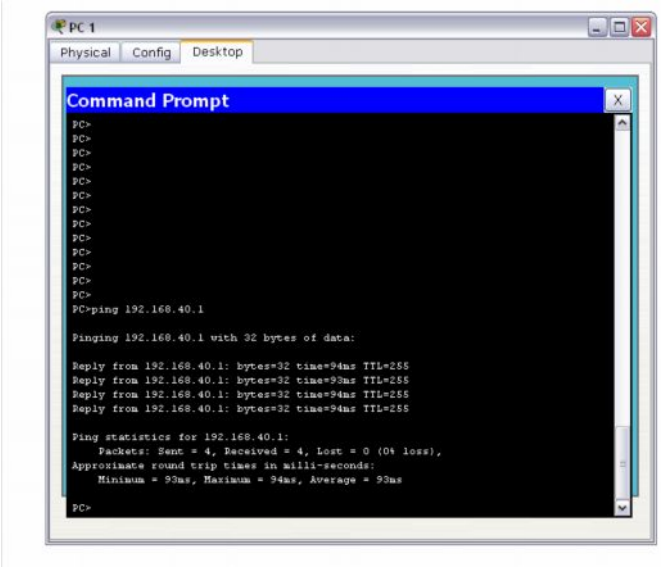


Obrázek č. 21: Okolní síť

- K základnímu nastavení AP to je vše, teď již stačí nastavit bezdrátovou síťovou kartu uživatele. Jedna z variant IP adres přiřazených zařízení je vidět na obrázku č. 22. Velmi důležité je dát si pozor na použitelný rozsah adres definovaný maskou sítě na AP. Po nastavení adres se již stačí připojit k AP, a protože není nastavena žádná úroveň zabezpečení sítě, zařízení by měla hned komunikovat bez dalšího případného ověřování uživatele.

Obrázek č. 22: IP adresa uživatele

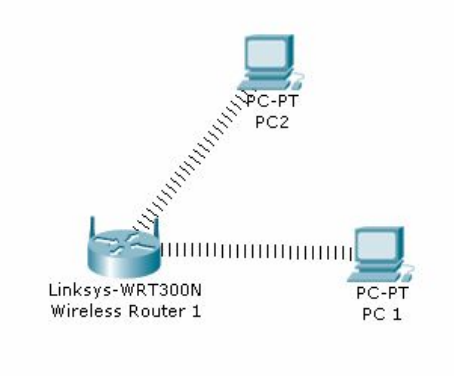
- Pro ověření funkčnosti je použit příkaz PING v příkazové řádce uživatele. Uživatel se snaží „pingnout“ k připojenému přístupovému bodu. Jak je vidět na obrázku č. 23, přístupový bod odpovídá a síť je tedy funkční.



Obrázek č. 23: PING na AP

5.1.2 DHCP

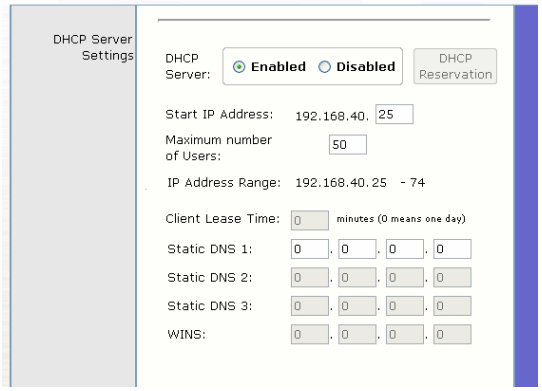
Stejně jako v kapitole 5.1.1, tak i při tomto nastavení se vychází z velmi podobného modelu sítě, jen byl přidán pro demonstraci DHCP serveru ještě jeden koncový uživatel, PC2. Schéma sítě je na obrázku č. 24. Přístupový bod na tomto modelu pracuje dle normy 802.11n, která je popsána v kapitole1.2.4.



Obrázek č. 24: AP s DHCP serverem

DHCP server, zmíněný v kapitole 4.1.3, je sice potencionální bezpečnostní riziko, ale jeho použití je téměř nezbytné při častém připojování více koncových uživatelů. Díky DHCP se administrátor sítě nemusí starat o přidělené adresy a nehrozí případná kolize, pokud by byla jedna a tatáž adresa omylem přidělena současně dvěma koncovým uživatelům.

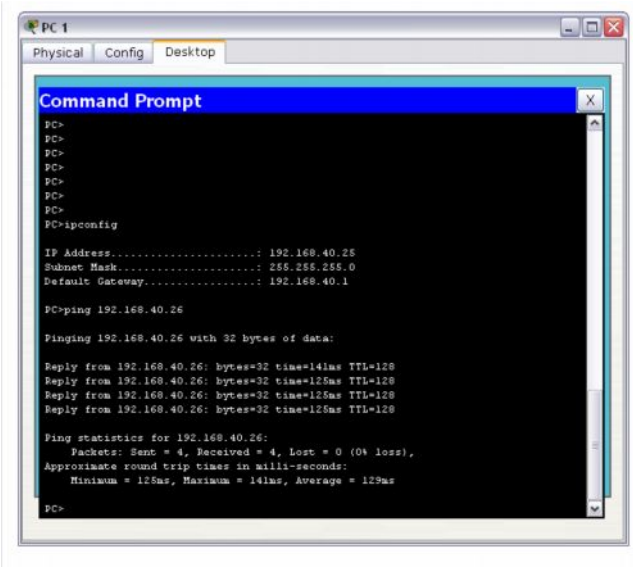
- Nastavení AP s DHCP serverem se liší od konfigurace v předchozí kapitole jen spuštěním DHCP serveru a zadáním nejnižší adresy, od které server bude přiřazovat IP adresy koncovým uživatelů. Při nastavení také udáváme maximální počet koncových uživatelů. Na obrázku č. 25 je vidět zadávací formulář.



Obrázek č. 25: Nastavení DHCP

- Konfigurace na straně uživatele je ještě snazší než při užití statické IP adresy. Tentokrát se nemusí zadávat žádná IP adresa, ale při pokusu o připojení je adresa uživateli přiřazena DHCP serverem.
- Po připojení obou koncových uživatelů je možné si příkazem ipconfig ověřit přidělenou IP adresu. K PC 1 byla přiřazena 192.168.40.25 a k PC 2 192.168.40.26. Dále je možné

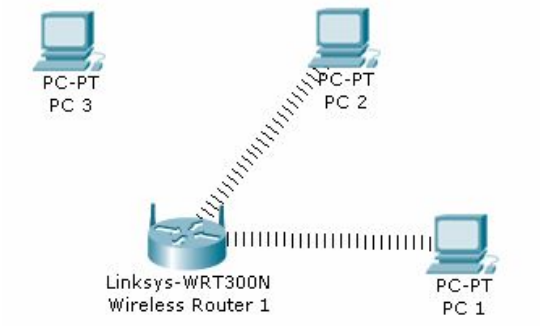
ověřit funkčnost komunikace mezi oběma uživateli příkazem PING. Na obrázku č. 26 je vidět výpis po zadání příkazu ipconfig a je také vypsána úspěšná odpověď od PC 2 na příkaz ping.



Obrázek č. 26: Ověření komunikace

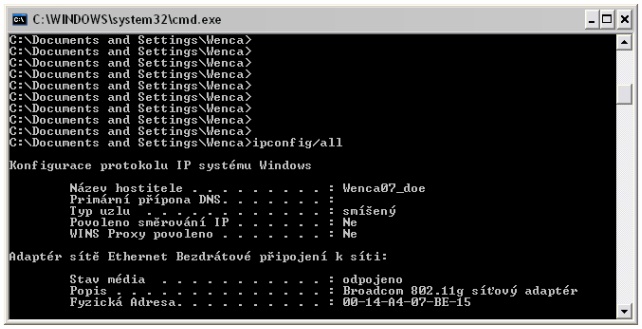
5.2 Filtrování MAC adres

O filtrování MAC adres na přístupovém bodu již byla zmínka v kapitole 4.1.2 MAC adresy. Natavení přístupového bodu je velmi jednoduché, stačí znát MAC adresy všech koncových uživatelů, kteří se k tomuto AP připojují. Tuto funkcionalitu zařízení Linksys WTR300N simulované v programu Packet tracer neumí, a proto je zde předvedeno nastavení z reálného bezdrátového přístupového bodu AirLive WL-5460AP v2 pracujícího dle normy 802.11n, tato norma je popsána v kapitole1.2.4. Schéma sítě je na obrázku č. 27. Namísto PC 1 a PC 2 byly použity notebooky a PC 3 byl desktopový počítač s wi-fi kartou.



Obrázek č. 27: Síť s fltrováním MAC adres

- MAC adresa uživatele se zjistí například příkazem ipconfig /all, výpis je na obrázku č. 28.



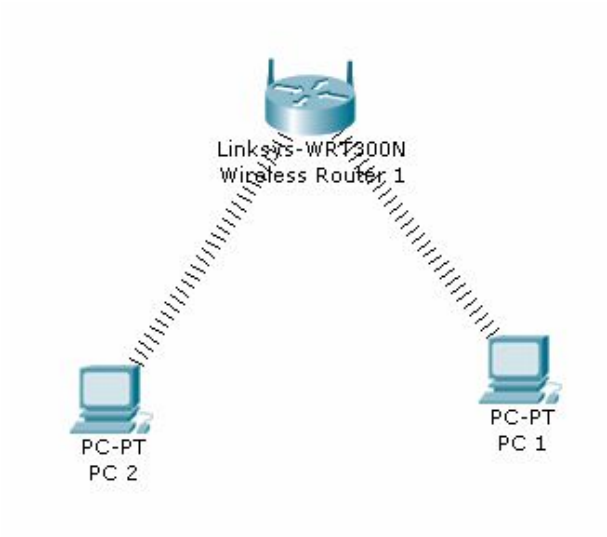
Obrázek č. 28: IPConfig

- Na obrázku č. 29 je vidět menu pro zadání MAC adresy a případného komentáře. Pak již stačí nastavit, zda se má zadané adrese povolit nebo zakázat přístup a přidat tuto adresu do přístupového listu, který je uložen v paměti zařízení. Při zadávání adres je třeba dát si pozor na správné opsání adresy, jinak nebude filtr pracovat správně.

Obrázek č. 29: MAC adresy

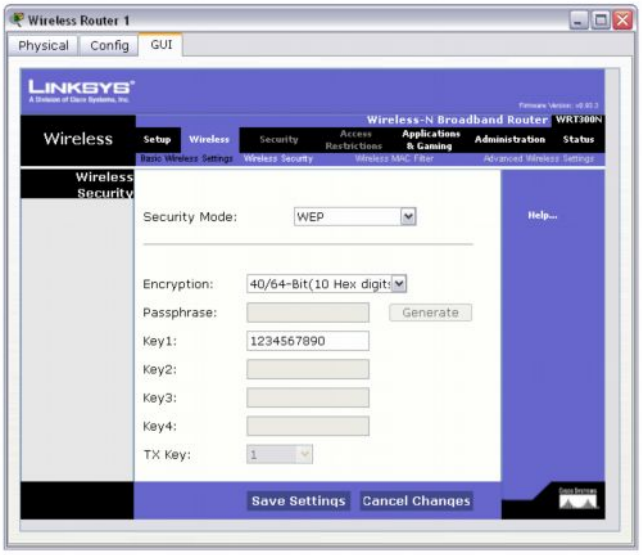
5.3 WEP

Následující model, jehož schéma je na obrázku č. 30, bude využívat pro zabezpečení WEP. Tento zabezpečovací protokol je podrobněji popsán v kapitole 4.2. Schéma se pro jednoduchost skládá ze dvou koncových uživatelů a jednoho AP. Na přístupovém bodě „běží“ DHCP server. Jeho nastavení už bylo probráno výše v kapitole 5.1.2 DHCP. Na AP je použita 64 bitová verze WEP. Přístupový bod pracuje dle normy 802.11n, ta je blíže popsána v kapitole 1.2.4.



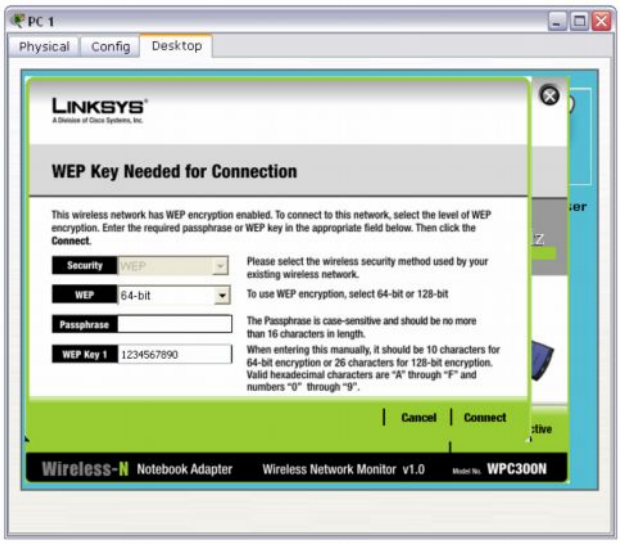
Obrázek č. 30: WEP

- Nastavení 64 bitové verze WEP je poměrně jednoduché, stačí zvolit druh šifrování a zadat klíč, v našem případě je to posloupnost deseti čísel. Zadávací formulář je na obrázku č. 31.



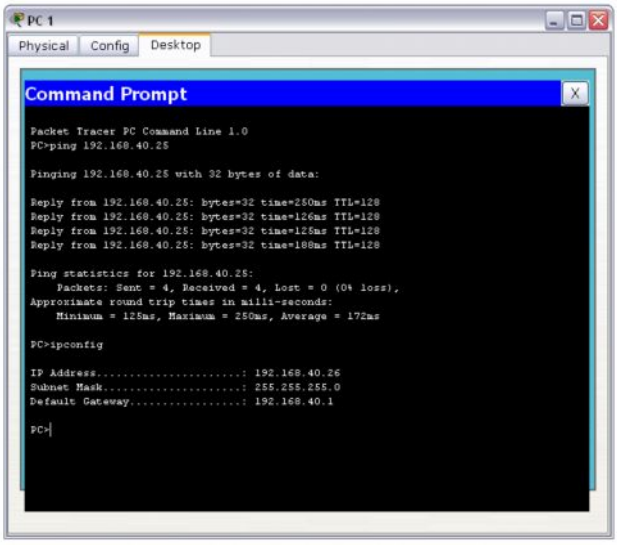
Obrázek č. 31: Nastavení WEP

- Koncový uživatel je při připojení k přístupovému bodu dotázán na klíč, který musí zadat do příslušného pole, viz obrázek č. 32. Po ověření klíče je uživatel připojen.



Obrázek č. 32: Zadání klíče

- Pro ověření připojení opět můžeme použít příkaz ping. V modelu jsou dva uživatelé, měli by být tedy schopni vzájemné komunikace. Výpis úspěšné komunikace mezi PC1 a PC 2 je na obrázku č. 33.

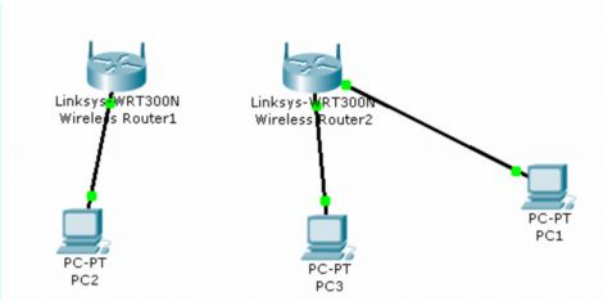


Obrázek č. 33: Ping mezi uživateli

5.4 Bridge – Point to point

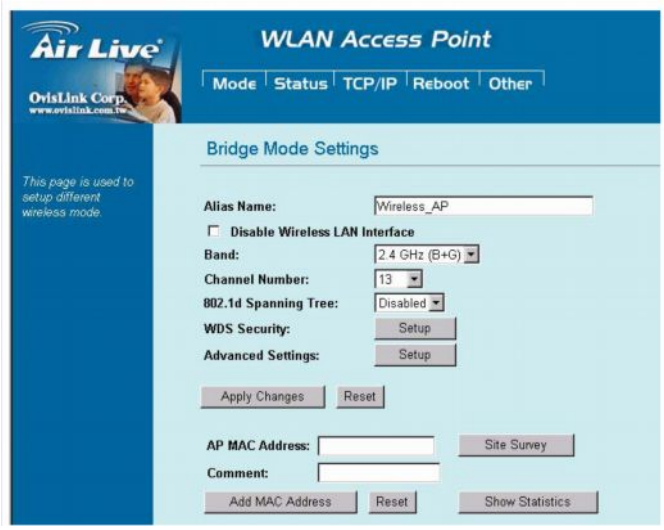
Model sítě s užitím bridge, přesněji point to point, je znázorněn na obrázku č. 34. Z důvodu nemožnosti simulovat toto nastavení v Packet Traceru byly použity dva bezdrátové

routery AirLive WL-5460AP v2, běžící podle normy 802.11b + g, ta je blíže popsána v kapitole 1.2.2 a 1.2.3.



Obrázek č. 34: Bridge - point to point

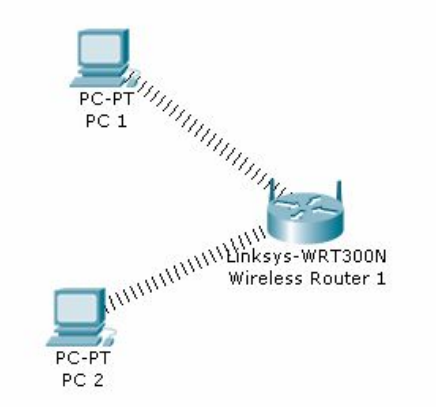
- Nastavení bridge, na obrázku č. 35, je na obou routerech téměř identické. Jediný rozdíl je v MAC adresách. Do pole pro MAC adresu se zadává vždy zařízení, se kterým chceme navázat spojení. MAC adresu zařízení můžeme zjistit na každém zařízení zvlášť, nebo v našem případě použít funkci Site Survey, která „naslouchá“ okolí a vypíše aktivní AP i s potřebnými informacemi. Pozor je třeba si dát při nastavení kanálu, na kterém zařízení komunikují, na obou stranách bridge musí být nastaven stejný kanál, jinak se spojení nezdaří. Uživatelé byli připojeni UTP kabelem, a proto bylo při nastavování vypnuto bezdrátové rozhraní bridge.



Obrázek č. 35: Nastavení bridge

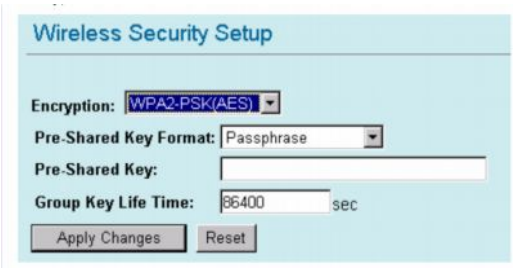
5.5 WPA2 – PSK/EAS

Pro síť využívající zabezpečení WPA2 – PSK/EAS, jejíž schéma je na obrázku č. 36, je opět použit bezdrátový router AirLive WL-5460AP v2 a dva notebooky s wi-fi kartou simulující uživatele. Z důvodu kompatibility bezdrátových zařízení byla AP nastavena norma 802.11g, blíže je popsána v kapitole 1.2.3.



Obrázek č. 36: WPA2

- Nastavení WPA2 – PSK/EAS probíhá přes jednoduchý formulář, je na obrázku č. 37. U položky s formátem předsdíleného klíče (Pre-shared Key Format) se doporučuje zvolit Passphrase. Potom se zadá písmenný klíč, doporučuje se zadat alespoň osm znaků. Při volbě Hex se musí zadat 64 znaků.



Obrázek č. 37: Nastavení WPA2

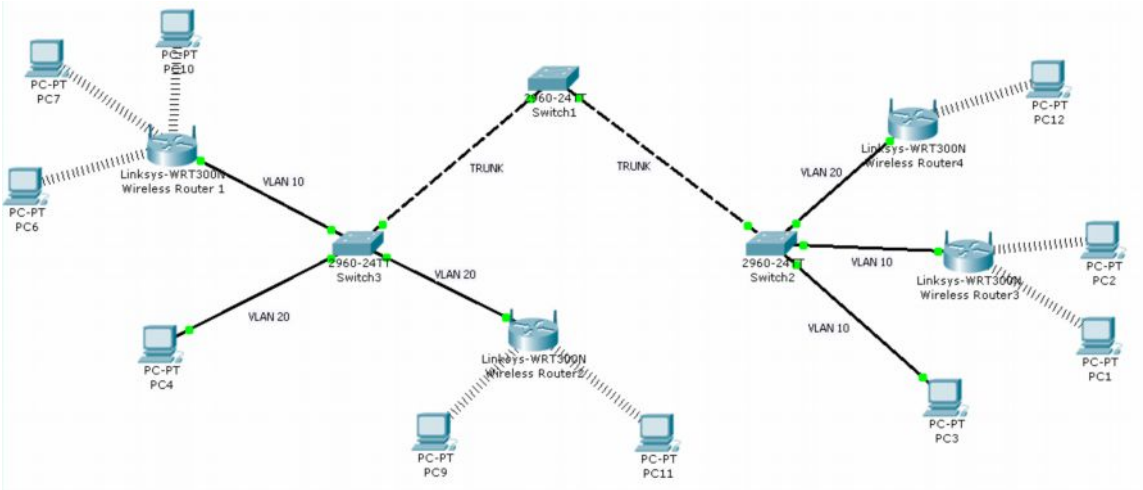
- Pro připojení koncového uživatele už stačí jen zadat stejný klíč jako se zadával na AP.

5.6 VLAN

Schéma následujícího modelu je na obrázku č. 38. V síti byla použita technologie VLAN (virtual LAN) a VTP (VLAN Trunking Protocol). V síti jsou tři VLAN:

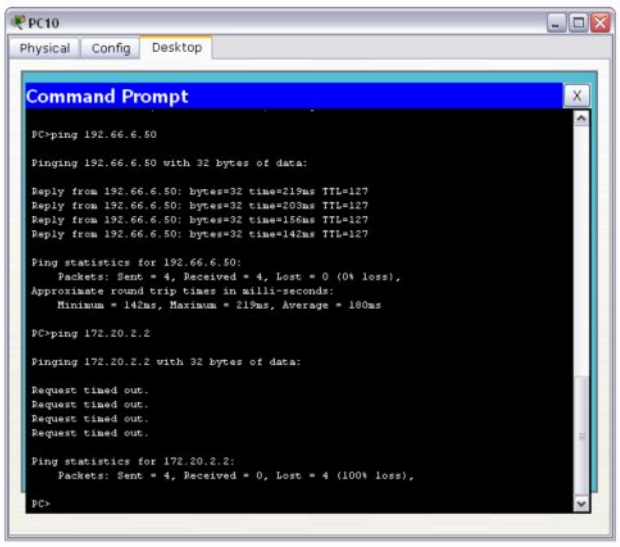
1. VLAN 10 - pojmenovaná Death, v ní jsou obsaženy bezdrátové routery č. 1 a č. 3 a dále PC 3.
2. VLAN 20 – nazvaná Black, obsahuje následující zařízení: bezdrátový router č. 2 a č. 4 a dále PC 4.
3. VLAN 30 – pojmenovaná Metal, využívají ji switche pro VTP.

Pro snazší práci s VLAN byl Switch1 nastaven jako VTP server a Switch2 a 3 jako VTP klient, tím byla zjednodušena správa nadefinovaných VLAN v síti. VTP doména je Deicide s heslem cisco. Přístupové body pracují podle normy 802.11n, ta je popsána v kapitole 1.2.4.



Obrázek č. 38: VLAN

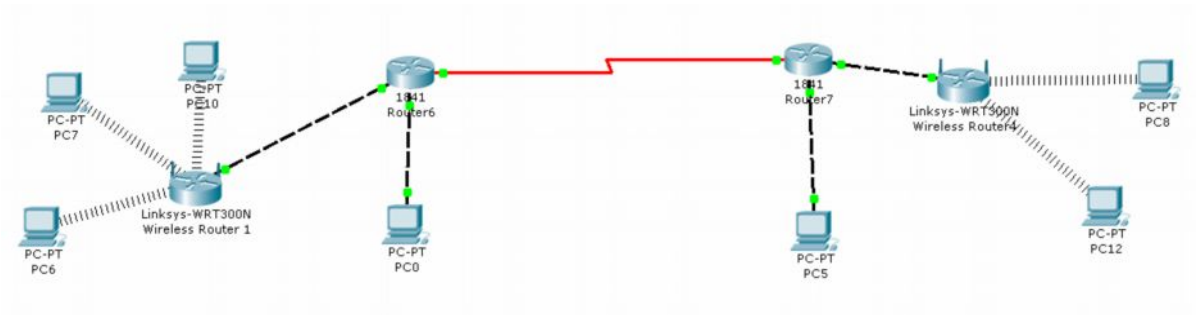
- Nastavení switche zde nebude popisováno, je součástí kurzu CCNA 3.
- Na všech přístupových bodech byl nastaven DHCP server, popis nastavení je v kapitole 5.1.2.
- Pro správnou funkci VLAN musí být všechna zařízení do ní spadající součástí stejné sítě, zde byla zvolena pro VLAN 10 síť 192.66.6.0 /24 a pro VLAN 20 síť 172.20.2.0 /24.
- Na AP byl z bezpečnostních důvodů nastaven WEP, popis jeho nastavení je už uveden v kapitole 5.3.
- Pro ověření funkce sítě byl proveden příkaz ping. Z obrázku č. 39 je patrné, že uživatelé náležící do jedné VLAN nemohou komunikovat s uživateli v jiné nadefinované VLAN, nastavení tedy proběhlo správně.



Obrázek č. 39: Ping na okolní zařízení

5.7 OSPF

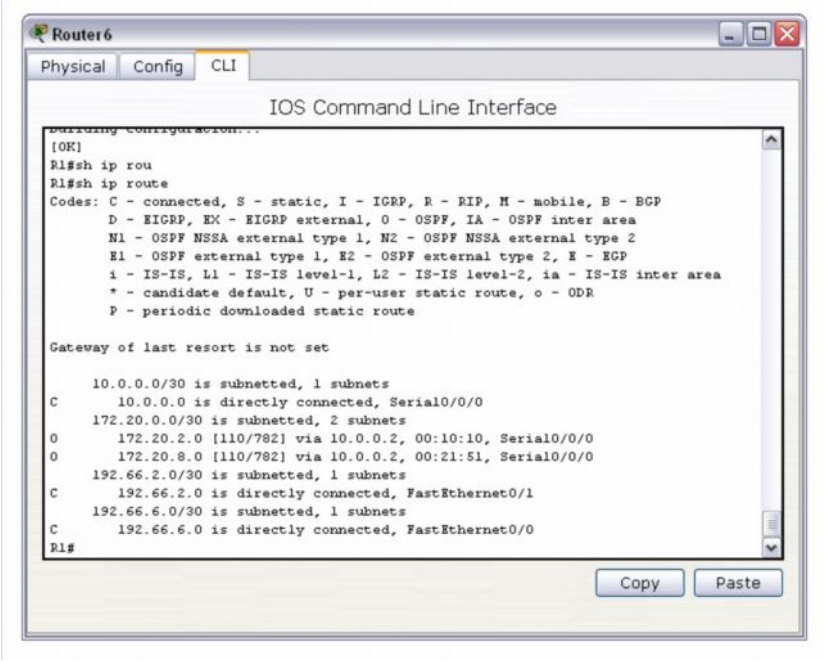
Schéma následujícího modelu je na obrázku č. 40. V modelu je využito dvou routerů a směrovacího protokolu OSPF, pro bližší informace doporučuji [12]. Cílem toho modelu je ukázat, že pro propojení dvou bezdrátových sítí lze použít i už vystavěnou metalickou síť. Přístupové body pracují podle normy 802.11n, ta je podrobněji popsána v kapitole1.2.4.



Obrázek č. 40: Model s využitím OSPF

- Nastavení routeru není cílem této práce. Routery jsou propojeny sériovou linkou, Router6 je DCE a Router7 je DTE. AP a počítače PC0 a PC5 jsou k routerům připojeny křiženým

kabelem UTP. Na obou routerech je též zprovozněný telnet pro snazší správu zařízení. Jen pro příklad je na obrázku č. 41 výpis směrování na Routeru 6.



Obrázek č. 41: Router 6

- Na obou přístupových bodech byl nastaven DHCP server, popis nastavení je v kapitole 5.1.2.
- Na AP byl z důvodů zvýšení bezpečnosti nastaven WEP, popis jeho nastavení je už uveden v kapitole 5.3.
- Ověření funkce správné sítě bylo provedeno příkazem ping.

6 Závěr

Cílem bakalářské práce bylo vytvořit podpůrný materiál pro podporu výuky počítačových sítí, zaměřený na bezdrátové sítě.

Práce je rozdělena na striktně teoretickou část, která vysvětluje a objasňuje základní pojmy z oblasti bezdrátových sítí, vlastnosti bezdrátového přenosu dat a jejich bezpečnost.

Praktická část, která obsahuje modely sítí vytvořené v simulátoru Packet Tracer 5.0, využívá teoretické znalosti z první části práce a na jejich základě ukazuje jejich praktický význam a použití. Právě tato část tvoří vrchol pomyslné pyramidy znalostí z oblasti počítačových sítí, jelikož pro jejich pochopení a praktickou realizaci je nutné využít i znalostí z jiných oblastí počítačových sítí.

Z výše zmíněného plyne, že práce splnila své cíle a je připravena pro použití při výuce počítačových sítí a to nejen na DFJP UPCE. Kompletní konfigurace sítí a vytvořené modely sítí jsou na přiloženém DVD.

7 Seznam použitých zdrojů

[1] KABELOVÁ, Alena, DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP a systémem DNS. 5. aktualiz. vyd. [s.l.] : [s.n.], 2008. 488 s.

[2] ZANDL, Patrick. Bezdrátové sítě WiFi. [s.l.] : [s.n.], 2003. 204 s.

[3] SHELLY, Brisbin. Wi-Fi : postavte si svou vlastní wi-fi síť. [s.l.] : [s.n.], 2004. 248 s. ISBN 8086330133.

[4] ZANDL, Patrick. Bezdrátové sítě WiFi : Praktický průvodce. [s.l.] : [s.n.], 2003. 204 s. ISBN 807226632.

[5] PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace. [s.l.] : [s.n.], 2005. 179 s. ISBN 80-251-0791-4.

[6] SARKAR, Subir Kumar , BASAVARAJU, T.G. v, PUTTAMADAPPA, C. . Ad Hoc Mobile Wireless Networks : Principles, Protocols and Applications . 1st edition. [s.l.] : Auerbach Publications, 2007. 336 s. ISBN-10: 1420062212. ISBN-13 978-1420062212.

[7] Gold Sequences [online]. 1999 [cit. 2009-05-09]. Dostupný z WWW: <http://www.wirelesscommunication.nl/reference/chaptr05/cdma/codes/gold.htm>.

[8] Barker Code [online]. 2003 [cit. 2009-05-09]. Dostupný z WWW: <http://mathworld.wolfram.com/BarkerCode.html>.

[9] Cyclic Redundancy Checks [online]. 2007 [cit. 2009-05-16]. Dostupný z WWW: <http://www.mathpages.com/home/kmath458.htm>.

[10]Wi-Fi Products Tested [online]. 2005 [cit. 2009-05-17]. Dostupný z WWW: <http://broadbandhomecentral.com/bbhl/wifiproducts.html>.

[11] RC4 [online]. 2008 [cit. 2009-05-16]. Dostupný z WWW: <http://en.wikipedia.org/wiki/RC4>.

[12] OSPF Design Guide [online]. 2005 [cit. 2009-05-19]. Dostupný z WWW: <http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml>.

[13] Bezdrátová technologie Wi-Fi zbavená roušky tajemství [online]. 2005 [cit. 2009-05-01]. Dostupný z WWW: <http://pctuning.tyden.cz/bezdratova_technologie_wi-fi_zbavena_rousky_tajemstvi>.

[14] Wi-Fi 802.11n: průlom nebo propadák? [online]. 2008 [cit. 2009-05-01]. Dostupný z WWW: <http://www.svethardware.cz/art_doc27EE470F391C1776C12574B0004F01F6.html>.

[15] ICTS [online]. 2007 [cit. 2009-05-01]. Dostupný z WWW: <http://icts.amrita.ac.in/web/images/stories/wifi_logo.gif>.

[16] IEEE 802.11 [online]. 2008 [cit. 2009-05-01]. Dostupný z WWW: <http://en.wikipedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_(802.11b,g_WLAN).png>.

[17] Codecguru [online]. 2008 [cit. 2009-05-01]. Dostupný z WWW: <http://www.codeguru.com/dbfiles/get_image.php?id=12219&lbl=TCP03_GIF&ds=20060629>.

8 Seznam obrázků

Univerzita Pardubice
Dopravní fakulta Jana Pernera
Katedra informatiky v dopravě
Akademický rok: **2008/2009**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Václav BAŠTA**
Studijní program:	**B3709 Dopravní technologie a spoje**
Studijní obor:	**Aplikovaná informatika v dopravě**
Název tématu:	**Vytvoření podpory pro výuku počítačových sítí v oblasti bezdrátové komunikace**

Zásady pro vypracování:

Cílem práce je vytvoření studijních materiálů v českém jazyce, použitelných při výuce v předmětech Počítačové sítě, zaměřených na bezdrátové technologie. V práci budou rozebrány a popsány možnosti bezdrátových technologií a princip jejich fungování. Budou vytvořeny modely pro simulaci bezdrátových počítových sítí v simulátoru Packet Tracer. Přínosem práce bude studijní materiál pro podporu výuky počítačových sítí.

Rozsah grafických prací:
Rozsah pracovní zprávy: **minimálně 30 stran**
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **KABELOVÁ, Alena, DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP a systémem DNS. 5. aktualiz. vyd. [s.l.] : [s.n.], 2008. 488 s.**
2. **ZANDL, Patrick. Bezdrátové sítě WiFi. [s.l.] : [s.n.], 2003. 204 s.**
3. **http://ronja.twibright.com/**

Vedoucí bakalářské práce: **Mgr. Josef Horálek**
Katedra informatiky v dopravě

Datum zadání bakalářské práce: **5. prosince 2008**
Termín odevzdání bakalářské práce: **1. června 2009**

prof. Ing. Bohumil Culek, CSc.
děkan

L.S.

doc. Ing. Josef Volek, CSc.
vedoucí katedry

V Pardubicích dne 5. prosince 2008