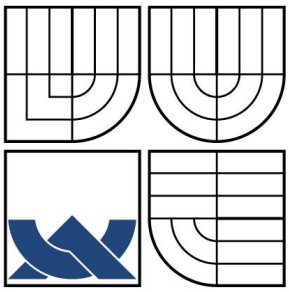
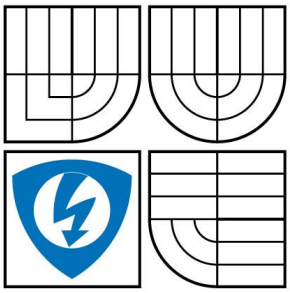


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKACNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

NOVÝ MODEL ZABEZPEČENÍ IMPLEMENTOVANÝ V METROPOLITNÍ SÍTI
NEW SECURITY MODEL IMPLEMENTED IN THE METROPOLITAN NETWORK

DIPLOMOVÁ PRÁCE
MASTER´S THESIS

AUTOR PRÁCE — **Bc. MICHAL DANČUK**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. VLADISLAV ŠKORPIL, CSc.**
SUPERVISOR

BRNO 2008

Oficiální zadání

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Bc. Michal Dančuk

Bytem: Sendražice 94, 50303 Smiřice

Narozen/a (datum a místo): 28.7.1984, Jaroměř

(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií

se sídlem Údolní 244/53, 602 00, Brno 2

jejímž jménem jedná na základě písemného pověření děkanem fakulty:

prof. Ing. Kamil Vrba, CSc.

(dále jen „nabyvatel“)

Článek 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - □ disertační práce
   - ☒ diplomová práce
   - □ bakalářská práce
   - □ jiná práce, jejíž druh je specifikován jako .....

(dále jen VŠKP nebo dílo)

Název VŠKP: Nový model zabezpečení implementovaný v metropolitní síti

Vedoucí/ školitel VŠKP: doc. Ing. Vladislav Škorpil, CSc.

Ústav: Ústav telekomunikací

Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v*:

- ☒ tištěné formě – počet exemplářů 2
- ☒ elektronické formě – počet exemplářů 2

* hodící se zaškrtněte

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - ☒ ihned po uzavření této smlouvy
   - □ 1 rok po uzavření této smlouvy
   - □ 3 roky po uzavření této smlouvy
   - □ 5 let po uzavření této smlouvy
   - □ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: 10. 5. 2008

…….. ……

Nabyvatel Autor

ABSTRAKT

Tato diplomová práce se zabývá bezdrátovými počítačovými sítěmi, a to především z hlediska bezpečnosti. Shrnuje bezpečnostní zásady a standardy, používané v těchto sítích. Poukazuje na nedostatky starších mechanismů zabezpečení a popisuje modely založené na nových bezpečnostních standardech. Součástí práce je návrh metropolitní sítě a její následná realizace. Ve vybudované síti jsou implementovány vhodné metody zabezpečení, a to na základě získaných poznatků. Poslední část práce se zabývá tvorbou webových aplikací, vytvořených za pomoci programovacího jazyka PHP a databázového systému SQL.

KLÍČOVÁ SLOVA

wifi, bezdrátové sítě, zabezpečení, modely zabezpečení, 802.11, WEP, WPA, WPA2, návrh bezdrátové sítě, metropolitní síť, realizace bezdrátové sítě, webové aplikace, PHP, SQL, správa sítě

ABSTRACT

This diploma thesis deals with wireless computer networks in a point of view security. It contains security principles and standards used in these networks. It shows failings of old security methods in contrast of new standards. The result of the thesis is a design of the metropolitan network and its realization. In this network appropriate solutions of security are used. The last part of the thesis deals with a design of the web applications created in the PHP programming language and SQL database system.

KEYWORDS

wifi, wireless technology, security, 802.11, WEP, WPA, WPA2, design of the wireless network, realization of the metropolitan network, web applications, PHP, SQL

DANČUK M. *Nový model zabezpečení implementovaný v metropolitní síti*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2008. 68 s., Vedoucí diplomové práce doc. Ing. Vladislav Škorpil, CSc.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Nový model zabezpečení implementovaný v metropolitní síti“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne 10. 5. 2008 .....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce doc. Ing. Vladislavu Škorpilovi, CSc., za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.

V Brně dne 10. 5. 2008 ……..

(podpis autora)

OBSAH

SEZNAM POUŽITÝCH ZKRATEK

A

AP	Access Point - přístupový bod

B

BSS	Basic Service Set - síť stanic s přístupovým bodem

C

CCMP	Chaining Message Authentication Code Protocol - protokol dynamicky měnící klíče
CRC	Cyclic Redundancy Check - cyklický redundantní součet (kontrolní součet)

D

DHCP	Dynamic Host Configuration Protocol - protokol pro automatické přidělení IP adres
DS	Distribution System - distribuční systém

E

EAP	Extensible Authentication Protocol - rámec pro různé autentizační metody
ESS	Extended Service Set - síť stanic s distribučním systémem
ESSID	Extended Service Set ID - identifikátor rozšířené oblasti služeb

F

FTP	File Transfer Protocol - protokol pro přenos souborů mezi počítači

H

HTTP	Hypertext Transfer Protocol - protokol pro výměnu hypertextových dokumentů

I

IBSS	Independent Basic Service Set - síť nezávislých stanic
IP	Internet Protocol - protokol používaný pro přenos dat přes paketové sítě
IP adresa	jednoznačný identifikátor zařízení (počítače) v síti
IV	inicializační vektor

M

MAC	Medium Access Control - hardwarová adresa
NAT	Network address translation - překlad síťových adres

P

PSK	Pre Shared Key - před-sdílený klíč, nahrazuje autentizační server
POP3	Post Office Protocol version 3 - protokol pro stahování elektronické pošty
PoE	Power over ethernet – napájení po nevyužitých párech v UTP kabelu

Q

QoS	Quality of Servis – kvalita služeb

R

RC4	proudová šifra
RIP	Routing Information Protocol - směrovací protokol
RSN	Robust Security Network - bezpečnostní mechanismus 802.11i

S

SMTP	Simple Mail Transfer Protocol - protokol pro přenos elektronické pošty
SNMP	Simple Network Management Protocol – protokol pro správu sítě
SSID	Service Set ID - identifikátor bezdrátové sítě

T

TCP	Transmission Control Protocol - spojově orientovaný protokol pro přenos dat
TKIP	Temporal Key Integrity Protocol - protokol dynamicky měnící klíče

U

UDP	User Datagram Protocol – nespojový, nespolehlivý protokol pro přenos dat

V

VPN	Virtual Private Network – virtuální privátní síť

W

WEP	Wired Equivalent Privacy - šifrovací mechanismus bezdrátových sítí
WLAN	WirelessLAN - bezdrátová síť LAN
WPA	Wi-Fi Protected Access - šifrovací mechanismus bezdrátových sítí

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V současné době putuje obrovské množství informací, v elektronické podobě, z jednoho místa na druhé napříč celým světem, a to ve zlomcích sekund. Stále se vyvíjejí nové technologie za účelem zrychlení těchto přenosů a snazšího připojení účastníků do elektronické sítě. Jednou z takových technologií je i bezdrátové připojení podle standardu IEEE 802.11x, které zejména v posledních letech zaznamenává obrovský rozmach, kterému napomáhá stále se snižující cena zařízení a dostačující vlastnosti, které nám technologie poskytuje. Další velkou výhodou je možná mobilita stanic a možnost propojit místa, která jsou pro jiné druhy připojení těžko dostupná. Takto vzniká mnoho sítí, realizovaných nezkušenými uživateli, kde zaostává kvalita, a to především v oblasti bezpečnosti. Mnoho uživatelů si ani neuvědomuje rizika spojená s provozem takovýchto sítí. Nezabezpečují je vůbec nebo jen pomocí slabých, snadno prolomitelných mechanizmů. Vystavují se tak nebezpečí odposlechů a zneužití cenných dat ze strany útočníků. V úvodní, teoretické části této diplomové práce, budou popsány zabezpečovací mechanizmy, používající se v bezdrátových sítích. Bude poukázáno na jejich slabiny a možnosti jejich použití. Dále budou vytvořeny modely zabezpečené sítě a návrh topologie bezdrátové sítě pro konkrétní lokalitu. Podle tohoto návrhu bude síť realizována a budou do ní modely zabezpečení implementovány s cílem vybudovat bezpečnou a fungující síť. V další praktické části této práce se budu zabývat tvorbou webových aplikací. Tyto aplikace budou vytvářeny za využití programovacího jazyka PHP a databázových systému SQL. Cílem je vytvořit komplexní a hlavně bezpečný systém, který bude sloužit jak administrátorovi při správě a dohledu nad sítí, tak všem registrovaným uživatelům při získávání nejrůznějších informací.

1. Síťový model

V počítačových sítích se používají dva základní modely síťových vrstev. Novější, jednodušší, který se dnes nejvíce používá je model TCP/IP [1], [2]. Druhý je model ISO OSI, z kterého model TCP/IP vychází, který je mezinárodním standardem ISO.

1.1 TCP/IP

Tento model využívá čtyři vrstvy a to:

- Aplikační vrstva
- Transportní - TCP/UDP vrstva
- IP vrstva
- Linková vrstva

Přenos a zabezpečení dat v bezdrátových sítích se provádí na linkové vrstvě, a proto si ji v následujícím textu přiblížíme.

1.1.1 Aplikační vrstva

Na této vrstvě komunikují konkrétní aplikace s využitím aplikačních uživatelských protokolů jako jsou např. FTP, HTTP, POP3, SMTP, atd. a protokoly služební, které zajišťují provoz sítě, např. komunikace mezi směrovači protokolem RIP, správa sítě protokol SNMP.

1.1.2 Transportní vrstva

Tato vrstva se stará o doručení dat mezi jednotlivými aplikacemi a to za pomocí transportních protokolů, nejznámější jsou TCP (Transmission Control Protocol) a UDP (User Datagram Protocol). TCP protokol doručuje data aplikacím pomocí TCP segmentu a protokol UDP pomocí UDP datagramů. Pro určení cílové aplikace na dané IP adrese se používají tzv. porty, které ukožní výběr konkrétní aplikace pro doručení dat.

Protokol TCP nám zajišťuje spojovou spolehlivou službu, kde nám příjemce potvrzuje každý přijatý datový paket a v případě ztráty jsou data posílána znovu. Tímto máme zaručeno, že k cíli dorazí všechna data v pořádku. Proto tohoto protokolu využíváme pro aplikace, kde je pro nás důležitá správnost a kompletnost dat a nevadí nám časové zpoždění.

U protokolu UDP se žádné potvrzování neuskutečňuje. Zdroj pouze odešle data a už se o ně dále nestará. Případné potvrzování musí byt řešeno až na aplikační vrstvě. Tento protokol se využívá v aplikacích, kde potřebujeme data přenášet rychle a s minimálním zpožděním a nevadí nám malé ztráty v přenosu jako je například hlasová komunikace.

1.1.3 Síťová vrstva

Tato vrstva se stará o doručení dat na vzdálený počítač a přitom není závislá na použitém přenosovém médiu. Využívá se na ní protokolu IP (Internet Protokol), který přenáší data pomocí IP-datagramů, kde každý v hlavičce obsahuje adresu cílového počítače.

1.1.4 Linková vrstva

Tato vrstva má za úkol starat se o vysílaní a přijímání datových paketů. V modelu TCP/IP není tato vrstva blíže specifikována, protože závisí na použité technologii pro přenos. Například se používají linkové protokoly standardu 802.3 pro metalické sítě ethernet, 802.5 pro token-ring, 802.11 pro bezdrátové sítě.

2. Standardy bezdrátových sítí podle IEEE

2.1 IEEE 802

IEEE (Institute of Electrical and Electronics Engineers) se zaměřením na bezdrátové LAN zabývá od roku 1990. Jde o následující standardy [7]:

- **IEEE 802.11** - Bezdrátové lokální sítě WLAN (Wireless Local Area Network)
- **IEEE 802.15** - Bezdrátové osobní sítě WPAN (Wireless Personal Area Network)
- **IEEE 802.16** - Širokopásmový bezdrátový přístup WMAN(Wireless Metropolitan Area Network)

Dále si přiblížíme standard 802.11 WLAN, do kterého dnes zapadá široká škála doplňků, které si přiblížíme. Všechny využívají totožný protokol pro přístup k médiu tzv. MAC (Media Access Protocol), jednotlivé odlišnosti jsou na fyzické vrstvě. Pro přístup na médium je použita metoda CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). Stanici je umožněn přístup na médium pouze když je volné, z toho vyplívá, že stanice musí neustále naslouchat. Zařízení které vysílá do bezdrátové sítě nemá možnost detekovat kolize, proto se k jejich detekci využívá systému potvrzování. MAC protokol se tedy stará o samotný přenos dat a také obstarává procedury spojení stanic s přístupovým bodem.

2.2 IEEE 802.11

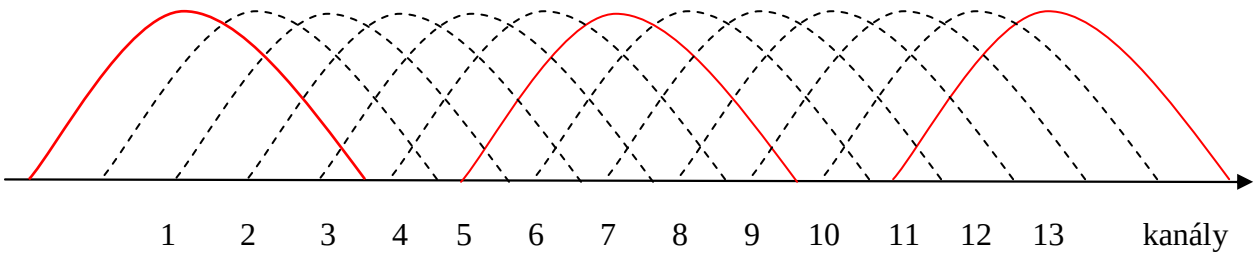
První bezdrátové lokální sítě vznikají od roku 1997 a jsou fyzicky založeny na [7], [8]:

- Přenos rádiových vln v kmitočtovém pásmu od 2,4 do 2,4835 GHz metodou s přeskakováním kmitočtů FHSS (Frequency Hopping Spread Spectrum). Metoda patentována v USA v roce 1940 a používá se dodnes. Pásmo je děleno na 79 kanálů s odstupem 1MHz. Vysílání probíhá na jednom kmitočtu v maximální době 400ms, následně dojde k přeskoku na jiný kmitočet a vysílá se dál. Typická doba setrvání na jednom kanále činí 20ms. Sekvence přeskoků vypadá jako náhodná, ale musí být dopředu známa jak vysílači tak přijímači. Přeskoky se v síti uskutečňují podle různých klíčů, aby se minimalizovala možnost současného vysílání na stejném kmitočtu několika stanic zároveň.

- Přenos rádiových vln v kmitočtovém pásmu 2,4 až 2,4835 GHz. Využívá se metoda DSSS (Direct Sequence Spread Spectrum) - přímo rozprostřené spektrum. Pásmo je rozdělené na 13 kanálů po 22 MHz, které se částečně překrývají (Obr. 1), pouze tři kanály se nepřekrývají vůbec (Evropa 1, 7, 13). Každý vysílaný symbol je kódován pseudonáhodným, binárním, 11bitovým řetězcem zvaný čipový kód, tím se 11x zvyšuje přenosová rychlost a zároveň i rozprostírá vysílaný výkon do 11x širšího pásma. V těchto sítích je podporována rychlost 1 Mbit/s pro zpětnou kompatibilitu, aby se i starší zařízení mohla připojit a pro případy provozu v zarušených prostředích.

- Metoda OFDM (ortogonální frekvenční multiplex) je rozšířením normy 802.11. Výhodou jsou vysoké rychlosti přenosu dat, které dosahují až 54 Mbit/s. Jsou využívány nepřekrývající se kanály o šířce 20 MHz. Jednotlivé kanály jsou rozděleny na 52 sub-kanálů o šířce 300 kHz. Bity se modulují a vysílají přes jednotlivé sub-kanály. Přenos tak probíhá paralelně na různých frekvencích. Na konci datového přenosu jsou všechny dílčí kanály složeny dohromady, tím ve výsledku docílíme velké propustnosti. Rozložení zátěže mezi jednotlivé sub-kanály je v ideálním případě rovnoměrné. V reálném provozu jsou některé sub-kanály zarušené, a proto se na nich posílají data s menší rychlostí a na nezarušených sub-kanálech rychlostí větší. Pro dosažení různých rychlostí se používají i různé modulace jako např. BPSK, QAM.

Pásmo 2,4 GHz ve kterém jsou tyto sítě provozovány není licencováno, a proto ho využívají i některá další zařízení jako jsou např. bezdrátové telefony, mikrovlnné trouby, bluetooth. Hlavně v městské zástavě jsou bezdrátové sítě velice rozšířeny a hraje zde velice důležitou úlohu vzájemné rušení.



Obr. 1 Překrývání kanálů.

2.2.1 IEEE 802.11a

Tato norma byla schválena roku 1999, ale přitom její vývoj začal dříve než na normě 802.11b. Důvodem delšího vývoje byl zejména složitější způsob přenosu na fyzické vrstvě, která pracuje v pásmu 5 GHz s teoretickou rychlostí až 54 Mb/s. Reálná přenosová rychlost se pohybuje kolem 33Mb/s. V této normě je poprvé v komunikaci kde se používá paketový přenos použit ortogonální multiplex s kmitočtovým dělením OFDM (Orthogonal Frequency-Division Multiplexing). Výhoda 802.11a oproti 802.11b je hlavně v použitém frekvenčním pásmu, které ještě není tak zarušeno jako pásmo 2,4 GHz a umožňuje použití více kanálů bez vzájemného překrývání, kdy máme k dispozici až 8 nepřekrývajících se kanálů. Použité rozdílné kmitočty znemožňují vzájemnou komunikaci těchto typů. Toto se řeší použitím hybridních zařízení, které zvládají komunikaci jak v pásmu 2,4 tak 5 GHz [7].

2.2.2 IEEE 802.11b

Tato norma přináší vetší přenosové rychlosti oproti normě 802.11 a poskytuje v pásmu 2,4 GHz rychlosti až 11 Mbit/s. Pro dosažení této přenosové rychlosti se využívá jiný způsob kódování, tzv. doplňkové kódové klíčování CCK (Complementary Code Keying) v rámci DSSS na fyzické vrstvě. Dále se v normě specifikuje dynamická změna přenosové rychlosti v závislosti na okolním rušení. V zarušeném prostředí je možnost automaticky snížit přenosovou rychlost a tím dosáhnou lepších přenosových vlastností. Naopak pokud rušení pomine, opět tuto rychlost zvýšit. Dostupné přenosové rychlosti jsou 11 Mbit/s; 5,5 Mbit/s; 2 Mbit/s; 1 Mbit/s. Maximální rychlost 11 Mbit/s je opět pouze teoretická, protože pro skutečná uživatelská data je k dispozici okolo 60% prostředků, kde zbylá procenta tvoří režie provozu.

2.2.3 IEEE 802.11g

Tato norma rozšiřuje schopnosti standardu 802.11b na přenosovou rychlost až 54 Mb/s. Umožňuje s ní komunikaci a je tedy zpětně kompatibilní. Fyzická vrstva je řešena stejně jako u normy 802.11a, tedy využívá technologie OFDM (Orthogonal Frequency-Division Multiplexing). Byla schválena v roce 2003. [8]

2.2.4 IEEE 802.11n

Tento standard má za úkol upravit fyzickou vrstvu a část linkové vrstvy MAC tak, aby byla schopna konkurovat metalický spojením ze stránky přenosové rychlosti. Cílem bylo dosáhnou reálných rychlostí přes 100 Mbit/s. Výsledná teoretická maximální rychlost může být až 540 Mbit/s. Tohoto výrazného navýšení se dosáhlo zejména použitím technologie MIMO (Multiple Input Multiple Output), kdy se využívá více vysílacích a přijímacích antén.

2.2.5 IEEE 802.11i

Rozšiřuje bezpečnost v MAC podvrstvě pro všechny fyzické vrstvy používané v sítích 802.11. Přechází na nový způsob šifrování AES (Advanced Encryption Standard) namísto standardu pro zabezpečení WEP (Wireless Encryption Privacy).

Standardů a doplňků normy IEEE 802.11 je velké množství a jejich popis by byl značně obsáhlý. Tato práce má za cíl zasáhnout zejména do oblasti bezpečnosti, proto ostatní standardy se stručným popisem uvádím v následující tab.1 jen pro doplnění [7], [11].

Doplněk	Rok schválení	Popis
802.11a	1999	Rychlost až 54 Mbit/s v pásmu 5 GHz
802.11b	1999	Rychlost až 11 Mbit/s v pásmu 2,4 GHz
802.11d	2001	Pro země, kde pásmo 2,4 GHz není přístupné
802.11c	2003	Mosty (Bridge) mezi přístupovými body
802.11f	2003	Spolupráce přístupových bodů od různých výrobců
802.11g	2003	Rychlost až 54 Mbit/s v pásmu 2,4 GHz
802.11h	2004	Dynamický výběr kanálu a regulace výkonu
802.11i	2004	Zabezpečovací a ověřovací mechanismy na MAC vrstvě

802.11j	2004	Využití pásma 4,9 a 5 GHz v Japonsku
802.11e	2005	Podpora pro QoS na MAC vrstvě
802.11k	2006	Měření rádiových prostředků
802.11m	2006	Revize standardů
802.11p	2008	Bezdrátový přístup pro mobilní zařízení
802.11r	2008	Rychlý roaming pro aplikace v reálném čase
802.11u	2008	Spolupráce s externími sítěmi
802.11v	2008	Vzdálený management koncových zařízení
802.11s	2008	Multi-hopping
802.11w	2008	Podpora integrity, autenticity, utajení a ochrany dat
802.11y	2008	3650-3700 MHz pro USA
802.11t	2009	Měření a testování WLAN zařízení
802.11n	2009	Vysoká datová propustnost až 540 Mb/s

Tab. 1 Přehled doplňků standardu IEEE 802.11.
(řazeno podle roku schválení)

Standard	**Rok vydání**	**Pásmo [GHz]**	**Max. rychlost [Mbit/s]**	**Fyzická vrstva**
IEEE 802.11	1997	2,4	2	FHSS
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM
IEEE 802.11n	2007	2,4; 5	až 540	MIMO

Tab. 2 Přehled standardů IEEE 802.11.
(řazeno podle roku schválení)

3. Mechanismy zabezpečení podle IEEE

Hlavní problém při návrhu zabezpečení bezdrátových sítí je, že nemají žádné pevné hranice, odkud by se na ně dalo připojit. Aby se případný útočník mohl připojit do metalické sítě, musí se fyzicky připojit např. na switch, hub. Toto u bezdrátové sítě neplatí, protože se muže připojit, nebo odposlouchávat kdokoliv, kdo je v dosahu šířeného signálu. Proto je velice důležité odlišit oprávněné uživatele od ostatních. Z naznačeného principu vyplývá, že

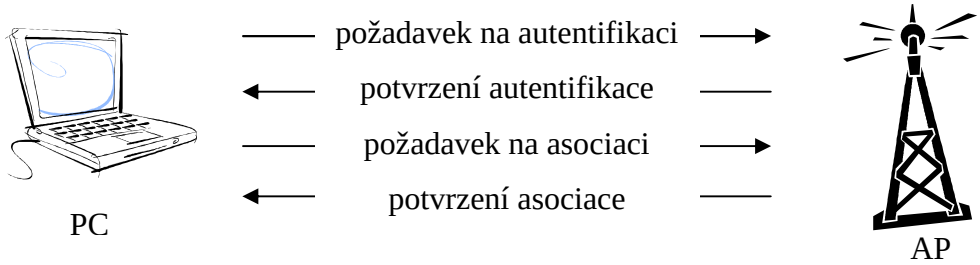
musíme zajistit, aby neoprávnění uživatelé nemohli do sítě přistoupit a ani nebyli schopni přenášená data odposlechnout nebo modifikovat.

4. Připojení klienta do bezdrátové sítě

Pro přístup stanice do sítě se využívají dvě metody. Metoda otevřeného systému (Open-System) a metoda sdíleného klíče (Shared Key). U obou metod stanice nejdříve pošle dotaz na broadcast adresu, zda se v okolí vyskytuje nějaký přístupový bod (Probe Request). Broadcast adresa má v části adresy příjemce samé 1, hexadecimálně vyjádřeno FF:FF:FF:FF:FF:FF. V případě prohledávání okolí na existující přístupové body, stanice opakuje toto vysílání na všech kanálech. Pokud takový bod je v dosahu tak na tento dotaz odpoví (Probe Response). Podle SSID (Service Set ID) přístupový bod pozná, zda je paket určen pro něj a ostatní přístupové body na tomtéž kanále požadavek ignorují [7], [8].

4.1 Otevřený systém (Open-System)

Tato metoda není autentifikací. Stanice při připojovaní není ověřována. Využívá se pro připojení každé stanice, která o připojení požádá. Připojení stanice k přístupovému bodu probíhá v následujících částech (viz. Obr. 2), [4], [13].



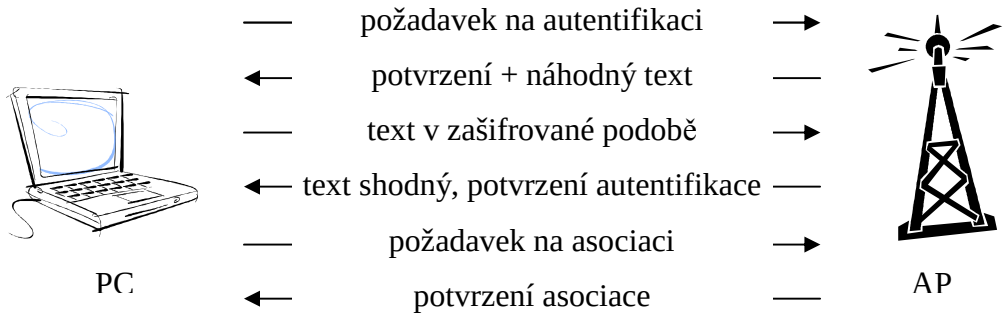
Obr. 2 Připojování stanice pomocí otevřeného systému.

Když přístupový bod potvrdí autentifikaci tak má stanice právo na připojení. Požadavkem na asociaci stanice předává informace o svém nastavení. Po provedení těchto kroků je stanice připojena do sítě a může komunikovat.

4.2 Mechanismus sdíleného klíče

Tato metoda neumožňuje připojení jakékoli stanice do sítě která zná SSID, ale navíc ještě vyžaduje znalost sdíleného klíče. Toto ověření probíhá tak, že přístupový bod vygeneruje náhodný text a zašle ho stanici, která žádá o připojení. Stanice tento text zašifruje

pomocí svého klíče a odešle zašifrovaný text zpátky přístupovému bodu. Ten text zašifruje svým klíčem a pokud se shodují, je autentifikace potvrzena. K šifrování se používá šifra RC4. Slabé místo této metody je posílání náhodného textu v nezašifrované a poté v zašifrované podobě. Průběh komunikace klienta s AP ukazuje Obr. 3, [4], [13].



Obr. 3 Průběh připojování stanice pomocí metody sdíleného klíče.

5. Základní bezpečnostní prvky

Tyto metody představují elementární možnosti zabezpečení bezdrátové sítě. V dnešní době jsou považovány za nedostatečné a doplňují se robustnějším zabezpečením podle nových bezpečnostních standardů. Přesto je dobré i tyto metody zabezpečení implementovat v bezdrátové síti v kombinaci s modernějšími metodami a tím dosáhnou co nejsilnějšího zabezpečení [10], [12].

5.1 SSID

Je to identifikátor bezdrátové sítě, nastavuje se na každém přístupovém bodu AP (Access Point), představuje nejnižší stupeň zabezpečení pro komunikaci v bezdrátových sítích. Informaci o SSID může přístupový bod pravidelně vysílat nebo muže být toto vysíláni vypnuto čímž se stane pro klienty neznalé tohoto identifikátoru AP neviditelné. SSID může být na stanici nastaveno manuálně nebo se klient se na něj sám dotáže. Toho může provést i případný útočník, a proto skrytí SSID je pouze základní ochranou, která odradí jen neznalé útočníky. SSID je v otevřené podobě posíláno v mnoha dalších paketech. Nutnost jeho znalosti je důležitá snaze asociovat se s přístupovým bodem. Každý oprávněný klient vysílá SSID v nešifrované podobě pokaždé, když se snaží připojit do sítě. Spousta softwaru tohoto dokáže využít a je jen otázkou času, kdy útočník dokáže skryté SSID za pomocí patřičného programu získat.

5.1.1 De-asociace uživatele

Případný útočník ani nemusí čekat až se oprávněný klient bude znovu připojovat. Nejjednodušší cestou, jak zjistit SSDI skryté sítě, je vynucené odpojení oprávněného uživatele, který je takto donucen odeslat žádost o re-asociaci a útočník lehce odposlechne skryté SSID. Toto je možné díky tomu, že řídící pakety nejsou autentifikovány. Když uživateli zašleme paket, který vypadá jakoby přišel od přístupového bodu, uživatel nemá možnost odlišit ho od pravého paketu a stanici odpojí od přístupového bodu.

De-asociace uživatele je efektivní bez ohledu na to, jaký typ šifrování byl použit. Ani standard WPA2 tomuto nezabrání, protože řídící pakety stále zůstávají nešifrovány a neautentifikovány.

5.2 Filtrace hardwarových adres

Hardwarová adresa MAC (Medium Access Control), jako jednoznačný identifikátor síťové karty, nám může sloužit k identifikaci jednotlivých uživatelů a tím pádem k omezení stanic, které se mohou přihlásit na daný přístupový bod. Přístup bude umožněn jen zařízením, které mají uvedený záznam o své MAC adrese v seznamu povolených adres na straně přístupového bodu. Toto je nevýhodné pří větším množství přístupových bodů, u rychle se měnící nebo rostoucí sítě, a to zejména z důvodu složitější administrace seznamů povolených adres. Avšak ochrana filtrováním MAC adres je spolehlivá jen do jisté míry, protože podvržení MAC adresy není pro zkušenějšího uživatele příliš náročné. Proto se využívá jako doplňková ochrana, jako další překážka pro případné útočníky [4].

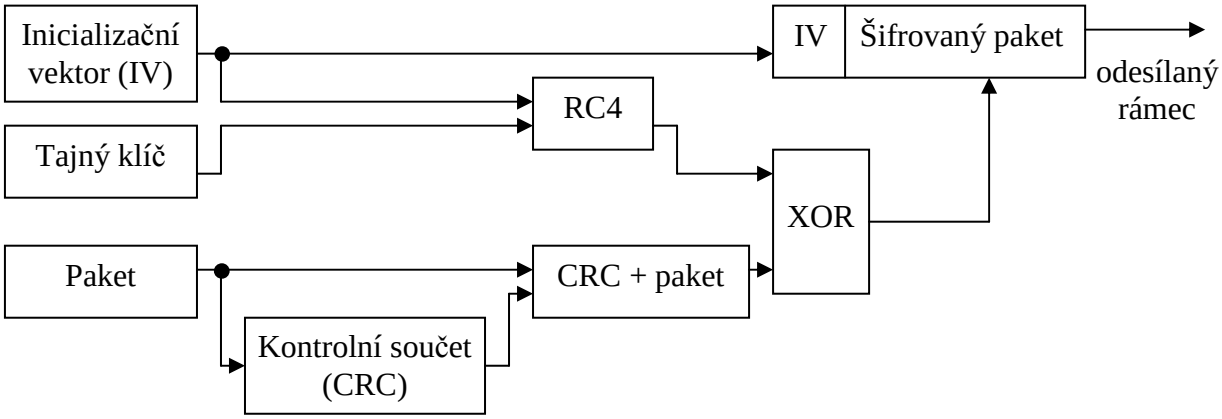
5.3 WEP

Protokol WEP (Wired Equivalent Privacy) [4], [5], [7] byl navržen za účelem ochrany přenášených dat, protože v případě bezdrátové komunikace distribuovaná data nedorazí pouze k určené stanici jako na metalickém vedení, ale může je odposlechnout i neoprávněná stanice. Byl nasazen pro své vlastnosti, kterými jsou odolnost proti útoku hrubou silou, samosynchronizace (není náchylný na ztráty paketů), snadná implementovatelnost a jeho použití je volitelné. Protože je implicitně na přístupových bodech vypnut, stále mnoho sítí ani toto základní zabezpečení nepoužívá, takže nejsou proti případným útočníkům prakticky nijak chráněny.

WEP je symetrický šifrovací mechanismus, kdy se pro šifrování a dešifrování používá stejný algoritmus i statický klíč. Nejčastěji používá 64 nebo 128 bitový klíč. V této délce je již

obsažen 24 bitový inicializační vektor IV. Klíč o délce 40 bitů byl již v době návrhu naprosto nedostačující. Šifrování přenášených dat se provádí klíčem, který je složen z uživatelského klíče a dynamicky se měnícího vektoru IV (Initialization Vector). Inicializační vektory jsou voleny pseudonáhodně ze všech variant, kterých je 224. Výsledná šifra je jedinečná pro každý jednotlivý paket. K samotnému šifrování se používá proudová šifra RC4. Autentizace ve WEP pracuje pouze jednostranně, nikoli vzájemně. V závislosti na výrobci může nabízet i silnější zabezpečení ve formě klíče o délce 192 nebo 256 bitů.

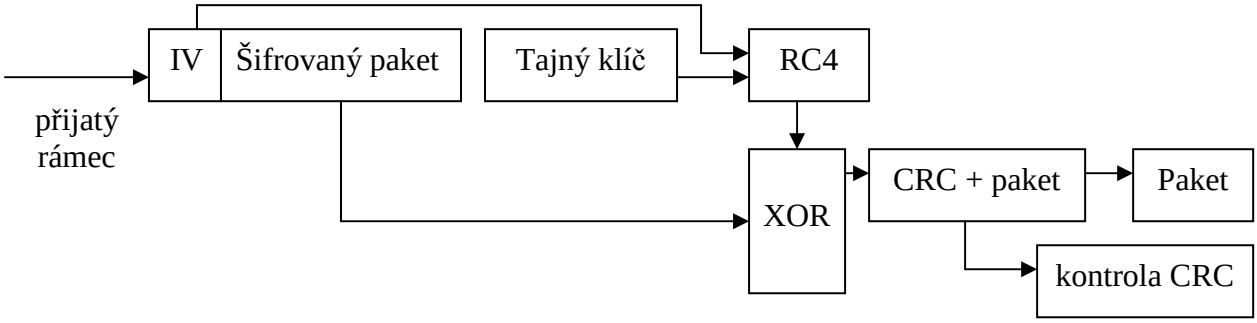
Bezpečnost takto zabezpečené sítě je možné narušit na základě odposlechu přenášených paketů a za použití veřejně dostupného softwaru (např. AirSnort, WEPcrack). Z tohoto důvodu je třeba použít doplňkové metody zabezpečení.



Obr. 4 Šifrování paketu mechanismem WEP.

Postup šifrování paketu (Obr. 4):

- Přenášený paket je doplněn kontrolním součtem CRC (Cyclic Redundancy Check) o délce 32 bitů. CRC se používá pro zjištění chyb vzniklých při přenosu.
- Náhodný inicializační vektor IV spolu se zadaným pevným klíčem tvoří šifrovací klíč pro daný paket.
- Použitím algoritmu RC4 na aktuální klíč vzniká heslo.
- Paket spolu s CRC je operací exklusive-or přičten k heslu, tím získáme šifrovaný blok.
- Před šifrovaný blok je přidán inicializační vektor.
- Následuje předání takto vytvořeného rámce na přenosové médium.



Obr. 5 Dešifrování paketu mechanismem WEP.

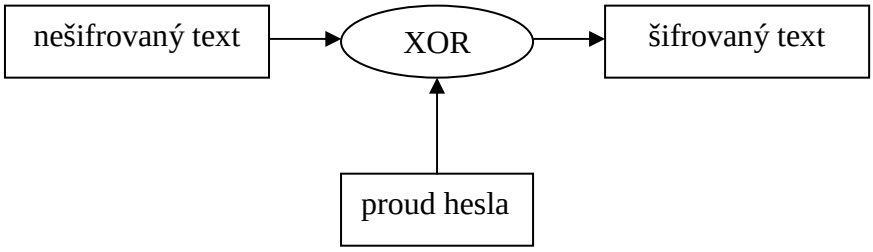
Postup dešifrování paketu (Obr. 5):

- Příjemce za pomocí zaslaného inicializačního vektoru a pevného klíče generuje aktuální šifrovací klíč.
- Na šifrovací klíč je použit algoritmus RC4 a tím získáme heslo. Přičtením hesla pomocí operace exklusive-or k šifrovanému paketu získáme nešifrovaný paket a příslušné CRC.
- Proběhne ověření CRC jeho opětovným vypočtením a srovnáním se zaslaným CRC. V případě, že je CRC v pořádku, je paket předán vyšší vrstvě modelu OSI. V opačném případě je paket zahozen.

5.3.1 Šifra RC4

Jedná se o symetrickou šifru, která je dílem firmy RSA Data Security, Inc [16]. Její algoritmus nebyl oficiálně publikován, ale v roce 1994 byl algoritmus šifry RC4 získán zpětným inženýrstvím a zveřejněn na internetu.

Šifra RC4 je šifrou proudovou, tzn. že data se šifrují po jednotlivých bajtech a nikoli v blocích. Vstupem šifry je klíč volitelné délky s teoretickým omezením na 256 bajtů. Když je klíč kratší než 256 bajtů je zopakován, aby naplnil délku 256 bajtů, jenž inicializuje konečný automat, který generuje jednotlivé bajty hesla. Mezi jednotlivé bajty hesla a bajty nezašifrovaného textu se aplikuje funkce XOR (Obr. 6). Při dešifrování se použije funkce XOR na bajty hesla a bajty zašifrovaného textu.



Obr. 6 Princip šifry RC4.

5.3.2 Slabiny šifrovacího protokolu WEP

Největší slabinou protokolu WEP je klíčové hospodářství. Sdílená pevná část klíče je trvale zadána do zařízení sítě a prakticky není vůbec měněna. Stejná situace je i při variantách klíčů s větší délkou. Proměnou hodnotou u paketů je pouze inicializační vektor s konstantní délkou 24 bitů. Existuje tedy pouze 2^{24} možných heslových posloupností. Snadným zachytáváním paketů může útočník vytvořit databázi paketů tříděných podle inicializačních vektorů. Inicializační vektory se při velkém objemu dat začnou opakovat. Výsledkem analýzy síťového provozu je databáze všech inicializačních vektorů a jim přiřazených heslech. Připomeňme, že inicializační vektor je přenášen v každém kryptogramu nešifrován a že heslo je získáno aplikací algoritmu RC4 na kombinaci tohoto inicializačního vektoru a neměnného klíče.

6. Vývoj bezpečnostních standardů

Standard	Rok vydání	Přínos	Popis
IEEE 802.11	1999	WEP	minimální autentizace, slabé utajení dat
IEEE 802.1x	2001	IEEE 802.1x	autentizace a správa klíčů podle 802.1x, WEP pro přenášená data
IEEE 802.1x + TKIP	2002	WPA	autentizace a správa klíčů podle 802.1x, TKIP pro přenášená data
IEEE 802.11i	2004	WPA2	autentizace a správa klíčů podle 802.1x, AES-CCMP pro přenášená data

Tab. 3 Vývoj podpory bezpečnosti.

7. Pokročilejší metody zabezpečení

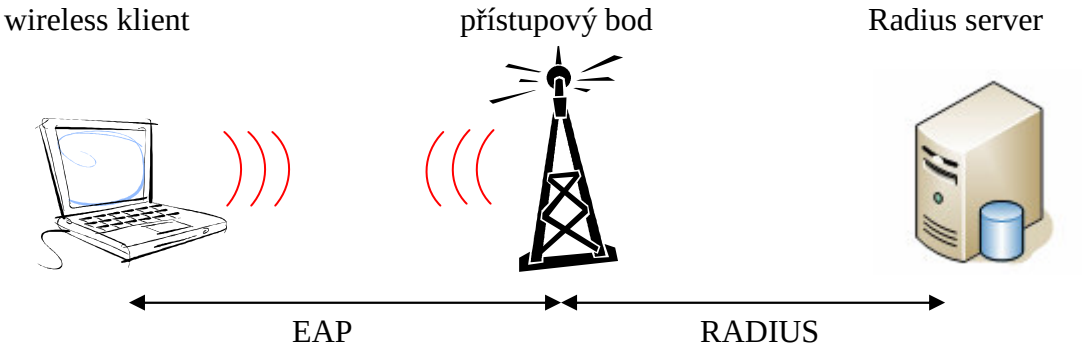
V předchozí kapitole jsme si ukázali základní bezpečnostní mechanismy zabezpečení bezdrátové sítě. Tyto metody nám v dnešní době poskytují nedostatečné zabezpečení, a proto se vyvíjejí stále nové metody a schvalují standardy, které nám umožní WLAN zabezpečit mnohem robustněji. Proto si dále ukážeme nové bezpečnostní standardy a mechanismy, které nám přináší zvýšení bezpečnosti na akceptovatelnou úroveň.

7.1 IEEE 802.11x

Jedná se o obecný bezpečnostní standard pro všechny typy sítí. Obsahuje např.: autentizaci uživatelů, integritu zpráv, distribuci klíčů. Pro bezdrátové sítě je ověřování realizováno u přístupového bodu na úrovni portů. Uživatelům bez patřičného oprávnění není umožněn přístup do sítě. Standard využívá protokolu EAP (Extensible Authentication Protocol). Na základě výzvy klienta provede přístupový bod jeho ověření za pomoci seznamu nebo autentizačního serveru např.: Kerberos, RADIUS. Přístup do sítě má tedy pouze autentizovaný uživatel [10], [12].

Obecný postup autentizace podle 802.1x:

- Klientovi, na základě detekce jeho přítomnosti, odešle přístupový bod zprávu EAP REQUESTID.
- Klient odpoví zprávou EAP RESPONSE-ID, která obsahuje jeho identifikační údaje. Přístupový bod zapouzdří zprávu EAP RESPONSE-ID do paketu RADIUS ACCESS_REQUEST a vyšle ji serveru RADIUS.
- Server RADIUS odpoví zprávou RADIUS ACCESS_ACCEPT/DENY, která buď povolí nebo zakáže přístupu pro daného klienta do sítě. Zpráva obsahuje informaci EAP SUCCESS/FAILURE, kterou přístupový bod přepošle klientovi.
- V případě zprávy EAP SUCCESS je port, přes který autentizační komunikace probíhala, otevřen pro přístup do sítě pro daného uživatele, který je na základě úspěšného výše popsaného procesu, považován za autentizovaného.



Obr. 7 Postup autentizace podle 802.1x.

U tohoto standardu se využívají k šifrování dat pro každou připojenou a autentizovanou stanici dynamické klíče, které jsou známy pouze dané stanici. Mají časově omezenou životnost a využívají se k šifrování dat na daném portu, dokud se stanice neodhlásí nebo neodpojí. Právě toto dynamické měnění klíčů značně ztěžuje případným útočníkům narušit bezpečnost oprávněných uživatelů a celé sítě. Ovšem už se prokázalo, že ani 802.1x není dostatečně odolný vůči některým způsobům útoku (man-in-the-middle).

7.2 WPA

WPA (Wi-Fi Protected Access) [6] je bezpečnostní mechanismus schválený v roce 2002. Jedná se o vylepšení stávajícího nedostatečného zabezpečení mechanismem WEP. Stejně jako WEP používá šifrovací algoritmus RC4, ale s 128 bitovým klíčem a 48 bitovým inicializačním vektorem (IV). Zásadní přínos v zabezpečení spočívá v dynamicky měnícím se klíči pro šifrování dat TKIP (Temporal Key Integrity Protocol). TKIP pracuje s automatickým klíčovým mechanismem, jenž mění dočasný klíč každých 10 000 paketů. Také je vylepšena kontrola integrity (správnosti) dat, a to použitím metody MIC (Message-Integrity Check), která nám nabízí podstatně lepší zabezpečení integrity zpráv než dosud užívaný kontrolní součet CRC.

WPA umožňuje několik možností, jak síť zabezpečit. Pro podnikové řešení a rozsáhlé sítě se využívá autentizační server např. RADIUS, který zasílá každému uživateli jiný klíč. Pro menší podnikové sítě se využívá autentizace pomocí PSK (Pre-Shared Key), kdy každý uživatel má stejný přístupový klíč. Zvětšení velikosti klíče a inicializačního vektoru IV, snížení počtu paketů s opakujícími se klíči a ověřování integrity zpráv, dělá zabezpečení WPA mnohem hůře prolomitelné.

7.3 WPA2 - IEEE 802.11i

Standard IEEE 802.11i, veřejnosti známý jako WPA2 [6], je dodatkem IEEE 802.11. Byl schválen 24. června 2004 a jedná se o komplexní řešení zabezpečení v bezdrátových sítích. Autentizace je řešena pomocí standardu 802.1x. Velký přínos WAP2 je v použití protokolu CCMP (Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol) se silným blokovým šifrováním AES (Advanced Encryption Standard), WEP a WPA používají proudovou šifru RC4. CCMP se přidal k protokolu TKIP (Temporal Key Integrity Protocol), který dynamicky mění klíče pro šifrování dat a může pracovat s minimálními požadavky na softwarový upgrade na stávajících zařízeních s hardwarem pro WEP.

Velikost šifrovacího klíče AES, který se využívá k vlastnímu šifrování, může být 128,192 nebo 256 bitů. Čím delší klíč zvolíme, tím docílíme větší bezpečnosti, ale zároveň potřebuje vyšší výpočetní výkon. Dříve stačilo útočníkovi odposlechnout dostatečný počet paketů a ty použít k výpočtu klíče WEP, kdy jedinou obranou bylo manuálně klíče měnit, což bylo značně administrativně náročné, zejména v rozsáhlých sítích. Se standardem 802.11i se mění šifrovací klíče automaticky a poskytuje nám tam větší bezpečnost a komfort administrace.

7.3.1 Slabiny WPA/WPA2

I tyto protokoly obsahují několik slabých míst, která však při správném používání nejsou příliš nebezpečná [6].

Při nejjednodušším způsobu používání jsou velmi zranitelné. Pokud je používán systém sdílených klíčů PSK namísto autentizace 802.1x a je použito krátké, slovníkové heslo, je takto zabezpečená sít náchylná na útoky tzv. off-line slovníkový útok, kdy se útočník zmocní několika paketů, v době navazování spojení oprávněné stanice a následně z nich rozluští používaný klíč.

Naštěstí tento typ útoku je zapříčiněn lidmi, kteří volí špatná hesla. Zkušený administrátor použije dlouhé a silné heslo, které útočník není v dnešní době v rozumné časovém horizontu schopen odhalit.

Dalším slabým místem WPA2 je útok typu DoS (Denial of Service - odepření služby), kde je cílem útoku znemožnění připojení oprávněné stanice k přístupovému bodu. Protože při čtyřcestné úvodní komunikaci (4-Way Handshake) není první zpráva autentizována, klient musí uchovávat každou první zprávu, dokud neobdrží zprávu třetí, která je již podepsaná.

Díky tomu hrozí stanici vyčerpání dostupné paměti a znemožnění připojení oprávněných klientů. Tento typ útoku je proveditelný pouze v případě, že na stanici jsou povoleny souběžné relace.

8. Linux vs. Windows

Většina volně dostupných nástrojů, které slouží k manipulaci s bezdrátovými sítěmi, je psána pro systémy Linux. Například program „Kismet“ slouží pro vyhledání okolních sítí vhodných k odposlechu, „Airodump“ pro zachytávání šifrovaných paketů na daném kanále bez nutnosti znalosti klíče a „Wepcrack“ pro prolomení šifry při dostatečném množství zachycených paketů. Pak už vám postačí jen notebook s bezdrátovou wifi kartou, nainstalovaný operační systém Linux a balíček programů „aircrack“ a můžete se pokusit o neoprávněné připojení do bezdrátových sítí ve vašem okolí.

Na platformě Windows neexistují žádné všeobecně použitelné nástroje, a to zejména proto, že nejsou napsány ovladače pro bezdrátové síťové karty, které by umožňovali pasivní odposlech paketů. Jednoduší je používat linuxové nástroje.

8.1 SSID

Pro de-asociaci uživatele existuje několik volně dostupných nástrojů, které jsou napsány pro operační systém Linux. Nejoblíbenější je program „aireplay“, který je součástí balíčku aircrack.

8.2 MAC

Podvržení fyzické adresy síťové karty je snadné v obou operačních systémech. V linuxu je to otázka pár řádků zapsaných do terminálu a na platformě Windows jde o pár kliknutí nebo úpravu záznamu v registrech systému.

8.3 WEP

Pro zjištění šifrovacího klíče z odchycených paketů se nejčastěji používá nástroj „WEP-crack“, který je také součástí balíčku „aircrack“. Tento program nám umožňuje paralelní výpočet WEP klíče a tím nám jeho zjištění značně urychlí. Pro Microsoft Windows se mi nepodařilo nalézt žádný podobný nástroj.

9. Topologie bezdrátové sítě

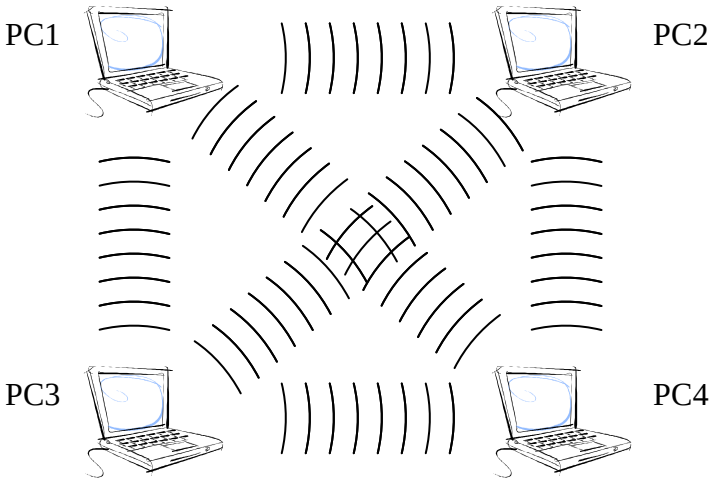
Při propojování počítačů pomocí sítě Wi-Fi je možné použití dvou topologií, Ad-Hoc a infrastrukturní [3]. Rozdíl mezi nimi je ve způsobu, jakými cestami mezi sebou počítače komunikují. Třetí možností je spojit několik infrastrukturních topologií a umožnit uživateli mezi nimi volně přecházet bez ztráty konektivity (tzv. roaming).

Možné topologie:

- IBSS (Independent Basic Service Set) nebo také síť stanic (tzv. ad-hoc) - Stanice komunikují jen navzájem mezi sebou.
- BSS (Basic Service Set) nebo také síť stanic s přístupovým bodem (AP) - Stanice v dosahu AP mají přístup ke službám.
- ESS (Extended Service Set) nebo také síť stanic s distribučním systémem (DS) - Stanice v dosahu DS mají přístup ke službám. Stanice nejsou omezeny pokrytím jediného AP a mohou využívat všechny AP daného DS.

9.1 Topologie Ad-Hoc

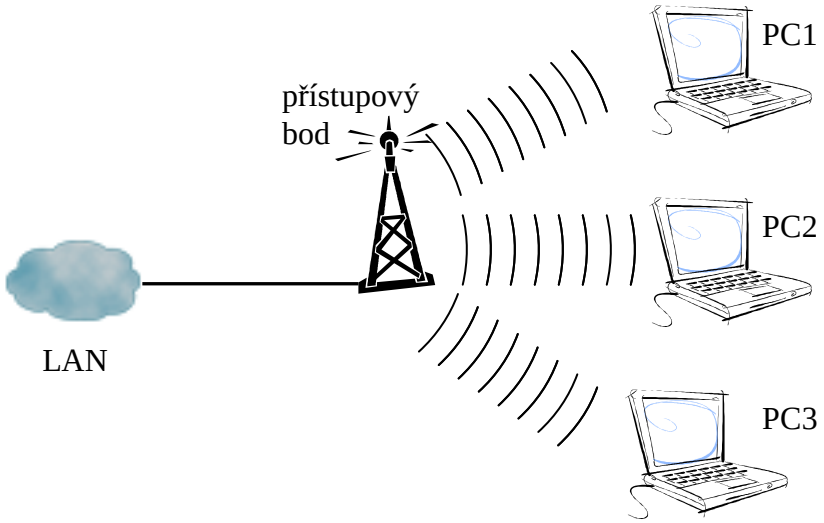
Nazývá se rovněž IBSS (nezávislý základní soubor služeb). Při tomto propojení komunikují jednotlivé stanice mezi sebou bez použití přístupového bodu. K propojení stačí minimálně dvě nebo více stanic s bezdrátovými kartami. Není použit žádný centrální prvek a síť může být považována za robustnější. Tento způsob lze uplatnit pouze při komunikaci na malou vzdálenost, protože každá stanice musí být v dosahu ostatních stanic. Používá se hlavně jako jednoduché propojení dvou stanic.



Obr. 8 Topologie IBSS (Ad-Hoc).

9.2 Infrastrukturní topologie

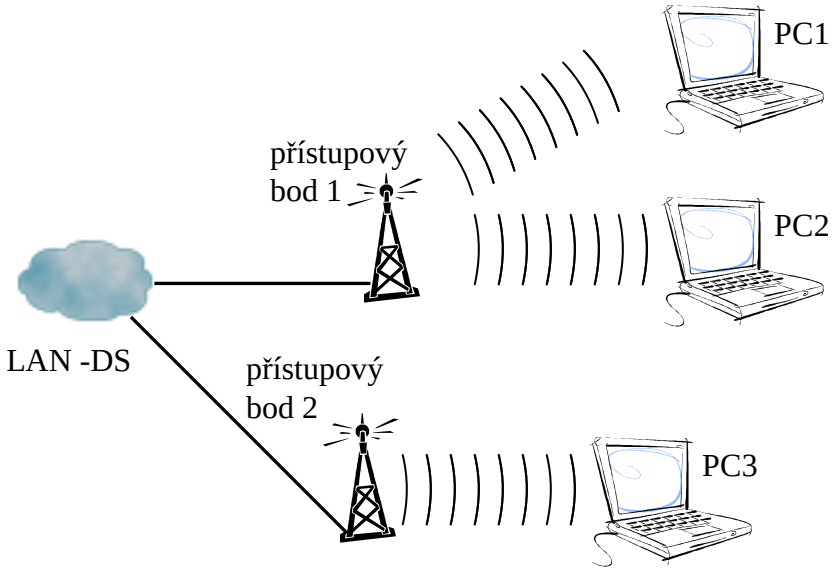
Jde o základní soubor služeb (BSS). Při použití této topologie je pro spojení jednotlivých stanic využit přístupový bod (AP) jako centrální prvek. Komunikace mezi stanicemi probíhá právě přes tento bod. Takto můžeme vybudovat značně rozsáhlé sítě. Postačí, aby každá stanice byla v dosahu přístupového bodu a pak nemusí být už v dosahu jednotlivé stanice mezi sebou. Díky tomu můžeme použít směrové antény s větším ziskem a překlenout tak větší vzdálenosti. Tato topologie se používá v naprosté většině budovaných bezdrátových sítí.



Obr. 9 Topologie BSS.

9.3 Překrývající se soubor služeb

ESS (Extended Service Set) - překrývající se soubor služeb. Rozšířený soubor služeb se skládá z několika sítí typu BSS, které jsou spojeny dohromady, aby umožňovaly mezi sebou přecházet (tzv. roaming). Zařízení, která mají přístup k ESS, mohou zůstat připojena k síti, pokud zůstávají v dosahu alespoň jednoho z přístupových bodů ESS.



Obr. 10 Topologie ESS.

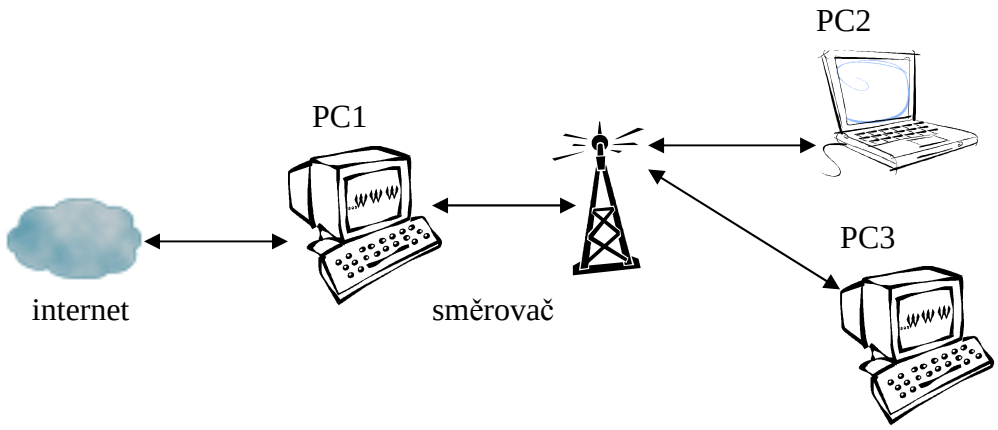
10. Návrh modelů zabezpečení sítě

Následující příklady jsou návrhem bezdrátových sítí a jejich zabezpečení v různých prostředích, s různými nároky na bezpečnost. Zabezpečení je realizováno za pomocí protokolu WPA2. Protokol WEP, jak je popsáno výše, obsahuje spoustu nedostatků a je nevhodný pro zabezpečení bezdrátové sítě, kde vyžadujeme vysokou úroveň bezpečnosti. Pouze v případě použití starších zařízení, které neumožňují jiné šifrování, má jeho použití smysl.

10.1 Domácnosti a méně rozsáhlé sítě

V domácnosti bývá většinou jeden počítač připojen k internetu a sdílí toto připojení dalším stanicím, které jsou k němu připojeny. Plní tak roli směrovače (Obr. 11). Jako přístupový bod může být použit samostatný přístupový bod, který je připojený pomocí ethernetového kabelu k počítači, ale toto řešení je dražší. Levnějším řešením je vybavit počítač, který je připojen k internetu, bezdrátovou síťovou kartou a pomocí vhodných ovladačů vytvořit přístupový bod a směrovač v jednom. Toto řešení má výhodu ve využití stávajícího počítače a není tak nutné kupovat samostatné AP (přístupový bod). Pro variantu počítače, doplněného bezdrátovou síťovou kartou, se více hodí operační systém Linux a bezdrátové karty Z-Com s ovladači HostAP. Ty nám umožní z karty, sloužící pro připojení

klientů, vytvořit přístupový bod, na který se klienti budou moci připojovat. Karta i ovladače podporují zabezpečení protokolem WPA2, který nám poskytne obranu proti útočníkům na vysoké úrovni.



Obr. 11 Modelová topologie domácí sítě.

Pro tento model je vhodné použít protokol WPA2 s ověřováním stanic pomocí předsdíleného klíče (PSK), který je nastaven na všech stanicích i přístupovém bodu. Pro domácnosti a méně rozsáhlé sítě, kde množství počítačů není příliš velké, je toto ověřování dostačující. Zřizování RADIUS serveru pro jejich ověřování je zbytečné. Důležité je, aby bylo zvoleno dostatečně dlouhé a silné heslo a tím si zajistíme odolnost proti jeho odhalení. Nastavení PSK klíče je srovnatelně jednoduché s nastavením WEP klíče a závisí na použitém přístupovém bodu.

Problém nastane, pokud máme stanici, která podporuje pouze šifrování protokolem WEP. Tato stanice nebude schopna komunikovat s přístupovým bodem nebo s ostatními stanicemi. S tímto problémem se můžeme setkat například u starších notebooků a bezdrátových síťových karet. Dnes už snad všechny prodávané prvky podporují tyto nové bezpečnostní standardy. V případě, že takové zařízení již máme, je nejvhodnějším řešením zakoupení novějšího vybavení, podporujícího WPA2. Další možností je použití méně bezpečného šifrování WEP. Pokud se rozhodnete pro použití mechanismu WEP, je vhodné dodržovat několik zásad, které zvyšují bezpečnost komunikace, a to:

- použití nejsilnějšího možného WEP klíče (typicky 128 bitů)
- pravidelná změna WEP klíče
- statické přidělení IP adres
- omezení přístupu pomocí tabulky MAC adres
- omezení fyzického přístupu k přístupovému bodu

- pravidelná kontrola záznamů přístupového bodu
- nastavení výkonu na nejnižší použitelnou hranici

Nastavením nejdelšího možného klíče se prodlouží čas nutný pro zachycení potřebného množství paketů na dobu, která může případného narušitele odradit. Pravidelná změna klíče je závislá na délce použitého klíče, a to tak, že čím delší klíč použijeme, tím může zůstat déle nezměněn a naopak. Častější změna klíče nám zaručí nízkou pravděpodobnost nalezení právě používaného klíče. Toto řešení je však administrátorsky značně nepohodlné a málo kdo toto pravidlo bude dodržovat.

Při používání pevných IP adres bude pro případného útočníka obtížnější připojit se do sítě, protože bude muset počkat, až bude některá volná. Současné připojení dvou stanic se stejnými IP adresami, může při sledování provozu na síti, vést k rychlému odhalení pokusu o neoprávněné připojení.

Omezením přístupu, pomocí tabulky povolených MAC adres, musí narušitel také vyčkat, až nebude uživatel s povolenou MAC adresou připojen. Současné připojení dvou stanic se stejnou MAC adresou je možné, ale snadno odhalitelné.

Omezením fyzického přístupu k přístupovému bodu zabráníme hardwarovému resetu tohoto zařízení, při kterém dojde k obnovení továrního nastavení a útočník tak získá přístup ke konfiguraci.

Pravidelnou kontrolou záznamů o provozu přístupového bodu lze zjistit, zda například nedošlo k připojování stanic, které v danou dobu byly vypnuté a na tuto situaci reagovat okamžitou změnou WEP klíče.

Omezením vysílacího výkonu na nejnižší možnou úroveň značně snížíme vzdálenost, na kterou je možné přenášená data zachytávat.

10.1.1 VPN

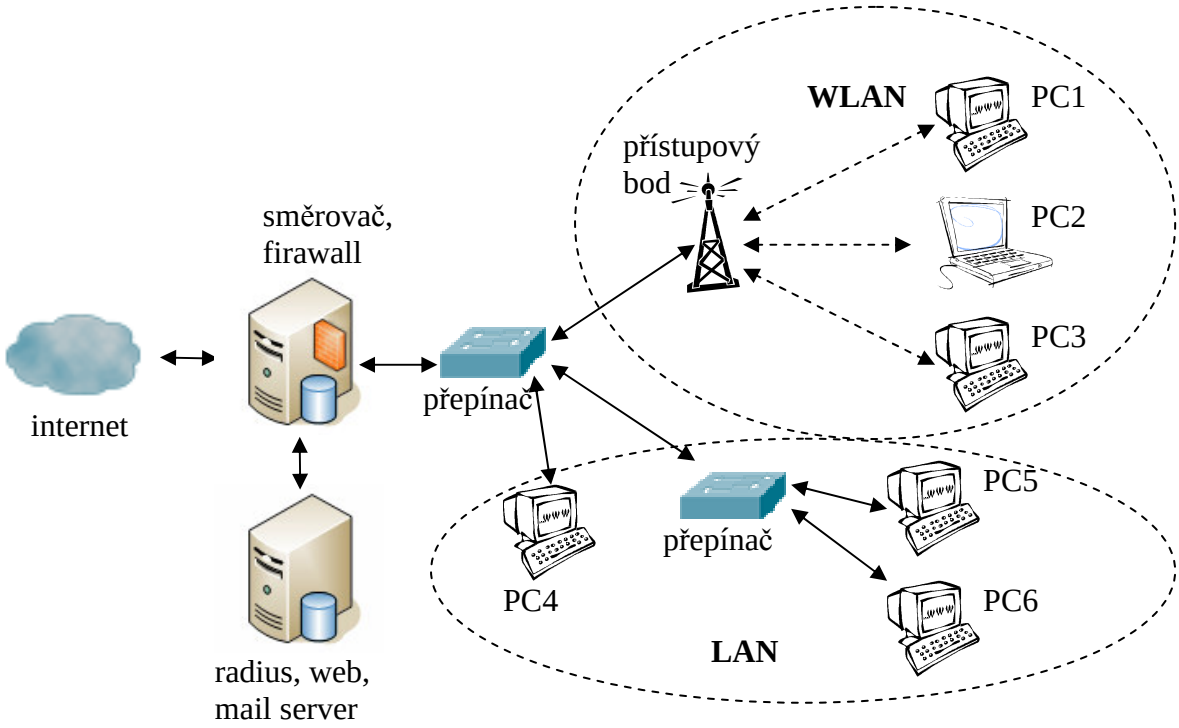
Další možností, jak zvýšit bezpečnost sítě používající mechanismus WEP, je použití šifrování na vyšší síťové vrstvě. Např. použití VPN (Virtual Private Network). Jedná se o vytvoření šifrované virtuální sítě, do které se počítače v sítí připojují. Pro virtuální síť lze nastavit používaný šifrovací algoritmus. Při správném nastavení je toto šifrování mnohem bezpečnější, než šifrování pomocí WEP. Všechny počítače budou komunikovat pomocí této virtuální sítě na jednom konkrétním portu a ostatní pakety přicházející na jiné porty budou zahazovat. Když se pak útočníkovi podaří získat šifrovací klíč, dostane se pouze opět k šifrované komunikaci, procházející skrz virtuální privátní síť.

10.2 Firemní a rozsáhlé sítě

Velká firma využívá na připojení do internetu svůj vlastní směrovač. Některé stanice se připojují po metalickém vedení, jiné za využití bezdrátových technologií. Modelové schéma takovéto situace nám ukazuje Obr. 12. V rozsáhlých sítích, kde počty připojených stanic jdou do stovek, se pro jejich ověřování vyplatí vlastní radius server a pro poskytovaní dalších služeb web a mail server. Počítače vnitřní sítě využívají neveřejné IP adresy třídy C a na směrovači je prováděn NAT (překlad síťových adres).

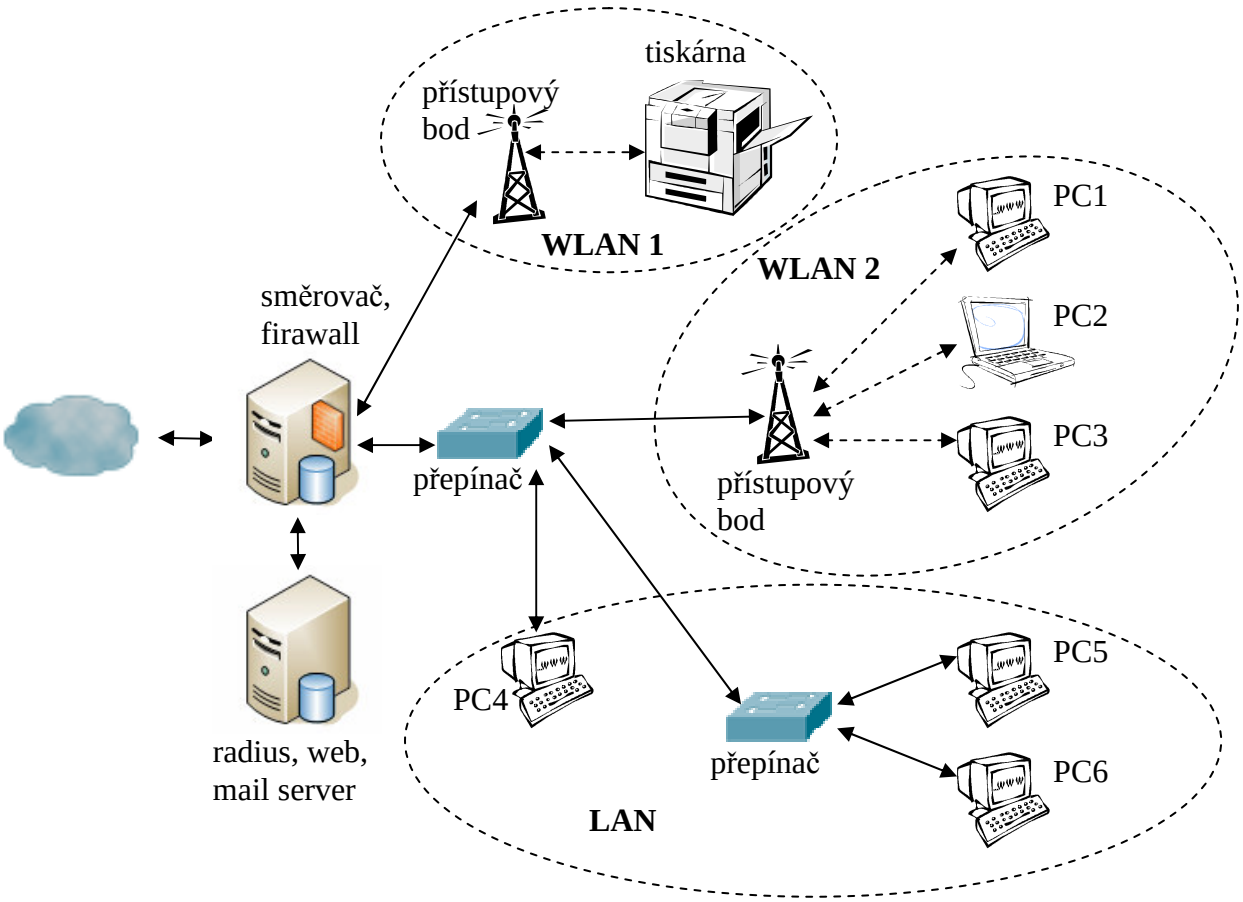
U firemní sítě je na bezpečnost kladen velký důraz. Zabezpečení na základě šifrovacího protokolu WEP je značně nevhodné, a proto je využito pouze protokolu WPA2. Každý uživatel takovéto sítě má vlastní přihlašovací údaje jako je uživatelské jméno a heslo, které využívá pro přístup k počítači a zároveň jsou využity pro ověření daného klienta pro přístup do bezdrátové sítě. O ověření se stará autentizační radius server, který uživateli povolí nebo zamítne přístup do této sítě. Po úspěšném ověření uživatele je už samotný přenos šifrován protokolem WPA2.

Slabinou může být útok typu man in the middle (muž uprostřed), kdy si uživatel myslí, že přihlašovací údaje vyplňuje na serveru, ale zatím je sdělí útočníkovi, který se za server vydává. Ten takto získané údaje snadno zneužije a získá přístup do sítě. Řešením tohoto problému je použití certifikátů, kdy stanice pošle přihlašovací údaje pouze přístupovému bodu s platným certifikátem. Tím zabráníme tomu, aby v případě podvržení přístupového bodu získal útočník uživatelská jména a hesla uživatelů.



Obr. 12 Modelová topologie firemní sítě.

Problém nastane, pokud firma využívá zařízení, které podporuje pouze zabezpečovací mechanismus WEP a výměna tohoto zařízení za novější, podporující šifrování WPA, by byla značně nákladná. Příkladem takového zařízení může být např. bezdrátová, barevná, laserová tiskárna. Řešením je vybudování vlastní sítě s šifrováním WEP pouze pro toto zařízení. Na Obr. 13 je takový model sítě znázorněn.



Obr. 13 Kombinace sítí s WEP a WPA.

Tiskárna se nachází ve vlastní síti WLAN 1, kde je použito zabezpečení mechanismem WEP. Tato síť je připojena přes směrovač s firewallem do vnitřní sítě, a to z důvodu bezpečnosti. Síť, zabezpečená pouze protokolem WEP, není považována za bezpečnou.

11. Návrh metropolitní sítě

Součástí této práce je i návrh a realizace metropolitní sítě, která by umožnila konektivitu uživatelů, jak do veřejné sítě internet, tak by umožnila využívat služby provozované v rámci této lokální sítě. Zejména pro finanční a realizační náročnost využití metalických spojení, bude ve velké míře využita bezdrátová technologie pro návrh celé sítě. Právě z tohoto důvodu je značná část této práce věnována právě možnostem využití těchto sítí a jejich zabezpečení, které u bezdrátových sítí hrají velmi důležitou roli.

11.1 Daná lokalita

Území, pro které se síť bude realizovat, je menší obec Sendražice, nedaleko Hradce Králové. Obec má okolo 400 obyvatel a má dosti podlouhlý tvar, což vylučuje použití centrálního přístupového bodu ve středu obce. Dané území je ze tří světových stran ohraničeno kopci, takže obec je v malebném údolíčku, což značně ztěžuje možnost připojení internetové linky z větších měst v okolí.

11.1.1 Porovnání typů lokalit

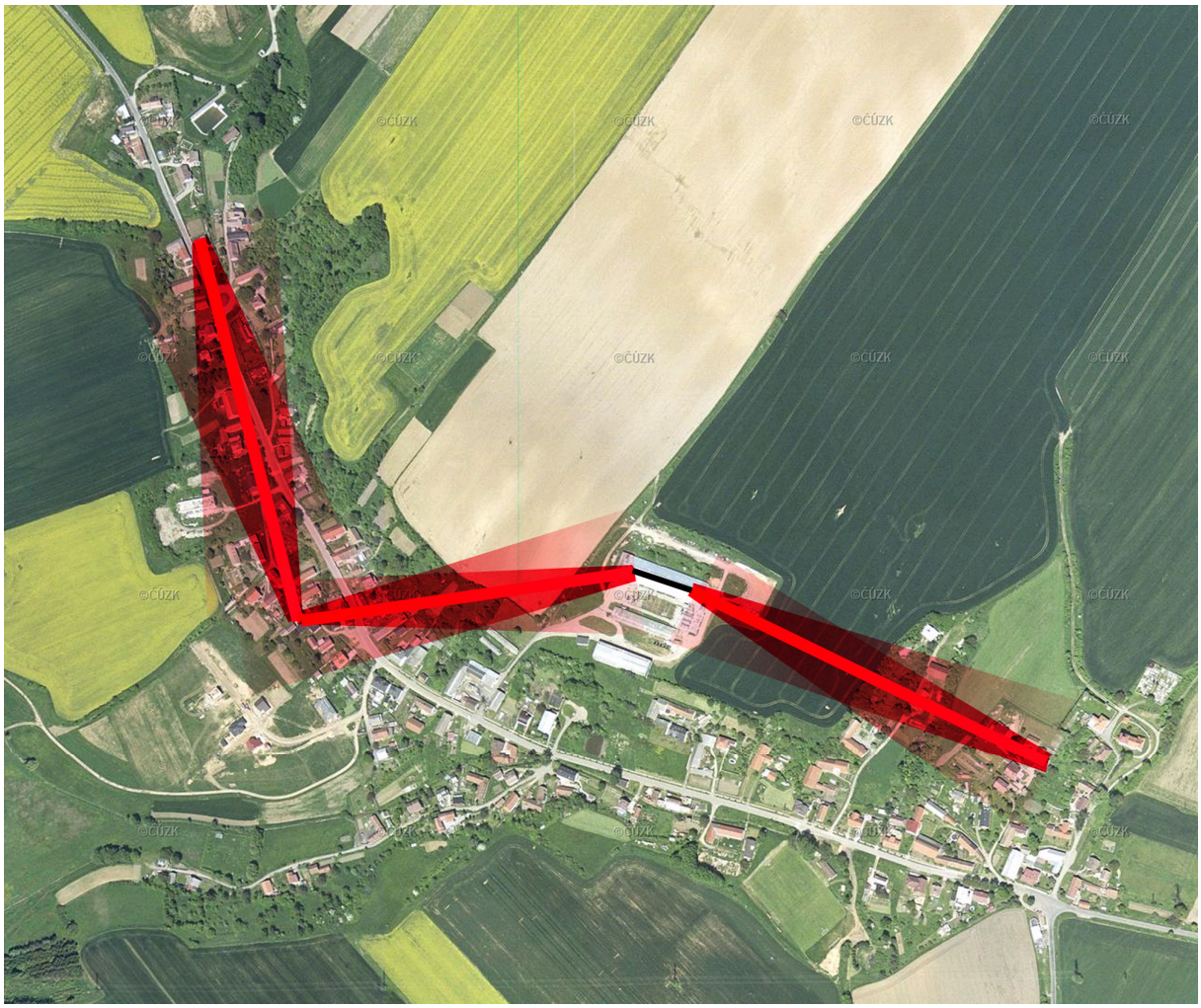
Návrh sítě a především její struktury se značně odvíjí od typu území pro které je určena. Pokud bude síť plánována pro obec s malým počtem uživatelů a tvar obce nebude podlouhlý, ale spíše kruhového tvaru, bude vhodné použít centrální všesměrovou anténu umístěnou ve středu obce, nebo například tři sektorové antény po 120° - 160°, které umožní připojení více uživatelů. Toto rozdělení antén do sektorů se používá např. i u systému GSM. Při tomto uspořádání jsme schopni s malými náklady kvalitně pokrýt danou lokalitu.

Při budování značně rozsáhlé sítě s velkým počtem uživatelů hraje návrh velice důležitou roly. Kvalitní plán nám je schopen při realizaci ušetřit řadu obtíží a především peněz. Postup návrhu bude obdobný jako níže popisovaný. Nejdůležitější je vhodné zvolení páteřních spojů, které prochází napříč celým územím a od nich se následné větví distribuční sítě k jednotlivým uživatelům.

11.2 Navržení páteřního spoje

Zástavba v obci má výrazně podlouhlý tvar a z tohoto důvodu musí být navržen páteřní spoj, který umožní propojit začátek s koncem obce. Tento spoj musí být dostatečně dimenzován, a proto je velice důležité pečlivě naplánovat jeho trasu s ohledem na terénní charakter cesty spoje i na případné rušící prvky, které by značně omezily propustnost tohoto

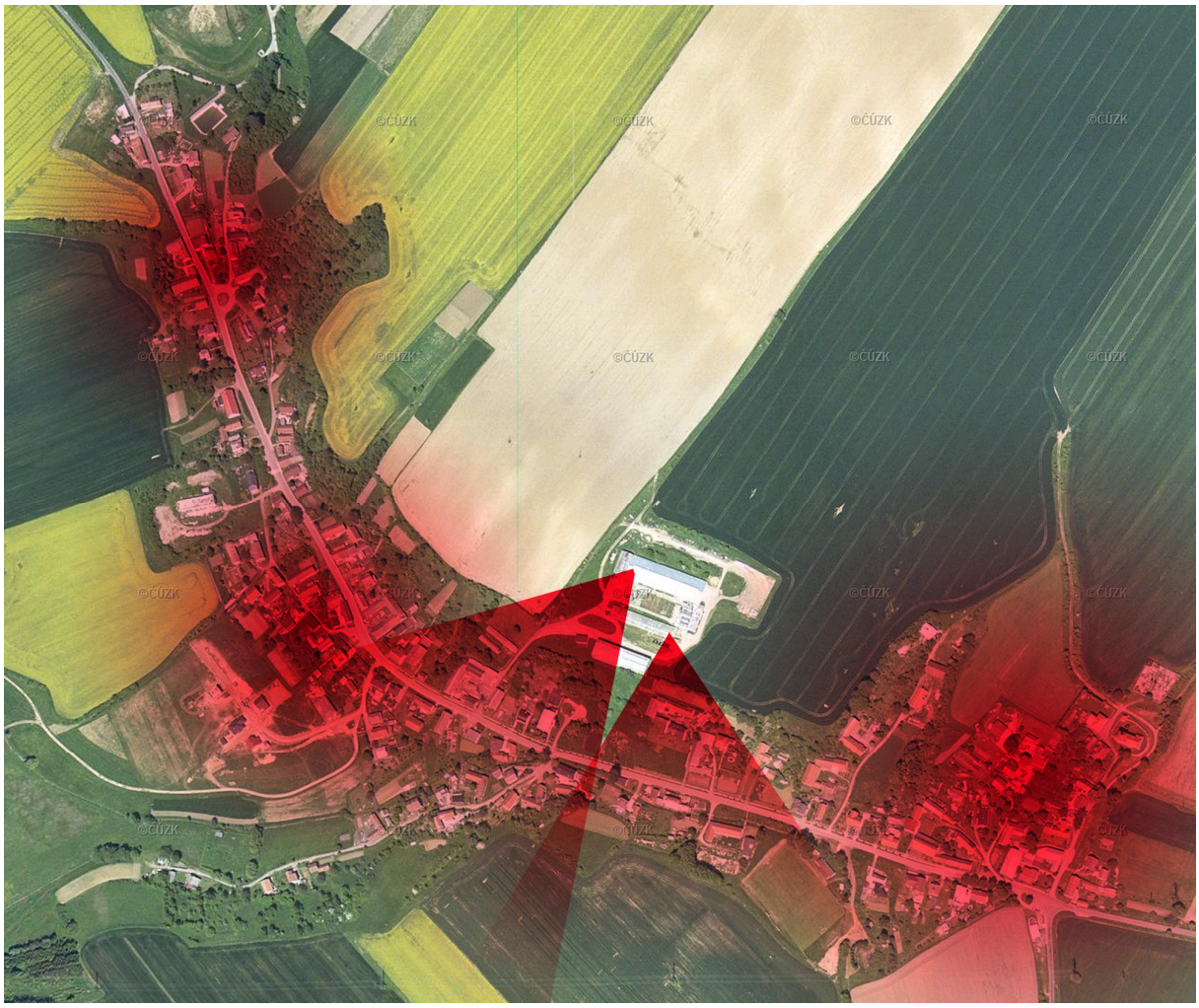
spoje, což je krajně nežádoucí. Právě z těchto důvodů jsem do okolí obce provedl mnohé výlety s dalekohledem a hledal jsem nejvhodnější cesty páteřního spoje. Zaměřil jsem se především na místa s nejvyšší výškou, která by umožnila co možná nejvíce přímý výhled mezi jednotlivými body páteřního spoje, s minimem překážek v cestě šířícího se signálu. Značným problémem jsou vzrostlé stromy, ale vhodným zvolením cesty se i tyto překážky dají obejít. Plánovaná cesta páteřního spoje je vyznačena na Obr. 14.



Obr. 14. Cesta páteřního spoje.

11.3 Plánované pokrytí

V plánu je pokrýt co největší území, v ideálním případě celé, a umožnit tak připojení a využívání služeb všem obyvatelům obce. Přibližnou mapu plánovaného pokrytí můžeme vidět na následujícím Obr. 15.



Obr. 15. Plánované pokrytí obce.

Mapové podklady jsou použity z veřejného serveru amapy.cz. Struktura pokrytí je tvořena třemi všesměrovými anténami a dvěmi sektorovými. Na Obr. 15 je vyznačena pouze mapa pokrytí pro možnost připojení uživatelů. Pro větší přehlednost nejsou znázorněny páteřní spoje, ty jsou řešeny v předchozí kapitole.

11.4 Rozmístění přístupových bodů

Je žádoucí, aby umístění přístupových bodů bylo co nejvíce efektivní. Podle návrhu bude značně korespondovat s páteřním spojem tak, aby se docílilo co největšího pokrytí přibližně znázorněného na Obr. 15. V centru a na krajích obce budou umístěny všesměrové antény, které umožní malým počtem zařízení pokrýt velké množství uživatelů. Na nejvyšší body místní zemědělské usedlosti, nacházející se na kopci nad obcí, se umístí dvě sektorové antény. Toto výše položené místo dobře poslouží k vykrytí zastíněných míst a umožní kvalitní příjem signálu. Viz. Obr. 15.

11.4.1 Zvolené antény

Na páteřních spojích budou použity úzce směrové antény, aby se docílilo dobrých přijímacích úrovní signálu a nedocházelo k obsazení a rušení pásma na velkém území. Naopak tomu pro šíření signálu k uživatelům budou použity všesměrové a sektorové antény, aby bylo pokryto co největší území co nejmenším počtem zařízení. Pro dosažení kvalitního příjmu signálu se u jednotlivých uživatelů budou instalovat antény dle potřeby. U připojených stanic, nacházejících se v blízkosti přístupových bodů, postačí malé panelové antény a pro vzdálenější nebo uživatele stíněné nějakou překážkou, se využijí antény s větším ziskem

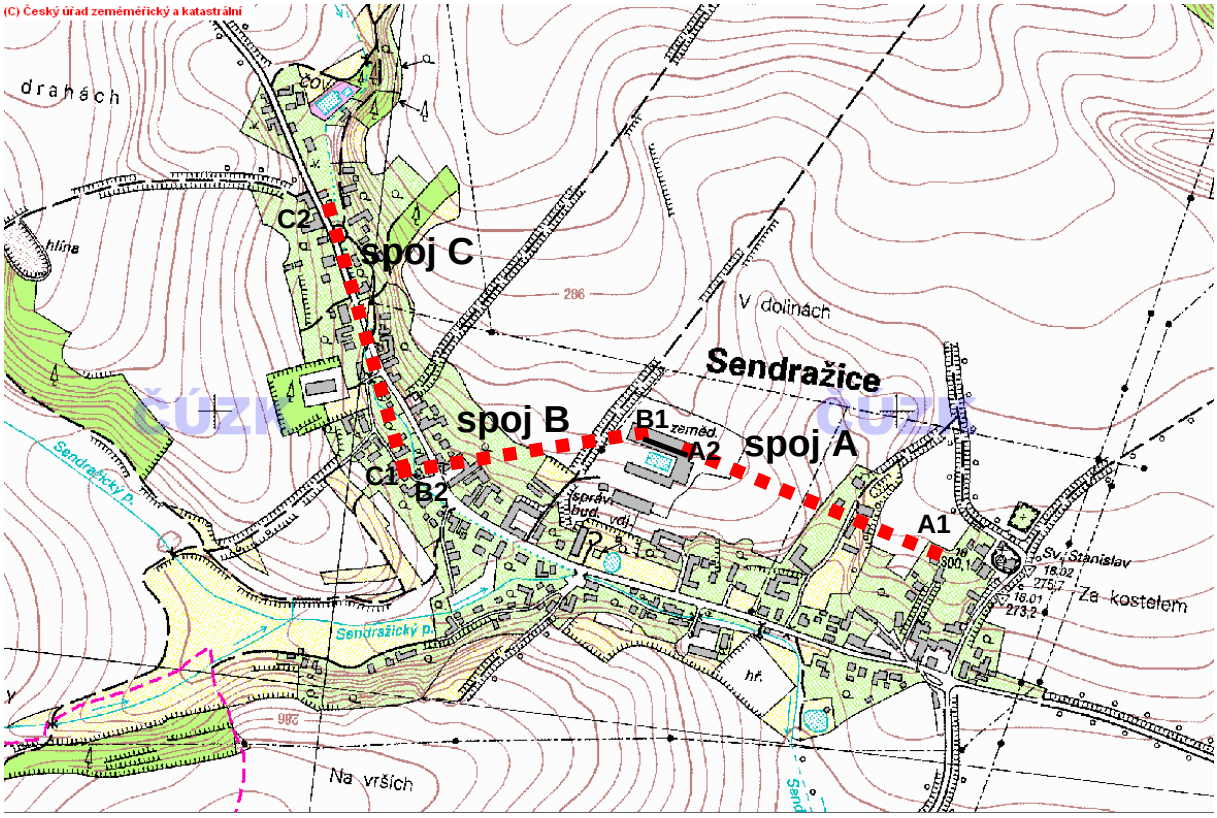
11.5 Výběr použité technologie

Použitou technologií chápeme zejména výběr frekvenčního pásma. Celá síť bude vybudována v bez-licenčním pásmu. Pro páteřní spoje bude využita frekvence 5GHz, a to hlavně z důvodu minimálního využití tohoto pásma v dané oblasti. Tedy i minimálního rušení, z čehož vyplívají i dobré přenosové podmínky. Ušetření kanály v pásmu 2,4GHz, se tak budou moci využít pro distribuční síť. Frekvence 2,4 bude použita zejména kvůli nižší ceně zařízení, které musí mít každý připojený uživatel. Tím se možnost připojení zpřístupní širokému počtu zájemců, jelikož cena je stále tím nejdůležitějším kritériem.

11.6 Plánované poskytování služeb

Základní a jistě nejžádanější službou bude možnost připojení do internetu. Síť bude provozována také za účelem obohacení obce ve směru možnosti podávat občanů rychle a aktuálně informace o dění v obci. Z tohoto důvodu bude na síti provozován lokální web-server, který umožní přístup na intranet, kde budou mít zastupitelé obce možnost právě tyto informace zveřejnit. Občanům bude umožněna interaktivní komunikace s vedením obce z pohodlí a tepla svého domova v podobě obecního fóra. V plánu je i vytvoření aplikace, která by jednotlivým uživatelům zobrazovala přehledné statistiky o provozu a vytížení celé sítě.

12. Realizace metropolitní sítě



Obr. 16 Páteřní spoj.
(mapové podklady ze stránek českého zemědělského úřadu)

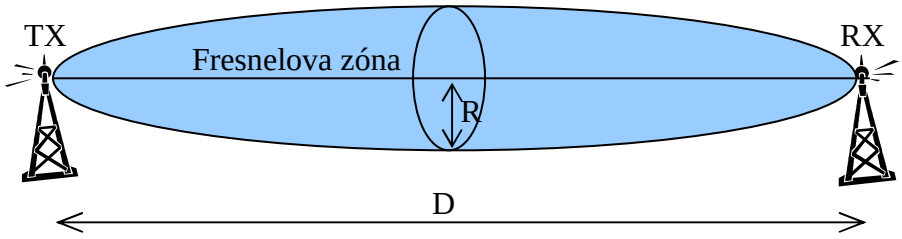
12.1 Budování páteřních spojů

Jednou z nejdůležitějších částí celé sítě je její páteř. Na těchto spojích jsou přenášeny největší datové toky z celé sítě. Je velmi důležité, aby tyto spoje byly dostatečně rychlé a spolehlivé, protože jakékoliv problémy na páteřním spoji se projeví ve funkčnosti celé sítě. Budovaná páteřní síť se skládá ze tří hlavních spojů, a to A, B, C. Jejich poziční umístění je možné vidět na Obr. 16. Protože od rychlosti těchto spojů se bude odvíjet pružnost a kapacita celé sítě, jsou zvoleny bezdrátové spoje v pásmu 5GHz, které poskytují nejlepší požadované vlastnosti v bez-licenčním pásmu.

12.1.1 Fresnelova zóna

U rádiových spojů je převážná část energie přenášeného signálu nesena v prostoru okolo přímky, spojující vysílací a přijímací antény. Jedná se o prostor, který se aktivně podílí na přenosu rádiového signálu. Tato oblast se nazývá Fresnelova zóna. Největší význam má první Fresnelova zóna, protože právě v této zóně probíhá přenos prakticky celého rádiového signálu a přenáší se v ní 90% energie. Má tvar elipsoidu, v příčném řezu pak tvar kruhu, jehož

poloměr se mění po celé délce přenosové trasy. Nejvyšší hodnoty dosáhne v jejím středu (Obr. 17). Při realizaci rádiových spojů je Fresnelova zóna jedním z nejdůležitějších parametrů, a proto je nutné se s tímto pojmem seznámit.



Obr. 17 Fresnelova zóna.

Kde:

D – vzdálenost mezi vysílací a přijímací anténou

R- poloměr Fresnelovy zóny

Tabulka průměrů první Fresnelovy zóny v jejím nejširším místě, pro různé délky přenosové trasy a pro frekvence 2,4 a 5 GHz. Pro výpočet lze použít vzorec:

$$d = 17{,}3 \cdot \sqrt{\frac{D}{4 \cdot f}} \qquad (12.1.1.)$$

d – průměr Fresnelovy zóny

f – frekvence radiových vln

Vzdálenost spoje [km]	**Průměr Fresnelovy zóny pro 2,4 GHz [m]**		**Průměr Fresnelovy zóny pro 5 GHz [m]**	
	100%	**60%**	**100%**	**60%**
0,1	1,8	1,1	1,2	0,7
0,2	2,5	1,5	1,7	1,0
0,3	3,1	1,8	2,1	1,3
0,4	3,5	2,1	2,4	1,5
0,5	3,9	2,4	2,7	1,6
0,7	4,7	2,8	3,2	1,9
1	5,6	3,4	3,9	2,3
1,2	6,1	3,7	4,2	2,5
1,5	6,8	4,1	4,7	2,8

2	7,9	4,7	5,5	3,3
2,5	8,8	5,3	6,1	3,7
3	9,7	5,8	6,7	4,0

Tab. 4 Velikost Fresnelovy zóny pro rádiové spojení o frekvenci 2,4 a 5 GHz.

Narušení Fresnelovy zóny nesníží výrazně úroveň signálu, ale projeví se nárůstem odrazů, které snižují kvalitu spojení a zvyšují ztrátovost paketů, zpoždění a rychlost přenosu dat. Pokud nezajistíme alespoň volných 60% průměru zóny, dochází ke značné degradaci kvality spoje.

12.1.2 Páteřní spoj A

Jedná se o spoj mezi body A1 a A2 viz. Obr. 16, který svou délkou přesahuje hodnotu 415m. Jde o nejdůležitější spoj na síti, protože v bodě A1 je umístěn server, který poskytuje konektivitu do internetu a přístup na webové aplikace v intranetu. Výpadek tohoto spoje by zapříčinil nedostupnost těchto služeb uživatelům za tímto spojem. V budoucnu je v planu vytvoření záložních spojů, které by tento problém v případě poruchy odstranili. Obě spojovaná místa se nacházejí na kopcích. Bod A1 je rodinný domek a A2 místní zemědělská usedlost. Díky této vyvýšené poloze je mezi body tohoto spoje dobrý výhled a antény mezi sebou nemají žádné výrazné překážky. Úroveň signálu dosahuje velmi dobrých hodnot a díky tomu malé chybovosti. Tento spoj dosahuje reálné přenosové rychlosti 13-18MB/s. Jak je vidět, od teoretické hodnoty 54MB/s se naměřený údaj velice liší. V praxi se jí nepodaří nikdy dosáhnout ani se jí výrazně přiblížit.

12.1.3 Páteřní spoj B

Propojení středu obce (bod B2) se zemědělskou usedlostí (B1). Délka spoje je 350m. Mírnou překážkou v cestě je třešeň, která zatím nezasahuje do přímé cesty signálu, ani do Fresnelovy zóny. V budoucnu, při jejím růstu, by mohla činit problém. Vliv na úroveň signálu je minimální. Tento spoj dosahuje obdobných přenosových vlastností jako spoj A.

12.1.4 Páteřní spoj C

Pokračováním v cestě páteřního spoje na okraj obce je spoj C. Zajišťuje spojení ze středu obce z bodu C1 na její okraj do bodu C2. Na vzdálenosti 410m je jedinou překážkou vzrostlý ořech, který z části zasahuje do Fresnelovy zóny. To má za následek mírný pokles

signálu a reálnou přenosovou rychlost 7-12MB/s. Tato kapacita spoje je zatím dostatečná, ale se zvyšujícími se nároky a počty uživatelů je možné, že bude muset být spoj upraven, a to nejlépe změnou polohy bodu C1.

Obr. 18 Páteřní spoj - bod B2, C1.

12.2 Problémy při budování páteřních spojů

Praxe ukázala, že vybudování takovýchto spojů není tak snadné, jak by se mohlo na první pohled zdát. Ze začátku dobu instalace značně prodlužovala především nezkušenost, ale po provedení několika instalací dostanete do ruky ten správný grif. Při montáži jednotlivých zařízení a následném testování vytvořených spojů, se vyskytla řada problémů, které bylo nutné odstranit. Samotná instalace, hledání problémů a jejich následné odstraňování, zabralo až desítky hodin, strávených na střechách domů a u počítače.

12.2.1 Napájení přístupových bodů

Problém, který způsoboval největší obtíže, byl s přivedením napájení k přístupovým bodům (AP). Je žádoucí, aby AP bylo co nejblíže anténě a aby anténa byla umístěna co možná nejvýše. Tím zajistíme signálu nejmenší ovlivnění případnými překážkami a díky použití krátkého kabelu mezi anténou a AP i malý útlum na vedení. Dále si již signál rozvedeme pomocí klasického síťového kabelu UTP, kde nás útlum trápí až okolo 150m délky kabelu, zatímco u anténního kabelu je znát každý metr. Takto se nám AP dostanou

někdy na značně nepřístupná místa a nastává problém, kde vzít zásuvku s 230V. Tento problém se dá velice elegantně a levně vyřešit pomocí napájení PoE (Power Over Ethernet), kdy se pro napájení využijí dva nepoužité páry v UTP kabelu. Toto je lze použít na značně omezenou vzdálenost, protože při velmi malém průměru těchto vodičů a náročnosti odběru zařízení až 5V/2,5A prostě na přenesení výkonu nestačí. Na toto zjištění jsem přišel až po několika hodinách zkoušení, kdy při testovacím provozu docházelo k naprosto nahodilým výpadkům a značnému kolísání rychlosti při přenosu dat sítí. Tyto výpadky byly způsobeny přístupovými body, které se nacházely na samé hranici možností PoE. Při zapojení proběhla startovací sekvence normálně a zařízení se tvářilo naprosto funkčně, ale při větší zátěži už nestačil dodávaný příkon a AP se prostě odpojilo. V zájmu spolehlivosti byl problém vyřešen přivedením síťového napětí co nejblíže přístupovým bodům.

12.2.2 Rychlost přístupových bodů

Z počátku byl v bodě A2 viz Obr. 16 umístěn starší typ AP, který způsoboval značné problémy. Při zatížení docházelo ke ztrátě konektivity a nedostupnosti služeb v části sítě. Problém byl způsoben nedostatečnou vyrovnávací pamětí a rychlostí tohoto staršího modelu, kdy při jeho zahlcení docházelo k totálnímu zahazovaní paketů. Velký problém byl v odhalení tohoto problému a jeho lokalizaci. Postupným sledováním stavu a chovaní sítě, kdy jsem z několika různých částí sítě testoval konektivitu a ztrátovost paketů při zatížení, jsem došel k tomuto AP v bodu A2. Po jeho výměně a následných testech jsem zjistil, že se propustnost sítě značně zvýšila a už nedocházelo k žádným výpadkům ani při zatížení.

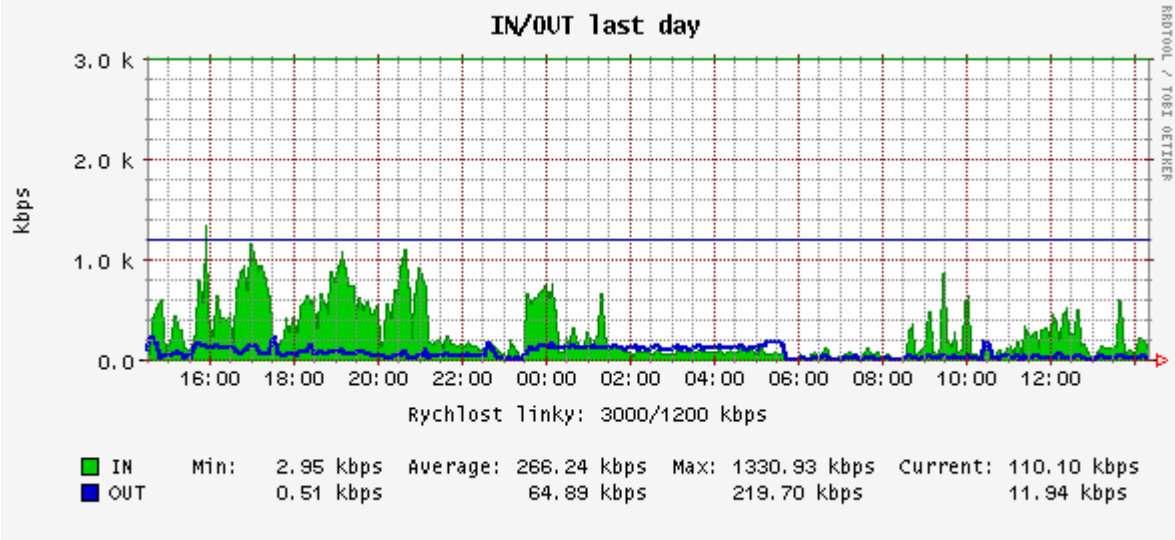
12.3 Budování přístupových bodů

Při budování sítě přístupových bodů jsem vycházel z návrhu podle Obr. 15. V obci jsou umístěny tři všesměrové antény, a to v bodech A1, B2, C2 (Obr. 16), které zajišťují pokrytí většiny území. Dále jsou na zemědělské usedlosti umístěny dvě sektorové antény pro lepší vykrytí postraních ulic signálem.

13. Internetové připojení

Připojeným uživatelům je v případě zájmu poskytováno internetové připojení. Přivedení dostatečně rychlého spojení, které by vyhovovalo dnešním nárokům, je na daném území problém. Obec se nachází na samé hranici dostupnosti technologie ADSL a rychlost takového spoje je pro sdílený internet naprosto nedostatečná. Proto je připojení řešeno bezdrátovou

technologií, ale tentokráte v licencovaném pásmu, kdy rychlost připojení činí 3MB pro download a 1MB pro upload. Přijímací bod je umístěn v bode A1 (Obr. 16) kde je přímá viditelnost na přístupový bod poskytovatele. V současné době tuto službu využívá asi 20 uživatelů. Jak je vidět z grafu využití šířky pásma (Obr. 19) je rychlost zatím dostačující.



Obr. 19 Graf vytížení internetového připojení.

14. Server

Za účelem řízení přístupu do internetu a intranetu, administrace a sledování sítě, přidělování rychlostí a správu uživatelů, je v bodě A1 (Obr. 16) umístěn server s operačním systémem linux, který tyto služby obstarává. Spuštěný webový server apache a databázový server SQL umožňuje přístup na webové rozhraní intranetu a k umístěným aplikacím.

15. Implementace zabezpečení

Dle poznatků získaných v úvodní teoretické části, jsou do zabezpečení sítě implementovány nejsilnější zabezpečovací mechanismy. Maximální odolnosti proti případným útočníkům je dosaženo kombinací všech možných mechanismů, které nám výše zmiňované standardy nabízejí. Jedná se o použití WPA2 pro šifrování přenosu s použitým silným heslem PSK, filtrování fyzických adres na všech přístupových bodech, zabezpečení AP proti neoprávněné konfiguraci, nevysílání identifikátoru sítě, povolení přístupu jen registrovaným IP adresám na firewallu a sledování provozu na těchto adresách.

15.1 Zabezpečení přístupových bodů

Přístupové body jsou umístěny na soukromých pozemkách, v domech, většinou na běžně nepřístupných místech. Aby se útočník dostal k těmto zařízením přímo, je téměř nemožné. Co se týká síťového útoku, na všech AP byly hned po instalaci změněny přístupové kódy, aby se nemohl nikdo bez jejich znalosti dostat ke konfiguraci těchto zařízení.

15.2 Filtrování MAC adres

Povolení jen oprávněných fyzických adres na přístupovém bodu nepřináší při klasické modelu sítě AP – klient přílišné zlepšení bezpečnosti. Jak už bylo řečeno výše, přístupový bod má seznam fyzických adres, které se k němu mohou připojit. Také bylo řečeno, že podvržení této adresy není pro útočníka problém, ale musí vyčkat, až uživatel například vypne svůj počítač a daná adresa bude volná. A v tom právě tkví síla tohoto zabezpečení! Veškeré spoje jsou tvořeny z přístupového bodu do přístupového bodu v klientském režimu. Nedochází tedy k jejich vypnutí jako počítače a fyzická adresa se tak útočníkovy nikdy neuvolní. Díky tomu se toto bezpečnostní opatření stává, pro případného útočníka, těžko překonatelné a při pokusu o neoprávněné připojení snadno zjistitelné, protože případný provoz dvou stejných MAC adres lze totiž jednoduše detekovat tak, že oprávněné stanici budou doručovány pakety, který si nevyžádala. Pro administrátora je udržování a upravování seznamu platných MAC adres náročné, ale v takto malé, příliš se neměnící síti, to není žádný problém. Je to jen malá oběť za velký přínos k bezpečnosti sítě.

16. Administrace a správa sítě

Jedná se převážně o dohledovou činnost nad funkčností, vytížením a stabilitou sítě, správu uživatelských účtů a spuštěných aplikací, přidávání nových účtů do databáze serveru v případě připojení nového uživatele. Sledování značně ulehčují aplikace, které jsem za tímto účelem vytvořil. Podrobněji si je popíšeme v samostatné kapitole.

Dalším velmi silným nástrojem pro zjištění stavu sítě je příkaz ping, který otestuje dostupnost jednotlivých zařízení. V praxi se ukázal jako nepostradatelný pomocník, především při hledání problémů. Existuje řada programů, které testují, pomocí příkazu ping, IP adresy podle zadaného seznamu. Takto zjistíte během okamžiku dostupnost všech zařízení, případně které je nedostupné. Mnoho programů disponuje i grafickým znázorněním doby odezvy, které nám také hodně řekne o stavu sítě.

16.1 Konfigurace serveru

Nejprve je nutné nastavit jednotlivá rozhraní LAN a WAN, aby byla funkční konektivita s vnitřní a venkovní sítí. Dále je nutné do nastavení firewallu přidat záznamy IP adres všech uživatelů, kteří můžou přes server komunikovat, aby jim byl přístup umožněn a neoprávněným uživatelům zamítnut. Další konfigurace spočívá v přidělení přenosových rychlostí jednotlivým uživatelům a to za pomocí QoS tříd, kdy má každý uživatel na dané IP adrese přidělenou rychlost. Díky tomu nemůže jeden uživatel neúměrně zatížit připojení k internetu a tak omezit dostupnost této služby ostatním uživatelům. Nastavení DHCP rezervací spočívá v přidání záznamu MAC adresy síťové karty uživatele a k ní příslušné IP adresy. V případě, že má klient nastaveno na svém počítači automatické přidělování adres, tak po přihlášení do sítě počítač žádá o přidělení IP adresy. Server mu vždy nabídne tu, kterou má definovánu v tomto záznamu. Takto má daný uživatel vždy stejnou IP adresu. Dalších nastavení, např. web serveru a jiných služeb, je velké množství, ale není to cíl této práce, a proto je nebudu dále podrobně popisovat.

16.2 Statistiky přenesených dat

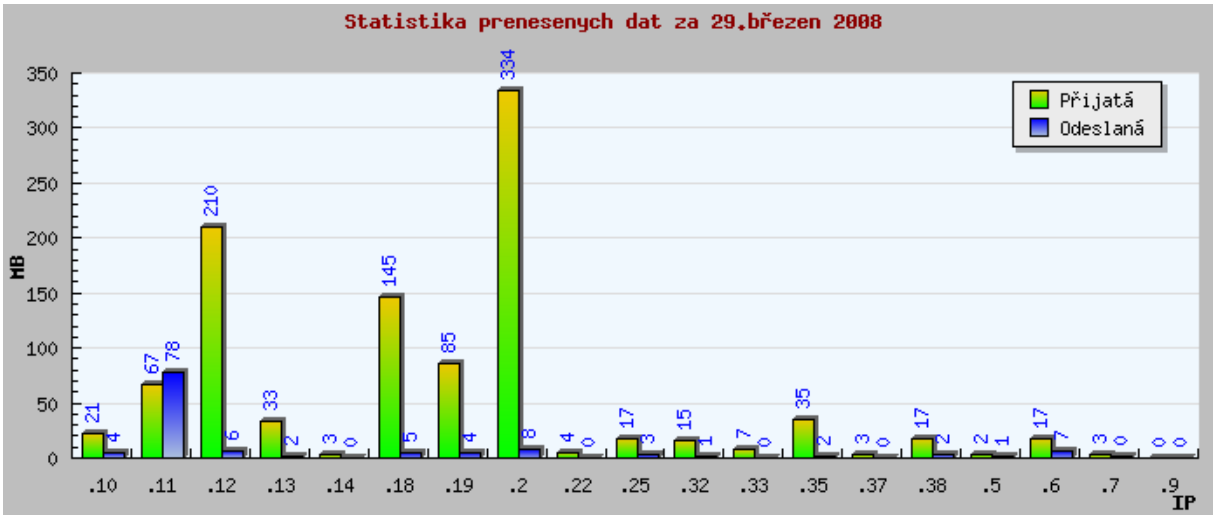
Po seznámení s programovacím jazykem PHP a databázovými systémy SQL jsem začal vyvíjet aplikaci, která by mi umožnila lépe sledovat množství přenesených dat. Výsledkem je komplexní systém, který administrátorovi umožňuje snadno, rychle a přehledně zobrazit statistiky přenesených dat, a to jednotlivých nebo všech uživatelů za daný měsíc nebo konkrétní den.

Velkou výhodou aplikace je její autonomní chod, kdy se uživatel nemusí starat např. o dodaní nových dat pro statistiky a jejich aktualizaci v databázi. Aplikace sama stahuje nová data ze serveru a provádí jejich zápis do databáze, ze které jsou následně čerpány informace pro zobrazení statistik. Při větším počtu uživatelů na síti by bylo značně náročné manuální zavádění každého do databáze. Proto aplikace zvládne sama načíst a zapsat všechny uživatele, které si vytáhne přímo z konfiguračního souboru serveru pro DHCP rezervace.

16.2.1 Denní statistiky

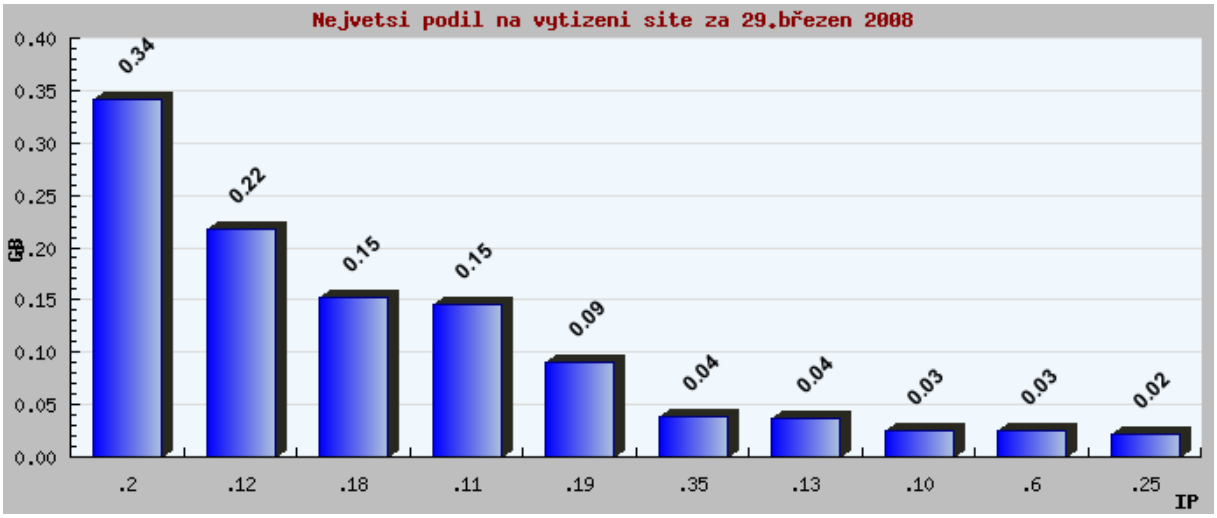
Aplikace nám umožňuje volbu konkrétního dne a následně zobrazí tabulkový přehled s informacemi, kde každý řádek odpovídá záznamu jednotlivých IP adres, které byly ten den aktivní, s údajem o přijatých, odeslaných a celkových přenesených datech daný den. Na konci tabulky jsou celkové hodnoty, které nám prozradí kolik bylo daný den celkem přeneseno dat

z a do internetu. Výstupem aplikace je i přehledný graf (Obr. 20), který je mnohem čitelnější něž tabulka plná čísel a umožňuje nám rychlou orientaci v zobrazených informacích. Například z následujícího Obr. 20 administrátor jedním pohledem zjistí, že nejvíce přijatých dat bylo na IP adrese s koncovkou 2. Snadno rozpoznatelný je také uživatel využívající BitTorrent (protokol pro distribuci souborů), který se prozradí velkým množstvím odeslaných dat v poměru k přijatým. V našem případě je to uživatel s koncem IP adresy 11.



Obr. 20 Denní statistika přenesených dat.

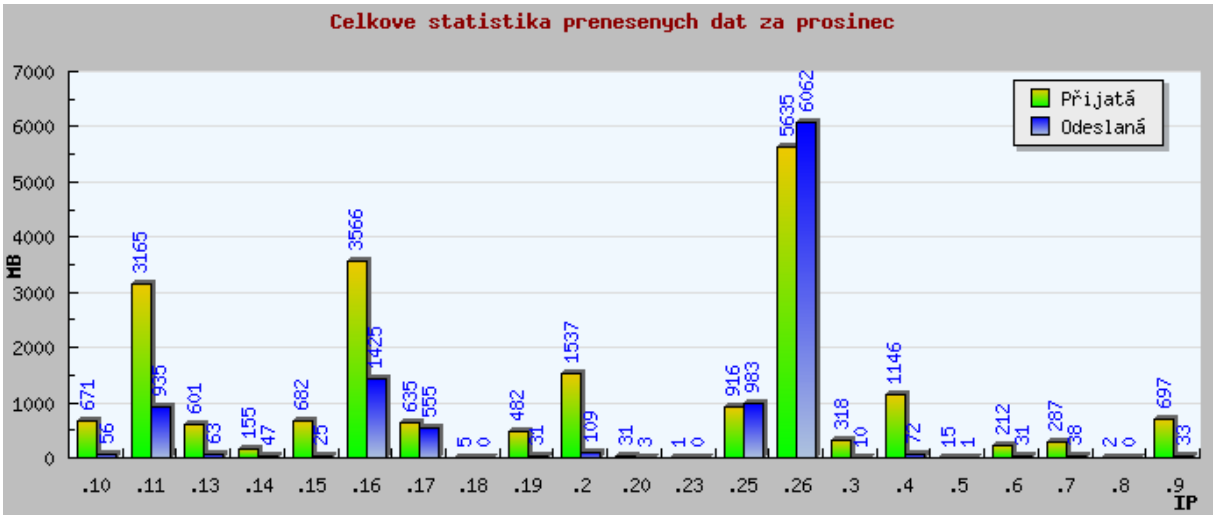
Dalším výstupem aplikace je graf, který zobrazí seřazené uživatele podle podílu na vytížení sítě daný den. Ukázka na následujícím Obr. 21.



Obr. 21 Graf podílu vytížení sítě.

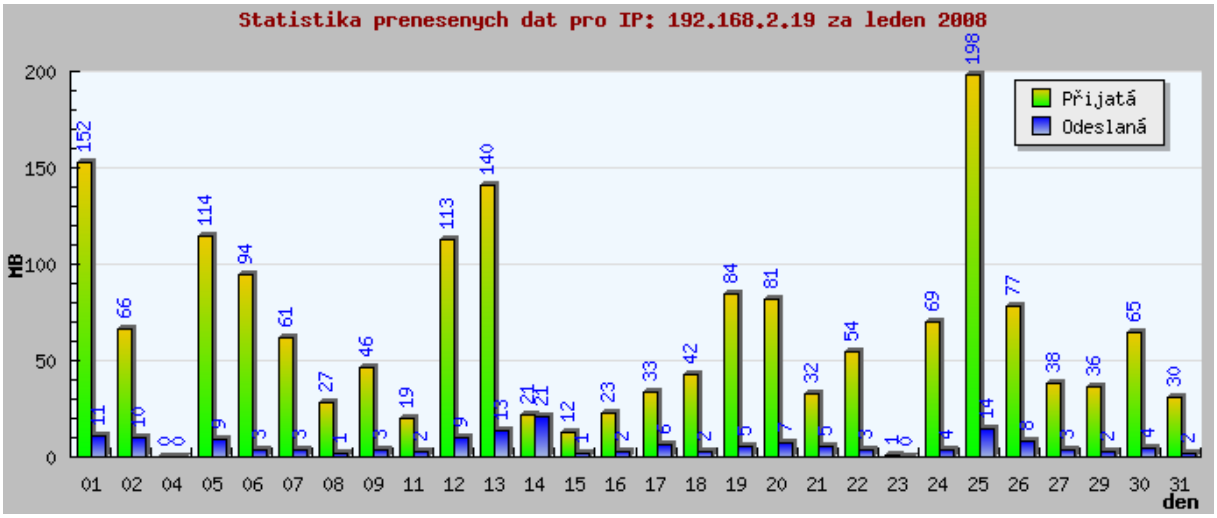
16.2.2 Celkové statistiky

Tato aplikace umožňuje náhled na statistiky v dlouhodobějším časovém měřítku. Máme možnost zvolit konkrétní nebo všechny IP adresy z registrovaných, libovolný měsíc nebo všechny mesíce a rok za který chceme statistiky získat. Kombinacemi všech možných voleb získáme nejrůznější statistiky, které se nám opět zobrazí v přehledných grafech. Například při zvolení všech IP adres, konkrétního měsíce daného roku se nám zobrazí statistika za daný měsíc všech uživatelů. Výstup z takto nastavené aplikace nám ukazuje následující Obr. 22.



Obr. 22 Celkové statistiky měsíce.

Další zajímavou volbou je zvolení konkrétní IP adresy a libovolného měsíce v daném roce. Zobrazený výsledek je opět uspořádán do grafu, který nám ukazuje jednotlivé dny zvoleného měsíce a v nich množství přijatých a odeslaných dat dané IP adresy. Ukázka na následujícím Obr. 23.



Obr. 23 Měsíční statistika zvolené IP adresy.

Takto velice snadno a rychle můžeme například odhalit podezřelý nárůst přenesených dat na nějaké IP adrese. I toto může vést k odhalení útočníka, který by zneužíval něčí IP adresu. Když například víme, že uživatel využívá internet jen občas ke stažení elektronické pošty a jím přenesená data se v minulých několika měsících pohybovala v jednotkách MB za den, tak bude krajně podezřelé, když v celkových statistikách odhalíme záznam s rapidním nárůstem přenesených dat.

16.3 Správa IP adres

Tato aplikace umožňuje snadnou orientaci ve stále narůstajícím množství IP adres uživatelů sítě. Vychází z požadavku, že dnešní uživatelé mají většinou více než jeden počítač, který chtějí připojit do sítě. Například rodiče mají počítač, jejich ratolesti mají vlastní a ještě hlava rodiny má notebook. Jejich požadavkem je připojení všech počítačů do sítě s přístupen na internet. Je příhodné takovouto skupinu adres logicky spojit dohromady, protože např. poplatek za internet platí jen hlava rodiny. Z tohoto důvodu je zvolena jedna hlavní IP adresa a ostatní jsou přidruženy pod ní. Takovýmto uspořádáním získáme přehlednou strukturu, kterou nám tato aplikace pomáhá administrovat.

Na začátku musí administrátor jednotlivé adresy rozřadit do příslušných skupin. Aplikace mu nabídne seznam nepřiřazených IP adres, kde jednoduchým zaškrtnutím zvolí hlavní (mastr) IP adresy. Potvrzením se vybrané adresy přiřadí do skupiny hlavních a jsou jim vytvořeny účty pro přehledy poplatků za připojení k internetu. Z toho vyplívá, že platící zákazník má vždy hlavní IP adresu. Následně se přiřazují vedlejší (slave) adresy, a to ve výše zmiňovaném případě, kdy je připojeno více počítačů v jednom domě. Přiřazení je velmi

snadné. Aplikace nám vypíše seznam nezařazených uživatelů s možností volby jedné z hlavních adres, které jsme vytvořili v minulém kroku. Jednotlivá nastavení můžeme měnit podle potřeby. Výstupem je přehledná tabulka všech přiřazených uživatelů.

Hlavní IP	Jméno	Přiřazené IP	Počet IP
192.168.2.4	Lenhart Petr	192.168.2.38 – Lenhart Ruda	2
192.168.2.5	Hrub st.	192.168.2.22 - Hrub ml. 192.168.2.26 - Hrub str.	3
192.168.2.9	H. Zdenek	-	1
192.168.2.10	H. Vasek st.	192.168.2.11 - H. Vasek ml. 192.168.2.12 - H. Katerina	3
192.168.2.13	R. Lubos	192.168.2.14 - R. Lucka	2
192.168.2.15	H. Lubos	-	1
192.168.2.24	Mexbaur	192.168.2.40 - Mexbaur Kuba	2
192.168.2.33	Luda	-	1
192.168.2.34	Iva Cerna	-	1

Tab. 5 Přidělení IP adres do skupin.

16.4 Přehled plateb

Díky této aplikaci má administrátor snadný přehled o tom, kdo již zaplatil poplatek za internet, nebo kdo dluží už za poslední dva měsíce a je na čase ho odpojit. Aplikace sama hlídá účty a když zjistí, že je nový nezaúčtovaný měsíc, automaticky položku vytvoří. Samozřejmostí je možnost editace cen, kdy se nová položka vytváří s aktuálně nastavenou cenou. Snadný je také přístup k placení, kdy se administrátorovi zobrazí jen nezaplacené položky a on pouze u daného uživatele potvrdí zaplacenou částku.

16.5 Vytížení připojení

Na serveru je spuštěna aplikace, která přes webové rozhraní zobrazuje grafy vytížení internetového připojení. K dispozici máme aktuální data v hodinovém intervalu. Další možností jsou grafy za posledních 8 hodin, za poslední den a za poslední týden. Ukázku grafu vytížení můžeme vidět na Obr. 19. Díky takovýmto přehledům můžeme určit, kdy jsou na síť kladeny největší nároky. Ze sledování vyplívá, že největší využití sítě je mezi 16 a 22 hodinou.

17. Webové aplikace pro uživatele sítě

Součástí této práce je i zpřístupnění nejrůznějších aplikací uživatelům sítě, kteří tak budou moci získávat informace například o dění v obci, stavu svých účtů a sítě. Díky těmto aplikacím budou snadno a rychle informováni.

17.1 Aktuality

Jedná se o jednoduchou komponentu, která návštěvníkům webové stránky intranetu zobrazí aktuální informace. Do současné doby byla převážná část zpráv charakteru informování o plánované odstávce sítě za účelem nějakých úprav. V současné době však můžu konstatovat, že sít je plně funkční, a to bez nejmenších problémů. Zprávy v aktualitách již spíše informují o poskytování nových služeb pro uživatele.

Administrátor spravuje aktuality velmi snadno, jelikož mu přímo webové rozhraní umožňuje nové zprávy vládat a mazat.

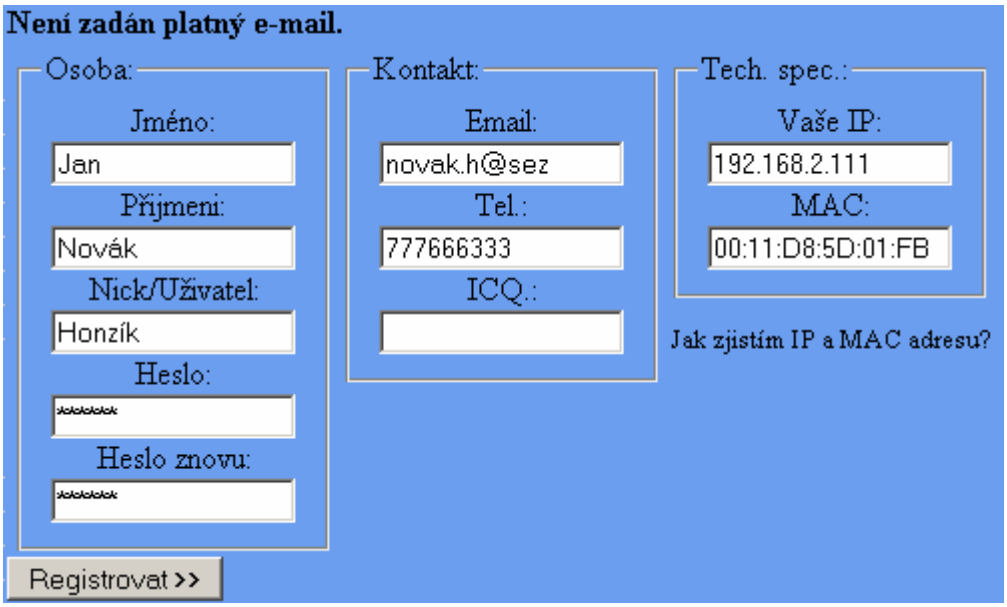
17.2 Přihlašovací portál

Jde o druhou nejrozsáhlejší praktickou část této práce, která se zabývá programováním webových aplikací. Po získání zkušeností a dovedností v jazyce PHP z předchozích aplikací, jsem vytvořil komplexní systém, který umožňuje registraci, přihlašování, správu uživatelských účtů, zobrazení statistik atd. Jeho jednotlivé části a jejich možnosti rozeberu v následujících kapitolách. Tento systém si bere za úkol umožnit registrovaným uživatelům nahlédnout do statistik a dat, která by jinak měl k dispozici pouze administrátor. Správce systému kontroluje veškerá získaná data. Registrovaný uživatel může nahlédnou pouze na informace, které se týkají jeho.

17.2.1 Registrace

Jedná se o klasickou registraci za pomoci formuláře (Obr. 24), kde uživatel vyplní požadované údaje jako je jméno, heslo, email atd. Další požadovaný údaje, které musí být vyplněn je IP adresa, kterou má od nás uživatel přidělenou a MAC adresa jeho síťové karty. Pro méně zdatné uživatele je i k dispozici návod, kde tyto informace zjistí. Vložené informace jsou důležité pro následné ověření uživatele, aby nedošlo někým k zneužití učtu. Veškeré vkládané informace jsou kontrolovány, zda projdou danou maskou. Například jméno a heslo musí být delší než tři znaky, email musí být email atd. V případě, že uživatel zadá některé údaje v neplatné podobě, je informován o tom, kde udělal chybu a čemu daná položka

nevyhověla. Dalším ověřením a zároveň bezpečnostním opatřením prochází uživatelské jméno, email, IP a MAC adresa. Tyto údaje jsou porovnávány s databází, zda se v ní již nenachází. Není možné, aby např. dva uživatelé měli stejnou IP nebo MAC adresu. V takovém případě se nejspíš útočník snaží vydávat za někoho jiného a zaregistrovat si jeho účet. Registrace nebude provedena a vypsaná varovná hláška vyzve ke kontaktování administrátora. V případě, že všechny údaje budou zadány korektně, zobrazí se uživateli poděkování za registraci s rekapitulací zadaných údajů a informací, že účet bude aktivní hned po schválení administrátorem.



Obr. 24 Registrační formulář.

17.2.2 Schválení

Jde o bezpečnostní prvek, který má za úkol zabránit registraci účtu, který dané osobě nepatří. Z tohoto důvodu není účet funkční hned po registraci a musí být nejprve ověřen a schválen administrátorem. Jak ale bezpečně ověřit uživatele, zda mu opravdu patří účet, který si registruje? Jedinou možností je údaj, který zná pouze daný uživatel a administrátor. Vhodné by bylo například číslo smlouvy a podobně. V tomto případě má administrátor k dispozici několik údajů, kterými může uživatele ověřit. Prověří ve svém seznamu zadané IP a MAC adresy, zda patří k sobě a jestli je vlastní osoba podle jména, které vyplnila při registraci. Dalším silným ověřovacím prvkem je záznam IP adresy, ze které byla registrace prováděna. Jak bylo popsáno výše, podvržení IP adresy je možné, ale zjistitelné. O tomto záznamu případný útočník neví, takže nemá možnost zjistit, proč jeho registrace nebyla ověřena. Dobré ověření může administrátor provést na základě kontaktních údajů. Nejlepším možným

ověřením je osobní nebo telefonický kontakt s daným uživatelem. Do jaké míry bude uživatel ověřen, záleží pouze na administrátorovi. Pečlivost ověření by měla korespondovat s citlivostí informací, které by případný útočník získal. V případě, že bude registrace uznána důvěryhodnou, administrátor jí potvrdí jedním klikem ve webové aplikaci.

17.2.3 Bezpečné přihlášení

Nejen z důvodu použitého přenosového média a nedostatcích, které přináší jeho zabezpečení je veškerá komunikace mezi klientem a serverem přenášena v šifrované podobě. Při použití klasického protokolu http je komunikace zasílána v otevřené podobě. Pokud si kdokoli zachytí pakety s registrací nebo přihlašovacími údaji uživatele, snadno si přečte uživatelské jméno a heslo klienta a dostane se tak k jeho účtu. Tento problém jsem vyřešil za pomoci implementace protokolu https, který celou komunikaci mezi serverem a klientem šifruje silným asymetrickým šifrovacím systémem RSA. Navíc server je ověřován certifikátem, díky kterému zabráníme podvržení webového serveru, kdy přihlašovací údaje vyplníme do formuláře útočníka (útoku typu man in the middle). V certifikátu je obsažen veřejný klíč serveru. S jeho pomocí klient zašifruje své přihlašovací údaje a odešle je serveru, který je dešifruje svým privátním klíčem a provede jejich ověření. Pokud se útočníkovy podaří prolomit šifrování WEP-WPA dostane se pouze k silně šifrované komunikaci mezi klientem a webovým serverem.

Systém také kontroluje při každé akci IP adresu uživatele, čímž zabráníme útokům na podvržení přihlášeného uživatele. Sledován je i čas mezi jednotlivými akcemi přihlášeného uživatele a při překročení určité doby je uživatel automaticky odhlášen.

17.2.4 Přehled účtů

Uživatelé, kteří využívají i možnosti připojení k internetu, platí poplatek na pokrytí nákladů. Pro přehled o účtech klientů, jsem vytvořil komponentu, která uživatelům tyto informace přehledně zobrazí. Po přihlášení uživatele se zobrazí přehledná tabulka s vystavenými účty, kde naleznou veškeré informace jako datum vystavení, splatnosti, částku a kolik bylo zaplaceno. Pro snadnou přehlednost jsou položky v tabulce zvýrazněny různou barvou podle jejich stavu. Pokud je položka zaplacena, pole je zelené, když ještě zaplacena není, ale doba splatnosti ještě nevypršela, je pole žluté a v případě prošlé doby splatnosti, je pole červené. Výstup z této aplikace můžete vidět v následující Tab. 6.

Datum vystavení	Datum splatnosti	Cena	Zaplaceno
2008-05-01	2008-05-28	250,-Kč	0,-Kč
2008-04-01	2008-04-28	250,-Kč	0,-Kč
2008-03-01	2008-03-28	250,-Kč	250,-Kč
2008-02-01	2008-02-28	250,-Kč	250,-Kč

Tab. 6 Přehled účtů.

17.2.5 Přehled adres

Tato komponenta je důležitá především pro uživatele, kteří mají připojeno více počítačů v domě, jak bylo rozebíráno výše v kapitole o správě IP adres. Komponenta se zobrazí pouze uživateli s tzv. hlavní IP adresou (kap. 16.3). Vypisují se zde adresy, které jsou k dané hlavní adrese registrovány. Komponenta také slouží k pohodlnému přecházení mezi statistikami, kdy vypsané adresy slouží jako odkaz k statistice dané IP. Takto se například otec může podívat, jaké datové přenosy mají jeho ratolesti.

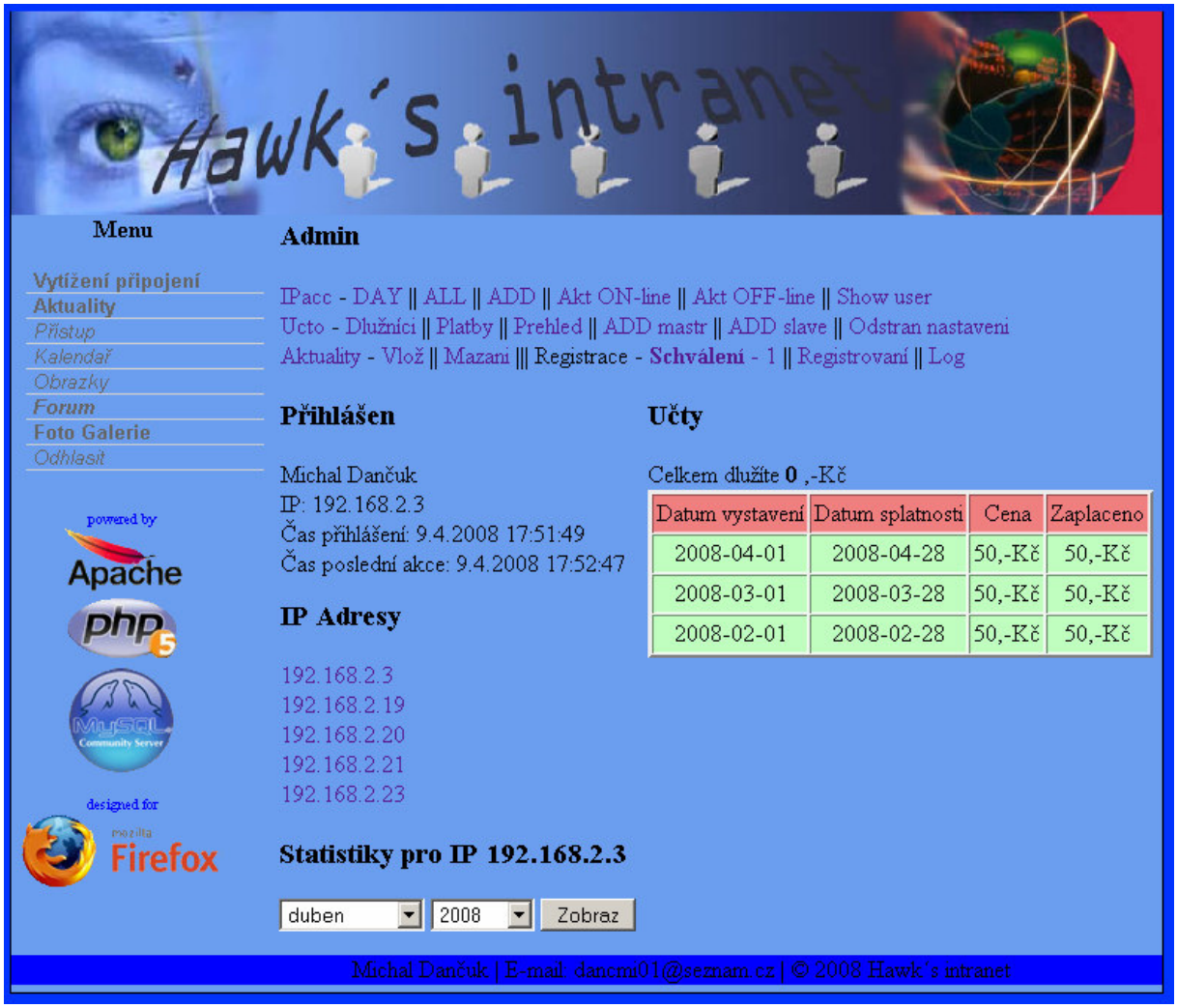
17.2.6 Statistiky

Každý registrovaný uživatel má po přihlášení možnost nahlédnout do statistik jím přenesených dat. Může si vybrat konkrétní měsíc daného roku a po odeslání dotazu mu bude zobrazen tabulkový výpis s přehledným grafem. V něm nalezne jednotlivé dny měsíce a k ním příslušné hodnoty přijatých a odeslaných dat, podobně jako na Obr. 23. Širší možnost výběru mají uživatelé s tzv. hlavní IP adresou (kap. 16.3), kteří si mohou prohlédnout statistiku všech IP adres k nim registrovaných. Samozřejmě největší možnost výběru má administrátor, který si může prohlédnou statistiky všech uživatelů jak bylo rozebíráno v kapitole 16.2 o statistikách přenesených dat.

17.2.7 Práva administrátora

Portál používá přístupová práva jednotlivých uživatelů, a to zejména za účelem usnadnění práce administrátora. V systému se nachází tři úrovně práv. Každý uživatel má práva 0, správce má práva 1 a administrátor má nejvyšší práva 3. Práva s označením 2 jsou zatím nevyužita a jsou připravena pro případné rozšíření aplikace. Při přihlášení se kontrolují práva uživatele a podle nich mu je zobrazen obsah. Normálním uživatelům se zobrazí komponenty popsané výše, ale uživateli s vyššími právy se navíc zobrazí i administrátorské menu, kde má rychlý přístup ke správě jednotlivých aplikací. Správce může prohlížet veškeré statistiky, registrované uživatele, kontrolovat a zapisovat platby, vkládat a mazat aktuality. Uživatel s právy administrátora může ještě navíc řídit tvorbu databáze, registraci nových

uživatelů, jejich kontrolu a schvalovaní, prohlížení záznamů o přihlašování, kde může snadno odhalit pokusy o neoprávněné přihlašování, četnost návštěv jednotlivých uživatelů atd. Výstup aplikace, který obdrží administrátor můžeme vidět na následujícím Obr. 25. Podobný výstup dostane každý registrovaný uživatel s tou výjimkou, že mu nebude zobrazeno menu administrátora. Z tohoto menu má administrátor přehled a rychlý přístup ke správě všech aplikací. Například jedním pohledem zjistí, že na schválení čeká jeden nově zaregistrovaný uživatel, a to tak, že položka schválení je v menu zobrazena tučně a číslovka za pomlčkou znázorňuje počet zatím neschválených uživatelů.



Obr. 25 Administrátorské rozhraní.

17.3 Fórum

Jedním z nejlepších způsobů, jak získat informace, je se jednoduše zeptat. Za tímto účelem je na webovém serveru spuštěno fórum s možností živých diskusí. Na vývoji takto rozsáhlé aplikace se spoustou nejrůznějších funkcí se podílí již celá skupina lidí, a proto jsem použil nejrozšířenější řešení v podobě phpBB fóra. Jde o velice oblíbený, bezplatný a open-

source systém pro vytvoření interaktivního fóra, který využívá také jazyk PHP a podporuje širokou škálu databázových systémů, jako MySQL, PostgreSQL, MSSQL, Microsoft Access. V mém případě byl použit systém MySQL. PhpBB fórum nabízí širokou paletu funkcí a tím splňuje veškeré požadavky, které jsou na dnešní fóra kladeny. Velkou výhodou je obrovská komunita uživatelů, kteří poskytnou bezplatnou podporu, modifikace a styly. Velkým plusem je i mezinárodní podpora, včetně české (phpBB.cz) a překlady do více než 50 jazyků světa, všechny aktualizované podle poslední verze. Jeho vývojáři se mohou pochlubit tím, že mají největší mezinárodní podporu ze všech internetových systémů pro fóra.

17.4 Galerie fotografií

Tato aplikace má za úkol i nezkušeným uživatelům snadno, rychle a efektně umožnit prezentaci svých fotografií a podělit se tak o ně s přáteli. Jedná se o veřejnou galerii přístupnou z lokální sítě. Na jednoduchost obsluhy ze strany uživatele byl kladen důraz od počátků vývoje. Výsledkem je, že i nezkušený uživatel zvládne prezentovat své fotografie v této galerii a jediné co musí zvládnout, je připojení na FTP server, se kterým mu případně pomůže návod.

17.4.1 Nahrání fotografií

Na serveru je spuštěný FTP server, který po přihlášení daného uživatele umožní přístup pouze do složky určené pro fotografie. Jediné, co tedy uživatel musí zvládnou je připojit se na tento server a zde umístit své fotografie. O všechno ostatní se aplikace už postará sama.

17.4.2 Generování náhledů a menu

Menu galerie se vytváří automaticky a je generováno dynamicky podle obsahu daného adresáře s fotografiemi.

Pří výběru položky z menu mohou nastat tři situace:

1. Vybraná galerie je otevřena poprvé.

   V tomto případě je nejprve nutné vygenerovat náhledy a fotografie v požadovaném rozlišení. Velikost rozlišení výsledných obrázků můžeme snadno nastavit v konfiguračním souboru aplikace. Adresář může obsahovat mnoho fotografií a jejich zpracování by serveru trvalo dlouho a došlo by k násilnému přerušení prováděného skriptu a nekompletního vygenerování obrázků. Tento problém je vyřešen tím, že

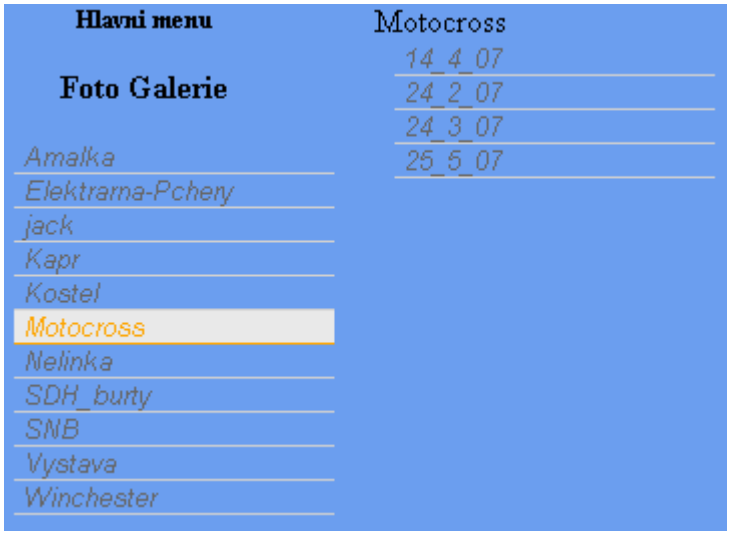
skript zpracovává pouze jeden obrázek a po jeho dokončení předá provádění dalšímu skriptu s dalším obrázkem. Takto zaručíme, že dojde ke korektnímu vygenerování všech náhledů. Aplikace rozpozná i nově přidané fotografie a při návštěvě dané galerie chybějící náhledy automaticky vygeneruje.

2. Vybraná galerie obsahuje podadresáře.

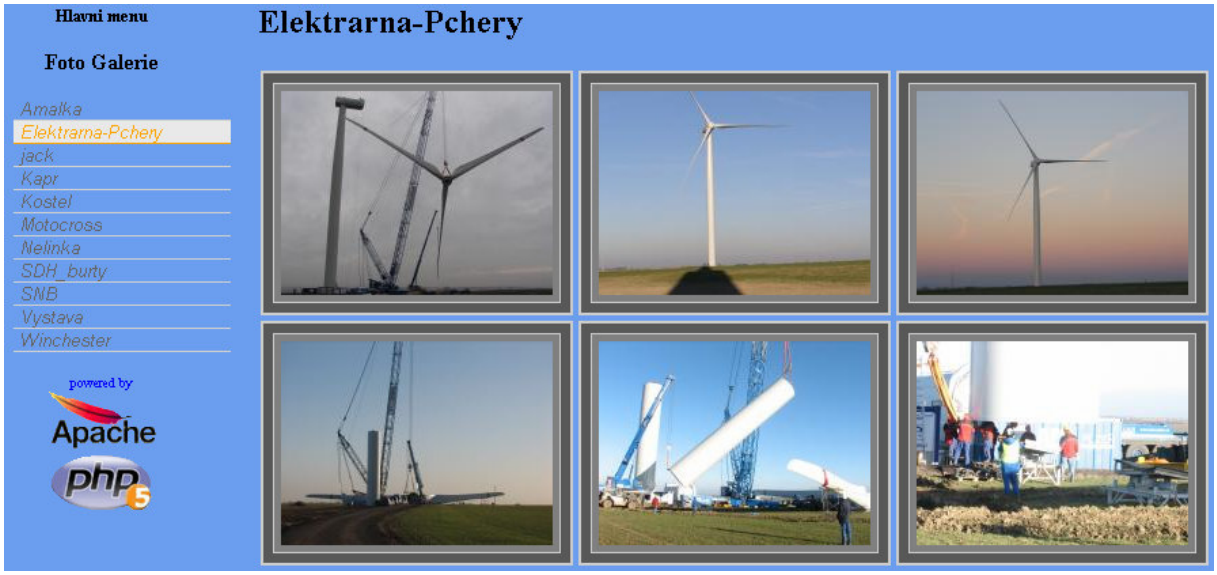
   V tomto případě aplikace zjistí, že zvolená složka neobsahuje fotografie, ale adresáře a jejich strukturu vygeneruje a zobrazí s možností volby. Jak ukazuje Obr. 26.

3. Zvolená složka obsahuje fotografie a náhledy jsou vygenerovány.

   V tomto případě se uživateli zobrazí náhledy zvolená složky a může si fotografie prohlížet. Ukázka na Obr. 27.



Obr. 26 Vygenerované menu s podadresáři.



Obr. 27 Ukázka náhledů foto galerie.

17.4.3 Prohlížení galerie

Po vybrání položky z menu a kliknutí na vybraný náhled se fotografie efektně rozvine do plné velikosti. Toho je docíleno za použití funkcí javaskriptu. Pro pohodlné prohlížení je možné listovat přímo mezi fotografiemi v plné velikosti.

Do galerie je implementována možnost prohlížení obrázků za pomocí aplikace PicLens, které se doinstaluje jako doplněk do prohlížeče. Je k dispozici jak pro Internet Explorer, tak pro Firefox. Tuto možnost prohlížení umožňuje například i vyhledávač google.com. Díky tomuto doplňku se doslova ocitnete ve virtuální galerii a prohlížení fotografií se stane opravdovým zážitkem. Doplněk naleznete na stránce http://www.piclens.com, doporučuji vyzkoušet.

18. Závěr

Tato diplomová práce se dotýká problematiky bezdrátových sítí, především jejich zabezpečení. V dnešní době, kdy stále ceny zařízení klesá, zažívá bezdrátová technologie velký rozmach a mnoho vznikajících sítí je na ní založeno. Snadná dostupnost dává prostor vzniku amatérských sítí, které značně pokulhávají zejména na poli bezpečnosti. Především z tohoto důvodu se snažím naznačit možnosti zabezpečení těchto sítí.

V úvodní teoretické části je stručně popsán síťový model TCP/IP, jednotlivé standardy bezdrátových sítí a v nich používané technologie. Je poukázáno na vážné bezpečnostní nedostatky především u starších bezpečnostních mechanismů. Jsou popsány nové bezpečnostní standardy jako WPA, které nedostatky předešlých mechanismů odstraňují. Jsou rozebrány modely sítí s využitím těchto zabezpečení.

V praktické části jsem navrhl bezdrátovou metropolitní sítí pro dané území, kterou jsem následně realizoval. Do sítě jsem implementoval vhodné bezpečnostní mechanismy, popsané v teoretické části. Především jejich kombinací je dosaženo vytvoření co nejbezpečnější bezdrátové sítě. Získáním dostatečného množství informací a jejich použití v praxi se podařilo vybudovat plně funkční bezdrátovou síť s úrovní zabezpečení odpovídající dnešním požadavkům. V závěru práce se zabývám vývojem webových aplikací, které jednak slouží pro dohled a sledování sítě, tak uživatelům k získávání informací o stavu jejich účtů.

Při realizaci sítě jsem měl možnost porovnal bezdrátové standarty pracující v pásmu 2,4 a 5 GHz. Z uskutečněných měření jsem došel k závěru, že pásmo 5GHz nám poskytuje lepší vlastnosti. Toto pásmo je mnohem méně zarušeno. Na takto realizovaných spojích dosáhneme vyšší přenosové rychlosti a propustnosti. Doba odezvy je výrazně kratší, což je důležité pro aplikace citlivé na zpoždění, jako jsou přenosy zvuku či videa v reálném čase. Na druhou stranu u technologie 2,4GHz je velkým lákadlem cena, kdy dnes pořídíme nejlevnější koncová zařízení v řádech stokorun. Z těchto důvodů je síť optimalizována tak, že využívá obě tyto technologie. Pro páteřní spoje je využito pásma 5GHz. Těchto spojů není velké množství a jsou na kladeny největší nároky z hlediska spolehlivosti a propustnosti. Proto je dobré si připlatit za kvalitní zařízení. Naopak distribuční síť se skládá z velkého množství zařízení, a proto je postavena na levnější technologii 2,4GHz. Její vlastnosti pro připojení klientů se ukázali jako naprosto dostačující.

Tato diplomová práce může sloužit i k výukovým účelům. Při pronikání do oblasti technologií bezdrátových sítí, které v dnešní době zaznamenávají obrovský rozmach. Jako ukázka postupu při návrhu takovéto sítě. Při tvorbě vlastních webových aplikací, kdy se

vývojem jednotlivých programů dostatečně seznámíte s programovacím jazykem PHP. Jazyk PHP je dnes nejvíce rozšířen pro psaní dynamických webových stránek a jeho znalost společně s databázovými systémy a jazykem SQL je velice přínosná.

19. Seznam použité literatury

[1] DOSTÁLEK, L. a KABELOVÁ, A. *Velký průvodce protokoly TCP/IP a systémem DNS*. Praha: Computer Press, 2002. ISBN 80-7226-675-6

[2] DOSTÁLEK, L. a kol. *Velký průvodce protokoly TCP/IP: Bezpečnost.* Praha: Computer Press, 2003. ISBN 80-7226-849-X

[3] ZANDL, P. *Bezdrátové sítě WiFi: praktický průvodce.* Brno: Computer Press, 2003. ISBN 80-7226-632-2

[4] PUŽMANOVÁ, R. *Bezpečnost bezdrátové komunikace: jak zabezpečit WiFi, Bluetooth, GPRS či 3G.* Brno: CP Books, 2005. ISBN 80-251-0791-4

[5] STALLINGS, W. *Cryptography and Network Security: Principles and Praktice.* Upper Saddle River: Pearson Education, 2003. ISBN 0-13-111502-2

[6] GUILLAUME, L. *Bezpečnost Wi-Fi – WEP, WPA a WPA2*. Praha: Software Media, č. 1/2006, s. 14–27. ISSN 1214-7710

[7] IEEE *Std 802.11*, 1999 Edition. IEEE. c1999. Dostupný z WWW: <http://standards.ieee.org/getieee802/download/802.11-1999.pdf>

[8] IEEE *Std 802.11g*, 2003 Edition. IEEE. c2003. Dostupný z WWW: <http://standards.ieee.org/getieee802/download/802.11g-2003.pdf>

[9] 802.1x and EAP-Based Authentication Across Congested WAN Links. Cisco Systems, Inc. c1992–2003. Dostupný z WWW: <http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/authp_an.pdf>

[10] PUŽMANOVÁ, R. *Bezpečnost WLAN podle IEEE* [online]. c2002. Dostupný z WWW: <http://www.lupa.cz/clanky/bezpecnost-wlan-podle-ieee/>.

[11] PUŽMANOVÁ, R. *Bezdrátové lokální sítě WLAN podle IEEE 1,2* [online]. c2002. Dostupný z WWW: <http://www.lupa.cz/clanky/bezdratove-lokalni-site-wlan-podle-ieee-ii/>, <http://www.lupa.cz/clanky/bezdratove-lokalni-site-wlan-podle-ieee/>.

[12] PUŽMANOVÁ, R. *WLAN konečně bezpečné* [online]. c2004. Dostupný z WWW: <http://www.lupa.cz/clanky/wlan-konecne-bezpecne/>.

[13] PUŽMANOVÁ, R. *Bezpečnost WiFi záleží jen na vás* [online]. c2004. Dostupný z WWW: <http://www.lupa.cz/clanky/bezpecnost-wifi-zalezi-jen-na-vas/>.

[14] PUŽMANOVÁ, R. *Jak na bezpečnost Wi-Fi?* [online]. c2005. Dostupný z WWW: <http://www.zive.cz/h/Uzivatel/Ar.asp?ARI=123761&CHID=1&EXPS=&EXPA=>.

[15] PUŽMANOVÁ, R. *Moderní komunikační sítě A-Z*. Computer Press, Brno 2007

[16] KLÍMA, V. *Šifra která míchá karty*. CHIP. Praha: Vogel, 1999. č. 9/1999