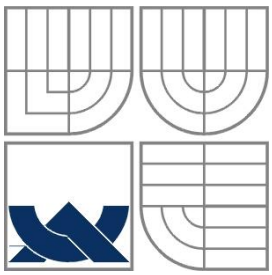
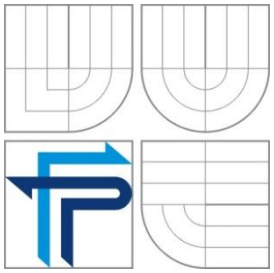


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

BEZPEČNOST BEZDRÁTOVÉ SÍTĚ POSKYTOVATELE INTERNETOVÝCH SLUŽEB

WIRELESS NETWORK SECURITY OF INTERNET SERVICE PROVIDER

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Ing. PAVEL PAROLEK

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Viktor Ondrák, Ph.D.

BRNO 2013

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2012/2013
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Parolek Pavel, Ing.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Bezpečnost bezdrátové sítě poskytovatele internetových služeb

v anglickém jazyce:

Wireless Network Security of Internet Service Provider

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

BARKEN, L. Wi-Fi : jak zabezpečit bezdrátovou síť. 1. vydání. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.
BIGELOW, J. S. Mistrovství v počítačových sítích. Brno: Computer press, 2004. 992s. ISBN 80-251-0178-9.
BURGESS, D. Learn RouterOS. Lexington: Dennis Burgess, 2009. 391 s. ISBN 978-055-7092-710.
SCHWALBE, K. Řízení projektů v IT. 1. vydání. Brno: Computer Press, 2011. 632 s. ISBN 978-80-251-2882-4.
ZANDL,P. Bezdrátové sítě WiFi : praktický průvodce. 1. vydání. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2012/2013.

L.S.

doc. RNDr. Bedřich Půža, CSc.	doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Ředitel ústavu	Děkan fakulty

V Brně, dne 22.05.2013

Abstrakt

Tato diplomová práce se zabývá analýzou stavu bezpečnosti bezdrátové sítě poskytovatele internetových služeb, konkrétně společnosti Net-Connect s.r.o. Identifikuje slabá místa a navrhuje opatření, která vedou ke zvýšení bezpečnosti.

Abstract

This thesis analyzes the wireless network security of the Internet service provider company Net-Connect s.r.o. It identifies its weak points and suggests measures that lead to the increase of the wireless network security.

Klíčová slova

Wi-Fi, 802.11, bezdrátové sítě, ISP, poskytovatel internetových služeb, RADIUS, bezpečnost, 802.1X, WPA2

Keywords

Wi-Fi, 802.11, wireless network, ISP, internet service provider, RADIUS, security, 802.1X, WPA2

Bibliografická citace

Ing. PAROLEK, P. *Bezpečnost bezdrátové sítě poskytovatele internetových služeb*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2013. 73 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

Bezpečnost bezdrátové sítě poskytovatele internetových služeb

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením svého vedoucího diplomové práce. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

……
Ing. Pavel Parolek
25. květen 2013

Poděkování

Rád bych poděkoval vedoucímu mé práce, Ing. Viktoru Ondrákovi, Ph.D. za cenné rady vedoucí k vypracování této práce. Dále bych chtěl poděkovat Ing. Janu Čechovi za technické konzultace ohledně bezdrátových sítích. Nakonec děkuji své rodině a blízkým za morální podporu.

Obsah

1 Úvod

Internetové připojení se pomalu stává nezbytnou a důležitou částí našich životů. Mnozí si bez neustálého přístupu k informační dálnici nedokáží svůj den představit. Internet nás neustále obklopuje a už se s ním nesetkáváme pouze na pracovišti nebo v domácnosti, ale i na veřejných místech jako jsou restaurační zařízení nebo také zastávky metra a vozy městské hromadné dopravy.

Neustále se zrychlující technologický vývoj dalšímu rozšiřování internetu také velmi pomáhá. Dnes již každý mobilní telefon má možnost připojit se k mobilnímu internetu. Jednodušší modely se musí spokojit s GPRS, modely střední a vyšší třídy nabízí připojení přes datové sítě třetích a čtvrtých generací nebo také připojení přes bezdrátové sítě Wi-Fi.

Zvyšováním penetrace internetového připojení mezi uživatele výpočetní techniky také roste riziko útoků a požadavky na zabezpečení. Díky velkému rozšíření bezdrátových technologií zabezpečení musí být důmyslnější než u kabelových sítí. Kabelové sítě fyzickým zabezpečením mohou eliminovat většinu hrozeb. U bezdrátových sítí vysíláme informace vzduchem a nevíme, kdo komunikaci může odposlouchávat. Je tedy nutné zajistit, aby odposlechnutá informace byla útočníkovi k ničemu.

A tím se zabývá tato práce. Zvýšením bezpečnosti bezdrátových sítí poskytovatele internetu, neboť tito poskytovatelé připojují své klienty i na několika kilometrové vzdálenosti, čímž se riziko odposlechu nebo připojení nežádoucího klienta výrazně zvyšuje.

Mnohé sítě lokálních poskytovatelů internetu po bezdrátových sítích vznikaly velmi divoce a rychle a na bezpečnost přenosu dat nebyl dáván velký důraz. I dnes se stačí se zapnutou WiFi kartou v notebooku nebo mobilním telefonu projet vesnicemi a zaručeně nachytáte několik přístupových bodů lokálních poskytovatelů bez zabezpečení přenosu dat, pouze s chatrným zabezpečením přístupu na samotný přístupový bod.

2 Vymezení problému a cíle práce

Má práce se zaměřuje na zabezpečení bezdrátových sítí poskytovatelů internetového připojení, konkrétně na bezdrátovou síť společnosti Net-Connect s.r.o. Cílem je provézt navrhnout taková opatření, která by vedla ke zvýšení bezpečnosti.

Práce zhodnotí jednotlivé možnosti bezpečnostních protokolů bezdrátových sítí, objektivně zhodnotí jejich výhody, nevýhody, složitost implementace a vhodnost použití v síti společnosti Net-Connect s.r.o. Navrhované změny budou prováděny s ohledem na stávající systémy společnosti, aby nedošlo k přerušení ani omezení nabízených služeb.

Po zvolení nejvhodnějšího bezpečnostního protokolu práce nastíní implementaci do sítě společnosti. Pokusí se identifikovat jednotlivé kroky, vedoucí k úspěšnému provozu nové technologie. Dále práce definuje rizika, které můžou ohrozit implementaci technologie, omezit provoz na síti společnosti a snížit tak kvalitu nabízených služeb.

V neposlední řadě práce nabídne ekonomické zhodnocení nákladů a přínosů. Pokusí se kvantifikovat veškeré výdaje spojené s implementací navrhované technologie a identifikovat možné přínosy plynoucí z této implementace.

3 Analýza problému a současné situace

3.1 Představení společnosti Net-Connect s.r.o.

Společnost Net-Connect s.r.o. byla založena v roce 2004 a patří mezi významné telekomunikační operátory na jižní Moravě. Mezi hlavní činnosti společnosti patří poskytování internetového připojení, digitální televize a IP telefonie. Tyto služby zákazníkům zpřístupňuje pomocí bezdrátových sítí a v poslední době i výstavbou sítě optických kabelů.

Obrázek 3.1: Logo společnosti Net-Connect. Zdroj: (7)

Společnost má 20 zaměstnanců, přičemž většinu tvoří technici, kteří se starají o výstavbu, údržbu a správné fungování sítě. Společnost řídí dva jednatelé - Ing. Jan Čech a Ing. Ivan Čech.

Firma sídlí v Hodoníně, kde začala budovat svou síť. Z počátku poskytovala své služby výhradně pomocí bezdrátových sítí. O roku 2008 společnost buduje svou metropolitní optickou síť a dnes nabízí připojení k síti přes optické kabely ve většině sídlišť Hodonína.

Obrázek 3.2: Mapa pokrytí optickými přípojkami. Zdroj: (7)

Společnost však nezanevřela na původní řešení bezdrátových sítí a tam, kde se nenachází přípojka k optické síti, jsou klienti připojováni právě přes bezdrátové sítě Wi-Fi. Domovské město Hodonín je pokryté celé bezdrátovým signálem a společnost poskytuje připojení i v těchto dalších obcích - Dolní Bojanovice, Dubňany, Josefov, Lužice, Mikulčice, Mutěnice, Petrov, Ratíškovice, Rohatec, Strážnice, Sudoměřice.

3.1.1 Základní údaje o firmě

Datum zápisu:	27. června 2007
Obchodní firma:	Net-Connect s.r.o.
Sídlo:	Hodonín, Velkomoravská 4036/33A, PSČ 695 01
Právní forma:	Společnost s ručením omezeným
Základní kapitál:	200 000,- Kč

Statutární orgán:

Jednatel: Ing. Jan Čech

Jednatel: Ing. Ivan Čech

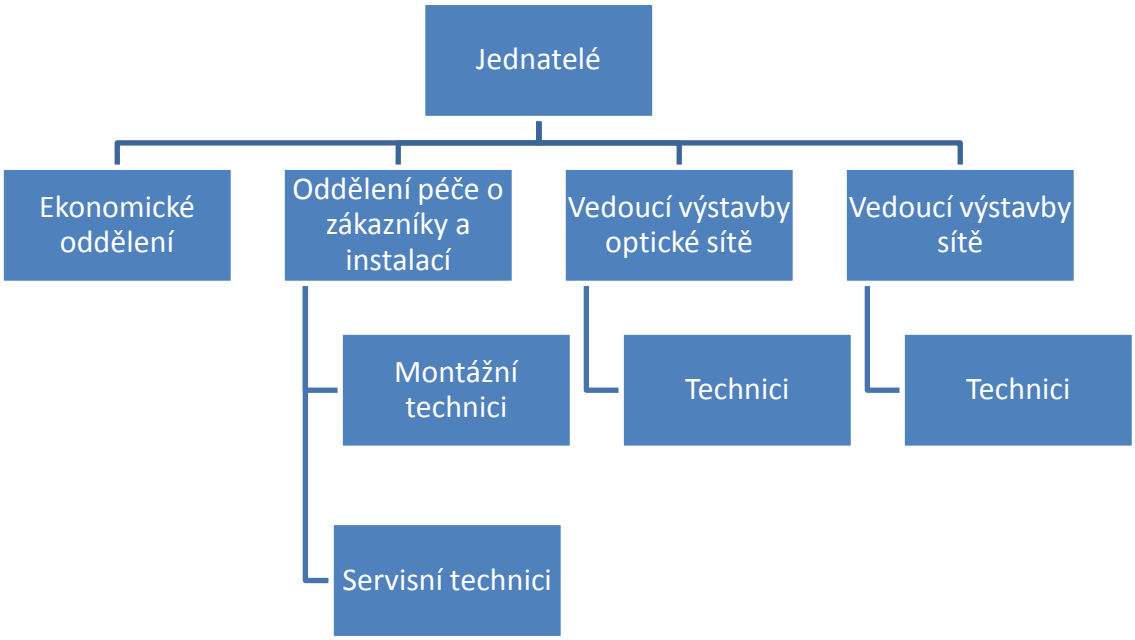
Předmět podnikání v letech 2007 - 2010

- výroba, instalace a opravy elektrických strojů a přístrojů
- specializovaný maloobchod a maloobchod se smíšeným zbožím
- výroba, instalace a opravy elektronických zařízení
- montáž, údržba a servis telekomunikačních zařízení
- výroba, instalace a opravy elektrických strojů a přístrojů, elektronických a telekomunikačních zařízení

Nynější předmět podnikání

- podnikání v elektronických komunikacích
- výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona
- výroba, instalace, opravy elektrických strojů a přístrojů, elektronických a telekomunikačních zařízení
- hostinská činnost

3.1.2 Organizační struktura společnosti



Obrázek 3.3: organizační struktura společnosti Net-Connect s.r.o. Vlastní zdroj.

3.2 Síťová infrastruktura společnosti

Počítačová síť je nejdůležitějším prvkem, na kterém stojí a padá podnikání společnosti. Tato část práce se zaměří na zmapování celé sítě a přiblížení použitých aktivních prvků sítě.

3.2.1 Aktivní prvky bezdrátové sítě

Společnost ve své síti využívá několik různých technologií a produktů od různých společností. Každý produkt má své výhody a nevýhody.

3.2.1.1 Produkty společnosti MikroTik

Lotyšská společnost MikroTik vyvíjí síťová zařízení pro náročná nasazení bezdrátových sítí. Mezi produkty patří základní desky RouterBOARD, které se vyznačují nízkou cenou, vysokým výkonem a výraznou flexibilitou. Tato zařízení obsahují několik MiniPCI portů sloužící pro osazení bezdrátovými kartami dle výběru nasazení.

Velkou devizou je také unixový operační systém RouterOS, který umožňuje obrovské možnosti konfigurace celého zařízení i jednotlivých karet. Přístup k tomuto operačnímu systému je pomocí utility WinBox, která nabízí přehledné grafické rozhraní a možnost nastavení všech potřebných položek.

Operační systém RouterOS nabízí nepřeberné množství funkcí od základního routování, DHCP serveru, firewallu až po pokročilé sledování sítě, omezování P2P provozu a limitace rychlostí jednotlivým klientům. Samozřejmostí je i podpora celé řady bezpečnostních schémat a protokolů. (4)

Společnost Net-Connect s.r.o. hojně využívá produkt RouterBOARD na své bezdrátové přístupové body, prvky páteřní sítě, ale také velmi často jako klientská zařízení. Při použití jako přístupový bod je RouterBOARD osazen bezdrátovými kartami standardu IEEE 802.11a, které jsou pak napojeny na segmentové, nebo všesměrové antény (v závislosti na lokalitě). V drtivé většině jsou použity segmentové antény, aby bylo minimalizováno riziko rušení. Standard IEEE 802.11a nabízí širší využití přenosového pásma, kde na rozdíl od standardu 802.11b lze využít 8 kanálů, aniž by se navzájem zařízení rušila. Toto množství je možné ještě navýšit na dvojnásobek změnou polarizace.

Ve většině případech jsou klienti připojeny k bezdrátové síti zařízením EapBoard, což je klientské zařízení postaveno na RouterOS a RouterBOARD s integrovanou 18dbi anténou. Výjimku tvoří staré klientské stanice nebo části sítě, kterou společnost Net-Connect s.r.o. odkoupila od jiného poskytovatele internetových služeb.

3.2.1.2 Produkty společnosti Alcoma

Společnost Alcoma je významný tuzemský výrobce vysokovýkonných bezdrátových spojů. Nabízí antény o vysokých rychlostech na licencovaných i nelicencovaných mikrovlnných frekvencích.

Antény společnosti Alcoma jsou v síti společnosti Net-Connect využívány v lokalitách, kde není možnost připojit přístupový bod optickým vláknem. Obvykle se používají 10GHz spoje typu bod-bod na vzdálenost několika kilometrů a tyto spoje tvoří významnou část páteřní sítě. Antény jsou pak připojeny k RouterBOARDu s příslušnými kartami.

Obrázek 3.4: Bezdrátové zařízení společnosti Alcoma. Zdroj: (1)

3.2.1.3 Produkty společnosti Ubiquity Networks

Klienti, kteří využívají připojení k bezdrátové síti, jsou vybaveni produkty společnosti Ubiquity Networks a konkrétně zařízením NanoStation5. Toto zařízení pracuje ve standardu IEEE 802.11a, je vybaveno jedním LAN portem, který slouží pro připojení k síti zákazníka, ale i pro napájení technologií POE - Power Over Ethernet.

Zařízení NanoStation5 je vybaveno unixovým operačním systémem s konfigurací přes webové rozhraní a je kompatibilní se všemi moderními bezpečnostními protokoly včetně WPA2-Enterprise.

3.2.2 Používaný software

Společnost provozuje několik fyzických serverů na operačním systému Linux, na kterých běží aplikace potřebné k bezproblémovému chodu sítě. Jedná se o dva DNS servery, emailový server, účetní aplikace a software řídící optickou síť.

3.2.2.1 The Dude

The Dude je volně šiřitelná aplikace vyvíjená společností Mikrotik na zjednodušení správy velkého množství RouterBOARDů v síti. Aplikace umožňuje skenovat síť a identifikovat všechna zařízení společnosti Mikrotik v síti. Díky tomu dokáže vytvářet interaktivní mapu sítě a umožňuje pomocí této mapy zjednodušený přístup k jednotlivým zařízením.

Aplikace také umožňuje komplexní monitoring sítě a hromadný update zařízení. Společnost Net-Connect s.r.o. tento software využívá k detekci a reportingu výpadků prvků sítě. Když aplikace zjistí, že některé zařízení sítě není dostupné nebo má potíže, upozorňuje pracovníka pohotovosti zprávou SMS. Tím je zajištěna rychlá reakce při poruše.

3.2.2.2 Produky společnosti EasyTV s.r.o.

Společnost EasyTV s.r.o. nabízí širokou škálu produktů pro správu služeb a sítě. Společnost Net-Connect s.r.o. využívá několik produktů.

EasyTV IPTV MiddleWare

Tento modul se stará o správu uživatelské databáze a její nahrávání do lokálních databází zařízení RouterBOARD, pomocí kterých jsou pak autentizovány klientské stanice. Tato databáze obsahuje nastavení parametrů sítě pro klientská zařízení.

EasyTV VoIP Server

Modul poskytující telefonní služby pomocí sítě internet. Tento modul umožňuje řídit telefonní stanice u zákazníků a nastavovat parametry a oprávěnění telefonních přístrojů pomocí webového rozhraní.

EasyTV Billing a CRM modul

Modul fakturaci a pouštění služeb zákazníkům. Je provázán jak s účetní aplikací Pohoda, tak s modulem MiddleWare a hlídá včasné platby zákazníků, případně přidání nového zákazníka. Pokud zákazník zmešká platbu, modul mu upraví nastavení služby tak, že zákazníka přesměruje na stránky s upomínkou.

EasyTV Network Manager

Aplikace sloužící ke správě sítě. Společnost Net-Connect s.r.o. ji využívá na kompletní správu optické sítě.

3.3 Zabezpečení bezdrátové sítě společnosti

3.3.1 Fyzické zabezpečení

Fyzické zabezpečení přístupových bodů a dalších aktivních prvků sítě je realizována pomocí zamykatelných skříní, ve kterých jsou všechny aktivní prvky kromě antén. Vzhledem k častému umístění těchto aktivních prvků do velmi špatně dostupných lokalit, obvykle se jedná o střechy budov, toto zabezpečení dostačuje.

3.3.2 Zabezpečení přístupu klientů k přístupovému bodu

Komunikace mezi klientskou stanicí a sítí společnosti je nutné stanici klienta připojit k přístupovému bodu. Protože komunikace probíhá výhradně bezdrátově pomocí standardu IEEE 802.11a a není možné fyzicky zakázat přístup, je nutné klientské stanice určitým způsobem identifikovat.

Tato identifikace probíhá pomocí MAC adresy klientského zařízení. Každý přístupový bod má vlastní databázi – Access List – autorizovaných MAC adres, kterým

umožňuje se připojit. Každé zařízení klienta má dále nastavenu statickou IP adresu. Přístupové body nemají zapnutý server DHCP na automatické přiřazování IP adres.

Na základě MAC a IP adresy je klientské zařízení ověřeno a povolen přístup do sítě. Nastavení parametrů sítě pro zařízení klienta je uloženo v Access Listu v jednom z páteřních RouterBOARDů. Údaje v těchto Access Listech spravuje modul EasyTV IPTV MiddleWare – drží si vlastní databázi a tu pak nahrává do Access Listů klíčových RouterBOARDů.

3.3.3 Zabezpečení přenosu mezi klientem a přístupovým bodem

Z principu bezdrátového přenosu dat nelze fyzicky omezit přístup k přenášeným informacím – každý, kdo je v dosahu, může poslouchat. Proto je vhodné přenášené data šifrovat pomocí některého bezpečnostního protokolu.

Bohužel společnost Net-Connect s.r.o. žádný takový protokol nevyužívá a data mezi klientskou stanicí a přístupovým bodem putují nezabezpečeně a je tedy na klientovi samotném, aby svůj přenos nějak zabezpečil.

3.4 Shrnutí zjištěných skutečností

Společnost Net-Connect s.r.o. provozuje velmi rozsáhlou bezdrátovou i optickou datovou síť s velkým počtem klientů. Správa této sítě probíhá centrálně pomocí několika softwarových aplikací a je velmi efektivní. Malým nedostatkem je roztroušená databáze autorizovaných MAC adres klientských stanic, která může způsobit zmatek v nastavení přístupu klientských stanic.

Velkým nedostatkem je ale absence šifrování bezdrátového přenosu dat mezi zařízením klienta a přístupovým bodem. Tímto se síť stává výrazně zranitelná a útok na ni nebo na data klienta není vůbec náročný.

4 Teoretická východiska práce

4.1 Bezdrátové sítě obecně

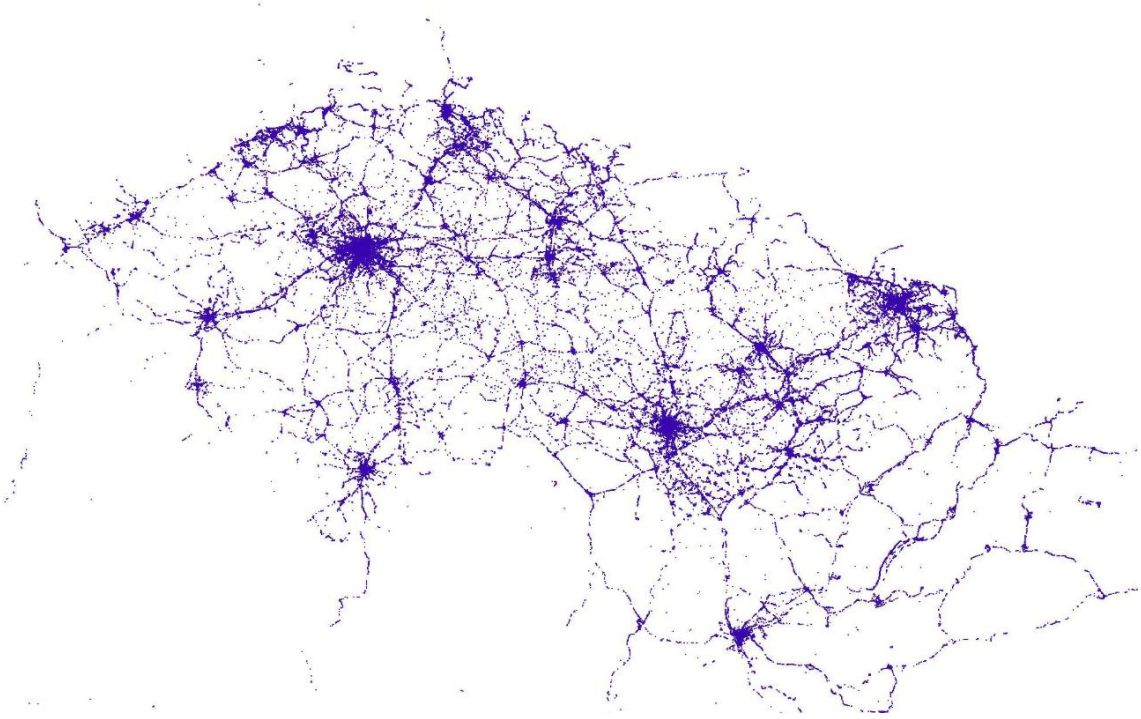
Bezdrátové sítě jsou velmi široký pojem. Mohou být velmi malé - pouze dva komunikující prvky, nebo také komplexní s několika tisíci prvky. Vzhledem k tomu, že tyto rozsáhlé bezdrátové sítě byly budovány pozvolna a oblasti IT jde technologický vývoj velmi rychle kupředu, mohou v sobě kombinovat několik různých technologií pro bezdrátový přenos informací.

Příkladem se nabízí bezdrátová síť mobilních operátorů. Velmi komplexní s několika desítkami tisíc vysílačů (BTS - base transceiver station) a několika milióny připojených klientů současně. Nabízené služby se však liší od lokality a technického vybavení vysílače. Jako příklad může sloužit dostupnost datových sítí třetích a čtvrtých generací.

V domácích podmínkách pak bezdrátovou síť představuje router s anténou, do kterého jde kabel od internetu a ke kterému jsou připojené notebooky, tablety nebo také mobilní telefony bez použití kabelů. Taková lokální bezdrátová síť obvykle obsahuje pouze jeden přístupový bod, pokrývá malou plochu a připojuje velmi malý počet klientů

Tato práce zabývá třetím typem bezdrátových sítí a to jsou rozsáhlejší bezdrátové sítě, pokrývající několik obcí a čítající několik desítek vysílačů a několik tisícovek klientů. Tyto sítě se nejčastěji používají k poskytování internetových služeb.

Česká republika je v tomto směru velmi specifická. 48% domácností je k internetu připojeno právě díky těmto lokálním poskytovatelům internetu. V Evropě je toto naprostý unikát. (5)



Obrázek 4.1: mapa pokrytí ČR Wi-Fi sítěmi. Zdroj: (5)

4.2 Typy bezdrátových sítí

Tato část práce specifikuje typy bezdrátových sítí a rozděluje je podle oblasti pokrytí a použité technologii

4.2.1 Osobní bezdrátová sít

Osobní bezdrátová síť (WPAN - wireless personal area network) pokrývá velmi malou plochu a slouží k přenosu datově nenáročných informací. V minulosti se k tomuto účelu používalo infračervených paprsků. Díky nízké přenosové rychlosti a hlavně nutnosti přímé viditelnosti vysílače a přijímače se tato technologie byla tato technologie vytlačena a nahrazena technologiemi Bluetooth, která pracuje v rádiovém pásmu 2,4GHz. (15)

Tato technologie nevyžaduje přímou viditelnost a zařízení mohou komunikovat až na vzdálenost 10 metrů bez externí antény. Obvykle slouží k připojení pouze velmi omezeného počtu klientů.

Příklady použití: bezdrátové handsfree sluchátka, přenos dat mezi počítačem a mobilním telefonem, periferie k počítači - myši, klávesnice, reproduktory, herní ovladače atd.

4.2.2 Lokální bezdrátová síť

Používanější zkratka pro tuto síť je WLAN - wireless local area network. Jedná se o velmi rozšířený typ bezdrátové sítě. Má dosah několika desítek metrů a nejčastější použití je bezdrátové připojení počítačů do jedné sítě a následné připojení do internetu.

Na rozdíl od WPAN tento typ sítě je připraven na vyšší počet klientů (až desítky na jeden přístupový bod) a umožňuje daleko vyšší rychlost datových přenosů v řádu megabajtů za vteřinu. Nejrozšířenější technologie pro tento typ sítě je standard IEEE 802.11 známější pod názvem Wi-Fi. Tento standard je pak dále v práci specifikován.

4.2.3 Bezdrátová síť typu mesh

Méně známý typ bezdrátové sítě se skládá z mnoha rádiových vysílačů. Každý vysílač přeposílá data v závislosti na ostatních vysílačích. Výhoda této sítě je, že pokud nějaký vysílač přestane fungovat, ostatní vysílače upraví směrování dat a ve výsledku tedy k výpadku dat nedojde. Velmi často bývá použitá technologie Wi-Fi (802.11) nebo Bluetooth (802.15) nebo WiMAX (802.16). (23)

Použití této sítě je například v armádě, kde velmi často hrozí zničení vysílače. Dále také satelitní síť Iridium nebo nízkonákladové počítače programu One Laptop per Child fungují na tomto typu sítě.

4.2.4 Metropolitní bezdrátová síť

Metropolitní bezdrátová síť je rozlehlá síť a může pokrývat pokrývající i celá města. Obvykle se skládají z několika menších sítí, které jsou pak spojeny páteřní linkou, která umožňuje přenášet velké množství dat v řádech gigabytů až terabytů za vteřinu.

Právě tento typ sítě je nejčastěji používán lokálními poskytovateli internetu. Takové společnosti vybudují síť přístupových bodů po celém městě nebo obci a k těmto bodům pak připojují své klienty. Technologie používané u koncových klientů jsou

nejčastěji některé verze standardu 802.11. Donedávna převládala 802.11g pracující v pásmu 2,4GHz, dnes je však nejrozšířenější standard 802.11a (pásmo 5GHz) a rozšiřuje se i nový standard 802.11n, který dokáže pracovat v pásmech 2,4GHz i 5GHz a nabízí tak výrazně vyšší přenosové rychlosti.

Páteřní spoje jsou pak realizovány bezdrátovými technologiemi pracující na frekvencích 10GHz a výš. Pokud to lokalita umožňuje, páteřní spoje jsou budovány optickými kabely, které výrazně zvyšují kvalitu přenosu i dosahované rychlosti.

4.2.5 Bezdrátová síť typu WAN

WWAN neboli Wireless Wide Area Network je bezdrátová síť, která je velmi rozsáhlá a pokrývá území několika měst až krajů. Často dochází ke kombinování různých technologií k dosáhnutí nejlepší kvality přenosu dat a nejvyšších rychlostí. Pro spojení vzdálených bodů se používají výkonné směrové parabolické antény namísto všesměrových antén u menších sítí. U těchto sítí je také rozšířené použití aktivních nebo pasivních retranslačních stanic, které pouze tvoří most mezi dvěma vzdálenými body.

4.3 Topologie bezdrátových sítí

Existuje několik síťových topologií, které vznikly současně se vznikem kabelových datových sítí. Existují topologie sběrnicová (bus), kruhová (ring), hvězdicová (star), stromová (tree) a mesh (částečný nebo plný). Ale pouze několik topologií má své použití v bezdrátových sítích.

4.3.1 Topologie typu mesh

Topologie typu mesh pro bezdrátová sítě byla původně vyvinuta pro vojenské účely. Ale neustále snižující se náklady na vysílače umožnily rozšíření této topologie i mimo vojenskou oblast. Nízké náklady na výrobu také umožnily modularitu uzlů - uzly mohou být vybaveny několik karet pro různé kmitočty a funkce. (16)

Jak již bylo řečeno, sítě typu mesh se skládají z několika navzájem propojených uzlů/vysílačů. Pokud je každý uzel spojený s každým uzlem, jedná se o plný mesh.

Pokud některý uzel nedokáže navázat přímé spojení s jiným uzlem sítě, jedná se o částečný mesh.

Výhodou této sítě je automatická konfigurace sítě a tím také spolehlivé směrování mezi uzly. Tato automatická konfigurace také zajišťuje připojování nových uzlů do sítě a vytvoření nových směrovacích cest v případě výpadku některého uzlu. Mesh síť je také schopná identifikovat trasu, která výrazně zatěžuje přenosové pásmo a díky tomu upravit směrování tak, aby se tomuto místu přenos vyhnul. (10)

Bezdrátovou síť na této topologii je možné postavit na technologii WiMAX (standard IEEE 802.16) nebo v budoucnu na standardu IEE802.11s, který je momentálně v přípravě.

4.3.2 Hvězdicová topologie

Jedná se o nejrozšířenější topologii. Klienti jsou připojeni k centrálnímu přístupovému bodu (AP, hub, switch). Ten pak zajišťuje komunikaci mezi jednotlivými klienty. Svůj název tato topologie dostala díky vzhledu připojených stanic, který připomíná hvězdici.

Tato topologie je stejná jak u kabelové sítě, tak u bezdrátové sítě, a sdílí většinu výhod a nevýhod. Výraznější nevýhoda u bezdrátové implementace této topologie může být zarušení bezdrátového pásma a snížení kvality přenosu dat.

Mezi výhody patří velmi jednoduchá implementace. Nevýhodou je, že při selhání centrálního přístupového bodu sít kompletně zaniká a klienti připojení na tento přístupový bod přestanou mít přístup ke službám sítě.

4.3.3 Stromová topologie

Jak již název topologie napovídá, jedná se o propojení síťových zařízení připomínající strom. Svou podstatou vychází z hvězdicové topologie a rozšiřuje ji o možnost propojení koncových přístupových bodů mezi sebou s jasnou hierarchií. Koncové hvězdy pak mohou představovat konkrétní patra budov, nebo u bezdrátových sítí přístupové body na domech a k nim připojení klienti, spojení mezi koncovými body pak páteřní linky s vysokou rychlostí přenosu dat.

Tato topologie se hojně používá jak v menších lokálních sítích, tak u rozlehlejších metropolitních sítí a to díky velmi jednoduché škálovatelnosti, snížení počtu kabelů a při selhání jednoho prvku síť nezaniká. Při poruše jsou připojená síťová zařízení pouze od části sítě, kde porucha vznikla.

V bezdrátových sítí je tato topologie velmi oblíbená z důvodů snadného zvýšení pokrytí signálem - do kanceláře se přivede jeden ethernetový kabel, na jehož konci se dá bezdrátový přístupový bod a celá kancelář má přístup k sítí. U poskytovatelů internetu rozšiřování dostupnosti je podobné jen s tím rozdílem, že přístupové body mohou být mezi sebou také propojeny bezdrátově.

4.4 Specifikace bezdrátových sítí IEEE 802.11

IEEE 802.11 je několik standardů bezdrátových sítí v pásmech 2,4, 3,6 a 5 GHz. Tyto standardy byly vytvořeny a jsou spravovány organizací IEEE - Institute of Electircal and Electronics Engineers (česky Institut pro elektrotechnické a elektronické inženýrsví).

První verze tohoto standardu byla zveřejněna v roce 1997 a finalizována v roce 1999. Dnes je však tento standard zastaralý a nahradily ho modernější verze. Původní standard počítal s dvěma přenosovými rychlostmi a to jedním nebo dvěma megabity za vteřinu a komunikoval ve frekvenčním pásmu 2,4 GHz. Frekvence zůstala, ale rychlost se několikanásobně zvýšila.

Původní standard specifikoval tři technologie fyzické vrstvy:

- infračervený přenos
- FHSS - Frequency-hopping spread spectrum
- DSSS - Direct-sequence spread spectrum

Přenos dat v infračerveném spektru se příliš neujal a nahradil ho standard organizace IrDA. V dnešní době se již nepoužívá ani jedna implementace infračerveného přenosu dat.

FHSS technologie spočívá v metodě přeskakování mezi několika frekvencemi. Má definováno 79 kanálů ve frekvenčním pásmu 2,4 GHz. Každý kanál má šířku 1 MHz a přeskakuje minimálně 2,5 krát za vteřinu. (8)

DSSS každý bit určený k přenosu nahradí určitou početnější skupinou bitů. Tato redundance zajistí rozprostření signálu do širší části frekvenčního pásma a signál získá na odolnosti vůči rušení. (6)

Přehled standardů IEEE 802.11

Standard	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva
původní IEEE 802.11	1997	2,4	2	DSSS a 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	2009	2,4 nebo 5	600	MIMO OFDM
IEEE 802.11y	2008	3,7	54	
IEEE 802.11ac	2013	5	1000	MU-MIMO OFDM
IEEE 802.11ad	2014	2,4 , 5 a 60	7000	

Tabulka 4.1 - Přehled standardů IEEE 802.11 (11)

Jak je však vidět z tabulky přehledu standardů, technologie fyzických vrstev se rozšířila o technologie OFDM - Orthogonal Frequency Division Multiplexing a o MIMO - Multiple-input Multiple-Output.

OFDM spočívá na širokopásmové modulaci využívající kmitočtové dělení kanálu. Signál je vysílán na několika frekvencích (stovky až tisíce). Frekvence jsou vzájemně ortogonální, což znamená, že maxima každé nosné se překrývají s minimy ostatních. Datový tok je pak rozdělen na stovky dílčích datových toků. (18)

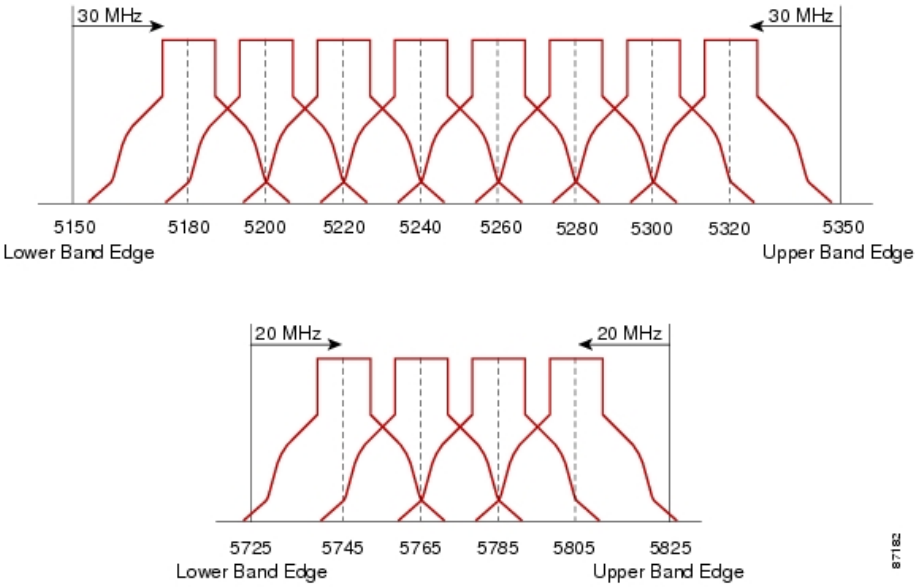
A poslední technologie MIMO spočívá ve více vstupech a více výstupech. K tomuto je zapotřebí několika antén, využívá se i odrazů signálů a zpoždění těchto signálů. (17)

4.4.1 IEEE 802.11a

IEEE 802.11a nebo také IEEE 802.11a-1999 je dodatek ke standardu IEEE 802.11, který přidává vyšší datovou propustnost. Maximální teoretická rychlost dosahuje až 54 megabitů za vteřinu za použití frekvenčního pásma 5GHz.

Standard využívá OFDM modulaci, která byla pak také použita standardem 802.11g ve frekvenčním pásmu 2,4GHz a proto obě specifikace sdílí přenosovou rychlost.

Původně tento standard popisoval 12/13 vzájemně se nepřekrývajících kanálů – 12 pro použití uvnitř budov, 4/5 z dvanácti pro použití ve venkovních prostorách pro spoje na dlouhou vzdálenost. Některé státy však toto pásmo rozšířily o kanály ze standardu 802.11h a tím se zajistily dalších 12/13 kanálů. Stejně jako u 802.11b/g se může lišit povolení vysílat na některých kanálech. V tomto případě jsou však rozdíly příliš velké, a proto je zde nebudu vypisovat. Tyto restrikce si hlídají sami výrobci, a tak by se nemělo stát, že koupíme produkt, který vysílá i v zakázaných kanálech. (12)



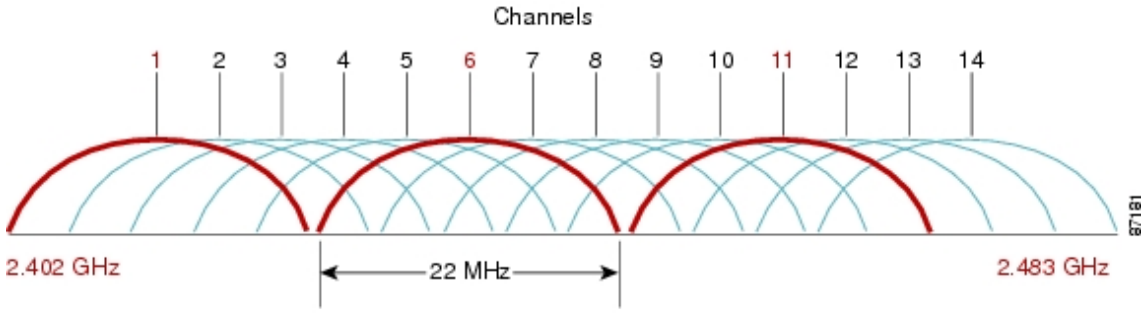
Obrázek 4.2: Rozprostření kanálů ve frekvenčním spektru standardu 802.11a. Nahoře evropská norma, dole americká. Zdroj: (24)

Vysoká pracovní frekvence 5GHz zapříčiňuje vysokou náchylnost na fyzické překážky, a proto je tento standard nevhodný pro použití v uvnitř budov. Na druhou stranu použití ve venkovních prostorách je velmi vhodné z důvodů nízkého zarušení 5GHz pásma. V současnosti poskytovatelé internetu přes bezdrátové sítě hojně využívají tento standard a úplně upustili od standardů pracující na frekvenci 2,4GHz.

4.4.2 IEEE 802.11b

IEEE 802.11b je jedním z prvních dodatků standardu IEEE 802.11. Výrazným zlepšením bylo navýšení maximální rychlosti z dvou megabitů na jedenáct megabitů za vteřinu za použití stejného frekvenčního pásma 2,4GHz. Díky tomuto zlepšení se tento standard masově rozšířil do celého světa pod obchodním názvem Wi-Fi.

Tento standard oproti původnímu návrhu pracuje pouze s DSSS modulací. Tato modulace zapříčiňuje využití velké části přenosové rychlosti na prevenci chyb a rušení. Tímto se maximální využitelná rychlost pro uživatele snižuje na 5 Mbps.



Obrázek 4.3: Rozprostření kanálů ve frekvenčním spektru standardu 802.11b. Zdroj: (24)

Standard počítá s provozem několika oddělených bezdrátových zařízení v jedné lokalitě. Je tedy vyčleněno celkem 14 pracovních kanálů, na kterých mohou tato zařízení komunikovat, aniž by docházelo k výpadkům komunikace. Problém nastává v případě, že jsou pracovní kanály dvou zařízení nastaveny příliš blízko.

Pracovní kanál má šířku 22MHz, ale jednotlivé kanály jsou od sebe vzdáleny pouze 5MHz, a proto se jednotlivé kanály překrývají. Pokud jsou tedy v lokalitě zařízení nastaveny na blízké kanály, navzájem se budou rušit a bude docházet k automatickému snižování rychlosti z 11 na 5,5 na 2 a nakonec na 1Mbps.

Dosah signálu záleží na použitých anténách. Uvnitř budov s všesměrovou 5dbi anténou lze dosáhnout i 20 metrů. Pro venkovní použití se velmi často připojovaly antény typu Yagi nebo sítové parabolické antény. Tyto antény mohly mít zisk i přes 20dbi a zvýšit tak dosah až na několik kilometrů.

4.4.3 IEEE 802.11g

Tento dodatek vznikl v roce 2003 a je zpětně kompatibilní se standardem 802.11b. Pracuje ve stejném frekvenčním pásmu 2,4GHz a při nižších rychlostech využívá stejnou modulaci jako 802.11b.

Došlo však k výraznému navýšení maximální přenosové rychlosti na 54Mbps změnou modulace na OFDM. Tato modulace je použita při rychlostech nekompatibilní se standardem 802.11b. (13)

Modulace opět spolkne určitou část přenosové rychlosti a proto tento standard dosahuje maxima okolo 20Mbps (asi 2,5MBps). Díky obrovské rozšířenosti tohoto standardu někteří výrobci bezdrátových zařízení vyvinuli vlastní modifikace tohoto standardu a navýšili tak teoretickou rychlost až na 100Mbps. V reálném nasazení se však tyto modifikace neujaly zvlášť kvůli vzájemné nekompatibilitě mezi jednotlivými výrobci.

Ještě v nedávné době byl tento standard jednoznačnou volbou pro poskytovatele internetu bezdrátovým připojením, kde klientské stanice byly připojeny zařízeními pracující právě na tomto standardu. Z důvodu vysokého zarušení frekvenčního pásma 2,4Ghz se ale i od toho standardu upouští a nahrazuje jej standard 802.11a nebo 802.11n.

Zařízení standardu 802.11b,g jsou však stále velmi populární a našly své místo v domácnostech, kancelářích, restauracích a v dalších lokalitách, kde je snaha připojit klientská zařízení do sítě na krátkou vzdálenost.

4.4.4 IEEE 802.11n

Nejmladší ze standardů, který vznikl v roce 2009. Opět výrazně navyšuje maximální datovou propustnost a to až na teoretických 600Mbps. Dále se zvyšuje i teoretický dosah uvnitř budov a to až na 300 metrů. Standard pracuje na frekvencích 2,4GHz a 5GHz.

Takto velké rychlosti a vzdálenosti jsou dosaženy spojením dvou nepřesahujících kanálů do jednoho a implementace MIMO technologie. Tato technologie používá několik antén pro několikanásobný příjem/vysílání. Spoléhá přitom na odražené signály, které dorazí až po přijetí signálu v přímé viditelnosti. Tyto odražené signály jsou ve specifikacích 802.11a/b/g brány jako rušení a snižují kvalitu přenosu.

Tento standard také počítá se zpětnou kompatibilitou starších zařízení. Zařízení standardu 802.11n jsou kompatibilní se zařízeními standardů 802.11a, 802.11b a 802.11g. Kombinovat však tyto zařízení se nedoporučují a pro maximální využití kapacit standardu 802.11n se doporučuje nasazovat zařízení pouze do frekvenčního pásma 5GHz. Toto pásmo má mnoho nepřekrývajících se kanálů a není tak výrazně zarušeno jako pásmo 2,4GHz. (14)

V minulých letech se začaly objevovat zařízení tohoto standardu, i když standard nebyl schválen a byl pouze v návrhu (draft). Tyto zařízení obvykle dosahovala teoretických rychlostí 150-300Mbps a pracovala na frekvenci 2,4GHz.

Dnes je standard plně schválen a zařízení, které ho využívají, jsou nasazována nejen do domácností a kanceláří, ale také jako přístupové body poskytovatelů internetu.

4.4.5 IEEE 802.16 - WiMAX

Tento standard nepatří pod rodinu standardů IEEE 802.11, vzniká však paralelně s ním a slouží jako jeho alternativa.

WiMAX neboli Worldwide Interoperability for Microwave Access je bezdrátová technologie zaměřená na venkovní prostory. První verze byla publikována v roce 2002 a definovala frekvenční pásma a přenosové rychlosti. Standard počítá jak s licencovanými frekvenčními pásmy - 3,5, 10,5, a 2,5-2,7GHz, tak s nelicencovanými - 5,7-5,8GHz.

Původní maximální dosahovaná rychlost byla až 134Mbps s dosahem 40-70 km za přímé viditelnosti obou vysílačů. Tato rychlost však klesá na 70Mbps standardem 802.16a a ruší nutnost přímé viditelnosti.

Použití tohoto standardu je široké. Může sloužit jako poskytování přístupu k internetu, bezdrátová kabelová televize nebo také páteřní spoje. V současné době se uvažuje o zařazení standardu WiMAX do mobilních datových sítí čtvrté generace, přičemž cena implementace je nižší než u sítí 3D, HDSPA nebo xDSL. (22)

4.5 Zabezpečení bezdrátových sítí

Bezpečnost bezdrátových sítí je velmi obsáhlé téma. Je tomu tak, protože z důvodů absence fyzické kabeláže je přenosové médium (vzduch) přístupné komukoliv v dostatečné vzdálenosti. Nelze tedy fyzicky zajistit nepřístupnost komunikaci nežádoucím uživatelům. Lze však informace přenášené vzduchem šifrovat řadou algoritmů a odmítnout komunikaci neautorizovaným klientům s vysílačem. Tato kapitola pojednává o nejběžnějších možnostech zabezpečení jak komunikace, tak samotného přístupu.

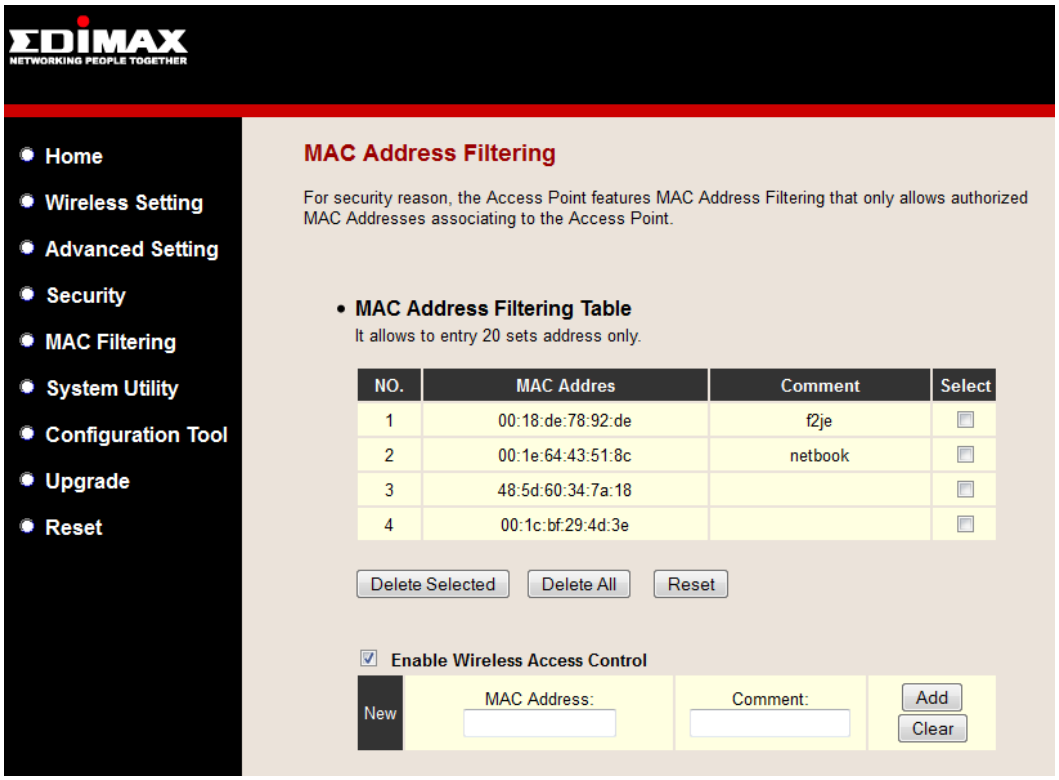
4.5.1 Filtrování MAC adres

Nejjednodušší a také nejstarší bezpečnostní schéma je filtrování klientů na základě jejich MAC adres. Každé síťové rozhraní (bezdrátové i drátové) má unikátní identifikátor, který se nazývá MAC adresa - Media Access Control.

Tato adresa se skládá z šesti skupin, každá obsahující dvouciferné hexadecimální číslo. Skupiny jsou odděleny pomlčkami nebo dvojtečkami a celá MAC adresa tedy může vypadat takto: 00:18:de:78:92:de. Z této adresy (z první dvou skupin) lze například vyčíst výrobce síťového rozhraní. (2)

Protože v teorii má každé síťové rozhraní unikátní MAC adresu, lze řídit přístup k síti jenom pomocí těchto adres. Na přístupovém bodu se vytvoří databáze MAC adres klientů, kteří mohou mít přístup k síti. Při pokusu o připojení klienta k přístupovému

bodu se provede ověření, jestli se MAC adresa klienta nachází v této databázi. Pokud ano, přístupový bod umožní komunikaci, pokud však není, připojení klienta zamítne.



Obrázek 4.4: ukázka nastavení povolených klientů na základě MAC adres. Vlastní zdroj.

Vážným nedostatkem tohoto bezpečnostního schématu je absence šifrování samotného přenosu dat mezi klientem a přístupovým bodem. Útočníkovi pak pouze stačí pasivně "poslouchat" přenos mezi autorizovaným klientem a přístupovým bodem, zachytat dostatečné množství paketů, až v některém z nich nalezne MAC adresu ověřeného klienta.

Jakmile je získána tato adresa, útočník nastaví své bezdrátové rozhraní tak, aby vystupovalo s touto odcizenou MAC adresou. Přístupový bod nic nepozná, protože útočník se identifikoval adresou, kterou má ve své databázi povolených adres a útočníkovi povolí přístup do sítě.

Dnes se toto bezpečnostní schéma využívá pouze výjimečně a pokud se využívá, tak v kombinaci s některou šifrovací technologií - WEP nebo WPA/2.

4.5.2 WEP

Dalším bezpečnostním schématem je WEP - Wired Equivalent Privacy. Název sice naznačuje, že se jedná o bezpečnost na úrovní kabelových sítí, ale skutečnost je dnes jiná a tuto formu zabezpečení je útočník schopný prolomit během několika minut.

Bezpečnostní schéma WEP je založeno na šifrování přenosu pomocí symetrické šifry RC4. Jak klient, tak přístupový bod znají šifrovací klíč (10 nebo 26 hexadecimálních číslic), pomocí kterého je přenos šifrován. Protože je klíč známý oběma stanicím, mohou obě strany snadno komunikovat.

Navázání komunikace probíhá tak, že klient vyšle požadavek o autentizaci přístupovému bodu. Přístupový bod odpoví klientovi a pošle klientovi nešifrovaný text s požadavkem o zašifrování. Klient tento text zašifruje pomocí šifrovacího klíče a odešle zpět přístupovému bodu, který zprávu rozšifruje. Protože přístupový bod vygeneroval prvotní nešifrovaný text, tak může porovnat, jestli klient má stejný šifrovací klíč. (2)

Jak bylo uvedeno v úvodu, i toto bezpečnostní schéma lze lehce prolomit. Útočníkovi opět stačí, aby pasivně poslouchal komunikaci mezi klientem a přístupovým bodem a zachytával datový přenos. Tyto data pak analyzuje speciální aplikací a pokud je zachycena dostatečně dlouhá komunikace (až gigabyte), aplikace během několika málo minut zjistí šifrovací klíč.

Dříve bylo toto bezpečnostní schéma velmi populární v kombinaci s filtrací MAC adres a i dnes je velmi hojně využíváno v domácích podmínkách i přes jeho výrazné nedostatky. Odborná veřejnost se však shoduje a nedoporučuje toto zabezpečení používat.

4.5.3 WPA/WPA2

WPA - Wi-Fi Protected Access - je odpověď na nedostatky WEP. Bezbečnostní schéma vzniklo v roce 2003, o rok později byla vydána nová verze v podobě WPA2, která první verzi rychle nahradila. Obě verze sou navzájem kompatibilní, ale dnes se používá výhradně druhá verze.

První verze WPA používá stejně jako WEP šifrování RC4, ale implementuje protokol TKIP - Temporal Key Integrity Protocol. Tento protokol zajišťuje dynamickou

změnu šifrovacího klíče pro každý vysílaný paket. WPA2 nahrazuje šifrování RC4 šifrováním CCMP založené na AES šifrování. (3)

Distribuce šifrovacích klíčů

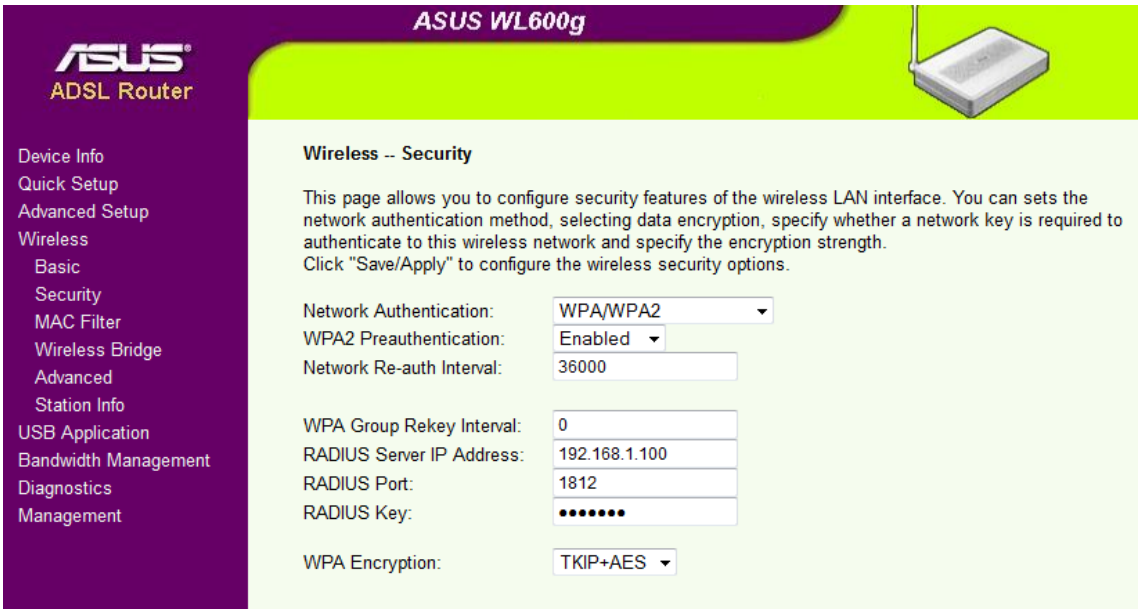
Toto bezpečnostní schéma nabízí umožňuje nasazení jak v náročném firemním prostředí, tak v malé lokální síti a podle toho zvolit autentizaci uživatelů a distribuci šifrovacích klíčů klientům.

V malých sítích lze využít model WPA2-PSK, kde zkratka PSK znamená Pre-Shared Key, česky tedy předem sdílený klíč. Schéma je podobné jako u autorizace WEP - ověření klienti znají šifrovací klíč a přístupový bod si tuto znalost ověří.

Firemní nasazení a nasazení v rozsáhlých sítích si však vyžaduje pokročilejší správu uživatelů a proto využívá protokolu 802.1X. Tento protokol je rozveden dále.

Použití	WPA	WPA2
Firemní nasazení	Autentizace: IEEE 802.1X/EAP Šifrování: TKIP/MIC	Autentizace: IEEE 802.1X/EAP Šifrování: AES-CCMP
Osobní nasazení	Autentizace: PSK Šifrování: TKIP/MIC	Autentizace: PSK Šifrování: AES-CCMP

Tabulka 4.2: Přehled typů zabezpečení ve WPA/WPA2 (21)



Obrázek 4.5: Nastavení zabezpečení WPA2 pro firemní nasazení na přístupovém bodě. Vlastní zdroj.

4.5.4 IEEE 802.1X

Tento protokol slouží k zabezpečení fyzického přístupu do sítě. Byl původně vyvinut pouze pro kabelové sítě ethernet, ale jeho implementace našla své místo i v bezdrátových sítích. U velkých kabelových sítích je obtížné získat fyzickou kontrolu nad každou ethernetovou zásuvkou, proto byl vyvinut tento protokol.

Jeho fungování pracuje na principu zablokování komunikace při připojení nového zařízení, dokud se toto zařízení neprokáže identifikačními údaji. Obvykle v podobě uživatelského jména a hesla, které je ověřeno pomocí vzdáleného serveru.

“Ověřování v bezdrátové síti provádí přístupový bod pro klienty na základě jejich výzvy, pomocí seznamu nebo externího autentizačního systému, založeného na serveru Kerberos nebo RADIUS, Remote Authentication Dial In User Service. Pouze ověřený uživatel má přístup k síti.“ (25) str. 134

Tento protokol je daleko náročnější na implementaci než ostatní bezpečnostní schémata. Pro správné fungování tohoto protokolu je nutné, aby přístupový bod (bezdrátové AP, switch) byl kompatibilní s tímto protokolem. Dále je nutné mít v síti

dostupný některý autentizační server s databází autentizačních a autorizačních dat. Na druhou stranu však tento protokol nabízí nejvyšší formu zabezpečení.

Proces autentizace nového klienta v síti

1. **Inicializace** - přístupový bod nebo switch detekoval nové zařízení a komunikaci na tomto portu (nebo s tímto klientem v bezdrátové síti) nastavuje do stavu "neautorizováno". V tomto stavu je povolená komunikace pouze protokolem EAP a ostatní pakety (TCP/IP, UDP) jsou zahazovány.
2. **Iniciace** - přístupový bod vyšle požadavek na identifikátor nového zařízení. Zařízení odešle své identifikační údaje přístupovému bodu, ten tyto údaje zabalí do RADIUS Access-Request paketu a odešle ho autentizačnímu serveru.
3. **Autentizace** - autentizační server ověří totožnost nového klienta v sítí a odešle výsledek rozhodnutí přístupovému bodu.
    a. Autentizace proběhla úspěšně - ve zprávě o úspěšné autentizaci jsou odesílány také autorizační údaje obsahující celou řadu nastavení spojení mezi přístupovým bodem a klientem a klientovi je povolena komunikace na jiných protokolech. Mezi tyto údaje patří například IP adresa, výchozí brána, adresa DNS serverů, maximální přenosové rychlosti a celá řada dalších údajů.
    b. Autentizace selhala - v tomto případě je klient vyrozuměn o špatných identifikačních údajích a přístupový bod nechává port v neautorizovaném stavu komunikace probíhá pouze protokolem EAP.

V bezdrátových sítích se protokol IEEE 802.1X využívá pro dynamickou distribuci šifrovacích klíčů bezpečnostního schématu WPA2-Enterprisse. Každý ověřený klient komunikuje s přístupovým bodem šifrovaným přenosem s šifrovacím klíčem, který je unikátní pouze pro tuto komunikaci a je časově omezený. Šifrovací klíč vyprší při odhlášení/odpojení klienta od sítě a při novém přihlášení je mu vytvořen klíč nový. (25)

4.5.4.1 RADIUS

RADIUS nebo také Remote Authentication Dial In User Service je síťový protokol umožňující autentizaci uživatelů v počítačových sítích. Vznikl v roce 1991 a používá se u rozsáhlých sítí. V praxi se s ním dalo setkat u vytáčeného telefonního připojení, dnes u připojení k internetu za použití xDSL, datových mobilních sítích a u poskytovatelů internetu bezdrátovou sítí, kde právě uživatelské údaje jsou ověřovány pomocí RADIUS protokolu.

Protokol nabízí centralizované AAA - Authentication, Authorization, Accounting. Česky jde o autentizaci, autorizaci a účtování a umožňuje centrální správu uživatelů přes ověření, zabezpečení a nastavení parametrů služby.

Autentizace slouží k ověření identity nově připojeného klienta do sítě. Pro nové zařízení to znamená předložení identifikačních údajů, které jsou následně zkontrolovány autentizačním serverem. Identifikátor může být v podobě obyčejného jména a hesla, ale dají se použít také digitální certifikátory, čipové karty, data z biometrických snímačů atp.

Autorizace znamená povolení komunikace a přístup k vybraným službám sítě. Tento protokol umožňuje nastavit parametry síťového připojení na základě identifikace uživatele/klienta a mít tak naprosto rozdílné služby na stejné síti.

Zajímavé u tohoto protokolu jsou accountingové data. Přístupový bod pravidelně odesílá tyto data zpět na RADIUS server, který je může archivovat v rozsáhlých databázích. Tyto data pak slouží k monitoringu využití síťových služeb uživatelem a dají se využít na sledování vytížení koncových bodů, identifikaci problémů v síti.

FreeRADIUS

FreeRADIUS je softwarová implementace RADIUS serveru distribuována zdarma pod GPL licencí. Aplikace je aktivně vyvíjena a běží na celé řadě unixových operačních systémů.

Jedná se o světově nejrozšířenější RADIUS aplikaci hlavně z důvodů obrovské modularity a možnostem nastavení. Velkou výhodou je také možnost ověření uživatelů ve velkých databázových systémech jako je SQL a velké možnosti nastavení šifrovacích protokolů.

4.6 Útoky na bezdrátové sítě

Útoků na bezdrátové sítě je celá řada a není radno je podceňovat. U bezdrátových sítí je obrovská nevýhoda v téměř nemožnému fyzickému zabezpečení přístupu útočníka k přenosovému médiu, kterým putuje signál. Lze tedy předpokládat, že útočník není ve svém útoku příliš časově omezen. Útoky lze rozdělit do dvou kategorií: pasivní a aktivní.

4.6.1 Pasivní útoky

Jak už název napovídá, tento typ útoků je neinvazivní a spočívá na poslouchání komunikace v bezdrátové síti. Útočník je obvykle vybaven notebookem se speciální distribucí unixového operačního systému vybaveného aplikacemi právě na síťové útoky.

Útok začíná umístěním útočníka s notebookem do takové lokality, aby nebyl příliš rušen a byl v dosahu zvolené bezdrátové sítě. Pak už jen spustí aplikaci na zachytávání odposlechnutých paketů a čeká, až nachytá dostatečné množství dat. Tyto data pak analyzuje jinou aplikací.

Doba analýzy záleží na typu použitém šifrování a dostupném výpočetním výkonu. Například u zabezpečení typu WEP je nalezení hesla otázkou několika málo vteřin při zachycení dostatečného množství dat (100MB až 1GB).

Analýza paketů šifrování WPA2 je daleko náročnější na výkon a donedávna se považovala za neprolomenou ochranu. Dnes je známo několik útoků a dokonce existují webové aplikace, které nabízejí nalezení hesla ze zachycené počáteční komunikace mezi ověřeným klientem a přístupovým bodem.

Těmto útokům se lze velmi obtížně bránit protože, nevyžadují žádnou aktivní interakci se sítí. Jedinou obranou je nasazování neustále nových bezpečnostních technologií.

4.6.2 Aktivní útoky

Tyto útoky se vyznačují tím, že útočník aktivně komunikuje se sítí, na kterou útočí. Může tak dělat z důvodů zjištění existence bezpečnostních opatření, vynucení

přístupového bodu ke komunikaci a zachycení této komunikace, nebo k úplnému odstavení přístupového bodu. Aktivních útoků je několik typů.

Denial of Service

Je útok, který znemožní komunikaci přístupového bodu s klienty nebo narušení běhu celé sítě. Výsledek tohoto útoku není přístup do sítě, ale zablokování komunikace v síti. V bezdrátových sítích se tento útok realizuje instalací silnějšího vysílače, který zahltí frekvenční pásmo silnější nesmyslným signálem a klient přes tento šum přístupový bod "neuslyší".

Útok typu man-in-the-middle

Tento útok spočívá ve vytvoření přístupového bodu, který se tváří jako zabezpečená síť a čeká na připojení ověřeného klienta. Tento klient se pokusí přihlásit k falešnému přístupovému bodu svým identifikátorem. Falešný přístupový bod tento identifikátor přepošle pravému přístupovému bodu a přemostí komunikaci mezi klientem a pravým bodem.

Cílem tohoto útok může být zachycení komunikace mezi klientem a pravým přístupovým bodem. Protože datový přenos jde přes falešný přístupový bod, útočník má neomezený přístup k datovému toku. Dalším cílem může být pouze získání identifikačních údajů k síti.

5 Vlastní návrh řešení

Tato část práce se zabývá výběrem nejhodnějšího řešení problému a návrhu implementace tohoto řešení. Jak bylo v analytické části práce zjištěno, společnost nepoužívá žádný bezpečnostní protokol při přenosu dat mezi zařízením klienta a bezdrátovým přístupovým bodem. Toto představuje výrazné bezpečností riziko jak pro zákazníky společnosti, tak pro samotnou síť společnosti.

5.1 Výběr technologie

Každý bezpečnostní protokol má své výhody a nevýhody. Je proto nutné každý protokol prozkoumat, zda je vhodný pro nasazení v síti společnosti Net-Connect s.r.o.

Z možných bezpečnostních protokolů navrhují zvolit zabezpečení WPA/WPA2 v režimu WPA-Enterprise. Toto řešení vyžaduje investici do autentizačního serveru a zdlouhavou migraci klientských stanic na nový bezpečnostní schéma. I přes to se však jedná o nejlepší možnost zabezpečení jak přístupu, tak přenosu dat.

Dále je nutné zabezpečit samotný proces autentizace a autorizace bezdrátového klienta. Toto bude zajištěno zahrnutím protokolu MPPE (Microsoft Pont-to-Point Encryption) do nastavení autentizačního serveru. Tento protokol používá RSA RC4 šifru k zabezpečení přenosu autentizačních a autorizačních paketů v protokolu PPPoE.

5.2 Hardwarové požadavky

Všechna zařízení sítě společnosti Net-Connect s.r.o. podporují navrhované bezpečnostní schéma, proto je není nutné nahrazovat novými. Jedinou chybějící položkou je autentizační server, který je nutno pořídit. Z důvodů redundance budou pořízeny dvě totožné stanice. V případě selhání jedné by hrozilo omezení služeb klientům.

Společnost provozuje několik fyzických serverů s mnoho službami. Servery jsou postavené na platformě Linux a nevyužívají virtualizaci operačních systémů. Z toho důvodu je nutné pro autentizační server zakoupit novou fyzickou stanici. Předejde se tak

omezení prostředků stávajících služeb, nebo kompletní odstavení serveru při selhání instalace nebo případné nekompatibility aplikací.

Volba padla na produkt společnosti Lenovo s označením ThinkServer TS200v (SPP18EU) v následující konfiguraci:

Procesor	Intel Core i3-540 (4MB Cache, 3,06 GHZ)
Operační paměť	2 GB DDR3-1333MHz
Pevný disk	SATA 500GB, 7200RPM
Základní deska	Intel x3450 chipset, 1xPCIE 16x, 1xPCIE 1x, 2xPCI
Grafická karta	Integrovaná v chipsetu - Intel HD Graphics
Ostatní	10/100/1000Mbit Ethernet, RAID 0 a 1, DVD RW, 10xUSB

Tabulka 5.1: konfigurace serveru.

Tento server nabízí dostatečný výkon pro zvolené řešení za přijatelnou cenu. Společnost Lenovo nabízí k tomuto produktu záruku v trvání tří let, tak se dá očekávat i dlouhý a bezproblémový provoz. Cena produktu z 30.4.2013 je 14 753,- Kč.

5.3 Softwarové požadavky

Navrhované řešení spoléhá na několik aplikací, které vzájemně spolupracují. Jednotlivé aplikace zde budou specifikovány a vysvětlen jejich význam a role.

5.3.1 Platforma Linux

Platformou byl zvolen Linux z důvodů existence serverů postavených na Linux ve společnosti Net-Connect. Zaměstnanci s touto platformou umí pracovat, a proto není nutné je nijak zaškolovat.

Další výraznou výhodou platformy Linux jsou nulové náklady na licenci samotného operačního systému, ale i jednotlivých aplikací. Operační systémy na bázi Linuxu a většina aplikací běžící na tomto operačním systému jsou distribuovány zcela zdarma pro jednotlivce i společnosti pod licencí GNU GPL.

Operační systém Debian GNU/Linux

Linuxová distribuce Debian byla zvolena z důvodů velké rozšířenosti na poli serverů spravující počítačové sítě. Vyznačuje se vysokou stabilitou, kdy operační systém může běžet i několik let bez nutnosti restartu a z toho plynoucí přerušení služeb.

Protože je tato distribuce často používaná pro správu sítě, nabízí širokou řadu aplikací právě pro tento účel. Aplikace jsou distribuovány z některého z centrálních repozitářových serverů a nabízejí několik variant verzí. Pro použití ve společnosti Net-Connect s.r.o. budou používány pouze verze "stable". Toto označení znamená, že se jedná o poslední stabilní verzi aplikace a nejde o vývojovou rozpracovanou verzi, která může být neodladěná a způsobovat potíže.

Verze operačního systému Debian, která bude použita, je označena kódovým jménem "Wheezy" a jedná se o verzi s číslem 7.0. Bude použita 64 bitová verze tohoto operačního systému. Při instalaci bude zvolen pouze operační systém bez nabízených aplikací. Tyto aplikace se nainstalují dodatečně, aby byla zajištěna instalace nejnovější stabilní verze.

5.3.2 Autentizační, autorizační a accountingový server RADIUS

Autentizační, autorizační a accountingový (AAA) server RADIUS bude realizován pomocí aplikace FreeRADIUS. Jedná se o nejrozšířenější aplikaci pro RADIUS server a je hojně využívaná také v akademické sféře včetně sítě eduroam (9).

Aplikace FreeRADIUS nabízí autentizaci, autorizaci a accounting (reporting) uživatelů ve středních i velmi rozsáhlých sítích. Pro účely společnosti Net-Connect s.r.o. se jedná o nejlepší možné řešení. FreeRADIUS nabízí velmi rozsáhlé nastavení a podporuje širokou škálu síťových zařízení díky knihovnám atributů specifických pro výrobce zařízení.

Aplikace umožňuje brát data o uživatelských účtech z mnoha různých zdrojů. Jedná se především o databázové aplikace standardů LDAP nebo SQL, ale také dokáže načíst obyčejné strukturované textové soubory - flat files.

Veškeré nastavení se provádí pomocí editace konfiguračních souborů. Zde se také definují možnosti dodatečného zabezpečení jako například algoritmus šifrování hesel, síťová zařízení, která mají přístup k RADIUS serveru atp. Součástí instalace jsou také skripty pro nastavení databázových systémů. Jedná se o vytvoření tabulek a návazností, aby byla ulehčena instalace.

Bude použita verze aplikace 2.2.0 z 10.9.2012. Tato verze obsahuje nejnovější databáze atribut a vylepšenou stabilitu. (9)

5.3.3 Databáze MySQL

Databázový systém MySQL byl zvolen pro jeho kompatibilitu s aplikací FreeRADIUS. Další výhodou jsou nulové pořizovací náklady - je distribuován pod GNU GPL licencí - a obrovská rozšířenost, která zajišťuje dostatek informací při případných problémech.

Tato aplikace poběží souběžně s aplikací FreeRADIUS na jenom fyzickém serveru a bude obsahovat databázi o klientských stanicích. Bude se jednat zejména o položky:

- Přihlašovací jméno
- Zašifrované heslo pomocí SHA1 algoritmu
- Informace o nastavení síťového přenosu
    - IP adresa
    - Maska podsítě
    - Primární a sekundární server
    - Přenosové rychlosti
- Accountingové data o využívání sítě klientem

Databázi kompatibilní s aplikací FreeRADIUS je nutné vytvořit. To je možné pomocí skriptu, který je součástí instalace aplikace FreeRADIUS. Skript je uložen v souboru s názvem "schema.sql", kdy je nutné tento skript spustit pomocí MySQL.

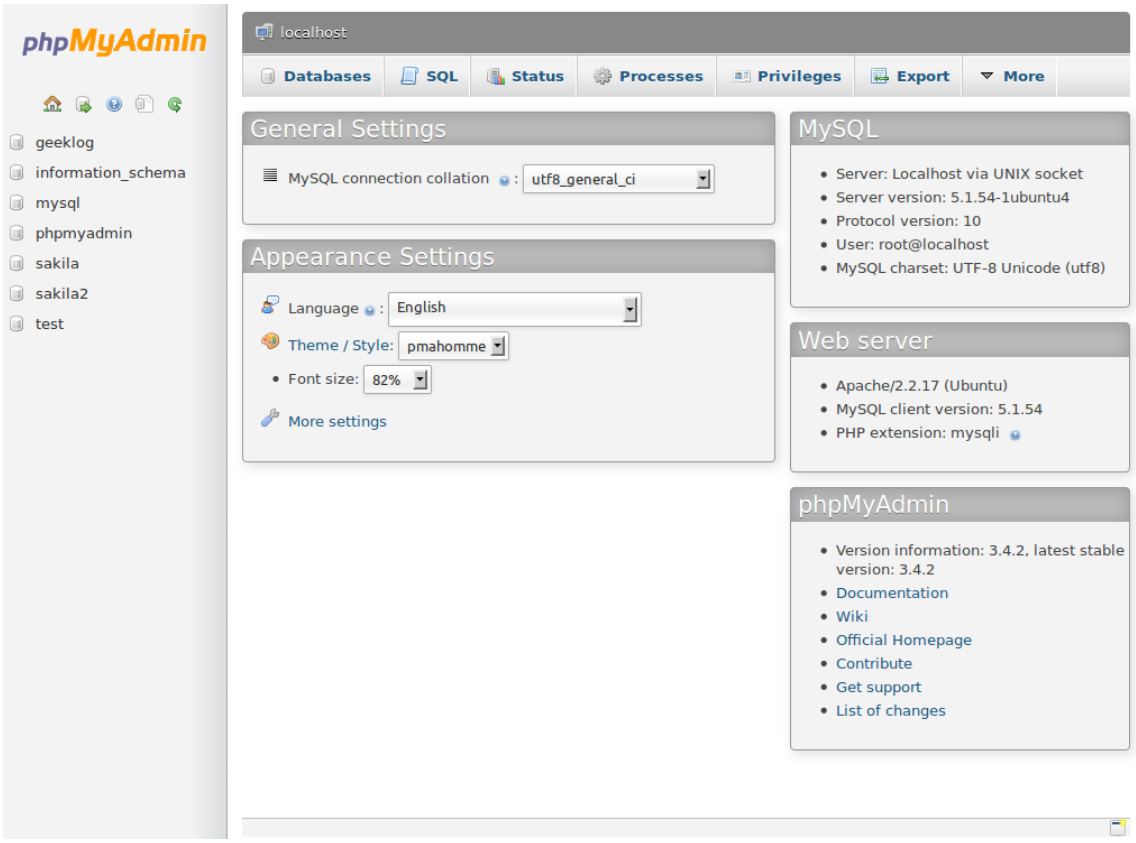
5.3.3.1 Webový server

Pro zjednodušenou správu MySQL databáze je vhodné na fyzický server nainstalovat také HTTP server s nástavbou phpMyAdmin, sloužící právě k přístupu na MySQL server a jeho databáze pomocí webového prohlížeče.

Aplikace pro webový server byla zvolena aplikace Apache ve verzi 2.4.4. Jedná se o nejrozšířenější webový server s aktivním vývojem a lze tedy očekávat bezproblémový provoz. Aplikace je dostupná pod GNU GPL licencí a je tedy poskytována zdarma pro soukromé i komerční účely.

Na tomto webovém serveru poběží nástavba phpMyAdmin ve verzi 3.5.8 z 8.4.2013, která je určena ke komunikaci s MySQL serverem. Uživatel má tak přístup k databázovému MySQL pomocí obyčejného webového prohlížeče, samozřejmě za předpokladu, že má potřebné přihlašovací údaje.

Tím se značně zjednoduší počáteční nastavování MySQL databáze a usnadní se přístup do databáze v případě hledání chyb nebo údržby.



Obrázek 5.1: Screenshot z webového prostředí phpMyAdmin. Zdroj: (19)

5.3.4 Provázání s existujícími systémy společnosti

Společnost Net-Connect s.r.o. v současné době provozuje komplexní a rozlehlou datovou síť, kterou spravuje několika moduly informačního systému a přímým přístupem na aktivní prvky sítě. Aby byl bezpečnostní protokol implementován s co nejnižšími náklady, je nutné zajistit integraci do stávající softwarové struktury společnosti.

5.3.4.1 Informační systémy společnosti

Společnost Net-Connect s.r.o. nyní pro správu své sítě používá produkty společnosti EasyTV s.r.o., konkrétně se jedná o produkty:

- **EasyTV IPTV MiddleWare** - slouží k správě Access Listů na přístupových bodech s nastavením parametrů datového přenosu klientských stanic bezdrátového připojení.
- **EasyTV Billing a CRM Modul** - komunikace s účetním systémem Pohoda a ostatními modulu systému EasyTV. Hlídá včasné placení faktur a omezuje služby při nezaplacení.
- **EasyTV VoIP Server** - správa a poskytování hlasových služeb pomocí protokolu IP.
- **EasyTV Network Manager** - kompletní správa provozu a konfigurace kabelové optické sítě a zařízení na této optické síti.

Pro potřeby implementace navrhovaného bezpečnostního schématu bude nutné zajistit komunikaci modulů EasyTV IPTV MiddleWare a EasyTV Network Manager s databází MySQL. Moduly nabízejí automatickou výměnu dat s externími systémy pomocí strukturovaného textového souboru - flat file.

Tento flat file však není kompatibilní s typem strukturovaného souboru, který dokáže číst aplikace FreeRADIUS. Bude tedy nutné tento flat file konvertovat do příslušného formátu pomocí automatického skriptu, který poběží na serveru. Nabízejí se dvě možnosti realizace:

1. Skript, jehož výstupem bude opět strukturovaný textový soubor, který aplikace FreeRADIUS dokáže načíst.
2. Skript, který výstupní data z modulu EasyTV IPTV MiddleWare automaticky načítá do MySQL databáze.

První řešení je technicky nejjednodušší a pro potřeby řešení dostačuje, jenže neumožňuje sběr accountingových dat a samotné prohlížení dat pro kontrolu by bylo velmi obtížné.

Druhá varianta eliminuje nedostatky první varianty, ale její implementace je o něco náročnější. Obě varianty však vyžadují zásah externí společnosti a vytvoření skriptu a vyšší náročnost druhé varianty je vyvážena lepšími vlastnostmi.

Vytvoření skriptu bude zadáno společnosti EasyTV s.r.o. z důvodů vývoje použitého informačního systému EasyTV. Náklady na práci programátora jsou ve výši 1500,- Kč za hodinu a po konzultaci se společností EasyTV byla náročnosti této implementace odhadnuta na 20 hodin.

Náklady na hodinu práce programátora	1500,- Kč
Náročnost	20 hodin
Celkové náklady	30 000,- Kč

Tabulka 5.2: náklady na vytvoření skriptu pro konverzi dat

Náklady na vytvoření konverzního skriptu byly odhadnuty na 30 000,- Kč, což není zanedbatelná částka. Avšak za tuto cenu společnost Net-Connect s.r.o. dostane fungující a spolehlivou integraci navrhovaného bezpečnostního protokolu do informačního systému společnosti.

Společnost Net-Connect s.r.o. již v minulosti se společností EasyTV s.r.o. podobně spolupracovala ke spokojenosti obou stran, takže se dá očekávat podobně úspěšný průběh implementace navrhovaného řešení.

5.3.4.2 Aktivní prvky sítě

Implementace navrhovaného bezpečnostního protokolu nevyžaduje výměnu aktivních prvků sítě ani update firmwaru (operačního systému) těchto zařízení, protože všechna používaná zařízení v síti společnosti Net-Connect s.r.o. navrhované bezpečnostní schéma plně podporují.

Bude však nutné upravit nastavení jednotlivých koncových přístupových bodů a u všech klientských stanic. Tato operace bude časově velmi náročná a dá se očekávat, že migrace všech klientů na nové zabezpečení bude trvat několik měsíců až rok. Z tohoto důvodu je nutné, aby oba systémy běžely současně a nezávisle na sobě.

Pokud však nastane situace, že koncové zařízení se nepodaří nastavit vzdáleně, je v takovém případě nutný výjezd servisního technika k zařízení a provést nastavení přímo na tomto zařízení.

Společnost Net-Connect s.r.o. má vzdálený přístup ke všem klientských stanicím, a proto může veškeré úpravy nastavení provádět bez nutnosti výjezdu techniků do terénu. Dá se však počítat s určitým počtem zařízení, na které se vzdáleně nepůjde z technických důvodů připojit a výjezd bude nutný.

5.3.4.3 Proces migrace stávajících uživatelů na nový systém

Nejvíce časově náročná činnost navrhovaného řešení je migrace všech klientských zařízení na nový systém. Technicky se nejedná o složité úkony, ale vysoký počet stanic tento proces velmi prodlouží.

Výhodou navrhovaného řešení je možnost provozovat jak starý systém ověřování uživatelů, tak nové bezpečnostní schéma současně a nezávisle na sobě. Je také možné, aby oba systémy běžely na jednom přístupovém bodě a není tedy nutné zřizovat dočasné přístupové body pro klientské stanice, které se nepodařilo úspěšně převést na nový systém.

Samotná migrace bude probíhat vzdáleně. Společnost Net-Connect s.r.o. má vzdálený přístup ke všem klientských stanicím, a proto může veškeré úpravy nastavení provádět bez nutnosti výjezdu techniků do terénu. Dá se však počítat s určitým počtem zařízení, na které se vzdáleně nepůjde z technických důvodů připojit a výjezd bude nutný.

Pracovník společnosti se tedy vzdáleně připojí na zařízení klienta, provede restart, nastaví nové parametry přístupu a znovu restartuje. Je možné, že zařízení klienta je staršího data výroby a potřebuje update vnitřního firmware. To také ověřuje a zajišťuje stejný pracovník. Bezproblémová migrace jedné stanice zabere průměrně deset minut a dá se předpokládat, že takových stanic bude 80%.

U zbylých 20% se očekává vyšší časová náročnost a to z důvodu možného výjezdu technika k samotné klientské stanice, nebo delší konfigurace z důvodů specifických služeb na zařízení. Průměrně u takové problémové stanice stráví 70 minut.

Bezproblémová zařízení	600
Problémová zařízení	1050
Celkem hodin	1650

Tabulka 5.3: časová náročnost migrace uživatelů v hodinách

V tabulce je uvedena odhadovaná časová náročnost samotné migrace uživatelů. Uvažuji s celkovým počtem stanic ve výši 4500, kde jsou zahrnuty i přístupové body.

Na přístupových bodech bude migrace postupovat segmentově. Technický vedoucí určí vybrané přístupové body, na jejichž klientech bude prováděna migrace. Technický pracovník se připojí na přístupový bod, vybere interface a provede konfiguraci na nové bezpečnostní schéma. Pak postupně převede všechny klienty na tomto interfacu na nový systém.

Až jsou převedeny všechny klientská zařízení na tomto interfacu, je zrušeno nastavení starého systému a pracovník pokračuje s migrací s klienty na jiném interfacu. Až takto postupně migruje všechny klienty, označí přístupový bod v dokumentaci jako kompletně migrovaný na nový systém a pokračuje stejným způsobem na jiném bodě.

U klientů, které se nepodařilo převést vzdáleně, nebo u kterých je to nemožné, je nutné zajistit fyzický přístup přímo k zařízení. Technik tak vyjedná schůzku přímo s

majitelem objektu, kde se zařízení nachází, naplánuje výjezd a následně provede migraci na místě.

Migrace bude probíhat za běžného provozu společnosti a samotné nastavování zařízení bude probíhat v dopoledních hodinách. V tuto dobu obvykle nebývá na stanicích žádný provoz a tím se tak minimalizuje možnost nestandardního chování. Dále je pravděpodobné, že v tuto dobu si zákazník nevšimne krátkých výpadků služby při restartu zařízení.

5.3.5 Souhrn

Navrhované bezpečností řešení pro bezdrátovou síť společnosti Net-Connect s.r.o. vyžaduje hardwarové, ale především softwarové úpravy. Nejvýraznější investice do nového zařízení je nákup nového fyzického serveru v ceně přesahující čtrnáct tisíc korun. Další zařízení však není nutné pořizovat ani modernizovat, protože všechny ostatní relevantní aktivní síťové prvky jsou s navrhovaných řešením plně kompatibilní.

Softwarové změny jsou daleko výraznější než hardwarové. Jedná se především o instalaci celé řady aplikací a vývoj skriptu na konverzi dat. Výraznou úsporou nákladů v softwarové části řešení je dosaženo výhradním použitím aplikací distribuovaných pod GNU GPL licencí a tedy zcela zdarma pro osobní i komerční využití.

Výrazným nákladem na softwarovou část řešení je však nutnost vývoje skriptu na automatickou konverzi dat ze stávajícího informačního systému a načítání těchto dat do databáze. Odhadované náklady jsou ve výši třiceti tisíc korun.

Pořizovací náklady na hardware	29 506,- Kč
Pořizovací náklady na software	30 000,- Kč
Celkem	**59 506,- Kč**

Tabulka 5.4: souhrn očekávaných nákladů na hardware a software

Jak je tedy zřejmé z uvedené tabulky, finanční náklady na implementaci bezpečnostního protokolu dosahují výše téměř čtyřiceti pěti tisíc. Není to zanedbatelná částka, ale také to není částka, která by finanční situaci společnosti výrazně zatížila. Za tuto cenu společnost získá vysokou úroveň zabezpečení vlastní sítě pro více než 4 000 klientů, využívající bezdrátové připojení.

5.4 Implementace technologie

Tato část práce se zaměří na jednotlivé činnosti, které je potřeba splnit, aby bylo dosaženo úspěšné implementace bezpečnostního protokolu, spuštění a migrace všech klientských zařízení na tento nový systém. Práce navrhne časový plán projektu a pokusí se identifikovat rizika a opatření vedoucí ke zmírnění dopadu, popřípadě kompletní eliminaci rizika.

5.4.1 Projektový tým

Protože se technologie bude implementovat projektově, je nutné vytvořit projektový tým, určit pravomoce a odpovědnosti. Projektový tým se bude skládat ze zaměstnanců společnosti Net-Connect s.r.o. V projektovém týmu budou následující role:

Vedoucí projektu - Ing. Jan Čech

Vedoucí projektu odpovídá za hladký průběh projektu, splnění všech cílů. Jeho role je plánovací, rozhodovací a koordinační. Dává pokyny členům týmu, zadává a rozděluje úkoly mezi ně. Průběžně kontroluje běh projektu, sleduje rizika a vypracovává opatření vedoucí k jejich eliminace. Odpovídá za finanční i časovou stránku projektu.

Technický vedoucí - Lukáš Stanický

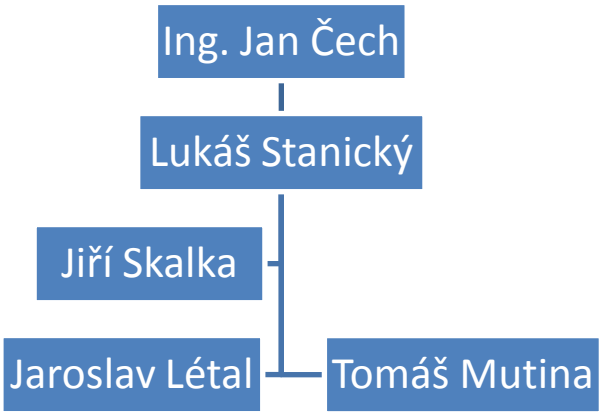
Technický vedoucí odpovídá za splnění technických cílů projektu. Provádí instalaci nových serverů a údržbu stávajících. Zajišťuje implementaci nových technologií do sítě společnosti. řídí tým techniků, zadává jim úkoly a kontroluje jejich práci. Tato role vyžaduje perfektní technické znalosti a přehled na poli informačních technologií a správy sítě.

Zástupce technického vedoucího - Jiří Skalka

Zástupce technického vedoucího má stejné kompetence jako technický vedoucí v případě jeho nepřítomnosti. Dále odlehčuje práci technickému vedoucímu a pomáhá při údržbě stávajících, ale i implementaci nových technologií. I zde jsou vyžadovány rozsáhlé znalosti informační techniky a sítových zařízeních.

Technici - Jaroslav Létal, Tomáš Mutina

Technici vykonávají montážní práce a odpovídají za správnou fyzickou instalaci, ale i nastavení některých zařízení společnosti. Jejich hlavní odpovědností bude však kompletní migrace klientských zařízení ze starého na nový systém.



Obrázek 5.2: Organizační struktura projektového týmu

Projektový tým je tedy pětičlenný a obsahuje vedoucího projektu, technického vedoucího se zástupcem a dva techniky.

5.4.2 Logický rámec projektu

Logický rámec specifikuje hlavní cíle, vedlejší cíle, klíčové činnosti, výstupy projektu, definuje způsoby ověření splnění těchto cílů a nahlíží i na rizika.

Hlavní cíl	**Objektivně ověřitelné ukazatele**	**Způsob a prostředky ověření**	**Předpoklady**
- Zavedení bezpečnostního protokolu do sítě společnosti	- Nemožnost připojení neautorizovaného klienta - Fungující AAA server - šifrovaná komunikace všech klientů	- Test připojení neautorizovaného zařízení - Nahlédnutí do logů serveru - Analýza zachycených paketů	- Technické znalosti projektového týmu - Ochota týmu pracovat na časově náročném úkolu - Dostatek finančních prostředů
Dílčí cíle	**Objektivně ověřitelné ukazatele**	**Způsob a prostředky ověření**	**Předpoklady**
- Pořízení serveru	- Přítomnost serveru v serverovně	- Nahlédnutí do serverovny	- Dostupnost zvoleného produktu u dodavatele
- Nainstalovaný a nakonfigurovaný software serveru	- Fungující server s aplikacemi	- Spuštění aplikací -Přihlášení uživatele na server	- Technické znalosti - Kompatibilita zvolených aplikací
- Provázání stávajícího IS s novým serverem	- Data klientů na novém serveru	- Nahlédnutí do databáze nového serveru	- Externí programátor - Kompatibilita obou systémů
- Provoz serveru na malém úseku sítě	- Logy serveru - Připojení klienti do sítě	- Nahlédnutí do systému přístupového bodu	- Funkční server - Databáze naplněná aktuálními daty
- Kompletní migrace uživatelů na nový systém	- Záznamy starého systému neobsahují připojené klienty	- Nahlédnutí do záznamů starého systému	- Funkční server - Kompatibilita klientů s novým systémem

Výstupy projektu	**Objektivně ověřitelné ukazatele**	**Způsob a prostředky ověření**	**Předpoklady**
- Zabezpečená sít	- Nemožnost připojení neautorizovaného zařízení - Přítomnost šifrování	- Pokus připojit neautorizované zařízení	- Fungující server - Aktuální databáze - Všichni uživatelé na novém systému
- Funkční AAA server	- Ověřování uživatelů	- Pokus o ověření uživatele	- Kompatibilita aplikací a hardwaru s řešením - Aktuální databáze
- Všichni uživatelé migrovaní na nový systém	- Starý systém vypnut	- Nahlédnutí do přístupových bodů	- Funkční AAA server - Aktuální databáze - Kompatibilita zařízení klientů s novým systémem
Klíčové činnosti projektu	**Objektivně ověřitelné ukazatele**	**Způsob a prostředky ověření**	**Předpoklady**
- Plánování projektu	- Projektová dokumentace	- Kontrola projektové dokumentace	- Kvalifikovaný zaměstnanec
- Pořízení serveru	- Přítomnost serveru v serverovně	- Nahlédnutí do serverovny	- Dostupnost zvoleného produktu u dodavatele
- Instalace softwaru na server	- Nainstalovaný software	- Spuštění serveru a aplikací	- Přítomnost serveru - Technické znalosti
- Testování funkčnosti serveru	- Funkční a nakonfigurovaný server	- Test autorizace uživatele přes server	- Nainstalovaný software
- Vývoj a implementace konverzního skriptu	- Funkční provázání stávajícího systému a nového serveru	- Nahlédnutí do databáze nového serveru	- Externí programátor - Kompatibilita obou systémů

- Interní testování funkčnosti systému	- Ověřování fiktivních klientů	- Pokus o ověření fiktivního klienta	- Technické znalosti - Funkční server
- Testování funkčnosti na malém segmentu sítě	- Ověřování reálných uživatelů	- Nahlédnutí do záznamů serveru	- Technické znalosti - Funkční server
- Migrace všech uživatelů na nový systém	- Ověřování uživatelů skrz nový server	- Nahlédnutí do záznamů serveru	- Funkční server - Kompatibilita zařízení klientů

5.4.3 Soupis činností

Projekt implementace nového bezpečnostního protokolu je rozdělen do mnoha dílčích činností. Každá činnost má svůj specifický cíl a osobu odpovědnou za splnění tohoto cíle.

Činnost 1 - Plánování

Cíl: Zpracování kompletního návrhu projektu.

Popis: Plánovací část projektu, kde se navrhne detailní postup plnění projektu a vytvoří se projektová dokumentace, určí se projektový tým, definují se odpovědnosti jednotlivých členů týmu, vytvoří se seznam věcí nutných k pořízení.

Vypracuje: Ing. Jan Čech, Lukáš Stanický, Jiří Skalka

Předpokládané trvání: 2 týdny

Předpoklad čistého času: 21 hodin

Činnost 2 - Pořízení serverů

Cíl: Pořízení serverových stanic s dostatečným výkonem na provoz autentizační aplikace

Popis: Pracovník společnosti provede analýzu nabídky serverových stanic a zvolí nejvhodnější typ pro provoz zvolených aplikací. Tyto servery pak objedná a zajistí včasné doručení do sídla společnosti. Dále servery instaluje do

infrastruktury společnosti a provede zběžné testování technického stavu hardwaru stanic.

Vypracuje: Lukáš Stanický

Předpokládané trvání: 1 týden

Předpoklad čistého času: 2 hodiny

Činnost 3 - Instalace softwaru na server

Cíl: Plně funkční serverové stanice s nainstalovanými a nakonfigurovanými aplikacemi

Popis: Pracovník společnosti nainstaluje na servery operační systém a provede jeho zabezpečení. Dále nainstaluje zvolené aplikace potřebné pro provoz autentizačního serveru. Aplikace důsledně zabezpečí (pokud to aplikace podporuje) a nastaví pro provoz v síti společnosti.

Vypracuje: Lukáš Stanický

Předpokládané trvání: 1 týden

Předpoklad čistého času: 8 hodin

Činnost 4 - Testování funkčnosti serveru

Cíl: Fungující autentizační server ověřující testovací uživatele

Popis: Pracovník společnosti naplní databázi údaji o fiktivních uživatelích a provede test ověřování těchto uživatelů na reálných přístupových bodech. Otestuje všechny možné konfigurace hardwarových zařízeních, které se v síti společnosti Net-Connect s.r.o. nacházejí

Vypracuje: Jiří Skalka

Předpokládané trvání: 1 týden

Předpoklad čistého času: 4 hodiny

Činnost 5 - Vývoj a implementace konverzního skriptu

Cíl: Provázání stávajícího informačního systému EasyTV IPTV MiddleWare s MySQL databází.

Popis: Vedení společnosti Net-Connect s.r.o. kontaktuje společnost EasyTV s.r.o. a zajistí vývoj konverzního skriptu. Programátor společnosti EasyTV s.r.o. pak vytvoří požadovaný skript a následně ho implementuje na server společnosti Net-Connect s.r.o. Dále je ověřeno správné fungování skriptu.

Vypracuje: Zadání práce Ing. Jan Čech, Lukáš Stanický, externí pracovník realizace.

Předpokládané trvání: 2 týdny

Předpoklad čistého času: 4 hodiny

Činnost 6 - Interní testování funkčnosti

Cíl: Ověření funkčnosti autentizačního serveru s reálnými daty bez ohrožení sítě

Popis: Pracovník společnosti otestuje, zda všechny komponenty nového autentizačního systému fungují správně pomocí testovacích klientských zařízení.

Vypracuje: Lukáš Stanický, Jiří Skalka

Předpokládané trvání: 2 týdny

Předpoklad čistého času: 16 hodin

Činnost 7 - Testovací provoz na malém segmentu sítě

Cíl: Ověření funkčnosti autentizačního serveru v reálném nasazení

Popis: Technici výstavby sítě zvolí určitý segment bezdrátové síťové infrastruktury společnosti (jeden až pět koncových přístupových bodů). Na těchto přístupových bodech provedou migraci klientských stanic na nový systém autentizace. Po dobu testování budou sledovat vliv nového bezpečnostního protokolu na stávající síť a fungování autentizačního serveru. Pokusí se odhalit problémy a odstranit je před kompletní migrací klientů.

Vypracuje: Lukáš Stanický, Jiří Skalka, Jaroslav Létal, Tomáš Mutina

Předpokládané trvání: 4 týdny

Předpoklad čistého času: 40 hodin

Činnost 8 - Migrace všech uživatelů

Cíl: Všechna klientská zařízení převést na nový bezpečnostní protokol

Popis: Technici výstavby sítě a servisní technici postupně provedou migraci všech klientských stanic na nový bezpečnostní protokol. U stanic, kde nepůjde vzdálená konfigurace, bude nutné domluvit přístup k zařízení přímo u majitele. Tímto se tato činnost stává nejvíce časově náročnou.

Vypracuje: Jiří Skalka, Jaroslav Létal, Tomáš Mutina

Předpokládané trvání: 60 týdnů

Předpoklad čistého času: 1650 hodin

Činnost 9 - Ukončení projektu a zhodnocení

Cíl: Závěrečné zhodnocení projektu

Popis: Projektový tým vypracuje vyhodnocení projektu a objektivně zhodnotí práce všech zainteresovaných stran, pokusí se identifikovat nevhodné postupy, aby bylo možné se jim vyvarovat v budoucnosti. Projekt se ukončí.

Vypracuje: Ing. Jan Čech, Lukáš Stanický, Jiří Skalka, Tomáš Mutina, Jaroslav Létal

Předpokládané trvání: 1 týden

Předpoklad čistého času: 5 hodin

Jak je tedy vidět, činností je mnoho a každá přímo navazuje na předchozí. Technologicky nejsložitější je činnost 3 - instalace softwaru na server, neboť je nutné všechny aplikace detailně nastavit.

Časově nejnáročnější je pak činnost 8 - migrace uživatelů na nový systém. Je to dáno nutností přístupu na každou stanici klienta a i když se dá většina nakonfigurovat vzdáleně, jedná se o migraci více než čtyř tisíc stanic a několik desítek aktivních prvků sítě. A to všechno za běžného provozu sítě.

Pouze dvě činnosti vyžadují pořízení nového vybavení - nákup serveru (činnost 2) a vývoj konverzního skriptu (činnost 5). Tyto dvě činnosti tvoří investiční náklady nových zařízení ve výši téměř čtyřiceti pěti tisíc korun.

5.4.4 Matice zodpovědnosti

Matice zodpovědnosti zobrazuje přehledně, který člen týmu má jaký úkol vypracovat a kdo které vypracování bude kontrolovat. V matici jsou tyto odpovědnosti označeny písmeny V pro vypracování a K pro kontrolu.

	Ing. Jan Čech	Lukáš Stanický	Jiří Skalka	Tomáš Mutina	Jaroslav Létal
1 Plánování	V/K	V/K	V/K		
2 Pořízení serveru		V	K		
3 Instalace softwaru na server		V	K		
4 Testování funkčnosti serveru		K	V		
5 Vývoj a implementace konverzního skriptu	V/K	V/K			
6 Interní testování funkčnosti		V/K	V/K		
7 Testovací provoz na malém segmentu sítě		V/K	V/K	V	V
8 Migrace všech uživatelů		K	V/K	V	V
9 Ukončení projektu a zhodnocení	V/K	V/K	V/K	V/K	V/K

Tabulka 5.5: Matice zodpovědnosti

5.4.5 Časová analýza

Jak již bylo uvedeno výše, projekt implementace nového bezpečnostního protokolu se skládá z mnoha činností, které na sebe navzájem navazují. Každá činnost má alokovaný určitý časový úsek. Je možné, že cíl činnosti bude splněn dřív, časy jsou odhadované za základě zkušeností s podobným projektem.

5.4.5.1 Harmonogram projektu

Činnost	Týden trvání projektu
	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 ... 70 71 72 73 74
1 Plánování	
2 Pořízení serveru	
3 Instalace softwaru na server	
4 Testování funkčnosti serveru	
5 Vývoj a implementace konverzního skriptu	
6 Interní testování funkčnosti	
7 Testovací provoz na malém segmentu sítě	
8 Migrace všech uživatelů	...
9 Ukončení projektu a zhodnocení	

Tabulka 5.6: časový harmonogram projektu

Z časového harmonogramu je patrné, že časově nejnáročnější činnost bude migrování uživatelů na nový systém, které bude trvat více než rok. Po tuto dobu budou v provozu oba systémy, nový autentizační server i stávající Access Listy na přístupových bodech.

Celý projekt od plánovací fáze po fázi ukončení by měl trval 74 týdnů, což je něco málo přes rok a půl. Přípravné a testovací činnosti zaberou čtrnáct týdnů. Je ale také možné, že se objeví neočekávané problémy s migrací uživatelů a tato fáze bude trvat ještě déle, než se očekává.

5.4.5.2 Časová náročnost jednotlivých činností

Každá činnost je jinak časově náročná a vyžaduje spolupráci několika členů týmu. V předchozí kapitole jsou uvedeny celkové časové náklady na každou činnost, zde jsou v tabulce rozděleny mezi členy týmu podle jejich kompetence a schopností.

Sloupec ostatní shrnuje časové náklady spojené s projektem, ale ne přímo s některou činností. U vedoucího projektu se jedná o kontrolní činnosti, u technického vedoucího zase správu a údržbu serveru a u zástupce o činnosti spojené s nepřítomnosti technického vedoucího.

	Činnosti									ost.	∑
	1	2	3	4	5	6	7	8	9		
Ing. Jan Čech	7				2				1	74	84
Lukáš Stanický	7	2	8		2	10	5		1	74	109
Jiří Skalka	7			4		10	5	250	1	100	377
Tomáš Mutina							15	700	1		716
Jaroslav Létal							15	700	1		716

Tabulka 5.7: Rozdělení časové náročnosti jednotlivých činností mezi jednotlivé členy týmu

5.4.5.3 Milníky

Každý splněný významný cíl projektu je značen milníkem. Tyto milníky tedy označují významnou událost a používají se pro kontrolu postupu projektu a od každého milníku se očekává určitý stav situace. Pro projekt implementace bezpečnostního schématu jsou definovány tyto milníky:

Milník 1

První milník je stanoven na konec druhého projektového týdne. Značí konec plánovacích fází projektu a start implementace technologie. Očekává se, že je vypracovaná projektová dokumentace a vytvořený projektový tým.

Milník 2

Zakončení fáze interního testování je značeno druhým milníkem. Značí stav, kdy má být správně funkční server, provázaný se stávajícím informačním systémem společnosti a správně ověřující uživatele. Server je tedy připravený na reálné nasazení.

Milník 3

Třetí milník je stanoven do 33. týden projektu - ukončuje první třetinu fáze migrace uživatelů na nový systém. V souvislosti s tímto milníkem projektový tým provede zhodnocení své dosavadní práce a pokusí se najít slabá místa.

Milník 4

Poslední milník ukončuje migraci uživatelů. Očekává se, že všichni uživatelé mají nastavená svá zařízení a jejich identitu ověřuje nový systém.

5.4.6 Reporting

Reporting je důležitou součástí projektu a pomáhá sledovat průběh, plnění cílů a práci členů týmu. Zprávy však musí být vypracovávány v určitých intervalech, v dostatečném rozsahu a podle předepsané šablony, aby z nich mohl vedoucí týmu vyvozovat jasné závěry.

V rámci prvních dvou milníků budou reporty vypracovávány buď jednou týdně, nebo při příležitosti zakončení určité činnosti (podle toho, které skutečnost nastane dřív). Tyto zprávy budou obsahovat soupis splněných úkolů a jakým způsobem ke

splnění došlo. Pokud byly provedeny nějaké zásahy do konfigurace aplikací, musí být tyto zásahy také uvedeny se zdůvodněním. Přístupové údaje je také nutno uvádět.

Od začátku migrace klientů budou zprávy vypracovávány při příležitosti kompletní migrace klientů jednoho přístupového bodu. Zprávy budou obsahovat soupis migrovaných klientů včetně typu zařízení. Tento soupis bude rozdělen podle složitosti migrace - jestli se klienta povedlo převést na nový systém vzdáleně a bez potíží, nebo jestli u zařízení musel být použit specifický postup.

Projektový tým své zprávy bude předávat na pravidelných týdenních poradách, kde se shrne dosavadní postup projektem a určí se úkoly na další týden. Zde se budou také diskutovat problémy a požadavky, které vzniknou v průběhu projektu.

5.4.7 Analýza rizik

Tato část práce se zabývá analýzou rizik. Protože se jedná o komplexní projekt, existuje celá řada možných vlivů, které mohou chod projektu ohrozit až úplně zastavit. Budou zde definovány nejdůležitější rizika, dopad rizika na projekt, opatření vedoucí k minimalizaci nebo eliminaci rizika a pravděpodobnost, s kterou můžeme vliv rizika na projekt očekávat. Hodnocení dopadu a pravděpodobnosti je číselně podle následujících kritérií:

Dopad - hodnocení 1 až 10, přičemž 1 znamená minimální dopad na společnost a 10 velmi vážný dopad.

Pravděpodobnost - hodnocení 1 až 10, přičemž 1 znamená nízkou pravděpodobnost výskytu a 10 velmi vysokou.

5.4.7.1 Rizika s důsledky ohrožující chod společnosti

Riziko 1 - Hardwarové selhání serveru

Popis: Některá hardwarová komponenta serveru se porouchá a způsobí zastavení serveru. V takovém případě nově se připojující klienti nebudou puštěni do sítě a již připojení budou postupně odpojováni díky nutnosti pravidelné reautentizace. Selhání serveru způsobí nedostupnost služeb pro všechny klientské stanice po dobu odstávky autentizačního serveru.

Dopad: 10 - nedostupnost služeb, ztráta důvěry klientů, ztráta klientů, vracení poplatků za vedení služby klientům po dobu výpadku.

Pravděpodobnost: 6

Opatření: Duplicitní server se stejnou hardwarovou i softwarovou konfigurací se spustí v případě selhání nebo údržby primárního serveru. Dále zajištění kvalitního hardware serveru, pravidelné údržby stanice, zajištění dostatečného chlazení aby nedošlo k přehřívání komponentů stanice.

Riziko 2 - Nedostupnost klíčového zaměstnance

Popis: Pokud zaměstnanec, který server umí obsluhovat, ze společnosti odejde nebo onemocní, vzniká společnosti riziko v případě poruše serveru nebo nutnosti upravit nastavení serveru.

Dopad: 9 - nedostupnost služeb, nízká kvalita služeb.

Pravděpodobnost: 4

Opatření: Zajistit redundanci znalostí mezi několik zaměstnanců. Ve společnosti musí umět server ovládat vždy alespoň tři lidé. Mít kontakt na společnost, která dokáže údržbu/opravu provést v případě nepřítomnosti žádného klíčového zaměstnance.

Riziko 3 - Nedostatečné zabezpečení autentizačního serveru

Popis: Aplikace nebo samotný operační systém autentizačního serveru nebude dostatečně zabezpečen a nepovolaný uživatel získá přístup k tomuto serveru. V takovém případě by útočník mohl získat data uživatelů, upravovat tyto data nebo celý server vyřadit z provozu.

Dopad: 8 - únik dat klientů třetí straně, omezení kvality služeb, ztráta důvěry klientů, poškození jména společnosti.

Pravděpodobnost: 3

Opatření: Zajištění dostatečné bezpečnosti operačního systému a všech aplikací. Změna přístupových hesel z továrního nastavení, nebo kompletní zakázání vzdálené konfigurace určitých aplikací po prvotním nastavení.

5.4.7.2 Rizika s vážnými důsledky

Riziko 4 - Chybně fungující skript na konverzi dat z informačního systému

Popis: Skript, který slouží k automatickému konvertování dat ze systémů EasyTV do MySQL databáze bude fungovat zcela chybně nebo bude některá data špatně převádět.

Dopad: 7 - nízká kvalita služeb až nedostupnost služeb pro některé klienty nebo segmenty sítě.

Pravděpodobnost: 2

Opatření: Důsledná kontrola fungování skriptu na testovacích datech, ale i reálných údajích. Otestovat veškeré dostupné datové formáty a limity, které se mohou v databázi vyskytnout. Při nalezení chyby kontaktovat společnost EasyTV s.r.o. a vyžadovat opravu.

Riziko 5 - Neúčinnost implementovaného bezpečnostního protokolu

Popis: Implementovaný bezpečnostní protokol nezabrání útočníkům odposlouchávat komunikaci mezi klienty a přístupovými body a/nebo nezabrání připojení nepovoleného zařízení na přístupový bod.

Dopad: 7 - únik dat klientů, ztráta důvěry klientů, poškození jména společnosti

Pravděpodobnost: 1

Opatření: Implementace dalších bezpečnostních protokolů, které ztíží útočníkům přístup k datům.

Riziko 6 - Chybně fungující autentizace reálných uživatelů

Popis: Některé nebo všechny klientské stanice budou vykazovat problémy při autentizaci pomocí RADIUS serveru.

Dopad: 7 - omezení služeb některým klientům, nedostupnost služeb některým klientům

Pravděpodobnost: 2

Opatření: Důsledné testování všech konfigurací síťových zařízení používaných v síti společnosti, odstranění nekompatibilních zařízení, nebo update jejich firmwaru.

Riziko 7 - Nedostatek finančních prostředků

Popis: Společnost nebude mít dostatek finančních prostředků na úhradu navrhovaných investic a tím celý projekt výrazně zbrzdí, nebo také může dojít k jeho úplnému zrušení.

Dopad: 7 - zdržení projektu, zrušení projektu.

Pravděpodobnost: 4

Opatření: Vyčíslení nákladů a zajištění dostatku financí před realizací projektu.

5.4.7.3 Rizika s mírnými důsledky

Riziko 8 - Nedostatečný výkon serveru

Popis: Při provozu autentizačního serveru v reálném nasazení nebude hardware výkonově dostačovat a klienti budou čekat na přihlášení do sítě.

Dopad: 4 - čekání na přístup ke službě.

Pravděpodobnost: 2

Opatření: Zajistit dostatečně výkonný hardware před spuštěním ostrého provozu. Pokud problém nastane až v posledních týdnech projektu, kdy server bude obstarávat více klientů než na začátku, provést upgrade procesoru a operační paměti.

Riziko 9 - Nekompatibilita aplikací

Popis: Aplikace instalované na server spolu odmítnou komunikovat.

Dopad: 5 - prodloužení trvání projektu.

Pravděpodobnost: 1

Opatření: Instalovat pouze aktuální stabilní verze aplikací.

Riziko 10 - Potíže s migrací klientských stanic

Popis: Při postupné migraci stanic uživatelů nebudou schopni pracovníci vzdáleně nastavit stanici, nebo stanice bude vykazovat problémy. Tímto se může trvání činnosti migrace výrazně prodloužit.

Dopad: 4 - nutnost vyjet k zařízení.

Pravděpodobnost: 7

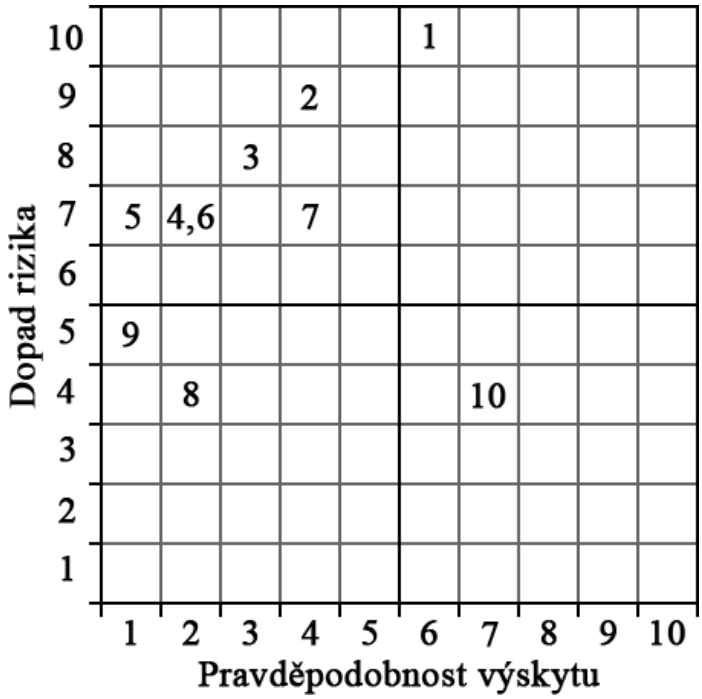
Opatření: Dodržování správného posloupnosti činností, aby nedošlo k znepřístupnění stanice - první nastavit stanice klientů, pak samotný přístupový bod.

Jak je tedy patrné, rizik hrozící tomuto projektu je mnoho. Pro bezproblémový průběh projektu je tedy nutné mít tyto rizika na paměti a důsledně kontrolovat celý průběh projektu. Je nezbytné, aby vedení společnosti se aktivně podílelo na této

kontrole, aby se daly včas identifikovat nastávající problémy a předešlo se tak zbytečným průtahům.

5.4.7.4 Mapa rizik

Mapa rizik nalezená rizika zanáší do grafu tak, že stanovené hodnoty pravděpodobnosti a dopadu rizika tvoří polohu na horizontální a vertikální ose.



Obrázek 5.2: Mapa rizik. Zdroj: vlastní

Jak je tedy z obrázku vidět, v kritické oblasti (dopad vyšší než 5, výskyt vyšší než 5) se nachází pouze jedno riziko a to možnost hardwarového selhání serveru. S tímto rizikem je počítáno a v rámci projektu je implementováno i opatření v podobě redundantní stanice.

V oblasti významných rizik (dopad vyšší než 5, výskyt 5 a menší) se nachází většina nalezených rizik. Tyto rizika nejsou tak pravděpodobná, ale je nutné mít připraven plán opatření v případě, že riziko opravdu nastane.

5.5 Ekonomické zhodnocení

Každá nová technologie přináší určité přínosy za cenu nákladů na implementaci. U některých technologií je množné velmi přesně finančně kvantifikovat jak náklady, tak přínosy. U jiných se obě položky určují jen velmi obtížně. Tato část práce shrne očekávané náklady a přínosy na implementaci navrhovaného bezpečnostního protokolu.

5.5.1 Očekávané náklady

Náklady navrhovaného řešení spočívají v investici do hardwaru a softwaru a mzdových nákladů projektového týmu. Hardwarová investice představuje nákup serverové stanice, která bude sloužit jako autentizační server pro všechny bezdrátové klienty. Není nutné dále investovat do aktivních prvků sítě ani do klientských zařízení, protože stávající navrhovaný bezpečnostní protokol plně podporují.

Další výraznou investicí je vývoj a implementace skriptu, který propojí stávající informační systémy společnosti s databázovým systémem MySQL, který je potřeba k chodu autentizačního serveru. Vývoj tohoto skriptu je nutné svěřit společnosti EasyTV s.r.o., která používaný informační systém vyvíjí a spravuje.

Člen týmu	Hodinové vytížení	Hodinová mzda Kč	Mzdové náklady Kč
Ing. Jan Čech	84	350	29 400,-
Lukáš Stanický	109	300	32 700,-
Jiří Skalka	377	300	113 100,-
Tomáš Mutina	716	250	179 000,-
Jaroslav Létal	716	250	179 000,-
Celkové mzdové náklady projektu			**533 200,-**

Tabulka 5.8: mzdové náklady na projekt

Nejvýraznější položkou jsou však mzdové náklady projektového týmu. Hodinové vytížení každého člena týmu se odvíjí od jeho pozice v týmu, technických znalostech a časové náročnosti činnosti spojené s projektem. Hodinové mzdy členů týmu jsou odhadnuty na základě informací od vedení společnosti.

Očekávané investice na hardware	29 506,- Kč
Očekávané investice na software	30 000,- Kč
Očekávané mzdové náklady projektu	533 200,- Kč
Celkové očekávané náklady	**592 706,- Kč**

Tabulka 5.: souhrn očekávaných nákladů

Tabulka shrnuje očekávané finanční náklady na implementaci bezpečnostního protokolu. Náklady dosahují téměř 600 tisíc korun, což není zanedbatelná částka. Na druhou stranu je nutné si uvědomit, že většinu z těchto nákladů tvoří mzdy členů týmu, kteří jsou zároveň i zaměstnanci společnosti.

Společnost bude tyto náklady hradit ze svých interních zdrojů a nebude využívat žádné úvěrové služby.

Vedle finančních nákladů navrhované řešení vyžaduje mnoho času stávajících zaměstnanců společnosti. Přípravné a testovací fáze zaberou několik týdnů, nejvíce času však spolkne migrace stávajících klientských stanic na nový systém. I když jsou tyto stanice přístupné vzdáleně, jedná se o velký počet zařízení.

5.5.2 Očekávané přínosy

Hlavním přínosem navrhovaného řešení je výrazné zvýšení bezpečnosti sítě společnosti Net-Connect s.r.o. Nyní společnost nevyužívá žádné zabezpečení bezdrátového spojení mezi klientskou stanicí a přístupovým bodem a jenom velmi jednoduché zabezpečení přístupu k samotnému přístupovému bodu a z toho důvodu navrhované řešení výrazně posílí bezpečnost sítě.

Navrhované bezpečnostní schéma zajistí nejlepší dostupnou ochranu jak přenosu, tak přístupu. Eliminuje náhodné a zvědavé útočníky vybavené pouze notebookem s bezdrátovým adaptérem a výrazně znesnadní útoky útočníků se specializovaným vybavením.

Přínosy tohoto řešení bohužel nejsou nijak finančně kvantifikovatelné, neboť nikde přímo nezvyšují příjmy nebo výkon samotné sítě. Lze však s jistotou říct, že navrhovaný bezpečnostní protokol patří k nejlepším možným a je celosvětově využívaný ve velmi rozsáhlých sítích.

Protože je navrhované řešení velmi versatilní a není závislé na typu sítě, může společnost Net-Connect s.r.o. toto řešení použít, když v budoucnu bude přecházet kompletně na optické sítě. Navrhované řešení je také velmi výkonné a dokáže obstarávat i několik desítek tisíc klientů současně. Z tohoto důvodu je také společnost připravena pojmout více klientů bez obav, že bude muset opět nějak měnit bezpečnostní schéma nebo ověřování uživatelů.

6 Závěr

Naše malá země v srdci Evropy je světový unikát na poli internetu poskytovaným pomocí bezdrátových sítí WiFi. Tomuto jevu můžeme děkovat společnosti Český Telecom (dnes O2), která v minulosti nabízela pouze zastaralou datovou ISDN linku a odmítala nabízet datové služby přes ADSL. Zájem o rychlý internet rychle nasytili malí lokální poskytovatelé internetu, kteří datové služby začali nabízet bezdrátově.

Mezi takové poskytovatele patří i společnost Net-Connect s.r.o., která svou síť začala budovat v městě Hodonín. Tyto malé sítě vznikaly velmi divoce bez výrazných bezpečnostních standardů. Většina takových sítí používá nedostatečné formy zabezpečení nebo neřeší bezpečnost vůbec.

Společnost Net-Connect s.r.o. využívá pouze slabé zabezpečení přístupu klientů k přístupovému bodu a již neřeší bezpečnost samotného bezdrátového přenosu.

Cílem této práce bylo navrhnout dostatečně silné zabezpečení bezdrátové sítě s ohledem na vývoj technologií do budoucna a nastínit implementaci takového bezpečnostního schématu.

Navrhovaným řešením je implementace ověřování klientských stanic pomocí serveru RADIUS. Toto řešení výrazně vylepšuje bezpečnost přístupu k síti a také zajišťuje nejlepší možné zabezpečení přenosu dat v bezdrátové síti. Navrhovaný server je také velmi universální a dokáže ověřovat klienty bez ohledu na technologii přenosu. Společnosti proto nic nebrání přesunout správu uživatelů optické sítě pod tento systém a celou správu tak centralizovat.

Samotná implementace pak bere v potaz stávající systémy společnosti Net-Connect s.r.o., a navrhované řešení integruje do něj s co možná nejnižšími náklady. Navrhované řešení je možné provozovat souběžně se stávajícími systémy, a proto nejsou omezeny žádné služby uživatelům.

7 Seznam použité literatury

(1) *AL11F MP360* [online]. 2013. [citováno 11.1.2013]. Dostupný z WWW: <http://www.alcoma.cz/cz/katalog/volne+pasmo/all+outdoor/al11f+mp360/>

(2) Barken,L. *Wi-Fi : jak zabezpečit bezdrátovou síť.* Vyd. 1. Brno : Computer Press, 2004. 174 s. ISBN 80-251-0346-3

(3) BIGELOW, J.S. *Mistrovství v počítačových sítích*. Brno: Computer press, a.s., 2004. 992s. ISBN 80-251-0178-9

(4) BURGESS, D. *Learn RouterOS. Lexington : Dennis Burgess*, 2009. 391 s. ISBN 978-055-7092-710

(5) Čížek J. *Počítačové Česko v číslech* [online]. 2012. [citováno 11.12.2012]. Dostupný z WWW: <http://www.zive.cz/clanky/pocitacove-cesko-v-cislech/sc-3-a-166729/default.aspx>

(6) *Direct-sequence spread spectrum* [online]. 2012. [citováno 29.12.2012]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum>

(7) *Dostupnost* [online]. 2013. [citováno 11.1.2013]. Dostupný z WWW: <http://net-connect.cz/dostupnost>

(8) *FHSS* [online]. 2012. [citováno 29.12.2012]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/FHSS>

(9) *The FreeRADIUS Project* [online]. 2013. [citováno 1.5.2013]. Dostupný z WWW: <http://freeradius.org/>

(10) Hynčica O. *Bezdrátové sítě typu mesh* [online]. 2012. [citováno 28.12.2012]. Dostupný z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=30826>

(11) *IEEE 802.11* [online]. 2012. [citováno 28.12.2012]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/IEEE_802.11 29.12.2012>

(12) *IEEE 802.11a-1999* [online]. 2012. [citováno 30.12.2012]. Dostupný z WWW: <http://en.wikipedia.org/wiki/IEEE_802.11a-1999>

(13) *IEEE 802.11g-2003* [online]. 2012. [citováno 30.12.2012]. Dostupný z WWW: <http://en.wikipedia.org/wiki/802.11g>

(14) *IEEE 802.11n-2009* [online]. 2012. [citováno 30.12.2012]. Dostupný z WWW: <http://en.wikipedia.org/wiki/802.11n>

(15) *Infrared Data Association* [online]. 2012. [citováno 28.12.2012]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Infrared_Data_Association 28.12.2012>

(16) *Mesh networking* [online]. 2012. [citováno 28.12.2012]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Mesh_networking>

(17) *Multiple-input multiple-output* [online]. 2012. [citováno 29.12.2012]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/MIMO>

(18) *Orthogonal frequency-division multiplexing* [online]. 2012. [citováno 29.12.2012]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing>

(19) *phpMyAdmin* [online]. 2013. [citováno 1.5.2013]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Phpmyadmin>

(20) SCHWALBE, K. *Řízení projektů v IT*. 1. vyd. Brno : Computer Press, 2011. 632 s. ISBN 978-80-251-2882-4

(21) ŠUSTR, Matej. *Analýza bezpečnosti štandartu IEEE 802.11*. Diplomová práce. Slovenská technická univerzita v Bratislavě, Fakulta elektrotechniky a informatiky. 2007. vedoucí diplomové práce Ing. Martin Rakús, PhD.

(22) *WiMAX* [online]. 2012. [citováno 30.12.2012]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Wimax>

(23) *Wireless mesh network* [online]. 2012. [citováno 28.12.2012]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Wireless_mesh_network>

(24) *WLAN Radio Frequency Design Considerations* [online]. 2012. [citováno 30.12.2012]. Dostupný z WWW: <http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/RFDesign.html>

(25) Zandl,P.: *Bezdrátové sítě WiFi : praktický průvodce*. Vyd. 1. Brno : Computer Press, 2003. 190 s. ISBN 80-7226-632-2

8 Přílohy

Seznam příloh

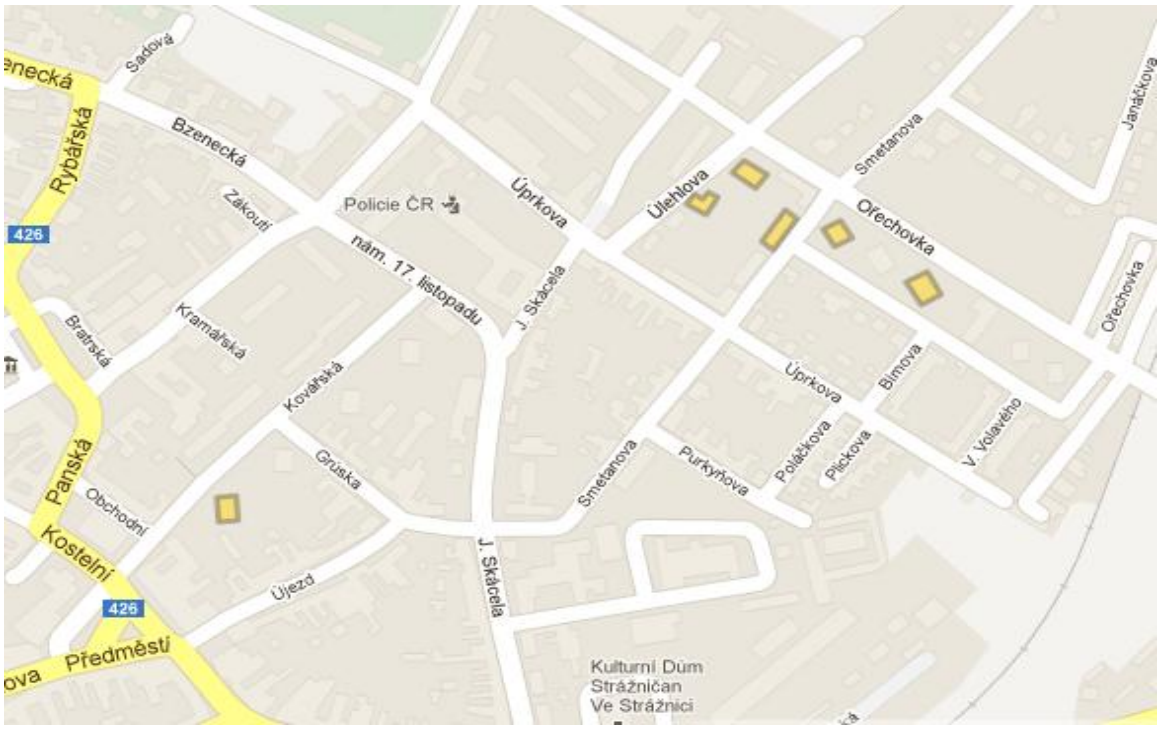
Příloha 1: Dostupnost optické sítě v městě Hodonín

Příloha 2: Dostupnost optické sítě v městě Strážnice

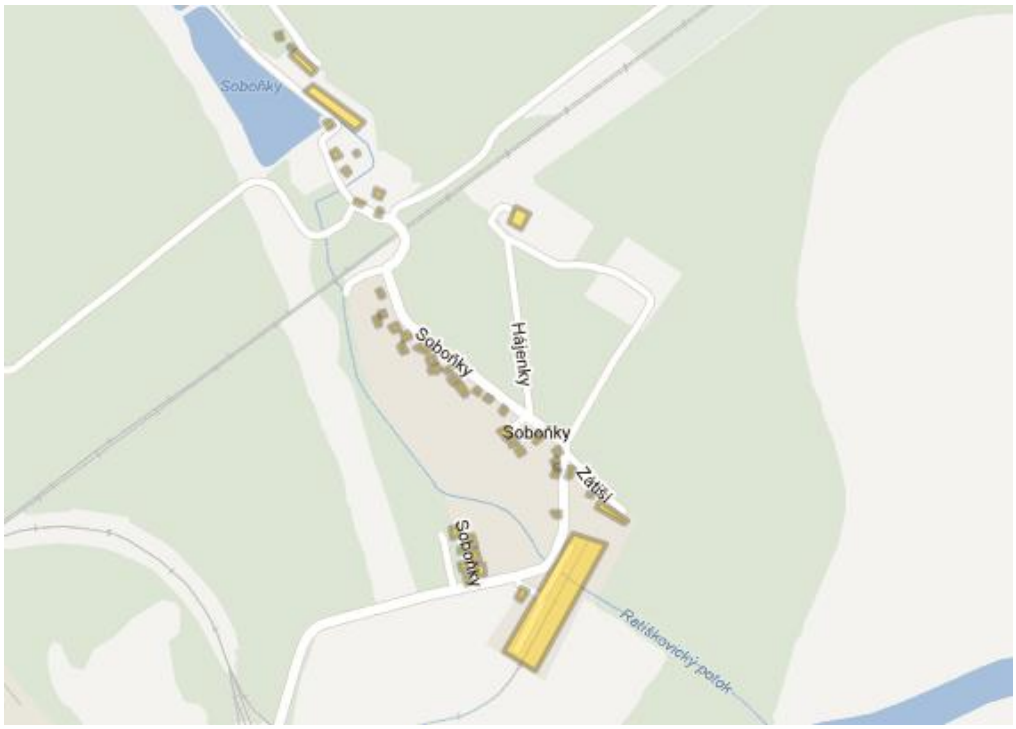
Příloha 3: Dostupnost optické sítě v obci Rohatec

Příloha 4: Organizační struktura společnosti Net-Connect s.r.o.

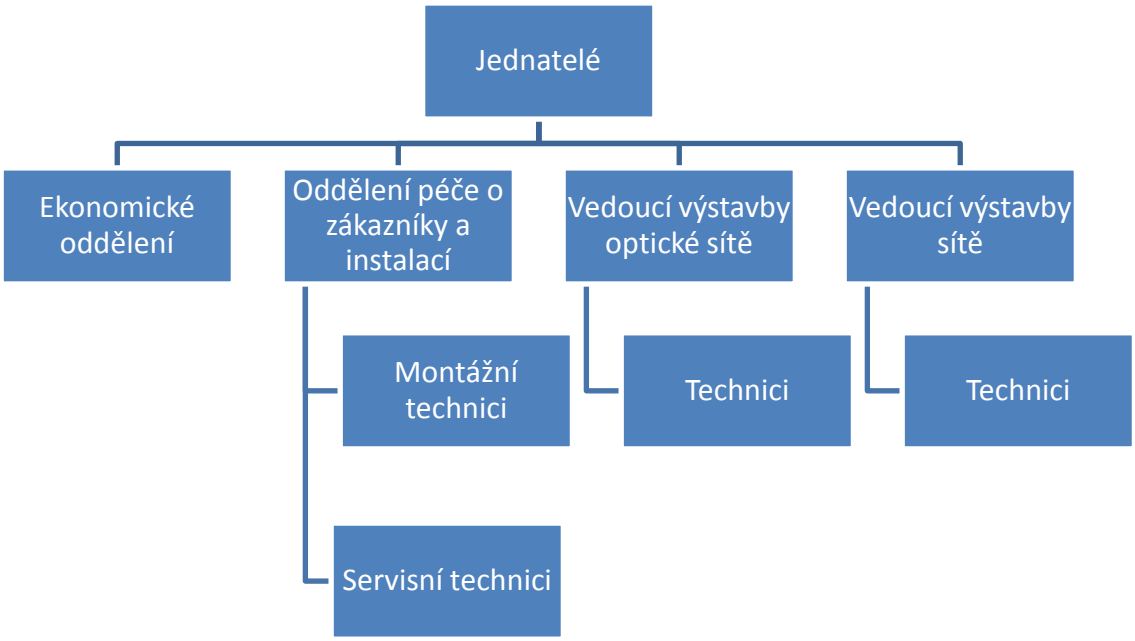
Příloha 1: Dostupnost optické sítě v městě Hodonín



Příloha 2: Dostupnost optické sítě v městě Strážnice



Příloha 3: Dostupnost optické sítě v obci Rohatec



Příloha 4: Organizační struktura společnosti Net-Connect s.r.o.