UNIVERZITA PARDUBICE
Dopravní fakulta Jana Pernera

Návrh řešení bezdrátových sítí pro služební i veřejné potřeby v železničním prostředí

Bc. Miroslav Koucký

Diplomová práce

2008

Univerzita Pardubice
Dopravní fakulta Jana Pernera
Katedra informatiky v dopravě
Akademický rok: **2007/2008**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Miroslav KOUCKÝ**
Studijní program:	**N3708 Dopravní inženýrství a spoje**
Studijní obor:	**Aplikovaná informatika v dopravě**
Název tématu:	**Návrh řešení bezdrátových sítí pro služební i veřejné potřeby v železničním prostředí**

Zásady pro vypracování:

V teoretické části porovnejte vlastnosti a vhodnost použití bezdrátových technologií typu WiMax a WiFi do prostředí Českých drah (nádraží, depa, osobní vozy a ucelené soupravy osobních vozů) s ohledem na bezpečnost a možnosti pokrytí dané oblasti signálem a s možností plynulého přechodu mobilních objektů mezi přístupovými body.
Zaměřte se na problematiku zabezpečení přístupu do bezdrátových sítí pro různé typy mobilních terminálů (např. služební PDA, zařízení cestujících, komunikační zařízení kolejových vozidel). Zpracujte možnost sdílení jediné infrastruktury pro služební potřeby i pro internet pro cestující.
V praktické části zpracujte konkrétní návrh bezdrátového řešení pro:

- pro osobní vůz,
- pro internet pro cestující (a přenosná zařízení zaměstnanců) v prostorách železniční stanice,
- pro komunikaci s kolejovými vozidly v železniční stanici s pokrytím železničních tratí v jejím okolí,
- pro depo kolejových vozidel.

Rozsah grafických prací:

Rozsah pracovní zprávy: **50 normostran**

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **PUŽMANOVÁ, R., ŠKRHÁ, P.** *Propojování sítí s TCP/IP*. **České Budějovice : Kopp, 1999. ISBN 80-7232-080-7.**
2. **PUŽMANOVÁ, R.** *Širokopásmový Internet. Přístupové a domácí sítě*. **Brno : Computer Press, 2004. ISBN 80-251-0139-8.**
3. **ZANDL, P.** *Bezdrátové sítě WiFi*. **Brno : Computer Press, 2003. ISBN 80-722-663.**
4. **PUŽMANOVÁ, R.** *Moderní komunikační sítě od A do Z*. **Brno : Computer Press, 2006. ISBN 80-251-1278-0.**
5. **LOCKHARD, A.** *Bezpečnost sítí na maximum*. **Brno : Computer Press, 2005. ISBN 80-251-0791-4.**
6. **PUŽMANOVÁ, R.** *Bezpečnost bezdrátové komunikace*. **Brno : Computer Press, 2005. ISBN 80-251-0791-4.**
7. **http://www.wimax.cz**

Vedoucí diplomové práce: **RNDr. David Žák, Ph.D.**
Ústav elektrotechniky a informatiky

Datum zadání diplomové práce: **4. prosince 2007**

Termín odevzdání diplomové práce: **4. června 2008**

prof. Ing. Bohumil Culek, CSc.
děkan

L.S.

doc. Ing. Josef Volek, CSc.
vedoucí katedry

V Pardubicích dne 30. listopadu 2007

Abstrakt:

Diplomová práce seznamuje se základními parametry technologie WiFi a Mobile WiMAX. Navrhuje implementaci technologie WiFi do železničního prostředí, jmenovitě do železničních vagónů a železničních stanic. Zabývá se rovněž zabezpečením přenášených dat. Dále se zabývá implementací technologie Mobile WiMAX pro vysokorychlostní přenos dat mezi železniční stanicí a vlakem.

Klíčová slova:

WiFi, WiMAX, železnice

Summary:

Thesis acquainted with the basic parameters of WiFi technology and Mobile WiMAX. It proposes the implementation of WiFi technology in the railway environment, namely in railway wagons and railway stations. It deals with the security of transmitted data. In addition, deals with the implementation of Mobile WiMAX technology for high-speed data transfer between the railway station and train.

Keywords:

WiFi, WiMAX, railway

Poděkování

Na tomto místě bych chtěl poděkovat vedoucímu mé diplomové práce RNDr. D. Žákovi, Ph.D. za zájem, připomínky a čas, který věnoval mé práci.

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek a pojmů

AES	Advanced Encryption Standard
AP	Access Point
BSD	Berkeley Software Distribution
CDMA	Code Division Multiple Access
CID	Connection ID
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
ESSID	Extended Service Set ID
GPL	General Public License
GSM	Global System for Mobile communications
GTK	Group Transient Key
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
MAC	Media Access Control
MAP	Media Access Protocol
MIMO	Multiple Input Multiple Output
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
PEAP	Protected Extensible Authentication Protocol
PKM	Public Key Management
PTK	Pairwise Transient Key

QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RC4	symetrická proudová šifra
RSA	algoritmus pro asymetrickou kryptografii
RSN	Robust Secure Network
SA	Security Association
SAID	Security Association ID
TCP/IP	protokolová architektura
VPN	Virtual Private Network
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WPA	Wi-Fi Protected Access

1 Bezdrátové technologie

V dnešní době jsou bezdrátové sítě pojmem skloňovaným v každém pádě. Používají se hlavně pro zajištění přenosu dat. U bezdrátových sítí je také často kladen důraz na mobilitu, což je u některých splněno dobře, např. u technologie GSM nebo CDMA a u některých hůře např. WiFi. Následující odstavce uvádí dva zástupce těchto technologií a to WiFi a WiMAX resp. jeho dodatek v podobě Mobile WiMAX.

1.1 Technologie Mobile WiMAX

Označení Mobile WiMAX je používáno pro spojení technologie WiMAX, která se řídí doporučením 802.16-2004 standardizační komise IEEE s přídavkem 802.16e od téže komise. Mobile WiMAX pokrývá 5, 7, 8,5, 10 MHz pásma v licencovaném rozsahu 2,3, 2,5, 3,3 a 3,5 GHz.

Význačné vlastnosti podporované Mobile WiMAX jsou:

- Rychlý přenos dat – se zahrnutím *MIMO* anténní techniky s flexibilní sub-kanalizací, pokročilým kódováním a modulací může dosahovat vrcholové rychlosti směrem k uživatelské stanici 63 Mb/s na sektor a směrem od uživatelské stanice 28 Mb/s na sektor při použití 10 MHz kanálu.

- Kvalita služby (Quality of Service) – sub-kanalizace a signální schéma založená na *MAP* poskytuje flexibilní mechanismus plánování frekvenčních a časových zdrojů po jednotlivých framech.

- Bezpečnost – zahrnuje autentizaci pomocí *EAP* nebo na základě klientského certifikátu *X.509*, šifrování pomocí *AES-CCM* a kontrolní schéma založené na *CMAC* a *HMAC*.

- Mobilita – podporuje optimalizované předávání klientské stanice mezi základnovými stanicemi se zpožděním menším než 50 ms.

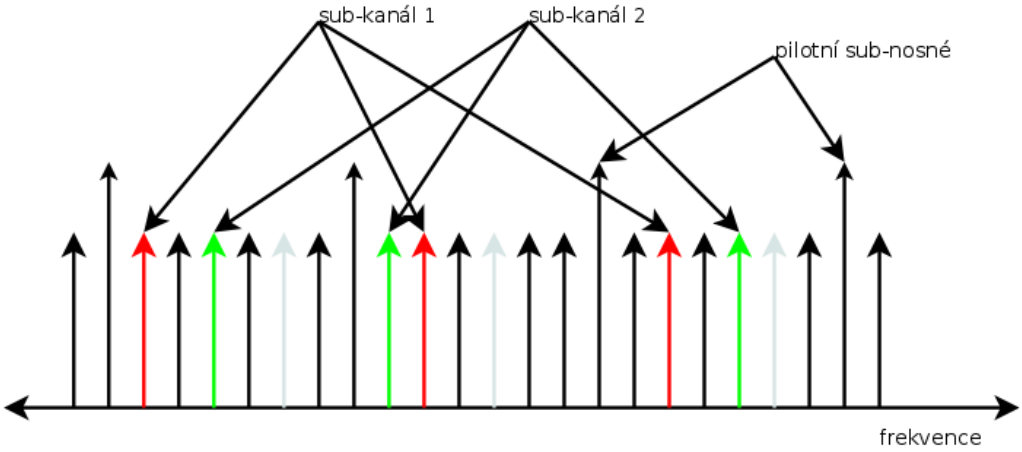
1.1.1 Fyzická a linková vrstva TCP/IP

1.1.1.1 OFDMA

Multiplexovací technologie OFDMA vychází z technologie OFDM. Ta rozděluje přidělený kanál na několik sub-nosných kanálů. Vstupní proud dat je rozdělen do několika paralelních sub-proudů s nižší datovou propustností. Každý z těchto sub-proudů je modulován a vysílán zvlášť na ortogonální sub-nosné. ODFMA poskytuje mutiplexování datových proudů od různých uživatelů v podobě sub-kanálů.

ODFMA symbol obsahuje tři typy sub-nosných.

- Data sub-nosná – slouží k přenosu dat.
- Pilot sub-nosná – slouží k synchronizačním účelům.
- Null sub-nosná – nepoužívá se pro přenos dat, slouží jako ochranné pásmo.



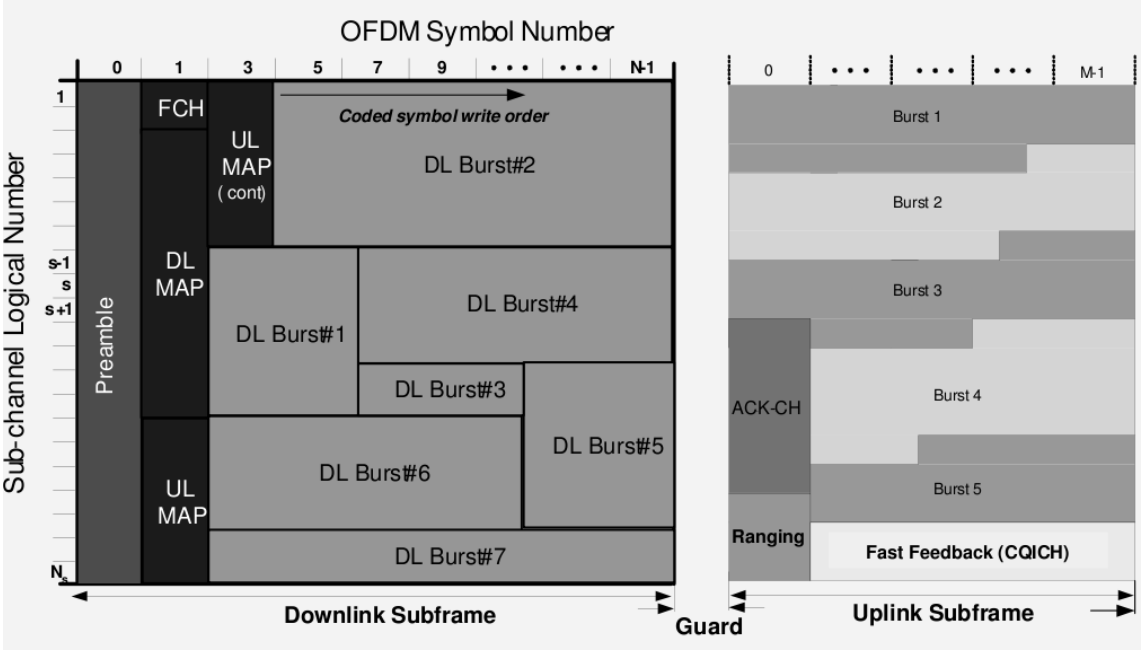
Obrázek 1: Sub-kanály při ODFMA

Sub-nosné určené pro přenos dat (data a pilost) jsou sdružené do logických skupin zvaných sub-kanály. Sub-kanalizace je podporována jak ve směru od základnové stanice ke klientovi, tak i ve směru opačném.

1.1.1.2 Frekvenčně a časově dělený duplex

Existují dva hlavní principy, jak oddělit provoz od základnové stanice směrem k uživateli a opačně. Časově dělený duplex (dvousměrný provoz) a frekvenčně dělený duplex.

Při použití časově děleného duplexu je jeden kanál přiřazen jak pro vysílání (směr od základnové stanice), tak pro příjem. Oba směry tak používají stejnou frekvenci, akorát každý v jinou dobu. Časově dělený duplex použitý v technologii WiMAX umožňuje měnit poměr mezi dobou vysílání (downlink) a dobou přijímání (uplink) v rámci každého rámce, což umožňuje dynamicky reagovat na přenosové požadavky.



Obrázek 2: Rámec při použití časově děleného duplexu [16]

- *Preamble* – první ODFMA symbol, používá se pro synchronizaci
- *FCH (Frame Control Header)* – obsahuje konfigurační informace, jako použité sub-kanály nebo schéma kódování
- *DL-MAP* a *UL-MAP* – obsahuje použité sub-kanály a ostatní kontrolní informace pro uplink resp. downlink rámec
- *ACK-CH* – obsahuje potvrzení downlink rámce při použití technologie *HARQ*

Při použití frekvenčně děleného duplexu se pro vysílání používá jeden kanál a pro příjem druhý kanál. To umožňuje paralelní provoz v obou směrech, ovšem za cenu použití dvou přenosových pásem.

V případě použití nižších frekvenčních pásem (2−11 GHz) v rámci technologie WiMAX a pro aplikace této technologie pro spojení bez přímé viditelnosti je lepší použití časově děleného duplexu. Frekvenčně dělený duplex nachází uplatnění v rámci vyšších frekvenčních pásem (okolo 66 GHz) a pro spojení s přímou viditelností.

1.1.2 Podpora kvality služby

Technologie Mobile WiMAX podporuje priorizaci provozu na základě jeho označení pomocí QoS [16]. Rozlišuje se pět kategorií QoS. Podle toho které kategorii daný provoz náleží, je upřednostněn nebo naopak opožděn oproti ostatnímu provozu.

Kategorie QoS	Aplikace	Specifikace provozu
UGS Unsolicited Grant Service	VoIP	• maximální potřebná rychlost • maximální tolerance zpoždění • tolerance rozptylu
rtPS Real-Time Polling Service	streamované audio nebo video	• minimální rezervovaná rychlost • maximální potřebná rychlost • maximální tolerance zpoždění • priorita provozu
ErtPS Extended Real-Time Polling Service	VoIP s detekcí aktivity	• minimální rezervovaná rychlost • maximální potřebná rychlost • maximální tolerance zpoždění • priorita provozu • tolerance rozptylu
nrtPS Non-Real-Time Polling Service	protokoly pro přenos souborů	• minimální rezervovaná rychlost • maximální potřebná rychlost • priorita provozu
BE Best-Effort Service	přenos dat, webové aplikace	• maximální potřebná rychlost • priorita provozu

Tabulka 1: Kategorie QoS

1.1.3 Předávání

U technologie Mobile WiMAX existují tři typy předávání (handoff) v případě přechodu klientské stanice od jednoho přístupového bodu k druhému [16].

- *HHO* (Hard Handoff) – základní způsob předávání, podporovaný všemi zařízeními

- *FBSS* (Fast Base Station Switching) – volitelný způsob předávání, kdy klientská stanice udržuje seznam přístupových bodů na které je možno se připojit. Tento seznam se nazývá *Active Set*. V něm je určen základní přístupový bod, přes který probíhá veškerá komunikace.

- *MDHO* (Macro Diversity Handover) – volitelný způsob předávání, kdy klientská stanice udržuje seznam přístupových bodů v okolí. Tentokrát však klientská stanice komunikuje pomocí všech přístupových bodů v *Active Set*u.

1.1.4 Zabezpečení přenosu

Autentizace, autorizace a šifrování provozu mezi mobilní stanicí a základnovou stanicí je již obsaženo v linkové vrstvě technologie WiMAX. Autentizace je zajištěna pomocí protokolu výměny veřejných klíčů, kterým se zabezpečuje také ustavení šifrovacích klíčů určených k šifrování provozu [16].

Autentizace je možná ve dvou formách.

- jednostranná – základnová stanice autentizuje mobilní stanici
- vzájemná – základnová stanice a mobilní stanici se autentizují navzájem

Každé zařízení s certifikací WiMAX musí implementovat jednostrannou autentizaci. Vzájemná autentizace je volitelná, avšak doporučená.

WiMAX standard definuje protokol PKM, který umožňuje tři typy autentizace.

- založenou na RSA – X.509 certifikáty spolu s RSA šifrováním
- volitelnou, založenou na EAP
- založenou na RSA následovanou EAP

PKM autentizační protokol ustavuje tajný sdílený klíč AK (*Authorization Key*) mezi mobilní a základnovou stanicí. Z něho je následně derivován KEK (*Key Encryption Key*). KEK je použit na následné výměny TEK (*Traffic Encryption Key*) podle protokolu PKM.

Při autentizaci založené na RSA základnová stanice autentizuje mobilní stanici na základě certifikátu X.509 vydaného výrobcem zařízení mobilní stanice. Certifikát X.509 obsahuje veřejný klíč stanice spolu s její MAC adresou. Při požadavku na AK mobilní

stanice pošle svůj X.509 certifikát základnové stanici, která certifikát ověří a použije privátní klíč z certifikátu k zašifrování AK, který je následně poslán zpět mobilní stanici.

Všechny mobilní stanice používající RSA autentizaci mají od výrobce instalován pár veřejného a privátního klíče (nebo algoritmus pro jejich náhodné generování) spolu s továrně nainstalovaným certifikátem X.509.

1.1.4.1 Security Association

Security Association (SA) je množina informací sdílená mezi základnovou stanicí a mobilní stanicí, sloužících k zabezpečení komunikace. Jsou definovány tři typy SA.

- primární – je ustaven každou stanicí v průběhu inicializačního procesu
- statický
- dynamický

Sdílené informace v SA obsahují použité šifrování v rámci SA, TEKy a inicializační vektory. Přesný obsah však záleží na použitém šifrování. SA jsou identifikovány pomocí SAID, které je stejné jako CID (identifikátor spojení) dané stanice.

Mobilní stanice využíváním PKM protokolu požaduje od základnové stanice „klíčové informace“, tedy používané šifrovací klíče a související informace, např DES klíč a CBC inicializační vektor. Základnová stanice musí zajistit, aby mobilní stanice mající přístup do dané SA byla autorizována pro přístup.

„Klíčové informace“ mají limitovanou životnost. Je záležitostí stanice, aby si vyžádala nové „klíčové informace“ od základnové stanice dříve, než vyprší jejich platnost.

1.1.4.2 Metody šifrování dat

Pro šifrování přenášených dat lze použít šifrování DES v CBC módu nebo šifrování AES v CCM módu.

Při šifrování pomocí AES je před užitečná data přidán 4 bytový PN (*Packet Number*), který není šifrován. Z užitečných dat je poté vypočítán ICV (*Integrity Check Value*) a přidán na konec užitečných dat. Šifrují se tak užitečná data spolu s ICV.

PN je nastaven na 1 při sestavení SA a instalování nového TEKu. Při každém přenosu užitečných dat se hodnota PN zvedne o 1. Při přenosu směrem od stanice k základnové stanici je PN před vyslání zXORován s hodnotou 0x80000000. PN tedy může nabývat hodnoty 0x00000001−0x7FFFFFFF pro data přenášená směrem k mobilní stanici (downlink) a 0x80000001−0xFFFFFFFF pro data přenášená směrem od mobilní stanice (uplink). Pokud dojde k přetečení čítače, je provoz v rámci dané SA zastaven do doby, než je nastaven nový TEK.

Pro šifrování TEK lze použít tři různé metody. Pomocí 3-DES v EDE módu, pomocí RSA nebo pomocí AES v ECB módu.

1.2 Technologie WiFi

Protokoly bezdrátových sítí *WiFi* podléhají doporučení *802.11* standardizační komise *IEEE*. Základním prvkem používaným rodinou protokolů *802.11* je *přístupový bod*. Jedná se o analogii k rozbočovači na metalických sítích. Jednotlivé stanice mezi sebou nekomunikují přímo, ale zprostředkovaně, právě pomocí přístupového bodu. Výjimku tvoří jen stanice propojené přímo mezi sebou metodou *ad-hoc*.

Oblast, kterou přístupový bod pokrývá, se nazývá *základní oblast služeb* (*basic service area*). Skupina stanic, které spolu komunikují v rámci jednoho přístupového bodu, se nazývá *základní soubor služeb* (*basic service set*). Minimální počet stanic tvořících základní soubor služeb jsou dvě stanice, propojené mezi sebou metodou ad-hoc. Jelikož oblast, kterou je možné pokrýt jedním přístupovým bodem je limitována, lze větší oblast pokrýt více přístupovými body a propojit je pomocí *distribučního systému* (*distribution system*). Tím vznikne rozšířená oblast služeb (*extended service area*) a stanice komunikující pomocí této oblasti služeb tvoří *rozšířený soubor služeb* (*extended service set*) [4].

Ke spojení jednotlivých přístupových bodů do rozšířeného souboru služeb lze použít v zásadě dva způsoby. Prvním z nich je roaming v podobě přístupových bodů propojených metalickou kabeláží. Druhým způsobem je použití technologie WDS, což je taktéž určitý druh roamingu, avšak bez použití metalické kabeláže. Ani jeden ze způsobů není uveden v doporučeních *802.11* a proto spojování přístupových bodů od různých výrobců nebo

dokonce různých typů od stejného výrobce je zatíženo rizikem nefunkčnosti takového řešení.

Ke slovnímu pojmenování přístupového bodu nebo rozšířené oblasti služeb se používá identifikátor *ESSID* (*Extended Service Set ID*), který by měl být v oblasti dosahu přístupového bodu nebo rozšířené oblasti služeb a stanice jedinečný. *ESSID* může být tvořen až 32 znaky.

1.2.1 Protokoly

Pro přehled v parametrech WiFi technologiích byly standardizační komisí *IEEE* zavedeny protokoly, lišící se znakem v označení doporučení. Protokoly se dále vyvíjí s rostoucími požadavky na bezdrátové spoje. V následující tabulce jsou uvedeny nejpoužívanější protokoly řady *802.11*.

Protokol	Pracovní frekvence	Maximální rychlost
802.11a	5 GHz	54 Mb/s
802.11b	2,4 GHz	11 Mb/s
802.11g	2,4 GHz	54 Mb/s

Tabulka 2: Protokoly 802.11 [9]

Kromě těchto protokolů existují ještě doporučení např. *802.11e*, *802.11h*, *802.11i*, které jsou rozšířením výše uvedených protokolů, zejména v rámci zabezpečení provozu.

1.2.2 Topologie

1.2.2.1 Ad-Hoc

Při propojení Ad-Hoc komunikují jednotlivé stanice mezi sebou bez použití přístupového bodu. K propojení stačí pouze dvě nebo více stanic vybavených bezdrátovými kartami. Není tím pádem použit žádný centrální prvek a síť může být považována za robustnější, např. z hlediska úmyslného rušení. Tento způsob lze prakticky uplatnit pouze při komunikaci na malou vzdálenost, neboť každá stanice musí být v dosahu ostatních stanic.

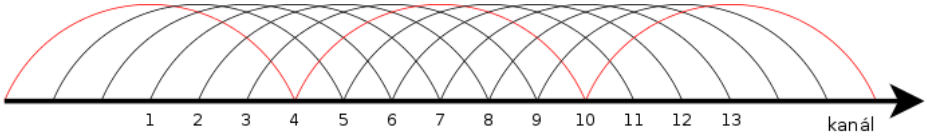
1.2.2.2 Infrastrukturní

Při použití infrastrukturní topologie je pro propojení jednotlivých stanic využit centrální prvek – přístupový bod (AP – *Access Point*). Veškerá komunikace mezi stanicemi probíhá právě přes tento bod. Díky tomu lze postavit geograficky rozsáhlejší síť, neboť stačí, aby každá stanice komunikovala pouze s přístupovým bodem a ostatní stanice již nemusí být v dosahu. Lze tak použít směrové antény s větším ziskem. Infrastrukturní topologie je použita v naprosté většině bezdrátových sítí. Další výhodou je možnost propojení jednotlivých přístupových bodů mezi sebou, např. pomocí LAN, a vytvořit tak rozsáhlou virtuální síť.

1.2.3 Fyzická a linková vrstva TCP/IP

1.2.3.1 Přímá sekvence

Při použití přímé sekvence je každý bit určený pro přenos nahrazen určitou sekvencí bitů a přenesen pomocí této sekvence. Tato metoda dělí dostupné pásmo 2,412–2,484 GHz na 14 kanálů [4]. Používat všechny kanály není v některých zemích povoleno, např. v České Republice je dovoleno používat pouze 13 kanálů. Šířka kanálu použitého pro přenos je 22 MHz a díky tomu se vedle sebe ležící kanály překrývají.



Obrázek 3: Rozdělení kanálů

Pro rychlosti 1 a 2 Mb/s je jeden přenášený bit nahrazen sekvencí 11 bitů, *chipem*. Sekvence bitů v chipu by měla být pseudonáhodná. V praxi bývá nahrazena *Barkerovým kódem*. Na přenášený bit se aplikuje chip pomocí funkce *XOR* . Výsledná sekvence bitů se pak odešle příjemci. Díky zavedení redundance se signál rozprostře do větší části spektra a stává se tak odolnějším vůči rušení.

1.2.3.2 ODFM

Metoda ODFM využívá nepřekrývající se kanály o šířce 20 MHz [9]. Tento kanál je rozdělen na 52 sub-kanálů o šířce 300 kHz. Pro přenos dat je využíváno 48 těchto sub-kanálů jako nezávislých pásem pro přenos dat. Odesílaná data jsou rozdělena a namodulována na jednotlivé dílčí sub-kanály. Rozložení zátěže mezi jednotlivé sub-kanály by v ideálním případě bylo rovnoměrné. V reálném provozu se zátěž rozděluje podle kvality signálu na daném sub-kanále. Pokud tedy budou některé kanály zarušeny, data se po nich budou posílat menší rychlostí a naopak po sub-kanálech, které nejsou zarušeny budou data posílána větší rychlostí. Základní rychlost je 6 Mb/s. Další rychlosti spolu s použitým kódováním jsou uvedeny v následující tabulce.

Rychlost [Mb/s]	Kódování	Poměr kódování
6	BPSK	1/2
9	BPSK	3/4
12	4-QAM	1/2
18	4-QAM	3/4
24	16-QAM	1/2
36	16-QAM	3/4
48	64-QAM	2/3
54	64-QAM	3/4

Tabulka 3: ODFM kódování

1.2.4 Zabezpečení přenosu

Pokud je třeba omezit připojení k přístupovému bodu nebo šifrovat přenášená data, je nutné použít některé z následujících možností. Některé jsou dnes již překonané a proti sofistikovanějšímu narušiteli nepoužitelné, např. WEP. Další tvoří pouze první z překážek a nasazení bez dalších doplňujících metod není příliš účinné (filtrace MAC adres). Poslední z metod jsou dodnes nepřekonané a při správném použití poskytují jak špičkovou ochranu přenášených dat, tak i řízení přístupu k přístupovému bodu (WPA2).

1.2.4.1 Filtrace hardwarových adres

Hardwarová adresa (MAC – *Medium Access Control*) slouží jako jednoznačný identifikátor (bezdrátové) síťové karty a může tedy posloužit k vytvoření seznamu stanic, kterým je dovoleno využívat služby daného přístupového bodu. Přihlásit se tedy mohou jen stanice, jejichž MAC adresa je na seznamu povolených adres.

Seznam povolených MAC adres je udržován na každém přístupovém bodu zvlášť, nejedná se tedy o centralizovanou správu. Při změnách v seznamu povolených MAC adres je nutno tento rozdistribuovat mezi všechny přístupové body. Toho je možno dosáhnout např. pomocí vzdálené správy jednotlivých přístupových bodů.

Ochrana přístupu do sítě pomocí filtrace MAC adres však není příliš spolehlivá, neboť potencionálnímu neoprávněnému uživateli stačí zachytit jediný paket putující mezi oprávněným klientem a přístupovým bodem či naopak. Každý takový paket obsahuje MAC adresu přístupového bodu a klientské stanice a právě tu je možno opsat a použít ji jako adresu své síťové karty.

1.2.4.2 WEP

Mechanismus WEP (Wired Equivalent Privacy) byl navržen za účelem ochrany přenášených dat, neboť v případě bezdrátové komunikace nedorazí data, na rozdíl od metalického vedení, pouze oprávněným stanicím, ale může je odposlechnout i neoprávněná stanice. Mechanismus WEP byl zaveden pro své vlastnosti, kterými jsou odolnost proti útoku hrubou silou, snadná implementovatelnost a jeho použití je volitelné. U většiny přístupových bodů je šifrování pomocí WEP implicitně vypnuto.

WEP používá 64 nebo 128 bitový klíč (výjimečně i více, např. 192 nebo 256 bitů). V této délce je již obsažen 24 bitový inicializační vektor stanovující počáteční nastavení šifry. K samotnému šifrování dat se používá proudová šifra RC4 [6].

Klíč používaný k šifrování komunikace se sestává z pevné části o délce 40 bitů u 64 bitového klíče, resp. 104 bitů u 128 bitového klíče, která je tajná a 24 bitového inicializačního vektoru (*Initialization Vector* – IV), který se mění pro každý paket. Inicializační vektory jsou voleny pseudonáhodně ze všech možných variant, kterých je 2^{24}.

Před odesláním je z paketu spočítán kontrolní součet (*Integrity Check Value* – ICV), který je spolu s celým paketem zašifrován pomocí klíče s pseudonáhodně vybraným inicializačním vektorem. Inicializační vektor je poté přidán k výsledku šifrování v nezašifrovaném tvaru.

Šifrovací klíč se nastavuje pro každý přístupový bod a každou stanici zvlášť a v čase se nemění. Není proto možné změnit naráz šifrovací klíče používané pro zabezpečení přenosu dat.

1.2.4.3 WPA

Protokol WPA vznikl jako odpověď na bezpečnostní slabiny protokolu WEP. Je částečnou implementací doporučení IEEE 802.11i [6]. Existuje ve dvou variantách. Jako varianta s předsdíleným klíčem a pak také jako Enterprise varianta, používající ověřování 802.1x a servery RADIUS.

Protokol WPA používá šifru RC4, stejnou jako WEP, avšak používá ji novým způsobem aby zabránil útokům používaným na protokol WEP. Hlavní rozdíly jsou:

- Zvětšení prostoru pro inicializační vektor na 48 bitů
- Přidává algoritmus *Michael* pro kontrolu integrity zpráv
- TKIP pro změnu šifrovacího klíče s každým paketem

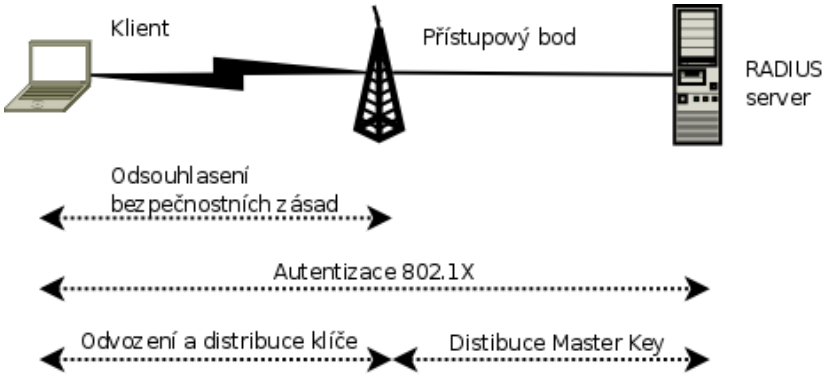
Zvětšením prostoru pro inicializační vektor dojde k výraznému snížení šance na zachycení dvou paketů se stejným inicializačním vektorem. Kontrola integrity zpráv obsahuje také počitadlo přenášených rámců, aby bylo zabráněno možnému útoku využívajícím opakování stejné zprávy (*Reply Atack*).

1.2.4.4 WPA2

Protokol je úplnou implementací doporučení IEEE 802.11i [6]. Oproti WPA používá blokovou šifru AES a pro kontrolu integrity zpráv CCMP. Následující popis zobrazuje tří fázový proces navazování spojení.

Používaná architektura se označuje jako *RSN* (Robust Security Network). Odvození a předání šifrovacích klíčů podle 802.11i se sestává z následujících fází (obr 4):

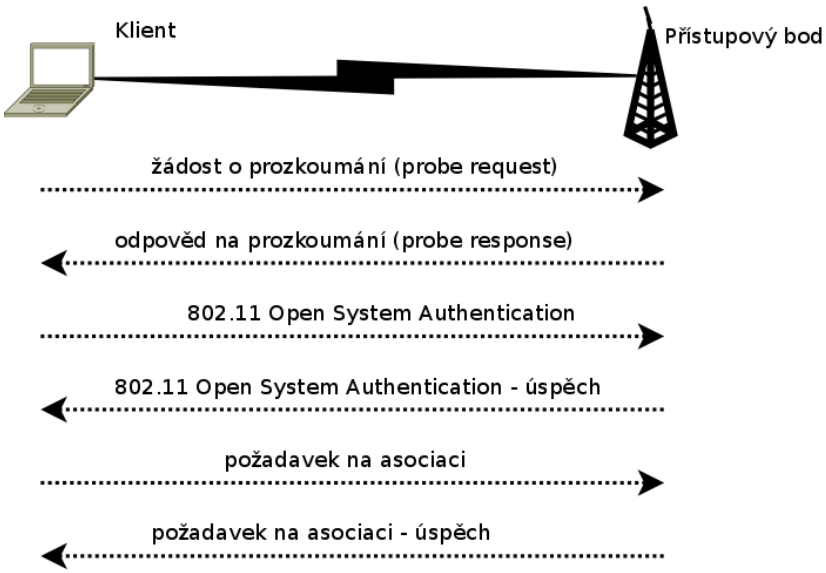
- odsouhlasení bezpečnostních zásad
- autentizace 802.1x
- odvození a distribuce klíče



Obrázek 4: Jednotlivé fáze sestavování komunikace

V první fázi se klientská stanice dohodne s přístupovým bodem na použitých bezpečnostních zásadách (obr. 5). Zásady podporované přístupovým bodem jsou oznamovány v rámcích *beacons*, které přístupový bod periodicky vysílá. Bezpečnostní zásady popisují:

- podporované autentizační metody
- bezpečnostní protokoly pro provoz dílčího vysílání
- bezpečnostní protokoly pro provoz skupinového vysílání
- podporu pre-autentizace

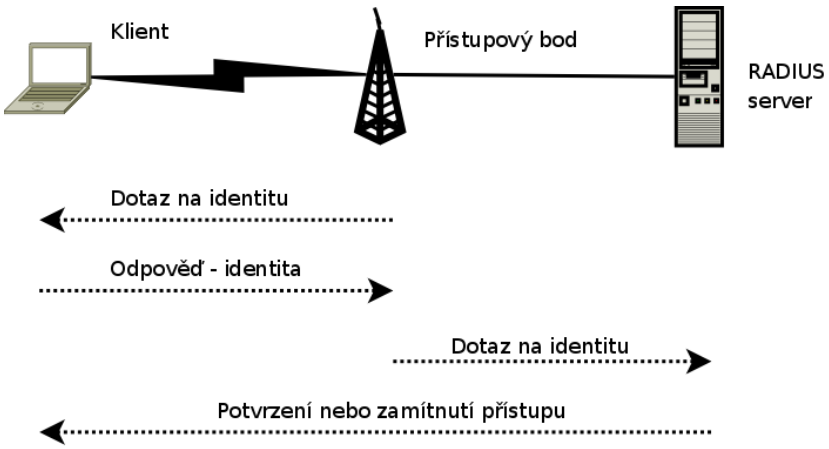


Obrázek 5: První fáze sestavování komunikace

Ve druhé fázi je provedena autentizace 802.1x na základě protokolu EAP (obr. 6). Následuje ověření identity stanice, kdy dojde k výměně zpráv mezi stanicí a autentizačním serverem *RADIUS*. Pokud vše proběhlo v pořádku, je na konci vygenerován hlavní klíč (*Master Key*). Ověřování se sestává z následujících částí:

- dotázání klienta na identitu
- odpověď na dotaz (identita)
- dotaz na RADIUS server
- zamítnutí nebo povolení přístupu

Pokud je místo autentizace 802.1x použita metoda předsdíleného klíče (*Pre-Shared Key*) je výše uvedená část vynechána.

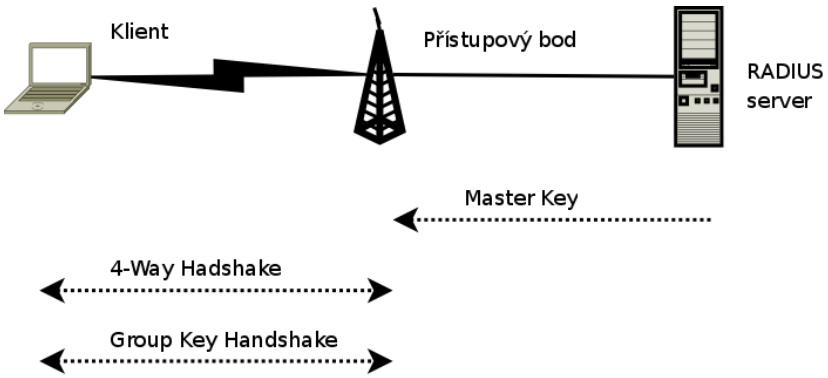


Obrázek 6: Ověřování stanice

RADIUS server slouží k povolení nebo zamítnutí uživatele na základě jeho identifikace. Pro identifikaci může být použito jméno a heslo nebo také uživatelský certifikát či autentizační token.

Bezpečnost spojení stojí a padá s bezpečností klíčů. V architektuře *RSN* má každý klíč omezenou dobu trvání. Bezpečnost se dále zajišťuje hierarchickým uspořádáním sady klíčů. Průběh odvozování se sestává z následujících komunikací (obr. 7):

- *4-Way Hadshake* pro odvození *PTK* a *GTK*
- *Group Key Handshake* pro obnovení *GTK*



Obrázek 7: Odvozování klíčů

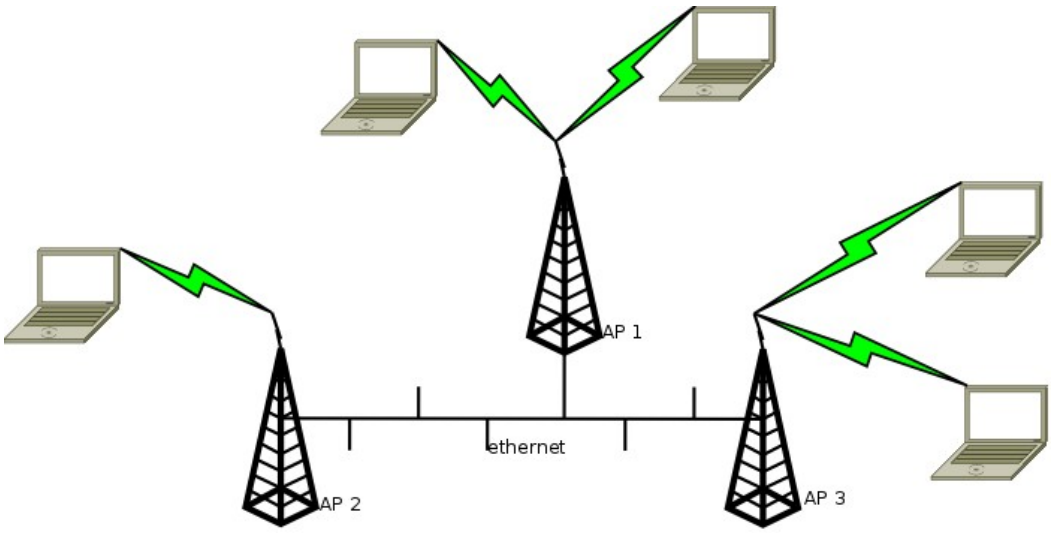
Klíč *PTK* slouží k šifrování vysílání unicast a klíč *GTK* je používán pro skupinové vysílání (multicast). Pokud není použita autentizace 802.1x, jsou klíče odvozeny pomocí předsdíleného hesla.

1.2.5 Roaming

Při roamingu jsou jednotlivé přístupové body propojeny pomocí ethernetu nebo pomocí WDS a umožňují mobilní stanici přecházení v rámci dosahu jednotlivých přístupových bodů. Propojení přístupových bodů pomocí ethernetu přináší možnost využití plné rychlosti daného bodu nezávisle na množství bodů pokrývajících oblast. Všechny přístupové body v rámci pokrývané oblasti musí mít nastaveno stejné ESSID. Pokud jsou přístupové body propojeny pomocí ethernetu, je možné používat k zabezpečení provozu mechanismy s dynamickým klíčem.

Vhodné je, aby sousedící přístupové body, pokud jsou propojeny pomocí ethernetu, měly nastaveny nepřekrývající se kanály, t.j. 1, 6 a 11. Nebude tak docházet ke kolizím ve vysílání jednotlivých přístupových bodů a ke snadnějšímu přechodu mezi přístupovými body.

Pro technologii Wi-Fi není přechod mobilní stanice mezi jednotlivými přístupovými body definován v doporučení IEEE a chování proto může být závislé na výrobci zařízení.



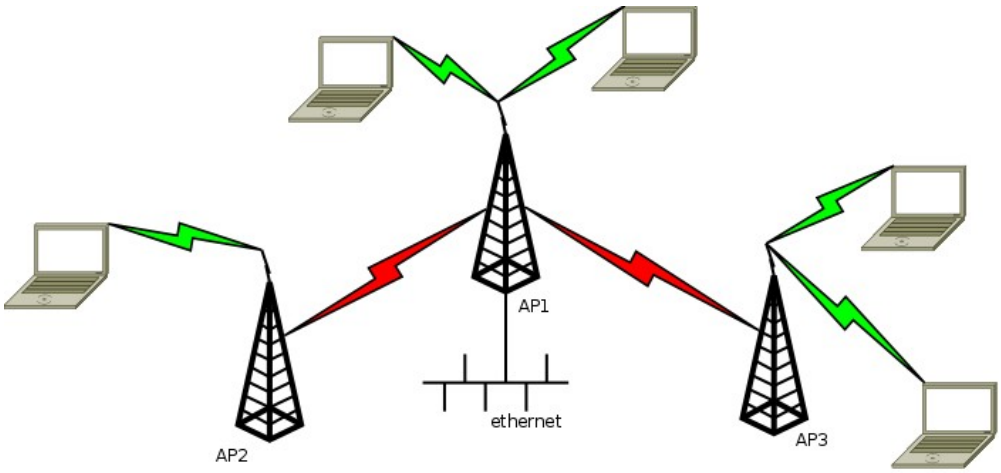
Obrázek 8: Roaming pri použití ethernetu

1.2.6 WDS

WDS (*Wireless Distribution system*) slouží k propojení jednotlivých přístupových bodů a k rozvodu konektivity bez pomoci kabelové sítě [4]. Umožňuje tak rozšířit pokrytí i do míst, kde by bylo obtížné natáhnout ethernetový kabel. Jedná se o nestandardizované rozšíření jednotlivých výrobců a není zaručena součinnost přístupových bodů od různých výrobců. Při použití WDS není možno používat dynamické klíče (WPA, WPA2) a jediným možným šifrováním provozu proto zůstává WEP i se všemi svými nedostatky. WDS je možno provozovat ve dvou základních režimech, přemostění a opakovače.

V režimu přemostění je mezi přístupovými body předávána pouze konektivita. V režimu opakovače dochází taktéž k předávání konektivity mezi přístupovými body, ale zároveň je dovoleno připojování klientů k těmto bodům. Nevýhodou WDS je, že s každým přeskokem mezi přístupovými body se snižuje rychlost pro připojené klienty na polovinu. Při použití přístupového bodu, ke kterému je vedena konektivita pomocí dvou přeskoků, je rychlost pro klienty tohoto bodu čtvrtinová, oproti klientům připojeným k prvnímu přístupovému bodu.

Při použití WDS musí všechny přístupové body používat stejný kanál, neboť obsahují pouze jednu bezdrátovou část. Rovněž nastavení WEP musí být pro všechny body totožné.



Obrázek 9: WDS v režimu opakovače

2 Návrh bezdrátového řešení

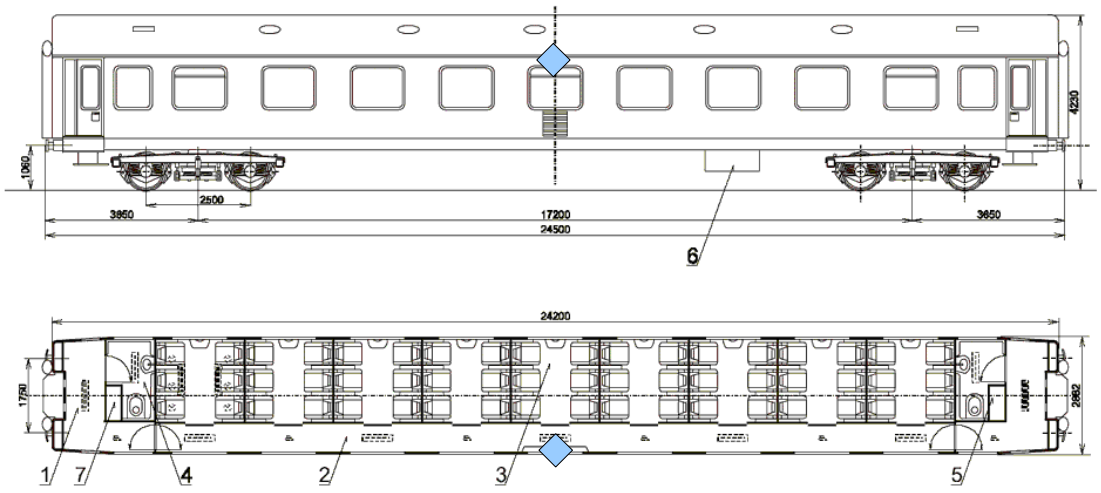
Čím dál častěji se objevují požadavky na mobilní přístup k informacím, ať už pro cestující v podobě přístupu k internetu nebo pro služební účely v podobě přístupu do služební sítě nebo k služebním serverům. Dostupnost těchto služeb by neměla být omezena pouze na budovy, ale pokrývat taky prostory uvnitř vlaků. Pod pokličku mobilní výměny dat spadá také vysokorychlostní výměna dat mezi vlakem a přístupovým bodem umístěným ve stanici. Výměna dat může probíhat jak mezi vozy umístěnými v depu, tak i mezi vlakem jedoucím přes stanici či zastávku nebo v ní zastavující.

Dnes nejvhodnějšími technologiemi pro mobilní přenos dat se jeví technologie WiFi a Mobile WiMAX. WiFi pro připojení cestujících k internetu a pro služebních terminálů do služební sítě. Mobile WiMAX naopak pro vysokorychlostní výměnu dat mezi vlakem a stanicí.

Následující scénáře nastiňují použití mobilního přístupu k informacím jak uvnitř vlaku, tak i v prostorách stanice. Uvedeny jsou vždy různé varianty technické realizace, ať už způsobem pokrytí, tak i možnostmi zabezpečení přístupu a přenášených dat. Jako poslední jsou uvedeny možnosti pokrytí stanice signálem pomocí technologie Mobile WiMAX. U této technologie odpadá volba různých možností zabezpečení přístupu a přenášených dat, neboť byla již v základu navržena s ohledem na vysoký stupeň zabezpečení.

2.1 Osobní vůz

Pokrytí osobního vozu je určeno cestujícím pro připojení k internetu a pro přístup do služební sítě pro vlakový personál. V rámci osobního vozu lze uvažovat pokrytí jedním přístupovým bodem, ale v rámci vlaku se jedná vlastně o přístupové body spojené pomocí ethernetu. Uvažovaná implementace je pro vagón Aee 145 (obr. 10). Umístění přístupového bodu je zvoleno v polovině vagónu, nad úrovní oken, na obrázku znázorněné modrým bodem. Použití jednoho přístupového bodu je dostačující i pro krajní části vagónu. Použití dvou přístupových bodů bylo zavrženo z důvodu možného neustálého přepojování z jednoho bodu na druhý u uživatelů sedících na pomezí těchto dvou bodů.

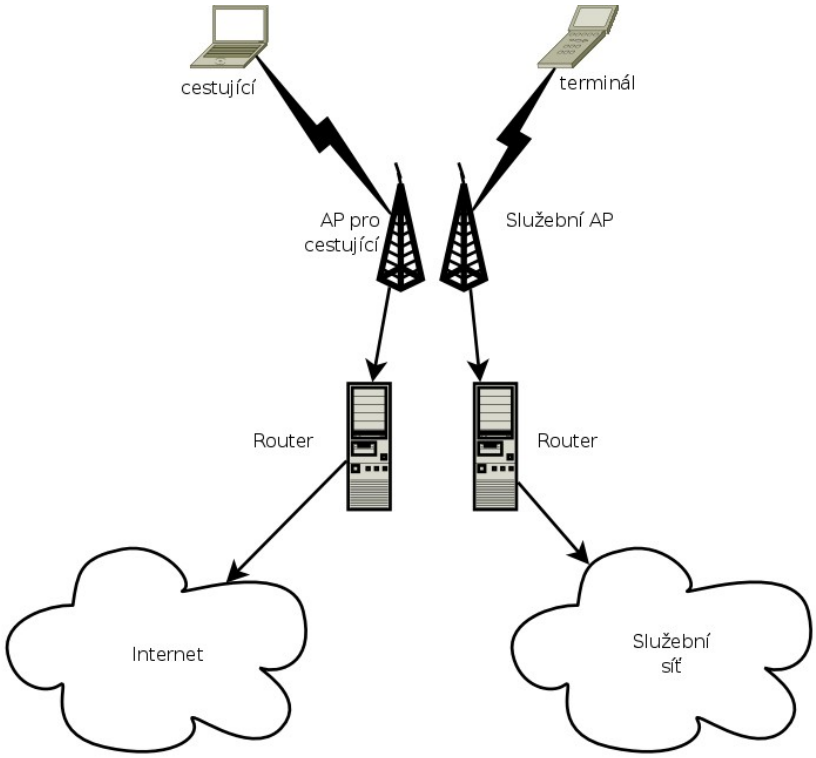


1 – nástupní prostor, 2 – postranní chodba, 3 – oddíl pro cestující, 4 – kompletní buňka WC, 5 – hlavní rozváděč, 6 – centrální zdroj energie, 7 – ruční brzda

Obrázek 10: Vagon Aee 145 a umístění přístupového bodu

2.1.1 Jeden zdvojený přístupový bod

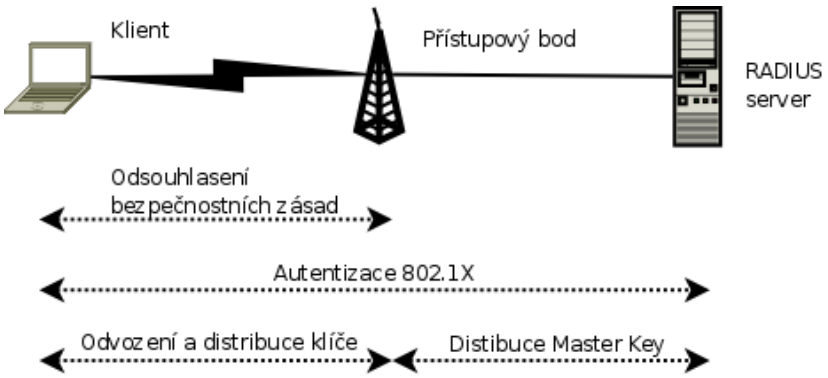
Jedná se o použití dvou přístupových bodů umístěných vedle sebe, případně zdvojeného přístupového bodu, kde jsou obě bezdrátové části umístěny v rámci jediného zařízení. Výhodou je snazší oddělení sítě pro služební provoz a pro přístup veřejnosti k internetu. Každý přístupový bod tak může používat jinou technologii zabezpečení. Nevýhodou zůstávají vyšší pořizovací náklady.



Obrázek 11: Zdvojený přístupový bod

2.1.1.1 Použití WPA2 Enterprise a nešifrovaného přístupu

Pro každý přístupový bod je zvolena jiná metodika zabezpečení přístupu. Pro přístupový bod obsluhující služební síť je zde využito zabezpečení pomocí WPA2 Enterprise, obsahující ověřování proti RADIUS serveru pomocí PEAP (obr. 12). Pro přístupový bod obsluhující připojení k internetu pro cestující není zvoleno žádné zabezpečení přístupu. Autorizace přístupu založená na PEAP vyžaduje, aby všechny přístupové body fungující v rámci přístupu do služební sítě byly vybaveny certifikáty, podepsanými určenou certifikační autoritou. Certifikát zajišťuje ochranu před vytvořením falešného přístupového bodu za účelem získání přihlašovacích údajů.



Obrázek 12: Přihlašování pomocí WPA2 Enterprise

Při přihlašování do služební sítě je možno ověřovat buď totožnost zařízení (terminálu, atd.), nebo uživatele pracujícího s daným zařízením. V případě ověřování zařízení je přihlašovací jméno a heslo uloženo v daném zařízení trvale a v případě potřeby a dosahu přístupového bodu dojde k jeho přihlášení do služební sítě. V případě ověřování uživatele je uživatelské jméno a heslo uživatele uloženo pouze dočasně. To pro případ, aby při novém přihlašování do sítě nebylo nutné znovu zadávat uživatelské jméno a heslo. Po připojení zařízení k přístupovému bodu dojde k poslání uživatelského jména a hesla pomocí protokolu PEAP RADIUS serveru. Ten podle oprávněnosti uživatelského jména a správnosti hesla rozhodne o povolení nebo zamítnutí autorizace klientského zařízení. V případě úspěšné autorizace dojde k přidělení IP adresy klientskému zařízení DHCP serverem.

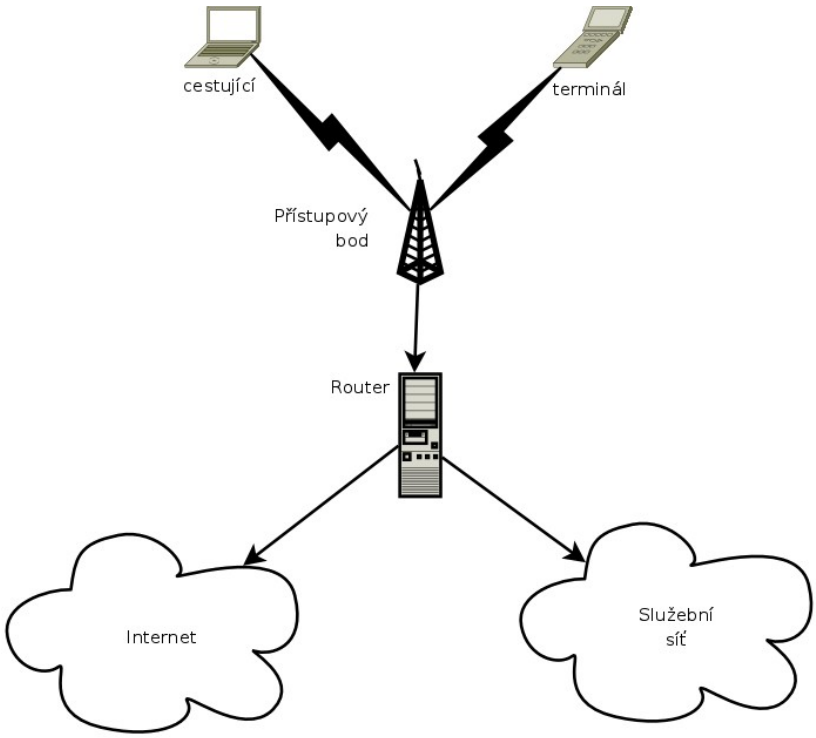
V případě pohybu připojeného služebního zařízení nad rámec dosahu přístupového bodu k němuž je zařízení připojeno a k poklesu síly signálu pod určitou mez, dojde k jeho přepojení na přístupový bod se silnějším signálem. To nastane vždy při přechodu personálu mezi vagóny, neboť pokrytí daným přístupovým bodem bude pouze v rámci daného vagónu. V tomto případě se po přihlášení k přístupovému bodu IP adresa od DHCP serveru znovu nežádá, neboť je určena doba propůjčení adresy danému zařízení. Pokud doba zapůjčení IP adresy ještě nevypršela, není nutná její obnova.

Použití bezdrátové sítě cestujícími v dosahu přístupového bodu pro přístup k internetu vyžaduje pouze zvolení sítě podle ESSID. Je tak možno učinit s jakýmkoliv zařízením obsahujícím Wi-Fi rozhraní (notebook, PDA, atd.). Po přihlášení zařízení

k veřejné síti dojde k přidělení IP adresy od DHCP serveru. Komunikace cestujících není mezi přístupovým bodem a jejích zařízením nijak šifrována.

Nevýhodou tohoto řešení je nutnost, aby veškerá zařízení určená pro komunikaci pomocí služební sítě zvládala protokol WPA2 Enterprise. To je na druhou stranu vykoupeno nekompromisním stupněm zabezpečení přístupu a šifrováním komunikace. Další nevýhodou je neomezený přístup cestujících i ostatních osob v dosahu přístupového bodu k internetu. Použití přístupového bodu nelze nijak regulovat ani omezovat. To vzhledem k umístění přístupového bodu (jedoucí vagón) není takový problém.

2.1.2 Jeden jednoduchý přístupový bod



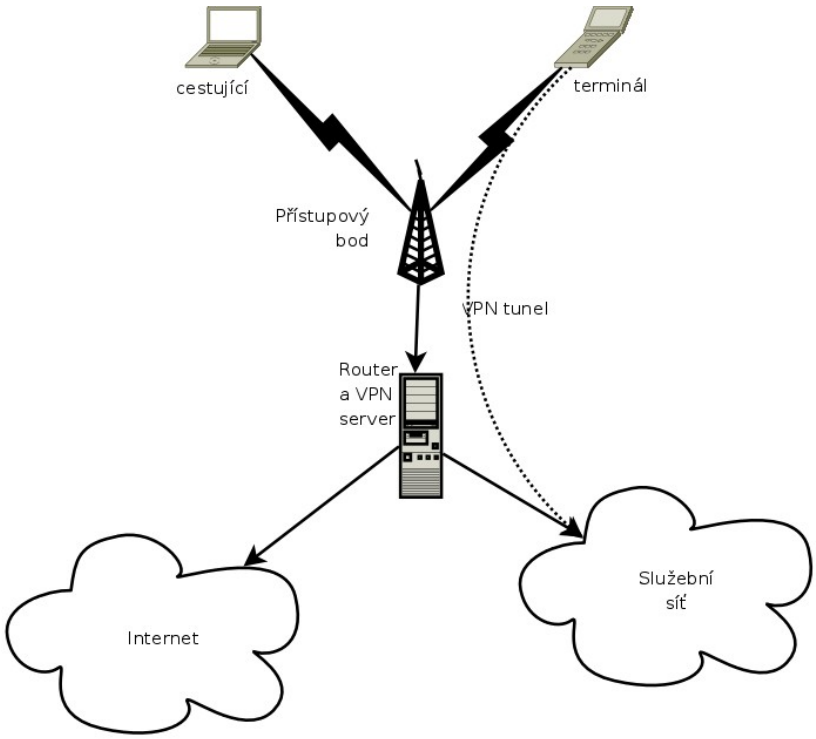
Obrázek 13: Jednoduchý přístupový bod

Jedná se o použití pouze jednoho přístupového bodu pro komunikaci jak služební, tak i pro cestující. Výhodou je jednodušší konfigurace, kdy se nastavuje pouze jeden přístupový bod. Nevýhodou je nutný kompromis v použití metodiky zabezpečení přístupu,

aby byl použitelný jak pro služební účely, tak pro cestující. Nutné je také oddělení služební sítě od sítě využívané cestujícími.

2.1.2.1 Použití nešifrovaného přístupu a VPN

Pro přístupový bod používaný jak pro služební účely, tak i pro přístup cestujících k internetu není zvoleno žádné zabezpečení přístupu. Jelikož na úrovni přístupového bodu není možné odlišovat služební zařízení od zařízení cestujících, je nutné vyřešit přístup do služební sítě pomocí VPN (obr. 14). Vhodným kandidátem na použití VPN je software OpenVPN, jenž je multiplatformní a je distribuován pod licencí GPL verze 2. S licencí souvisí dostupnost zdrojových kódů a tím pádem snadnější modifikace pro potřeby služebních zařízení.

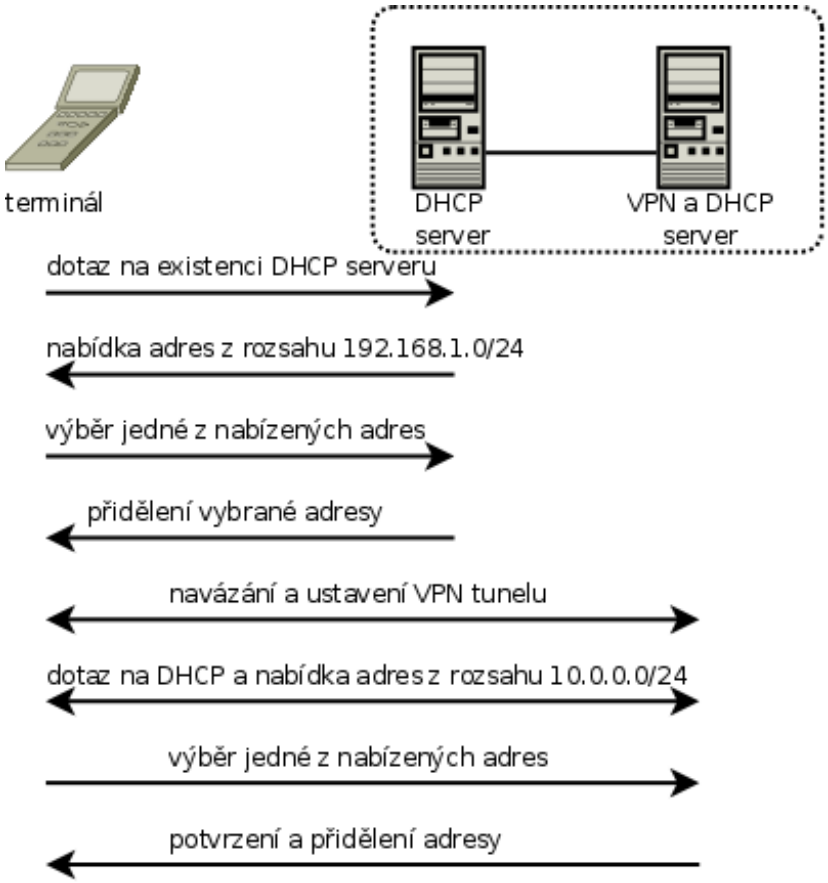


Obrázek 14: VPN

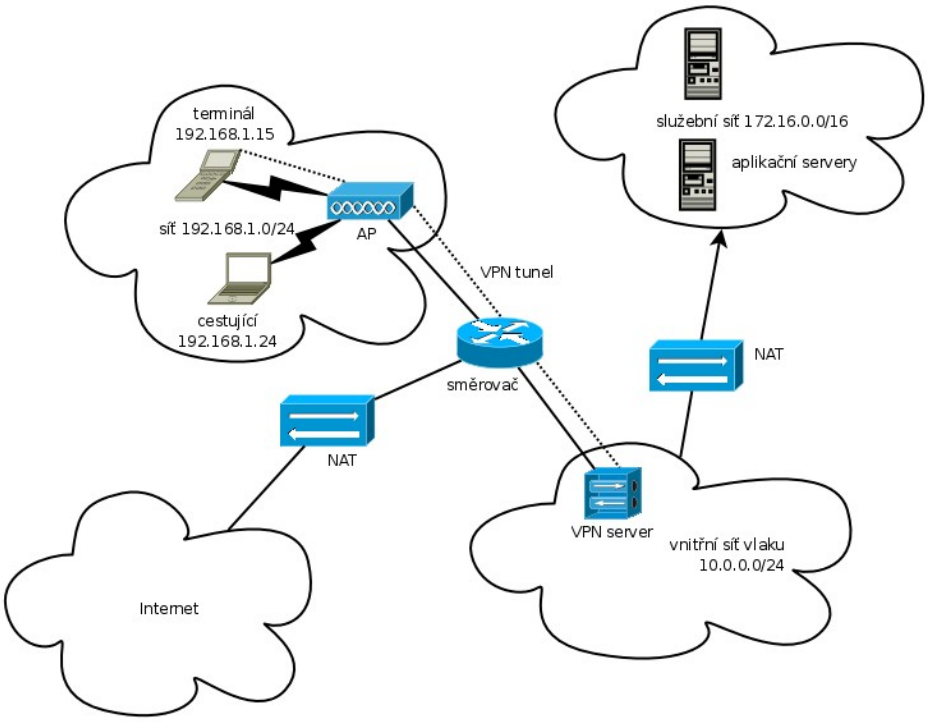
Při přihlašování do služební sítě dojde nejdříve k přihlášení služebního zařízení k přístupovému bodu a následnému přidělení IP adresy z rozsahu 192.168.x.0/24 od DHCP serveru. Poté je nutné, přihlásit se pomocí VPN do vnitřní služební sítě a oddělit a šifrovat tak služební provoz. Po přihlášení se do VPN dojde k opětovnému přidělení IP adresy pro

virtuální síťové rozhraní, tentokrát z rozsahu 10.0.0.0/24 (obr. 16). Celý proces přidělování IP adres se sestává z následujících kroků (obr. 15):

- broadcast dotaz na přítomnost DHCP serveru po přihlášení k AP
- nabídnutí použitelných IP adres z rozsahu 192.168.x.0/24 DHCP serverem
- výběr IP adresy klientem
- potvrzení a přidělení IP adresy
- navázání VPN spojení
- broadcast dotaz na DHCP server, tentokrát přes virtuální síťové rozhraní
- nabídnutí použitelných IP adres z rozsahu 10.0.0.0/24 DHCP serverem
- výběr IP adresy klientem
- potvrzení a přidělení IP adresy pro virtuální síťové rozhraní



Obrázek 15: Přidělování IP adres



Obrázek 16: Jednotlivé sítě a rozsahy adres

Přihlášení k VPN může být na základě certifikátu vydaném vnitřní certifikační autoritou a ověřovat tak totožnost zařízení (terminálu) nebo certifikát přiřadit každému uživateli terminálu např. na USB flash disku, jenž by bylo nutné do zařízení připojit ještě před přihlášením. Druhou možností, jak ověřovat totožnost uživatele, je použití uživatelského jména a hesla. V případě pohybu mezi vagóny dojde k přerušení připojení k danému přístupovému bodu a přihlášení k přístupovému bodu v dalším vagónu. V tomto případě se po přihlášení k přístupovému bodu IP adresa od DHCP serveru znovu nežádá, neboť je určena doba propůjčení adresy danému zařízení. Pokud doba zapůjčení IP adresy ještě nevypršela, není nutná její obnova. Spojení mezi klientským zařízením a VPN serverem není také nutno obnovovat. Spojení je dostatečně robustní a krátkodobý výpadek v podobě přepojování k jinému přístupovému bodu nezpůsobí jeho přerušení.

Použití bezdrátové sítě cestujícími v dosahu přístupového bodu pro přístup k internetu vyžaduje pouze zvolení sítě podle ESSID. Je tak možno učinit s jakýmkoliv zařízením obsahujícím Wi-Fi rozhraní. Po přihlášení zařízení k veřejné síti dojde k přidělení IP adresy od DHCP serveru.

Nevýhodou výše uvedeného řešení je složitější správa, zahrnující jak přístupový bod, tak i VPN server. Dále nutnost podpory VPN služebním klientským zařízením. Díky otevřenému a nekontrolovatelnému přístupu k přístupovému bodu je rovněž možné úmyslné rušení služební komunikace např. posíláním deautentizačních paketů. Použití nezabezpečené bezdrátové sítě nechává otázku zabezpečení přenášených dat na cestujících.

2.1.2.2 Použití WPA2 Enterprise a VPN

Pro přístupový bod používaný jak pro služební účely, tak i pro přístup cestujících k internetu je zvoleno zabezpečení přístupu pomocí WPA2 Enterprise. Jelikož na úrovni přístupového bodu není možné odlišovat služební zařízení od zařízení cestujících, je nutné vyřešit přístup do služební sítě pomocí VPN.

Při přihlašování do služební sítě je možno ověřovat buďto totožnost zařízení (terminálu, atd.) nebo uživatele pracujícího s daným zařízením. V případě ověřování zařízení je přihlašovací jméno a heslo uloženo v daném zařízení trvale a v případě potřeby a dosahu přístupového bodu dojde k jeho přihlášení do služební sítě. V případě ověřování uživatele je uživatelské jméno a heslo uživatele uloženo pouze dočasně. To pro případ, aby při přesunu personálu mezi vagóny nebylo nutné znovu zadávat uživatelské jméno a heslo. Po připojení zařízení k přístupovému bodu dojde k poslání uživatelského jména a hesla pomocí protokolu PEAP RADIUS serveru. Ten podle oprávněnosti uživatelského jména a správnosti hesla rozhodne o povolení nebo zamítnutí autorizace klientského zařízení. V případě úspěšné autorizace dojde k přidělení IP adresy klientskému zařízení DHCP serverem. Poté je nutné přihlásit se pomocí VPN do vnitřní služební sítě a oddělit tak služební provoz. Přihlášení do VPN může být na základě certifikátu vydaném vnitřní certifikační autoritou a ověřovat tak totožnost zařízení (terminálu) nebo certifikát přiřadit každému uživateli terminálu např. na USB flash disku, jenž by bylo nutné do zařízení připojit ještě před přihlášením. Druhou možností, jak ověřovat totožnost uživatele, je použití uživatelského jména a hesla.

Použití bezdrátové sítě cestujícími v dosahu přístupového bodu vyžaduje zvolení správného přístupového bodu na základě ESSID. Dále je nutné, autorizovat cestujícího pro přístup do sítě na základě uživatelského jména a hesla. Jako uživatelské jméno a heslo lze použít číslo vydané jízdenky, jenž by bylo uloženo v RADIUS serveru s dobou platnosti

odpovídající platnosti jízdenky. To by umožňovalo připojení k síti pouze cestujícím s platnou jízdenkou. Systém uživatelských jmen a hesel by bylo možné dále rozšířit např. o možnost přístupu do sítě jen pro jízdenky první třídy nebo jen pro dané kategorie vlaků. Další možnou variantou by bylo vybrání univerzálního, všeobecně známého jména a hesla. Odpadla by tím synchronizace uživatelských jmen a hesel s vydanými jízdenkami. Oproti tomu by nebylo možné kontrolovat, kdo do sítě přístup má a kdo ne. Přístup by měli všichni cestující, kteří by věděli uživatelské jméno a heslo.

V případě použití univerzálního jména a hesla by zabezpečení přenášených dat zůstalo na vysoké úrovni, neboť šifrovací klíče se odvozují pro každé přihlášené zařízení zvlášť a nebylo by tak možné odposlouchávat přenášená data, byť se znalostí přihlašovacích údajů.

Nevýhodou výše uvedeného řešení je nutná podpora WPA2 Enterprise ze strany služebních zařízení i zařízení cestujících. Dále je potřeba případná aktualizace uživatelských jmen a hesel na základě vydaných jízdenek.

2.1.3 Doporučení

Jako vhodnou variantu pro případnou realizaci bych doporučoval použití jednoduchého přístupového bodu spolu s nezabezpečeným připojení v kombinaci s VPN. Použití jednoduchého přístupového bodu je zvoleno z důvodu nižší finanční náročnosti. Nezabezpečený přístup byl vybrán proto, že i v dnešní době existuje spousta klientských zařízení, zejména u cestujících, které nepodporují technologii WPA2 Enterprise. Je tak dáno buď omezením v podobě hardwaru nebo nedostatečné podpory ze strany operačního systému.

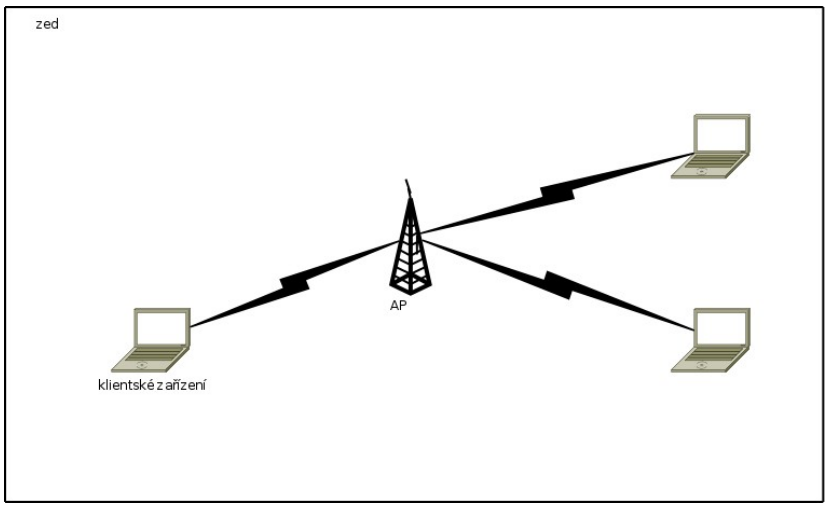
Použití VPN bylo zvoleno z důvodu vysokého stupně zabezpečení i přes nepoužití zabezpečeného připojení na úrovni fyzické vrstvy. Dále také dostupnost snadno modifikovatelné implementace v podobě OpenVPN, dnes již ve verzi 2.x. S tím souvisí snadnější nasazení než v případě použití nějaké proprietární verze VPN.

Zabezpečení pomocí WEP nebylo zvoleno záměrně proto, neboť neposkytuje žádnou kontrolu nad přístupem do sítě. Přístup mají všichni, kteří znají WEP klíč, což by v případě

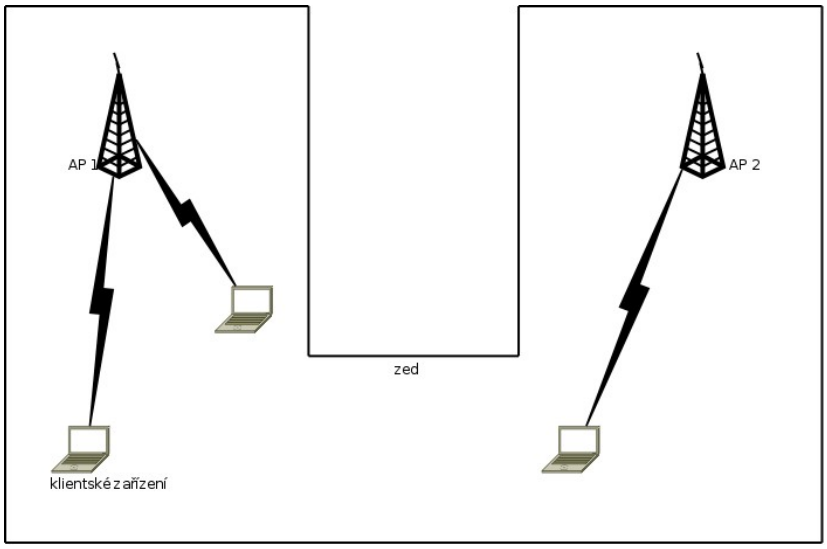
veřejně použitelného bodu byli všichni. Ani větší úroveň zabezpečení než u nešifrovaného spojení zde není, neboť každý kdo zná klíč, může přenášená data snadno dešifrovat.

2.2 Železniční stanice

Pokrytí železniční stanice je určeno cestujícím pro připojení k internetu a pro přístup do služební sítě pro vlakový personál. Uváděny jsou případy jak pro prostory bez architektonických překážek, kde pokrývané místo je tvořeno jednou halou, např. nádraží v Pardubicích (obr. 17), tak i pro prostory, které nelze jedním přístupovým bodem pokrýt, např. hlavní nádraží v Praze (obr. 18). Přístupový bod by byl ve všech uváděných případech umístěn pod stropem haly, aby bylo dosaženo co nejlepšího pokrytí.



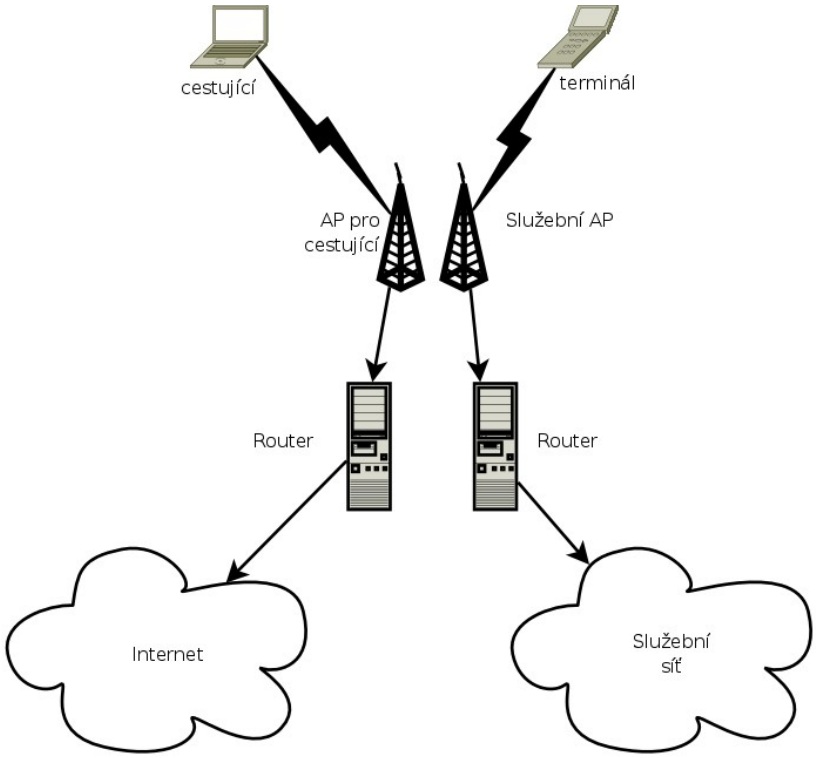
Obrázek 17: Jednoduchá stavba



Obrázek 18: Složitá stavba

2.2.1 Jeden zdvojený přístupový bod

Jedná se o použití dvou přístupových bodů umístěných vedle sebe, případně zdvojeného přístupového bodu, kde jsou obě bezdrátové části umístěny v rámci jediného zařízení. Výhodou je snazší oddělení sítě pro služební provoz a pro přístup veřejnosti k internetu. Nevýhodou zůstávají vyšší pořizovací náklady.

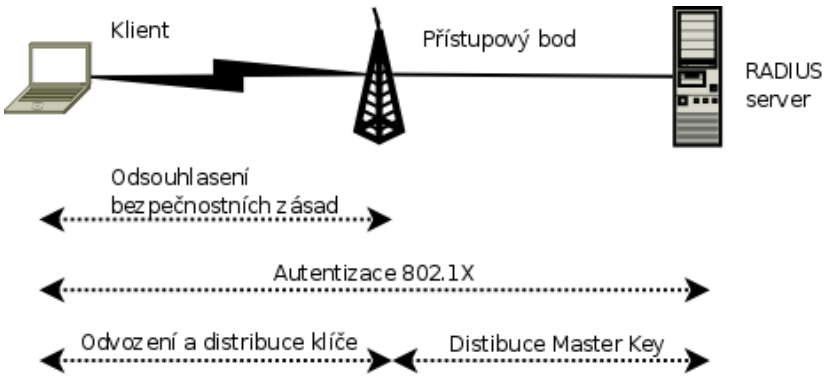


Obrázek 19: Zdvojený přístupový bod

Modelová situace uvažuje, že pro pokrytí oblasti bude jeden zdvojený bod se všesměrovou anténou stačit. Jedná se tedy o pokrytí nádražních hal bez výrazných architektonických překážek.

2.2.1.1 Použití WPA2 Enterprise a nešifrovaného přístupu

Pro každý přístupový bod je zvolena jiná metodika zabezpečení přístupu. Pro přístupový bod obsluhující služební síť je zde využito zabezpečení pomocí WPA2 Enterprise, obsahující ověřování proti RADIUS serveru pomocí PEAP (obr. 20). Pro přístupový bod obsluhující připojení k internetu pro cestující není zvoleno žádné zabezpečení přístupu. Autorizace přístupu založená na PEAP vyžaduje, aby všechny přístupové body fungující v rámci přístupu do služební sítě byly vybaveny certifikáty, podepsanými určenou certifikační autoritou. Certifikát zajišťuje ochranu před vytvořením falešného přístupového bodu za účelem získání přihlašovacích údajů.



Obrázek 20: Přihlašování pomocí WPA2 Enterprise

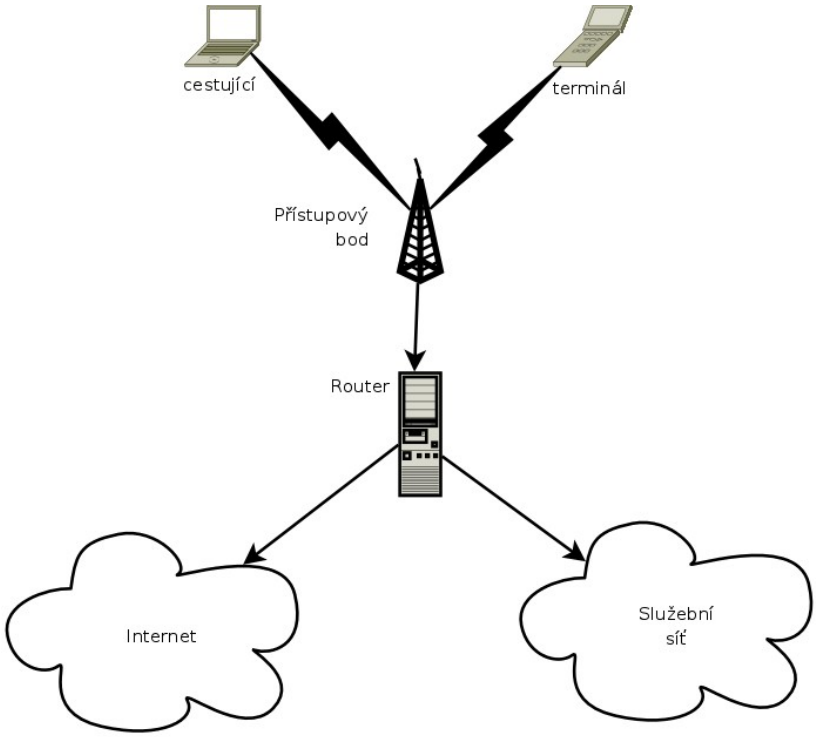
Při přihlašování do služební sítě je možno ověřovat buďto totožnost zařízení (terminálu, atd.) nebo uživatele pracujícího s daným zařízením. V případě ověřování zařízení je přihlašovací jméno a heslo uloženo v daném zařízení trvale a v případě potřeby a dosahu přístupového bodu dojde k jeho přihlášení do služební sítě. V případě ověřování uživatele je uživatelské jméno a heslo uživatele uloženo pouze dočasně. To pro případ, aby při novém přihlašování do sítě nebylo nutné znovu zadávat uživatelské jméno a heslo. Po připojení zařízení k přístupovému bodu dojde k poslání uživatelského jména a hesla pomocí protokolu PEAP RADIUS serveru. Ten podle oprávněnosti uživatelského jména a správnosti hesla rozhodne o povolení nebo zamítnutí autorizace klientského zařízení. V případě úspěšné autorizace dojde k přidělení IP adresy klientskému zařízení DHCP serverem.

Použití bezdrátové sítě cestujícími v dosahu přístupového bodu pro přístup k internetu vyžaduje pouze zvolení sítě podle ESSID. Je tak možno učinit s jakýmkoliv zařízením obsahujícím Wi-Fi rozhraní (notebook, PDA, atd.). Po přihlášení zařízení k veřejné síti dojde k přidělení IP adresy od DHCP serveru. Komunikace cestujících není mezi přístupovým bodem a jejích zařízením nijak šifrována.

Nevýhodou tohoto řešení je nutnost, aby veškerá zařízení určená pro komunikaci pomocí služební sítě zvládala protokol WPA2 Enterprise. To je na druhou stranu vykoupeno nekompromisním stupněm zabezpečení přístupu a šifrováním komunikace. Další nevýhodou je neomezený přístup cestujících i ostatních osob v dosahu přístupového bodu k internetu. Použití přístupového bodu nelze nijak regulovat ani omezovat.

2.2.2 Jeden jednoduchý přístupový bod

Jedná se o použití pouze jednoho přístupového bodu pro komunikaci jak služební, tak i pro cestující. Výhodou je jednodušší konfigurace, kdy se nastavuje pouze jeden přístupový bod. Nevýhodou je nutný kompromis v použití metodiky zabezpečení přístupu, aby byl použitelný jak pro služební účely, tak pro cestující. Nutné je také oddělení služební sítě od sítě využívané cestujícími.



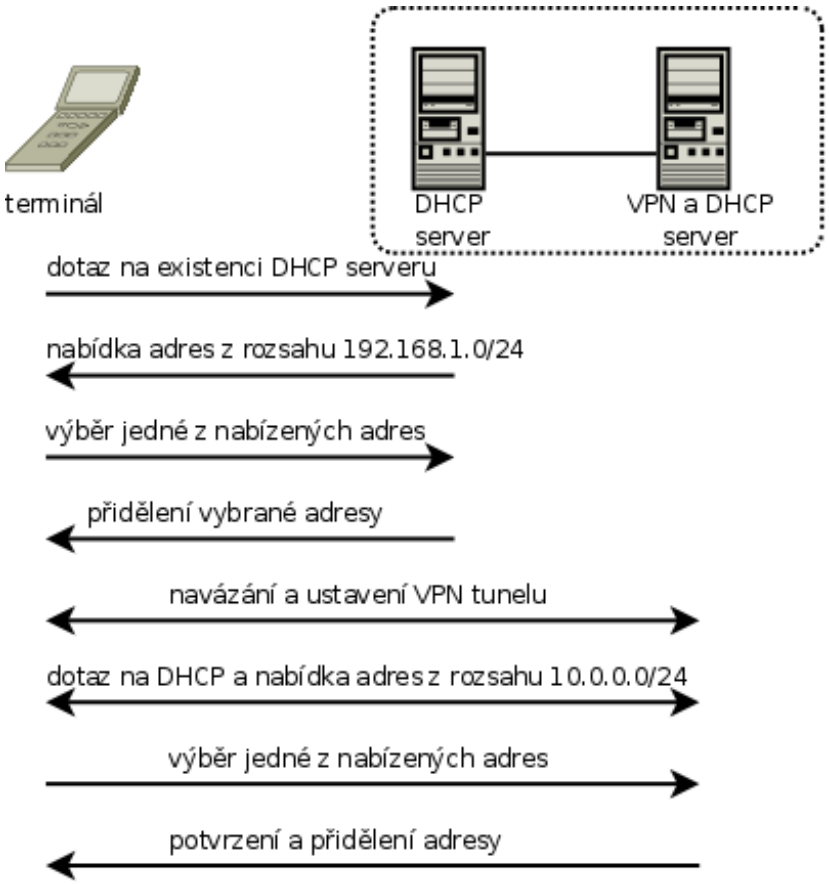
Obrázek 21: Jednoduchý přístupový bod

2.2.2.1 Použití nešifrovaného přístupu a VPN

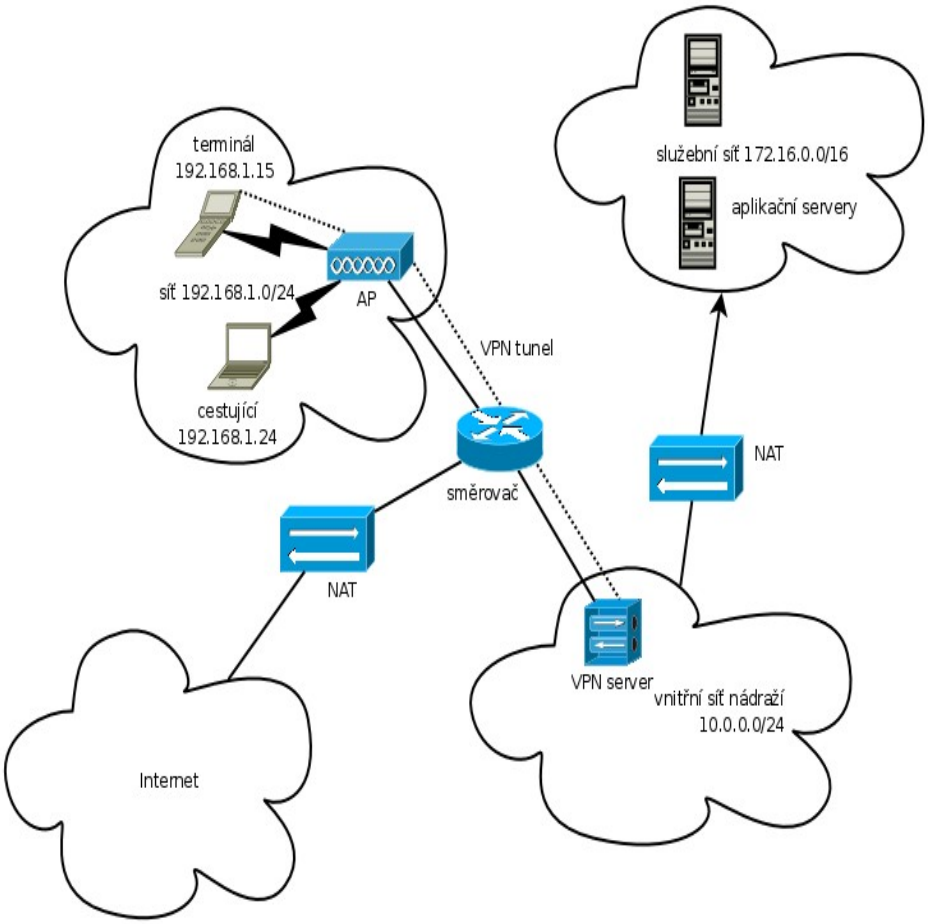
Pro přístupový bod používaný jak pro služební účely, tak i pro přístup cestujících k internetu není zvoleno žádné zabezpečení přístupu. Jelikož na úrovni přístupového bodu není možné odlišovat služební zařízení od zařízení cestujících, je nutné vyřešit přístup do služební sítě pomocí VPN. Vhodným kandidátem na použití VPN je software OpenVPN, jenž je multiplatformní a je distribuován pod licencí GPL verze 2. S licencí souvisí dostupnost zdrojových kódů a tím pádem snadnější modifikace pro potřeby služebních zařízení.

Při přihlašování do služební sítě dojde nejdříve k přihlášení služebního zařízení k přístupovému bodu a následnému přidělení IP adresy z rozsahu 192.168.x.0/24 od DHCP serveru. Poté je nutné, přihlásit se pomocí VPN do vnitřní služební sítě a oddělit a šifrovat tak služební provoz. Po přihlášení se do VPN dojde k opětovnému přidělení IP adresy, tentokrát pro virtuální síťové rozhraní a z rozsahu 10.0.0.0/24 (obr. 23). Celý proces přidělování adres se sestává z následujících kroků (obr. 22):

- broadcast dotaz na přítomnost DHCP serveru po přihlášení k AP
- nabídnutí použitelných IP adres z rozsahu 192.168.x.0/24 DHCP serverem
- výběr IP adresy klientem
- potvrzení a přidělení IP adresy
- navázání VPN spojení
- broadcast dotaz na DHCP server, tentokrát přes virtuální síťové rozhraní
- nabídnutí použitelných IP adres z rozsahu 10.0.0.0/24 DHCP serverem
- výběr IP adresy klientem
- potvrzení a přidělení IP adresy pro virtuální síťové rozhraní



Obrázek 22: Přidělování IP adres



Obrázek 23: Jednotlivé sítě a rozsahy adres

Přihlášení k VPN může být na základě certifikátu vydaném vnitřní certifikační autoritou a ověřovat tak totožnost zařízení (terminálu) nebo certifikát přiřadit každému uživateli terminálu např. na USB flash disku, jenž by bylo nutné do zařízení připojit ještě před přihlášením. Druhou možností, jak ověřovat totožnost uživatele, je použití uživatelského jména a hesla. Přihlašovací údaje v druhém případě, se posílají již zašifrovaným komunikačním kanálem a nehrozí tak jejich odposlechnutí.

Použití bezdrátové sítě cestujícími v dosahu přístupového bodu pro přístup k internetu vyžaduje pouze zvolení sítě podle ESSID. Je tak možno učinit s jakýmkoliv zařízením obsahujícím Wi-Fi rozhraní. Po přihlášení zařízení k veřejné síti dojde k přidělení IP adresy od DHCP serveru. Komunikace cestujících není mezi přístupovým bodem a jejích zařízením nijak šifrována. Vnější rozhraní VPN serveru je pro cestující dostupné, nicméně bez certifikátu prakticky nepoužitelné a nehrozí tak jeho zneužití.

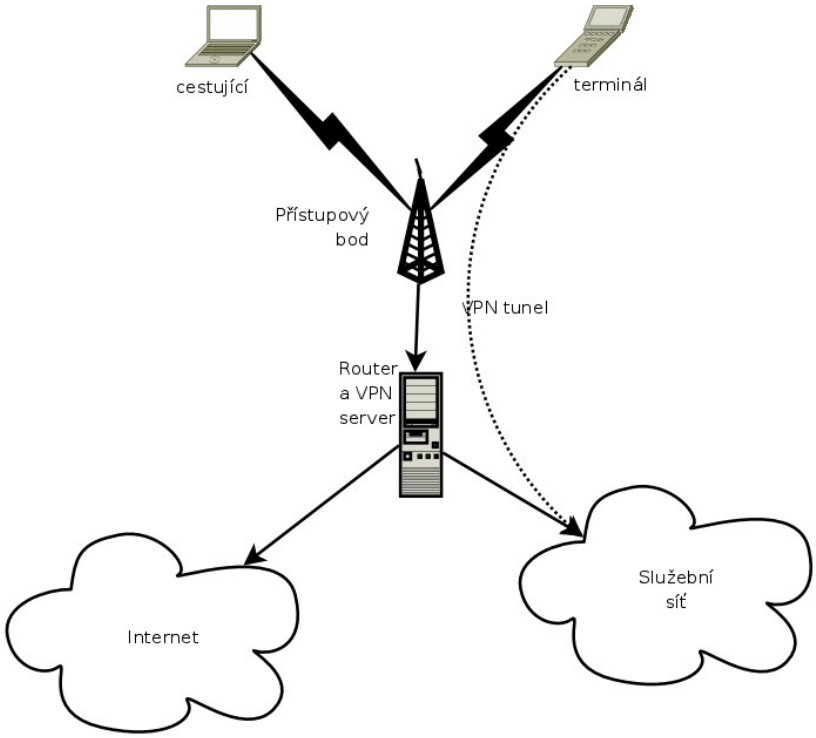
Nevýhodou výše uvedeného řešení je složitější správa, zahrnující jak přístupový bod, tak i VPN server. Dále nutnost podpory VPN služebním klientským zařízením. Díky otevřenému a nekontrolovatelnému přístupu k přístupovému bodu je rovněž možné úmyslné rušení služební komunikace např. posíláním deautentizačních paketů. Použití nezabezpečené bezdrátové sítě nechává otázku zabezpečení přenášených dat na cestujících. Ať už používáním zabezpečeného spojení pomocí SSL pro citlivá data nebo vytvořením vlastní VPN, pokud by bylo třeba šifrovat veškerý provoz.

2.2.2.2 Použití WPA2 Enterprise a VPN

Pro přístupový bod používaný jak pro služební účely, tak i pro přístup cestujících k internetu je zvoleno zabezpečení přístupu pomocí WPA2 Enterprise. Jelikož na úrovni přístupového bodu není možné odlišovat služební zařízení od zařízení cestujících, je nutné vyřešit přístup do služební sítě pomocí VPN (obr. 24).

Při přihlašování do služební sítě je možno ověřovat buďto totožnost zařízení (terminálu, atd.) nebo uživatele pracujícího s daným zařízením. V případě ověřování zařízení je přihlašovací jméno a heslo uloženo v daném zařízení trvale a v případě potřeby a dosahu přístupového bodu dojde k jeho přihlášení do služební sítě. V případě ověřování uživatele je uživatelské jméno a heslo uživatele uloženo pouze dočasně. To pro případ, aby při novém přihlašování do sítě nebylo nutné znovu zadávat uživatelské jméno a heslo. Po připojení zařízení k přístupovému bodu dojde k poslání uživatelského jména a hesla pomocí protokolu PEAP RADIUS serveru. Ten podle oprávněnosti uživatelského jména a správnosti hesla rozhodne o povolení nebo zamítnutí autorizace klientského zařízení. V případě úspěšné autorizace dojde k přidělení IP adresy klientskému zařízení DHCP serverem. Poté je nutné, přihlásit se pomocí VPN do vnitřní služební sítě a oddělit tak služební provoz. Další šifrování v podobě VPN již není nezbytně nutné a jedná se v tomto případě o zbytečnou vlastnost VPN. Při šifrování komunikace na úrovni fyzické vrstvy se používá pro každé zařízení jiný *Master Key* a není proto prakticky možné komunikaci odposlouchávat. Přihlášení do VPN může být na základě certifikátu vydaném vnitřní certifikační autoritou a ověřovat tak totožnost zařízení (terminálu) nebo certifikát přiřadit každému uživateli terminálu např. na USB flash disku, jenž by bylo nutné do zařízení

připojit ještě před přihlášením. Druhou možností, jak ověřovat totožnost uživatele, je použití uživatelského jména a hesla.



Obrázek 24: VPN

Použití bezdrátové sítě cestujícími v dosahu přístupového bodu vyžaduje zvolení správného přístupového bodu na základě ESSID. Dále je nutné, autorizovat cestujícího pro přístup do sítě na základě uživatelského jména a hesla. Jako uživatelské jméno a heslo lze použít číslo vydané jízdenky, jenž by bylo uloženo v RADIUS serveru s dobou platnosti odpovídající platnosti jízdenky. To by umožňovalo připojení k síti pouze cestujícím s platnou jízdenkou. Systém uživatelských jmen a hesel by bylo možné dále rozšířit např. o možnost přístupu do sítě jen pro jízdenky první třídy nebo jen pro dané kategorie vlaků. Další možnou variantou by bylo vybrání univerzálního, všeobecně známého jména a hesla. Odpadla by tím synchronizace uživatelských jmen a hesel s vydanými jízdenkami. Oproti tomu by nebylo možné kontrolovat, kdo do sítě přístup má a kdo ne. Přístup by měli všichni cestující, kteří by věděli uživatelské jméno a heslo.

V případě použití univerzálního jména a hesla by zabezpečení přenášených dat zůstalo na vysoké úrovni, neboť šifrovací klíče se odvozují pro každé přihlášené zařízení zvlášť a nebylo by tak možné odposlouchávat přenášená data, byť se znalostí přihlašovacích údajů.

Nevýhodou výše uvedeného řešení je nutná podpora WPA2 Enterprise ze strany služebních zařízení i zařízení cestujících. Dále je potřeba případná aktualizace uživatelských jmen a hesel na základě vydaných jízdenek.

2.2.3 Doporučení

Jako vhodnou variantu pro případnou realizaci bych doporučoval rovněž použití jednoduchého přístupového bodu spolu s nezabezpečeným připojením v kombinaci s VPN. Použití jednoduchého přístupového bodu je zvoleno z důvodu nižší finanční náročnosti. Nezabezpečený přístup byl vybrán proto, že i v dnešní době existuje spousta klientských zařízení, zejména u cestujících, která nepodporují technologii WPA2 Enterprise. Je tak dáno buď omezením v podobě hardwaru nebo nedostatečné podpory ze strany operačního systému.

Použití VPN bylo zvoleno z důvodu vysokého stupně zabezpečení i přes nepoužití zabezpečeného připojení na úrovni fyzické vrstvy. Dále také dostupnost snadno modifikovatelné implementace v podobě OpenVPN. S tím souvisí snadnější nasazení než v případě použití proprietární verze VPN.

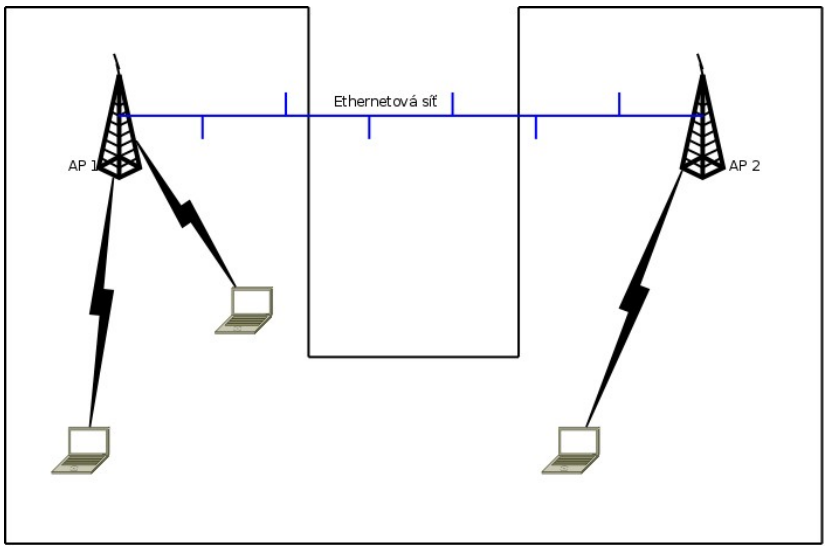
V případě, že by byl zájem na striktním omezení přístupu k internetu pouze pro cestující s platnou jízdenkou a zamezení tak využívání všemi, kdož mají přístup na nádraží či do okolí nádražních budov, by bylo nutné použít variantu s jednoduchým přístupovým bodem a zabezpečením pomocí WPA2 Enterprise spolu s použitím VPN.

Zabezpečení pomocí WEP ani zde nebylo zvoleno záměrně proto, neboť neposkytuje žádnou kontrolu nad přístupem do sítě. Přístup mají všichni, kteří znají WEP klíč, což by v případě veřejně použitelného bodu byli všichni. Ani větší úroveň zabezpečení než u nešifrovaného spojení zde není, neboť každý kdo zná klíč, může přenášená data snadno dešifrovat.

2.2.4 Více přístupových bodů spojených ethernetem

Jedná se o spojení více přístupových bodů v rámci jedné lokality pomocí ethernetu. Každý přístupový bod slouží jak pro služební účely, tak i pro připojení cestujících k internetu. Umožněna je mobilita připojených zařízení, byť s jistými omezeními. Jelikož se

jedná o samostatné přístupové body mající společné pouze ESSID, lze použít stejné mechanismy pro šifrování dat a řízení přístupu jako v případě jednotlivého přístupového bodu.



Obrázek 25: Stavba s překážkami

2.2.4.1 Použití nešifrovaného přístupu a VPN

Pro přístupový bod používaný jak pro služební účely, tak i pro přístup cestujících k internetu není zvoleno žádné zabezpečení přístupu. Jelikož na úrovni přístupového bodu není možné odlišovat služební zařízení od zařízení cestujících, je nutné vyřešit přístup do služební sítě pomocí VPN.

Při přihlašování do služební sítě dojde nejdříve k přihlášení služebního zařízení k přístupovému bodu a následnému přidělení IP adresy od DHCP serveru. Poté je nutné, přihlásit se pomocí VPN do vnitřní služební sítě a oddělit a šifrovat tak služební provoz. Přihlášení může být na základě certifikátu vydaném vnitřní certifikační autoritou a ověřovat tak totožnost zařízení (terminálu) nebo certifikát přiřadit každému uživateli terminálu např. na USB flash disku, jenž by bylo nutné do zařízení připojit ještě před přihlášením. Druhou možností, jak ověřovat totožnost uživatele, je použití uživatelského jména a hesla. V případě pohybu připojeného služebního zařízení nad rámec dosahu přístupového bodu, k němuž je zařízení připojeno a k poklesu síly signálu pod určitou mez, dojde k jeho přepojení na přístupový bod se silnějším signálem. V tomto případě se po

přihlášení k přístupovému bodu IP adresa od DHCP serveru znovu nežádá, neboť je určena doba propůjčení adresy danému zařízení. Pokud doba zapůjčení IP adresy ještě nevypršela, není nutná její obnova. Spojení mezi klientským zařízením a VPN serverem není také nutno obnovovat. Spojení je dostatečně robustní a krátkodobý výpadek v podobě přepojování k jinému přístupovému bodu nezpůsobí jeho přerušení.

Použití bezdrátové sítě cestujícími v dosahu přístupového bodu pro přístup k internetu vyžaduje pouze zvolení sítě podle ESSID. Je tak možno učinit s jakýmkoliv zařízením obsahujícím Wi-Fi rozhraní. Po přihlášení zařízení k veřejné síti dojde k přidělení IP adresy od DHCP serveru. V případě pohybu připojeného zařízení nad rámec dosahu přístupového bodu, k němuž je zařízení připojeno a k poklesu síly signálu pod určitou mez, dojde k jeho přepojení na přístupový bod se silnějším signálem. V tomto případě se po přihlášení k přístupovému bodu IP adresa od DHCP serveru znovu nežádá, neboť je určena doba propůjčení adresy danému zařízení. Pokud doba zapůjčení IP adresy ještě nevypršela, není nutná její obnova.

Nevýhodou výše uvedeného řešení je složitější správa, zahrnující jak přístupový bod, tak i VPN server. Dále nutnost podpory VPN služebním klientským zařízením. Díky otevřenému a nekontrolovatelnému přístupu k přístupovému bodu je rovněž možné úmyslné rušení služební komunikace např. posíláním deautentizačních paketů. Použití nezabezpečené bezdrátové sítě nechává otázku zabezpečení přenášených dat na cestujících. Další nevýhodou je nutná podpora na aplikační úrovni ze strany připojených zařízení, kvůli přepojování z jednoho přístupového bodu na druhý v případě poklesu signálu.

2.2.4.2 WPA2 Enterprise a VPN

Pro přístupový bod používaný jak pro služební účely, tak i pro přístup cestujících k internetu je zvoleno zabezpečení přístupu pomocí WPA2 Enterprise. Jelikož na úrovni přístupového bodu není možné odlišovat služební zařízení od zařízení cestujících, je nutné vyřešit přístup do služební sítě pomocí VPN (obr. 24).

Při přihlašování do služební sítě je možno ověřovat buď totožnost zařízení (terminálu, atd.), nebo uživatele pracujícího s daným zařízením. V případě ověřování zařízení je přihlašovací jméno a heslo uloženo v daném zařízení trvale a v případě potřeby a dosahu

přístupového bodu dojde k jeho přihlášení do služební sítě. V případě ověřování uživatele je uživatelské jméno a heslo uživatele uloženo pouze dočasně. To pro případ, aby při novém přihlašování do sítě nebylo nutné znovu zadávat uživatelské jméno a heslo. Po připojení zařízení k přístupovému bodu dojde k poslání uživatelského jména a hesla pomocí protokolu PEAP RADIUS serveru. Ten podle oprávněnosti uživatelského jména a správnosti hesla rozhodne o povolení nebo zamítnutí autorizace klientského zařízení. V případě úspěšné autorizace dojde k přidělení IP adresy klientskému zařízení DHCP serverem. Poté je nutné, přihlásit se pomocí VPN do vnitřní služební sítě a oddělit tak služební provoz. Další šifrování v podobě VPN již není nezbytně nutné a jedná se v tomto případě o zbytečnou vlastnost VPN. Při šifrování komunikace na úrovni fyzické vrstvy se používá pro každé zařízení jiný *Master Key* a není proto prakticky možné komunikaci odposlouchávat. Přihlášení do VPN může být na základě certifikátu vydaném vnitřní certifikační autoritou a ověřovat tak totožnost zařízení (terminálu) nebo certifikát přiřadit každému uživateli terminálu např. na USB flash disku, jenž by bylo nutné do zařízení připojit ještě před přihlášením. Druhou možností jak ověřovat totožnost uživatele je použití uživatelského jména a hesla.

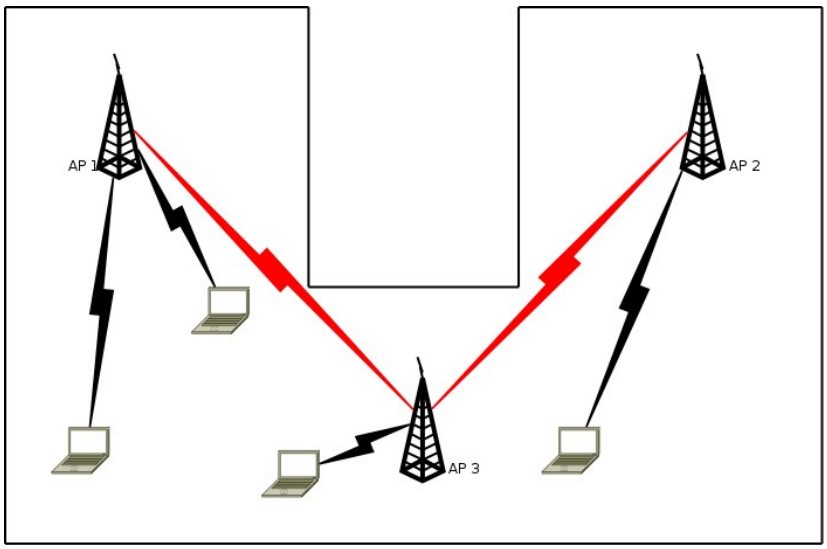
Použití bezdrátové sítě cestujícími v dosahu přístupového bodu vyžaduje zvolení správného přístupového bodu na základě ESSID. Dále je nutné, autorizovat cestujícího pro přístup do sítě na základě uživatelského jména a hesla. Jako uživatelské jméno a heslo lze použít číslo vydané jízdenky, jenž by bylo uloženo v RADIUS serveru s dobou platnosti odpovídající platnosti jízdenky. To by umožňovalo připojení k síti pouze cestujícím s platnou jízdenkou. Další možnou variantou by bylo vybrání univerzálního, všeobecně známého jména a hesla. Odpadla by tím synchronizace uživatelských jmen a hesel s vydanými jízdenkami. Oproti tomu by nebylo možné kontrolovat, kdo do sítě přístup má a kdo ne. Přístup by měli všichni cestující, kteří by věděli uživatelské jméno a heslo.

V případě použití univerzálního jména a hesla by zabezpečení přenášených dat zůstalo na vysoké úrovni, neboť šifrovací klíče se odvozují pro každé přihlášené zařízení zvlášť a nebylo by tak možné odposlouchávat přenášená data, byť se znalostí přihlašovacích údajů.

Nevýhodou výše uvedeného řešení je nutná podpora WPA2 Enterprise ze strany služebních zařízení i zařízení cestujících. Dále je potřeba již v předchozí části zmíněná případná aktualizace uživatelských jmen a hesel na základě vydaných jízdenek.

2.2.5 Více přístupových bodů spojených WDS

Jedná se o propojení přístupových bodů v rámci jedné lokality pomocí WDS. To s sebou přináší nevýhodu v podobě možné nekompatibility přístupových bodů od různých výrobců, ale také nemožnost použití pokročilých metod řízení přístupu a šifrování dat.



Obrázek 26: Stavba s překážkami

2.2.5.1 Použití nešifrovaného přístupu a VPN

Pro přístupový bod používaný jak pro služební účely, tak i pro přístup cestujících k internetu není zvoleno žádné zabezpečení přístupu. Na úrovni přístupového bodu není možné odlišovat služební zařízení od zařízení cestujících a je proto nutné vyřešit přístup do služební sítě pomocí VPN.

Při přihlašování do služební sítě dojde nejdříve k přihlášení služebního zařízení k přístupovému bodu a následnému přidělení IP adresy od DHCP serveru. Poté je nutné, přihlásit se pomocí VPN do vnitřní služební sítě a oddělit a šifrovat tak služební provoz.

V případě pohybu připojeného služebního zařízení nad rámec dosahu přístupového bodu, k němuž je zařízení připojeno a k poklesu síly signálu pod určitou mez, dojde k jeho přepojení na přístupový bod se silnějším signálem. V tomto případě se po přihlášení k přístupovému bodu IP adresa od DHCP serveru znovu nežádá, neboť je určena doba propůjčení adresy danému zařízení. Pokud doba zapůjčení IP adresy ještě nevypršela, není nutná její obnova. Spojení mezi klientským zařízením a VPN serverem není také nutno obnovovat. Spojení je dostatečně robustní a krátkodobý výpadek v podobě přepojování k jinému přístupovému bodu nezpůsobí jeho přerušení.

Použití bezdrátové sítě cestujícími v dosahu přístupového bodu pro přístup k internetu vyžaduje pouze zvolení sítě podle ESSID. Po přihlášení zařízení k veřejné síti

dojde k přidělení IP adresy od DHCP serveru. V případě pohybu připojeného služebního zařízení nad rámec dosahu přístupového bodu, k němuž je zařízení připojeno a k poklesu síly signálu pod určitou mez, dojde k jeho přepojení na přístupový bod se silnějším signálem.

Nevýhodou výše uvedeného řešení je složitější správa, zahrnující jak přístupový bod, tak i VPN server. Dále nutnost podpory VPN služebním klientským zařízením. Použití nezabezpečené bezdrátové sítě nechává otázku zabezpečení přenášených dat na cestujících. Další nevýhodou je nutná podpora na aplikační úrovni ze strany připojených zařízení, kvůli přepojování z jednoho přístupového bodu na druhý v případě poklesu signálu. Rychlost přenášených dat je v tomto případě limitována použitím WDS.

2.2.6 Doporučení

Jako vhodnou variantu pro případnou realizaci bych doporučoval použití přístupových bodů spojených ethernetem spolu s nezabezpečeným připojení v kombinaci s VPN. Nezabezpečený přístup byl vybrán proto, že i v dnešní době existuje spousta klientských zařízení, zejména u cestujících, které nepodporují technologii WPA2 Enterprise. Je tak dáno buď omezením v podobě hardwaru nebo nedostatečné podpory ze strany operačního systému. Spojení přístupových bodů pomocí ethernetu bylo vybráno z důvodu možného zvýšení zabezpečení až na úroveň WPA2 Enterprise, což by v případě použití WDS nebylo možné. Dále je toto řešení vhodnější vzhledem k výším přenosovým rychlostem, neboť u WDS se s každým dalším „přeskokem“ rychlost snižuje na polovinu.

Použití VPN bylo zvoleno z důvodu vysokého stupně zabezpečení i přes nepoužití zabezpečeného připojení na úrovni fyzické vrstvy. Dále také dostupnost snadno modifikovatelné implementace v podobě OpenVPN. S tím souvisí snadnější nasazení než v případě použití proprietární verze VPN.

V případě, že by byl zájem na striktní omezení přístupu k internetu pouze pro cestující s platnou jízdenkou a zamezení tak využívání všemi, kdož mají přístup na nádraží či do okolí nádražních budov, by bylo nutné použít variantu s jednoduchým přístupovým bodem a zabezpečením pomocí WPA2 Enterprise spolu s použitím VPN.

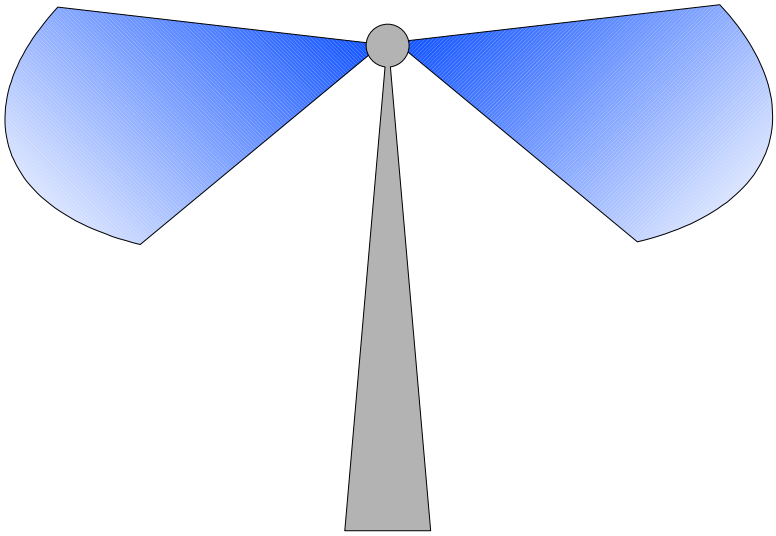
Zabezpečení pomocí WEP nebylo zvoleno záměrně proto, neboť neposkytuje žádnou kontrolu nad přístupem do sítě. Přístup mají všichni, kteří znají WEP klíč, což by v případě veřejně použitelného bodu byli všichni. Ani větší úroveň zabezpečení než u nešifrovaného spojení zde není, neboť každý kdo zná klíč, může přenášená data snadno dešifrovat.

2.3 Kolejová vozidla v okolí stanice

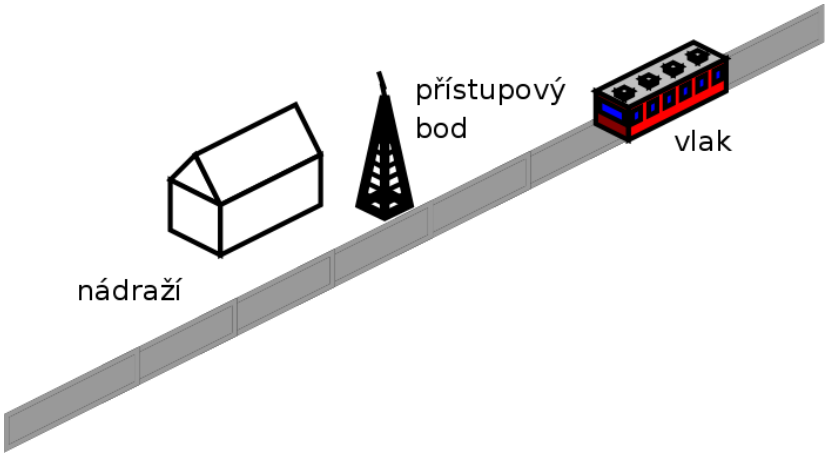
Modelová situace uvažuje pokrytí okolí stanice signálem z přístupových bodů pracujících s technologií Mobile WiMAX. To má za účel umožnit zde zastavujícím nebo projíždějícím vlakům vysokorychlostní spojení do služební sítě nebo do internetu v případě cestujících. Uváděny jsou možnosti pokrytí stanice pomocí jednoho přístupového bodu nebo pomocí více bodů, jenž by si mezi sebou předávaly pohybující se klienty (vlaky). Pro pohybující klienty platí omezení v podobě maximální rychlosti, při níž je spojení stabilní. Ta je u technologie Mobile WiMAX 120 km/h.

2.3.1 Jeden přístupový bod

Pokrytí pomocí jednoho přístupového bodu je určeno pro potřeby malých stanic nebo pro místa na trati určená pro vysokorychlostní výměnu dat. Přístupový bod je umístěn na stožáru ve vhodné výšce nad tratí (obr. 28). Vzhledem k předpokládanému obousměrnému provozu by bylo vhodné využít možnosti technologie Mobile WiMAX a přístupový bod vybavit dvěma anténami, každá na jednu stranu. Dohromady by vyzařovací diagram obou antén tvořil lehce deformovanou ležatou osmičku (obr. 27).



Obrázek 27: Vyzařovací diagram antén

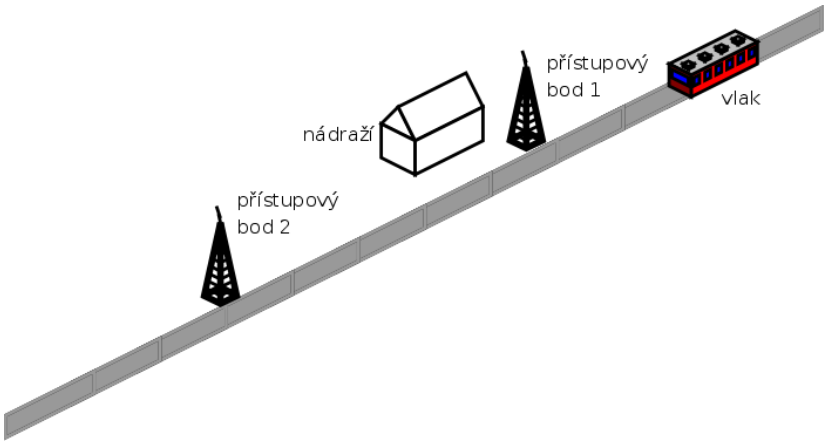


Obrázek 28: Jeden přístupový bod

Pokud je vlak v dosahu přístupového bodu, dojde k přihlášení a ověření totožnosti koncového bodu, v tomto případě umístěného ve vlaku. Koncové stanici je poté přidělena IP adresa z DHCP serveru z rozsahu 172.16.x.y/28. Vzhledem k tomu, že k přístupovému bodu se mohou přihlásit pouze stanice s platným certifikátem, není nutné oddělit provoz pomocí VPN neboť se nebudou moci připojit jiné, než předem určené stanice. Při výměně dat je ovšem nutno na aplikační úrovni ošetřit hlídání kvality signálu, aby nedošlo k náhlému přerušení přenosu vlivem slabého signálu.

2.3.2 Více přístupových bodů

Pokrytí signálem pomocí více než jednoho přístupového bodu (obr. 29) je vhodné pro stanice s větší rozlohou nebo pro případ, že výměna dat bude probíhat mezi přístupovým bodem a jedoucím vlakem. V takovém případě by si jednotlivé přístupové body mezi sebou klienta (vlak) předávaly a nedocházelo by tak k výpadkům spojení, resp. docházelo, ale v řádu desítek ms, což je dostatečně krátká doba i pro aplikace typu VoIP natož pro datové spojení.



Obrázek 29: Více přístupových bodů

Pokud je vlak v dosahu krajního přístupového bodu, dojde k přihlášení a ověření totožnosti koncového bodu, v tomto případě umístěného ve vlaku. Koncové stanici je poté přidělena IP adresa z DHCP serveru z rozsahu 172.16.x.y/28. I zde je při výměně dat ovšem nutno na aplikační úrovni ošetřit hlídání kvality signálu, aby nedošlo k náhlému přerušení přenosu vlivem slabého signálu.

2.3.3 Doporučení

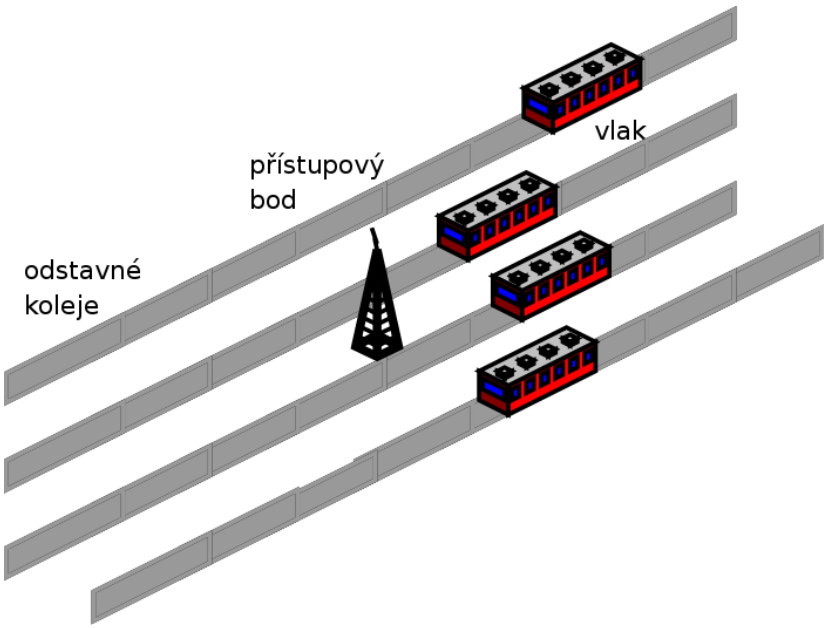
Pro větší stanice, resp. stanice s velkým provozem bych doporučoval použití varianty s více přístupovými body. Řešení je sice nákladnější, ale umožňuje vysokorychlostní datovou výměnu i pro vlaky, které pouze projíždějí a v případě jednoho přístupového bodu by nemusely být v dosahu signálu po dostatečně dlouhou dobu.

2.4 Depo kolejových vozidel

Modelová situace uvažuje použití vysokorychlostního datového spojení mezi přístupovým bodem a vlaky umístěnými v depu kolejových vozidel. Lze jej využít například pro přenos informací o aktivním odstavení elektrických jednotek řady 471.

2.4.1 Jeden přístupový bod

Pro dostatečné pokrytí je přístupový bod umístěn ve vhodné výšce nad depem kolejových vozidel (obr. 30). Přístupový bod je vybaven všesměrovou anténou pokrývající celou oblast depa. Místo jedné všesměrové antény je možné použití např. čtyř sektorových antén, každá s vyzařovacím úhlem 90°. To by přineslo výhodu v podobě pokrytí prostoru blízko stožáru, na němž by anténa byla umístěna, neboť všesměrová anténa má podle charakteristik omezené vertikální vyzařování a pod stožárem vniká hluché místo bez signálu. Sektorové antény by bylo možné natočit o vhodný úhel směrem k zemi a zmenšit tak hluché místo v okolí stožáru na minimum.

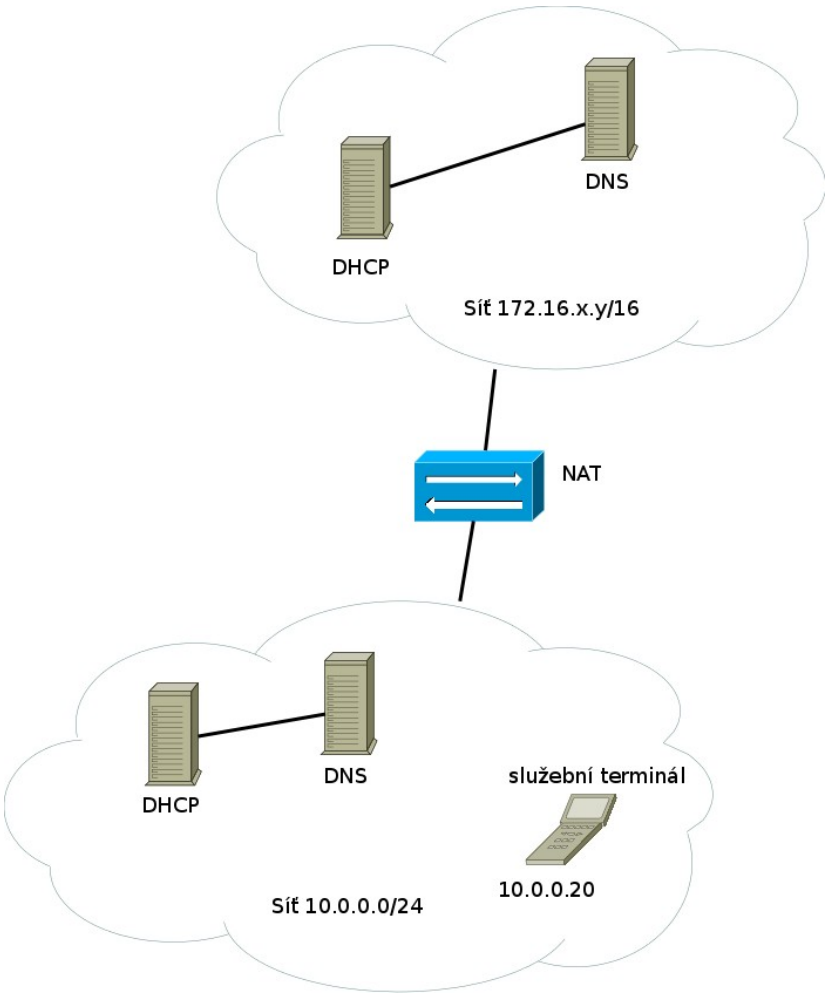


Obrázek 30: Odstavné kolejiště a umístění přístupového bodu

Pokud je vlak v dosahu přístupového bodu, dojde k přihlášení a ověření totožnosti koncového bodu, v tomto případě umístěného ve vlaku. Koncové stanici je poté přidělena IP adresa z DHCP serveru z rozsahu 172.16.x.y/28. Vzhledem k tomu, že k přístupovému budu se mohou přihlásit pouze stanice s platným certifikátem, není nutné oddělit provoz pomocí VPN, neboť se nebudou moci připojit jiné, než předem určené stanice. Není zde potřeba hlídat kvalitu signálu, neboť ta se bude v čase měnit jen velmi nepatrně a na přenos dat nebude mít vliv.

2.5 Použití DHCP a DNS serverů

Pokud má být nastavování klientských zařízení co nejjednodušší je potřeba, aby se o nastavování správných IP adresy nemuseli starat cestující, potažmo uživatelé přenosných terminálů, ale byla tato věc svěřena DHCP serverům. Použití DNS serverů je zase vhodné kvůli jednoduché adresaci zařízení v síti bez nutnosti znalosti jejich IP adresy. Pro každou síť, ať už 172.16.x.y/16 nebo 10.0.0.0/24 (obr. 31), která je za symetrickým NATem je zařízen jeden nebo více DHCP serverů a rovněž jeden primární a jeden sekundární DNS server. Důležitá je taktéž spolupráce těchto dvou typů serverů.

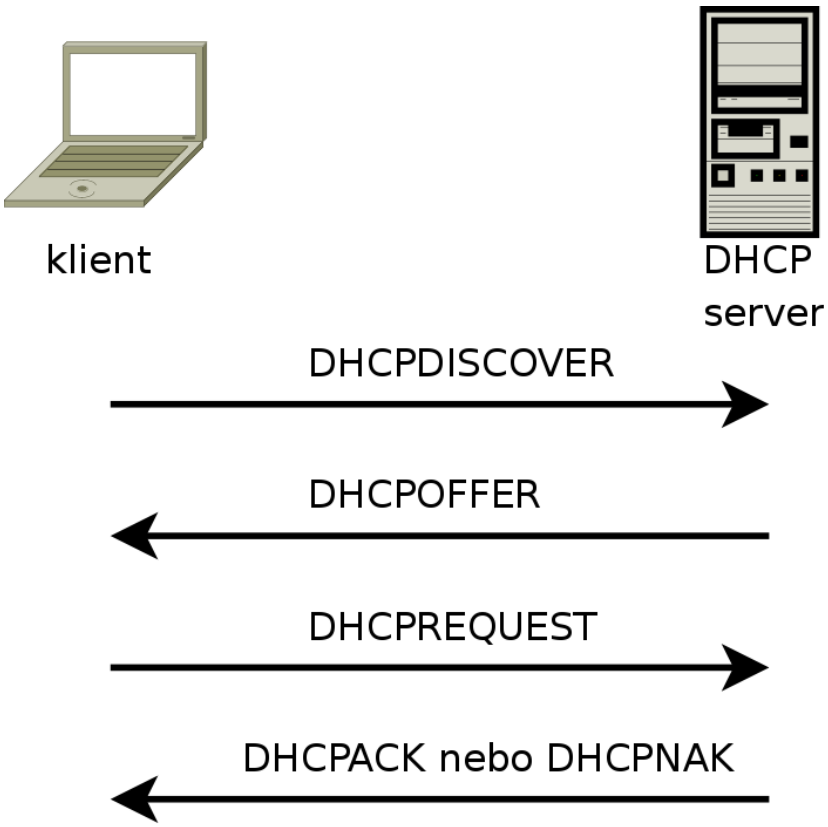


Obrázek 31: DHCP a DNS servery

2.5.1 DHCP

DHCP server slouží k nastavení klientské IP adresy, brány a DNS serverů, které by bylo jinak nutno nastavovat automaticky. Pokud klient použije DHCP server pro získání informací o nastavení, sestává se toto ze čtyř kroků (obr. 32).

- klient pošle na omezenou všeobecnou vysílací adresu paket DHCPDISCOVER se svojí identifikací (MAC adresa, jméno)
- server odpoví paketem DHCPOFFER
- klient vybere odpovídající nastavení a odpoví paketem DHCPREQUEST
- server výběr potvrdí paketem DHCPACK nebo zamítne paketem DHCPNAK



Obrázek 32: Postup získávání informací od DHCP serveru

Poté co klient získá potřebné informace od DHCP serveru, nastaví potřebné parametry podle nich. DHCP server zaktualizuje záznam DNS serveru, aby byl nově připojený klient snadno adresovatelný podle svého jména v dané doméně.

Jako konkrétní implementaci DHCP serveru je možno použít DHCP server konsorcia ISC, který je šířen pod licencí GPL verze 2.

2.5.2 DNS

DNS server slouží ke snadnější adresaci koncových zařízení pomocí slovních názvů namísto IP adres. Je pak možno adresovat např. terminál průvodčího ve vlaku č. 5648 zadáním „*pruvodci.5648.vlaky.cdrail*“. Kde *cdrail* bude kořenová doména, *vlaky* bude doména obsahující čísla vlaků, *5648* bude číslo konkrétního vlaku a *pruvodci* je koncové zařízení v daném vlaku. V každém vlaku rovněž poběží DNS server, který určí, kterou konkrétní IP adresu mám v danou dobu terminál průvodčího přidělenou od DHCP serveru.

Jako konkrétní implementaci DNS serveru doporučuji použít buďto server BIND verze 9 nebo server Unbound verze 1.0. Oba dva servery jsou šířeny pod licencí BSD. Rovněž oba dva servery podporují technologii DNSSEC sloužící k ověření pravosti odpovědi od DNS serveru.

3 Závěr

Technologie WiFi je vhodná pro nasazení v železničních stanicích a vagonech a všude tam, kde nedochází k velkému pohybu připojených klientů nad rámec pokrytí přístupovým bodem. Zabezpečení je vhodné zvolit slabší a dodatečné zabezpečení řešit až na úrovni síťové vrstvy, vzhledem k poměrně vysoké penetraci zařízení neumožňujících použití pokročilých metod zabezpečení.

Naproti tomu technologie Mobile WiMAX je vhodným kandidátem pro pokrytí rozsáhlejších oblasti i za předpokladu přecházení od jednoho přístupového bodu k druhému. Zabezpečení je zde na velmi vysoké úrovni již od základu a není proto nutné volit další bezpečnostní opatření.

Seznam použité literatury

[1] DOSTÁLEK, L. a KABELOVÁ, A. Velký průvodce protokoly TCP/IP a systémem DNS. 3 vyd. Praha: Computer Press, 2002. ISBN 80-7226-675-6

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

[3] STALLINGS, W. Cryptography and Network Security: Principles and Praktice. 3rd ed. Upper Saddle River: Pearson Education, 2003. ISBN 0-13-111502-2

[4] ZANDL, P. Bezdrátové sítě WiFi: praktický průvodce. 1. vyd. Brno: Computer Press, 2003. ISBN 80-7226-632-2

[5] DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. 1. vyd. Brno: Computer Press, 2004. ISBN 80-251-0106-1

[6] GUILLAUME, L. Bezpečnost Wi-Fi – WEP, WPA a WPA2. Hakin9. Praha: Software Media, č. 1/2006, s. 14–27. ISSN 1214-7710

[7] PUŽMANOVÁ, R., ŠKRHÁ, P. Propojování sítí s TCP/IP. České Budějovice: Kopp, 1999. ISBN 80-7232-080-7

[8] PUŽMANOVÁ, R. Širokopásmový Internet. Přístupové a domácí sítě. Brno: Computer Press, 2004. ISBN 80-251-0139-8

[9] ZANDL, P. Bezdrátové sítě WiFi. Brno: Computer Press, 2003. ISBN 80-722-633

[10] PUŽMANOVÁ, R. Moderní komunikační sítě od A do Z. Brno: Computer Press, 2006. ISBN 80-251-1278-0

[11] LOCKHARD, A. Bezpečnost sítí na maximum. Brno: Computer Press, 2005. ISBN 80-251-0791-4

[12] PUŽMANOVÁ, R. Bezpečnost bezdrátové komunikace. Brno: Computer Press, 2005. ISBN 80-251-0791-4

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

[14] IEEE Std 802.11b-1999. IEEE. c2000. Dostupný z WWW: http://standards.ieee.org/getieee802/download/802.11b-1999.pdf

[15] IEEE Std 802.11g. IEEE. c2003. Dostupný z WWW: http://standards.ieee.org/getieee802/download/802.11g-2003.pdf

[16] IEEE Std 802.16-2004. IEEE. c2004. Dostupný z WWW: http://standards.ieee.org/getieee802/download/802.16-2004.pdf