Univerzita Pardubice
Dopravní fakulta Jana Pernera

Implementace bezdrátových sítí v prostředí ČEZ ICT Services, a. s.

Bc. Miroslav Jindra

Diplomová práce
2009

Univerzita Pardubice
Dopravní fakulta Jana Pernera
Katedra elektrotechniky, elektroniky a zabezpečovací techniky v dopravě
Akademický rok: **2008/2009**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Miroslav JINDRA**

Studijní program: **N3708 Dopravní inženýrství a spoje**

Studijní obor: **Dopravní infrastruktura-Elektrotechnická zařízení v dopravě**

Název tématu: **Implementace bezdrátových sítí v prostředí ČEZ ICT Services, a. s.**

Zásady pro vypracování:

V teoretické části porovnejte z hlediska bezpečnosti přístupové metody klientů k přístupovým bodům. Porovnejte nasazení izolovaných přístupových bodů a centrálně řízených přístupových bodů.
V praktické části zpracujte konkrétní návrh univerzálního bezdrátového řešení pro Office zaměstnance, poskytování Internetu, WiFi IP telefonii.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování diplomové práce: **tištěná**

Seznam odborné literatury:

1. **Fedor Kállay, Peter Peniak: Počítačové sítě a jejich aplikace**
2. **Pužmanová Rita: Moderní komunikační sítě od A do Z**
3. **L. Dostálek, A.Kabelová: Velký průvodce protokoly TCP/IP a systémem DNS**
4. **L. Dostálek a kolektiv: Velký průvodce protokoly TCP/IP Bezpečnost**
5. **Thomas M. Thomas: Zabezpečení počítačových sítí bez předchozích znalostí**
6. **Andrew Lockhart: Bezpečnost sítí na maximum**
7. **Evi Nemeth, Garth Snyder, Trent R.Hein: Linux Kompletní příručka administrátora**
8. **William R. Stanek: Microsoft Windows Server 2003 kapesní rádce administrátora**
9. **J. Dobeš, V. Žalud, Moderní Radiotechnika**
10. **http://www.cisco.com**

Vedoucí diplomové práce: **Ing. Martin Kaloč**
ČEZ ICT Services, a. s., Hradec Králové

Datum zadání diplomové práce: **11. prosince 2008**

Termín odevzdání diplomové práce: **25. května 2009**

prof. Ing. Bohumil Culek, CSc.
děkan

L.S.

prof. Ing. Vladimír Schejbal, CSc.
vedoucí katedry

V Pardubicích dne 17. února 2009

Prohlašuji:

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

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

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 22. 5. 2009

Miroslav Jindra

Abstrakt:

Diplomová práce zahrnuje zkušenosti nabyté při implementaci bezdrátových technologií v provozním prostředí firmy ČEZ ICT Services, a. s. V teoretické části jsou zpracovány základní požadavky kladené uživateli na komunikační sítě, využívajících k distribuci informací elektromagnetických vln (radiového přenosu). Jsou zde zpracovány základní možnosti nasazení radiových spojů ve vnějším a vnitřním prostředí budov. S tímto jsou zohledněny požadavky na design síťové technologie a bezpečnost.

V praktické části se zabývám implementací sítí WLAN ve vnitřních prostorách budov, s využitím dostupných technických prostředků. Využití služeb datové konektivity v podnikové síti pro přístup uživatelů, k síťovým zdrojům, k Internetu a IP telefonii. Uvádím zde implementaci reálně nasazenou na obchodních pobočkách v Budapešti a Varšavě. Dále zde zpracovávám praktické možnosti nasazení ve vnějším prostředí, k zajištění WAN dvoubodových spojů na větší vzdálenosti, případně zajištění přístupových sítí poslední míle.

Klíčová slova:

WLAN, MAN, WAN, vnitřní radiové sítě, přístupové sítě

Summary:

Diploma Thesis includes wireless technologies implementation from experience acquired in the environs of the copany ČEZ ICT Services, a. s. I elaborate basic requirement of users to communications network, making use of distribution information on electromagnetic waves (radio data communication) in theoretical parts. I basically summary oportunity of implementation radio channels outdoor and indoor environs of buildings. I make provision for network design and network security of course.

I consider implementation WLAN indoor with available technician appliances. Usage of data transfer in enterprise networks for user’s access to network sources, by Internet connection and use IP telephony. I demonstrate implementation on small branch office in Budapest and Warsaw. I demonstrate implementation of outdoor environment point to point WAN large distance connection and for up to resource last mile access.

Keywords:

WLAN, MAN, WAN, indoor radio network, access network

Poděkování

Na tomto místě bych chtěl poděkovat vedoucímu diplomové práce Ing. Martinu Kaločovi za zájem, připomínky a čas, který věnoval této práci.

OBSAH

ÚVOD

Možnosti počítačů a jejich možnosti jak programové tak i komunikační procházejí od 80 let minulého století neuvěřitelným vývojem. Stoupající nároky na spolehlivost, kapacitu, robustnost, územní pokrytí určují další vývoj a předně využití v každodenní praxi. V poslední době expanzí mobilních komunikačních technologií, bývají někteří zaměstnanci stále více závislí na přístupu do firemních databází, na sdílení výpočetních prostředků. Jejich zaměstnání odráží nutnost komunikovat prostřednictvím počítače, telefonu, případně se účastnit na videokonferencích. Jejich zaměstnavatelům poskytuje možnosti operativněji přidělovat, řídit a kontrolovat probíhající děje ve firemních strukturách. Mobilní uživatelé tak řeší otázku: Jak se dnes mohu nejsnáze připojit do firemní sítě? Odpověď můžete najít v této práci. Zde bych chtěl zmapovat možná technická řešení, která může aplikovat jejich zaměstnavatel, aby usnadnil přístup k informacím vlastním případně i cizím zaměstnancům (potenciálním zákazníkům) prostřednictvím bezdrátových sítí WLAN.

Na začátku práce jsou probírány základy z počítačových sítí, pojmy topologie, rozlehlost, standardizace, referenční model ISO/OSI, začlenění modelu TCP/IP, základy adresace IP v 4, popis konvergence v sítích. Dále zpracovávám model AAA zabezpečení sítí. Dál se v práci zabývám možnosti nasazení izolovaných (standalone) a centrálně řízených přístupových bodů.

V další části uvádím postupné etapy nasazování WiFi sítí ve Skupině dceřiných firem ČEZ, a. s.

1 Historie sítí

Na počátku, kdy ještě neexistovaly počítačové sítě, v době mnoha samostatných počítačů, sálových počítačů a terminálů, se data vstupní i výstupní přenášela prostřednictvím přenosných paměťových médií. Šlo převážně o děrné štítky, děrné pásky, magnetické pásky, a později další magnetická média jako diskety / disky. Takováto výměna dat vedla k takzvanému dávkovému zpracování úloh, neboli OFF-line komunikaci.

Dalším krokem je terminálový provoz. Stal se inspirací pro vznik přenosu dat v reálném čase, tzv. lokální ON-line komunikaci. Zpočátku byla využívána pomalá sériová a paralelní rozhraní, využívána k dvoubodovému spojení periferií počítačů, a tedy i vlastní komunikaci mezi nimi. Šlo o první terminálové sítě založené na firemních protokolech skupiny VT100 používané firmou DEC, a TN 3270 používané firmou IBM. S rozvojem výroby a stlačením výrobních cen personálních počítačů PC, kdy cena PC klesla pod cenu specializovaného terminálu, došlo k využívání programů k emulaci terminálů. Z pohledu dnešních lokálních sítí byla topologie hvězdicová. Sálový počítač tvořil střed hvězdy, a jednotlivé terminály, PC byli připojovány dvoubodovým spojem.

Omezujícím faktorem byla vzdálenost terminálů od centrálního počítače, daná použitou technologií spoje (nejčastěji šlo o rozhraní RS232 s dosahem 15m, případně s převodem na proudovou smyčku s dosahem do 1km). Na větší vzdálenosti se data přenášela prostřednictvím komutovaných telefonních linek a zařízení modemů. Modem převáděl digitální signál RS232 na analogový signál v hovorovém pásmu 300 Hz – 3400 Hz, a po přenosu telefonní linkou, zpět na signál RS232. Nevýhodou bylo drahé dvoubodové komutované spojení mezi modemy. Odpadla však nutnost přenášet data na externích paměťových médiích. Poplatky byly úměrné době přenosu dat. Z dnešního pohledu by se principiálně hovořilo o síti s přepojováním okruhů. Další možností bylo vybudování pevných spojení (okruhů) na stejné technologii, nebo na průmyslovém standardu sítí X.21/X.25. Cena za tyto permanentní spoje byla dosti vysoká, dostupná pro velké firmy. Pronájmem přenosových okruhů bylo možné realizovat od národních telefonních (telekomunikačních) společností.

Vybudování pevných spojení mezi více centrálními počítači bylo základem pro budování dnešních sítí. Nejdůležitějším zlomem bylo v roce 1969 vypsání soutěže na realizaci spojů PC

pro armádní účely, tj. model DoD (Department of Defense USA). Vzniká první experimentální síť s přepojováním paketů.

Od roku 1972 dochází k propojování počítačů na Univerzitní půdě. Jde o síť ARPANET. S rozvojem paketových sítí nastal problém se standardizací, a jednotným modelem komunikačních protokolů. Každá firma zabývající se sítěmi používá vlastní protokoly. Standard OSI/ISO ještě není dokončen.

V letech1977 – 79 vzniká základ architektury TCP/IP na Univerzitách ve Stanfordu a v Londýně. V roce 1980 dochází k implementaci protokolů TCP/IP do operačního systému BSD UNIX a zahájení experimentálního provozu TCP/IP v síti ARPANET. Viz literatura.

Po úspěšné implementaci, v roce 1983, dochází k nasazení TCP/IP jako standardu komunikačních protokolů do sítě ARPANET, a vyčlenění Univerzitní sítě od armádní. V letech 1985 – 1986 jsou prostřednictvím sítě ARPANET propojena velká super-počítačová centra. Centra se stala základem dnešní sítě INTERNET.

INTERNET je síť založená na technice přepojování paketů. Veškerá propojení mezi sítěmi jsou realizována specializovanými počítači směrovači (routery), které zajišťují směrování paketů v síti. Routery směrují pakety na základě cílové adresy sítě. Všechny sítě jsou z pohledu protokolů TCP/IP rovnocenné.

Mobilita uživatelů – po roce 1989 v ČR uvolněn obchod s dříve nedostatkovým zahraničním zbožím. Dochází k budování první generace sítě mobilních telefonů. Jde zatím jen o přenos hlasu. Za nedlouho v roce 1994 je nasazován nový systém GSM900 1. generace. Zde se ověřila možnost používat tuto mobilní síť i k transportu dat a to formou výměnné služby SMS. Pak přichází 2. generace s rozšířenou možností přenosu dat rozšířením GPRS. Od roku 1999 je umožněn přístup k datové informační síti INTERNET protokolem WAP (Wireless Application Protocol) prostřednictvím mobilních telefonů.

Od roku 2000 nastává rozmach plně datových sítí založených na standartu ANSI/IEEE 802.11 vydání 1999 (ISO/IEC 8802-11:1999) - výrobci označované WiFi. Dále IEEE 802.11b-1999/ verze 1-2001; IEEE 802.11a-1999 (2003).

2 Topologie sítí

V topologii sítí vycházíme z umístění jednotlivých uzlů v sítí na fyzické vrstvě, tak i v souvislosti s přenosovými možnostmi sítě, přenosovou rychlostí, vzdáleností uzlů, aplikacemi a přístupem k nim v takzvané logické vrstvě. Každá zde uvedená topologie může používat jiných principů v obou těchto na sobě nezávislých složkách. V případě logické vrstvy se hovoří také o způsobu řízení a přístupu k fyzické složce. Více viz literatura [1].

2.1 Dvoubodové spojení

Nejedná se přímo o topologii sítě, je však základem veškerých dalších spojů v dnes převažujících přepínaných sítích.

2.2 Sběrnice

Propojení rovnocenných počítačů prostřednictvím centrálního přenosového média – sběrnice. Sdílené médium je však limitní z kapacitních důvodů, a nutností řešit přístupové metody jednotlivých uzlů médiu. Populárním představitelem v letech 1983 – 1993 byla síť Ethernet 10-Base2, 10-Base 5.

2.3 Kruh

Veškeré uzly jsou propojeny do kruhu. Výhodou je přesně definovaný (deterministický) způsob přístupu uzlů k médiu, zajištění přenosu dat i při náhodném rozpojení kruhu. Nevýhodou jsou drahé specializované síťové adaptéry a rozšiřitelnost sítě. Je zde omezená propustnost daná standardem. Typickým představitelem jsou sítě Token Ring (IBM) a optické sítě FDDI.

2.4 Hvězda

Základem je centrální uzel, od kterého vede ke každé stanici datový komunikační kanál. Z pohledu přenosových kapacit a spolehlivosti, je nejvíce zatěžován centrální uzel. V případě výpadku jednotlivého spoje, je ohrožen pouze postižený uzel. V případě výpadku centrálního uzlu, stává ze sítě množství izolovaných uzlů. Jde o přímou analogii ke klasickým analogovým telefonním ústřednám.

2.5 Distribuovaná hvězda

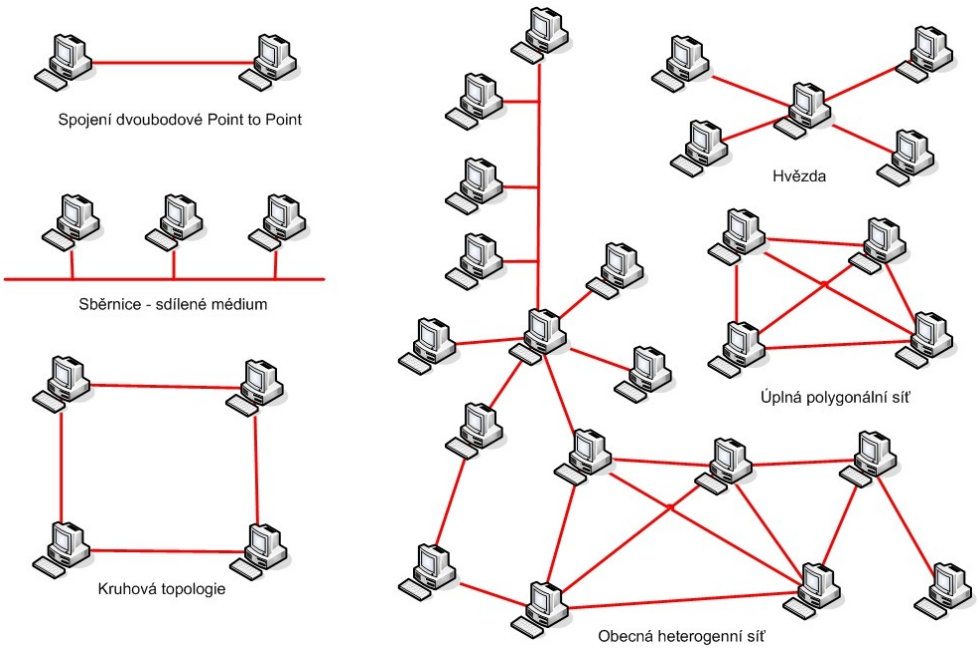
Vzájemné propojení sítí typu hvězda do ještě větších rozlehlejších celků. Distribuovaná hvězda odpovídá matematickému modelu strom z teorie grafů.

2.6 Polygonální

Buď ve variantě úplné polygonální sítě – každý jednotlivý uzel sítě je přímo spojen do každého dalšího uzlu, nebo částečná polygonální síť – některé spoje oproti úplné polygonální sítě chybí. Nevýhodou nutnost realizovat veliké množství dvoubodových spojů, nutnost použití speciálních technologií na podporu přenosu informace z uzlu A do uzlu B – vyloučení smyček a znásobení přenášených informací vedoucích k zahlcení sítě. Při vyřešení těchto komplikací přináší nejlepší odolnost proti přerušení / výpadkům spoje na fyzické vrstvě.

2.7 Heterogenní

Síť sdružující kombinace výše uvedených sítí bez dalších omezení na použité technologie přenosu dat, rozlohu, prostor a kapacitu. Typickým představitelem je dnešní globální síť Internet.



Obrázek 2.7.1 Heterogenní topologie

2.8 Buňková

První známé veřejné buňkové sítě, vznikají v 90. letech minulého století s příchodem mobilní telefonie. Jde o síť radiových převaděčů, jejichž signál by pokud možno pokrýval požadované území. Musí se dodržet přidělený frekvenční plán, při minimalizaci vzájemného rušení jednotlivých základnových stanic umístěných ve středu jednotlivých buněk. Každá buňka je dále omezena regulátorem na maximální možný vyzářený výkon – hygienické maximum – „vyzářenou hustotu elektromagnetického pole“. Dosah je také omezen způsobem šíření radiových vln v okolním prostředí v daném kmitočtovém pásmu.

2.9 Mesh

Síť s jistou dávkou inteligence, která je schopná v případě potřeby klienta na změnu kvality spojení (kapacita spoje, QoS, chybovost spoje) rekonfigurovat svou topologii. Uplatňuje se převážně v novějších radiových sítích, WLAN/GSM/3G. V těchto mobilních sítích, které jsou budovány buňkovým systémem převaděčů / Access Pointů / POPů, je možné díky centrálnímu řízení a managementu RF obvodů, průběžně přidělovat kmitočtová spektra, přidělovat vyhrazenou kapacitu spoje, tím ovlivňovat propustnost mezi spoji převaděčů, měnit RF výkon, případně polohovat doplňkové anténní systémy. Využití je převážně v sítích LAN/MAN v hustě osídlených aglomeracích, kde by úplné buňkové pokrytí území bylo neekonomické, nebo by bylo problematické řešení kabelového vedení. Část převaděčů je vždy připojena pevným vedením (vyhrazeným dvoubodovým spojem) ke zdroji dat a bodům integrovaných do centrálního řízení. S výhodou se dá principů řízení využít také ve větších instalacích budov.

3 Sítě z hlediska rozlehlosti

Z pohledu rozlehlosti sítí vycházíme ze vzdálenosti komunikujících uzlů (počítačů).

vzdálenost vedení	hranice	rozlehlost	technologie podporující přenos protokolů TCP/IP
5 m	místnost	LAN	opto, metalické vedení, připojení do LAN
90 m	patrový rozvaděč	LAN	opto, horizontální vedení, WLAN
550 m	budova	LAN	opto, vertikální vedení, propoje budov, WLAN
10 km	město	MAN	opto, WLAN, ISDN, xDSL, 3G mobilní sítě, WLAN
100 km	stát	WAN	opto, WDM, CWDM, SDH, ATM, MPLS, SAT
1000 km	kontinent	WAN	opto, DWDM, SAT

Tabulka 3.1 Rozdělení sítí podle vzdálenosti komunikujících uzlů

3.1 LAN (Local Area Network)

- lokální, místní síť propojuje jednotlivá zařízení na krátké vzdálenosti
- je rychlá
- je v našem vlastnictví
- je k dispozici nepřetržitě

3.2 MAN (Metropolitan Area Network)

- síť omezená rozlehlostí na obec, město
- rychlost je omezená podle použité přenosové technologie na danou vzdálenost
- je v našem vlastnictví, případně spoluvlastnictví, část pronajímáme
- je k dispozici nepřetržitě

3.3 WAN (Wide Area Network)

- rozlehlá síť, propojuje zařízení na velké vzdálenosti
- vlastníkem je cizí subjekt
- pronajímáme fyzické okruhy
- pronajímáme virtuální okruhy pevné, nebo přepínané – logické okruhy
- je k dispozici pouze v okamžiku, kdy potřebujeme přenášet data

Globální počítačovou síť INTERNET si z tohoto pohledu můžeme představit, jako počítačovou síť, která je propojením PC (personálních/osobních počítačů) do veřejných uzlů LAN propojených většinou přes privátní pronajaté linky poskytovatelů připojení k Internetu ISP (Internet Service Provider) sítě LAN/MAN/WAN.

Síť INTERNET lze také považovat za sdílený zdroj datových informací.

4 Přenos informací pomocí radiových vln

Přenos informace probíhá pomocí signálu generovaného vysílačem (příchozí elektrický signál je zde přeložen ze základního pásma modulací do vysokofrekvenčního pásma). Modulovaný VF elektrický signál se v anténním systému mění na elektromagnetické vlnění. Prostředím přenosu elektromagnetických vln se stává okolní prostředí – vzduch. Na cílové straně je signál v podobě elektromagnetických vln indukován do antény, kde se přemění na signál elektrický. Dále se zpracovává v obvodech přijímače. Na kvalitu přenosu informací má vliv, kromě samotného technického řešení vysílače, přijímače a anténních systémů, především samotné prostředí, nežádoucí rušení z okolního prostředí, nejrůznější odrazy, pohlcení signálu na překážkách.

frekvence	zkratka	délka vlny	Název
10 – 30 kHz	VLF Very Low Frequency	100 – 10 km	velmi dlouhé
30 – 300 kHz	LF Low Frequency	10 – 1 km	Dlouhé
300 – 3000 kHz	MF Medium Frequency	1000 – 100 m	Střední
3 – 30 MHz	HF High Frequency	100 – 10 m	Krátké
30 – 300 MHz	VHF Very High Frequency	10 – 1 m	velmi krátké
300 – 3000 MHz	UHF Ultra High Frequency	10 – 1 dm	ultra krátké
3 – 30 GHz	SHF Super High Frequency	10 – 1 cm	Centimetrové
30 – 300 GHz	EHF Extra High Frequency	10 – 1 mm	Milimetrové
300 – 3000 GHz	SB Submilimeter Band (IR)	1 – 0,1 mm	Submilimetrové

Tabulka 4.1 rozdělení radiového frekvenčního spektra

5 Standardizované sítě

Standardizace je zdlouhavý proces. Zabývá se jím několik institucí. Jmenujme již zmíněnou organizaci ISO (International Organisation for Standardization), IEEE (Institute of Electrical and Electronics Engineers), ANSI (American National Standardization Institute s Evropskou obdobou ETSI (Europe Technician Standardization Institute), ITU (International Telecommunication Union), IETF (Internet Engineering Task Force). Většina nových dokumentů, než je převzata standardizační institucí, je publikována v tzv. RFC (Request For Comments), RIPE, PKCS a je možné je stáhnout z Internetu.

5.1 WLAN

frekvence [GHz]	Pásmo
3,5	Licencované, mezinárodní pásmo
10,5	Licencované, mezinárodní pásmo (v ČR zatím bezlicenční)
2,5 – 2,7	Licencované, USA, S. Amerika
2,4	Nelicencované, mezinárodní
5,725 – 5,825	Nelicencované, mezinárodní

Tabulka 5.1 Rozdělení radiového frekvenčního spektra, a licencování WLAN

WLAN (Wireless Local Area Network) jsou bezdrátové LAN založené na standardu IEEE 802.11 výrobci označovaném WiFi. K přenosu informací používá radiové vysílání s využitím radiového frekvenčního spektra na kmitočtech 2,4 – 2,48 GHz, a v pásmu 5,15 – 5,82 GHz. Tuto technologii popisují standardy IEEE 802.11 a/b/g/n. Přenosové rychlosti se pohybují podle daného standardu, „čistoty“ rušení prostředí od cizích elektromagnetických zdrojů, a vzdálenosti od přístupového bodu (AP - Access Point). Reálně se dá uvažovat od 5,5 Mbps 802.11b do 300 Mbps 802.11n. Předností sítě je úspora financí jinak potřebná při budování datového vedení mezi PC a AP a radiový dosah srovnatelný s pevnou instalací propoje strukturované kabeláže LAN, tj. 100 m. Se vzdáleností WiFi klientské stanice od AP však reálná rychlost komunikace snižuje, podle daných podmínek radiové cesty, dané použitou modulací přenosu signálu. V případě že k danému AP najednou přistupuje více uživatelů, reálná přenosová rychlost také klesá. Více uživatelů najednou používá stejné přenosové pásmo, které musí být mezi více uživatelů přerozděleno.

WLAN Technologie WiMAX (Worldwide Interoperability for Microwave Access) popisuje standard IEEE 802.16. Jde o doplněk standardu IEEE 802.11 pro použití v externích

podmínkách. Překlenutelná vzdálenost podle pásma, standardu, a použitému kódování je až 70km s datovou propustností 70 - 134 Mbps.

Standard IEEE 802.16 – spojení na přímou viditelnost určená pro frekvenční pásma 10-66 GHz. Standard IEEE 802.16a frekvenční pásma definovaná v rozsahu 2-11 GHz, tedy jak licencované, tak bezlicenční frekvence – nevyžaduje přímou viditelnost. Přenosová rychlost do 70 Mbps. Další standardy: 802.16 c – podpora interoperatibility, 802.16d - profily zařízení, 802.16e - podpora mobility.

5.2 Telekomunikační regulátor pro ČR

V ČR je zákonem stanoven za národního telekomunikačního regulátora Český telekomunikační úřad (zkratkou označován ČTÚ). Podrobné informace lze najít na Internetové adrese http://www.ctu.cz/pusobnost-ctu/sprava-radioveho-spektra.html (odkaz platný k datu 16. 5. 2009).

Na výše uvedené kmitočty WLAN jsou vydány tyto Všeobecná oprávnění ČTÚ:

- VO-R/24/11.2008-16 k provozování zařízení infrastruktury pro šíření rádiových signálů uvnitř tunelů a vnitřních prostor budov.
- VO-R/14/12.2006-38 k využívání rádiových kmitočtů a k provozování zařízení v pásmu 10 GHz.
- VO-R/12/05.2007-6, kterým se mění všeobecné oprávnění č. VO-R/12/08.2005-34 k využívání rádiových kmitočtů a k provozování zařízení pro širokopásmový přenos dat na principu rozprostřeného spektra nebo OFDM v pásmech 2,4 GHz a 5 GHz.

Citace ze stránek ČTU http://www.ctu.cz/ctu-informuje/jak-postupovat/radiove-kmitocty/vyuzivani-vymezenych-radiovych-kmitoctu.html (odkaz platný k datu 16. 5. 2009).

Začátek citace: „

PROVOZOVÁNÍ ZAŘÍZENÍ V PÁSMU 2,4 GHZ A 5 GHZ

Pásmo 2400–2483,5 MHz je v současné době velmi intenzivně využívané pásmo. Na základě všeobecných oprávnění VO-R/12/08.2005-34 a VO-R/10/03.2007-4 toto pásmo sdílejí aplikace bezdrátových sítí včetně bezdrátového Internetu (RLAN, WLAN – standardy IEEE 802.11b, g, n), zařízení bluetooth a některé další aplikace (bezdrátové kamery, železniční aplikace, RFID, …). Státní kontrola elektronických komunikací řeší poměrně často problémy způsobené zejména nedodržením stanoveného výkonu a podle zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) je postihuje.

V oblasti 5 GHz je možný provoz podle VO-R/12/08.2005-34 a VO-R/10/03.2007-4 v pásmu 5,15–5,35 GHz (pouze uvnitř budov), v pásmu 5,470–5,725 GHz (standard IEEE 802.11a) a s malým výkonem (25 mW e.i.r.p.) též v pásmu 5,725–5,875 GHz.

POZNÁMKY PRO PROVOZ ZAŘÍZENÍ RLAN (WLAN):

Výrobce / distributor zařízení je povinen v návodu k použití (který musí být v češtině přiložen ke každému zařízení) uvést podmínky, za nichž lze zařízení v ČR provozovat v souladu se všeobecným oprávněním VO-R/12/08.2005-34. Zejména musí výrobce či distributor uvést, jaký druh nebo typ antény může být u zařízení použit, aby zařízení splňovalo podmínky, za nichž byla posouzena shoda. Provozovatel rádiového zařízení je povinen na základě těchto informací výrobce dodržovat režim vysílání, který odpovídá výše uvedenému všeobecnému oprávnění. Obecně platí, že při použití směrové antény (pokud výrobce / distributor tento druh antény připouští) musí provozovatel snížit výkon zařízení tak, aby vyzářený výkon byl v souladu s všeobecným oprávněním.

Jak vyplývá ze všeobecného oprávnění, stanice jsou provozovány na sdílených kmitočtech. Provoz stanice nemá zajištěnu ochranu proti rušení způsobenému vysílacími rádiovými stanicemi jiné radiokomunikační služby provozovanými na základě individuálního oprávnění k využívání rádiových kmitočtů nebo jinými stanicemi pro širokopásmový přenos dat na principu rozprostřeného spektra nebo OFDM. Případné rušení řeší fyzické a právnické osoby vzájemnou dohodou. Nedohodnou-li se, postupuje se podle § 100 zákona

o elektronických komunikacích, případně zastaví provoz ten uživatel, který uvedl do provozu stanici způsobující rušení později.

Konec citace“

Přehled o využití licencovaného pásma 3,5 GHz lze najít také na stránkách ČTÚ viz odkaz:

http://www.ctu.cz/ctu-online/vyhledavaci-databaze/aktualni-vyuzivani-kmitoctoveho-pasma-3510-3580-mhz-3410-3480-mhz.html (odkaz platný k datu 16. 5. 2009)

6 Referenční Model ISO/OSI

RM ISO/OSI (Reference Model Open System Interconnection). Jedná se o referenční model propojování otevřených systémů publikovaný v roce 1979 mezinárodní standardizační organizací ISO (International Organisation for Standardization).

Norma ISO 7498 popisuje základní model komunikace, vymezuje komunikaci do 7 vrstev. Dále norma popisuje komunikaci mezi jednotlivými vrstvami, a také se sousední vrstvou. Norma se nezabývá vlastní implementací komunikačních protokolů.

Podle tohoto modelu je síťová komunikace rozdělena do více protokolů, které spojují jednotlivé vrstvy komunikace. Toto je z důvodu zjednodušení složité problematiky přenosu informací. V literatuře se přirovnává k modelu cizinců hovořících různou řečí kteří, aby se domluvili, potřebují překladatele.

6.1 Fyzická vrstva

Fyzická vrstva je definována pro technické zařízení. Hovoří se zde o charakteristikách elektronického, elektromagnetického a optického přenosu. Je jím například technické zařízení Ethernet / IEEE 802.3. Normou jsou specifikovány především elektrické signály, napěťové prahové úrovně, typ použitého média a jeho fyzikální parametry, tvary konektorů, tvar spojek, modulace signálu v přeloženém pásmu, kódování v základním pásmu, způsob řízení přenosu signálu po médiu.

6.2 Linková vrstva

Vrstva linková je realizována rozhraním odpovídajícím typu technického zařízení. Jedná se o ukládání informací vyšších vrstev do rámců (Frames) a technické zajištění přenosu. Datový rámec se skládá ze záhlaví (Header), dat (Payload) a zápatí (Trailer). Představitelem v sítích jsou například používané Media konvertory, sloužící na propojení odlišných fyzických soustav.

6.3 Síťová vrstva

Vrstva síťová se věnuje způsobu komunikace s jinými uzly v síti. Informace se přenáší v síťovém paketu. Síťový paket se skládá ze záhlaví a datového pole. Síťová vrstva komunikuje přímo s ostatními směrovači na stejné síťové vrstvě. Fyzický přenos a jeho

protokoly nechává na zpracování nižší vrstvě. Z pohledu použitých protokolů jde o pravou vrstvu na rozhranní WAN, v níž má síťové rozhranní jednoznačnou identifikaci pomocí adresy. Síťová vrstva je prezentována datagramem. Tato vrstva zajišťuje odesílání dat po síti prostřednictvím směrovacích protokolů.

6.4 Transportní vrstva

Transportní vrstva je určena definicí přenosového protokolu. Například UDP (User Datagram Protocol). Transportní vrstvu lze prezentovat jako nastavený přenosový kanál mezi programy na komunikujících počítačích. Je charakterizovány adresou síťovou a adresou transportní. Data na této vrstvě se prezentují jako segment, který se skládá z transportního záhlaví a dat.

6.5 Relační vrstva

Relační vrstva je vrstvou vstupu uživatele do sítě. Zajišťuje výměnu dat mezi konkrétní aplikací běžící na počítači. Stará se o navázání spojení, jeho udržení, synchronizaci dat, a ukončení spojení.

6.6 Prezentační vrstva

Na úrovni prezentační vrstvy dochází ke kódování a komprimaci přenášených dat. Vrstva se stará o zabezpečení dat, tj. šifrování, zajištění integrity, digitálním podepisováním. Může dojít k úplné změně dat, prezentační vrstva může být na různých počítačích jiná. Vzájemně si však porozumí pouze počítače se stejně prezentovanými daty.

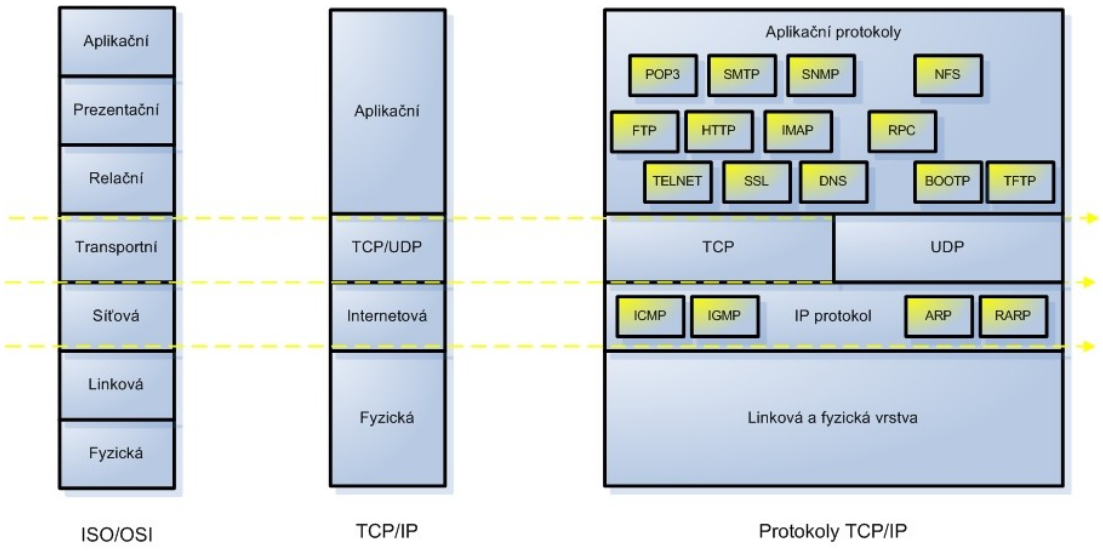
6.7 Aplikační vrstva

Aplikační vrstva je ryze uživatelská. Předepisuje, v jakém formátu mají být data předávána a přebírána z aplikačních programů. Z hlediska uživatele a vrstvy aplikační se od provozu sítě zejména vyžaduje:

- Výměna pošty a přenos souborů.
- Sdílení periferií, např. tiskárny, nebo disku.
- Spouštění programů ve vzdáleném uzlu, přístup do sdílených databází.
- Přihlášení ve vzdáleném uzlu, ověření uživatele, (autentizace, autorizace).

7 Model TCP/IP

Jak bylo popsánu v kapitole 1, model TCP/IP (Transmission Control Protocol / Internet Protokol) vznikl dříve, než byl model ISO/OSI standardizován. Každý z modelů používá vlastní definici svých vrstev, proto jsou obecně různorodé.



Obrázek 6.7.1Porovnání vrstev modelu ISO/OSI s modelem TCP/IP

7.1 Fyzická vrstva

V modelu TCP/IP je převážně totožná s fyzickou vrstvou ISO/OSI, je detailně popsána v normách IEEE 802. Linková vrstva podle ISO/OSI je rozdělena do vrstvy MAC (Medium Access Control), která částečně zasahuje do vrstvy fyzické, se zabývá přístupem k fyzickému přenosovému médiu. Dále do vrstvy LLC (Logical Link Control), která spravuje jednotlivá logická spojení mezi počítači v síti LAN.

V komunikačním řetězci je tato vrstva identifikována pomocí IEEE 802 MAC adresy. Podle doporučení IEEE výrobce síťového adaptéru NIC (network interface card) označuje touto adresou všechny síťové adaptéry jím vyrobené. Jde o univerzálně administrovanou adresu (universally administered address). Adresa je dlouhá 48 bitů. První 3 bajty adresy identifikují výrobce adaptéru OUI (Organizationally Unique Identifier), Druhé 3 bajty specifikují daný adaptér. Jde o unicast adresu, která jednoznačně identifikuje daný síťový adaptér. Existuji ještě lokálně administrované adresy (locally administered address). Lokálně administrovaná adresa neobsahuje OUI. Správce sítě (správce počítače) ji může programově změnit. Na této vrstvě můžeme pracovat i se skupinovými adresami. Například adresa hex

FF:FF:FF:FF:FF:FF označuje všechna rozhranní s adresami MAC. Výrobcům je přesně přidělen organizací IEEE význam prvních 2 bitů adresy LSB (Lest Significant Bit) MAC na identifikaci skupinových adres.

- 1. bit = 0: individuální adresa MAC
- 1. bit = 1: skupinová adresa MAC
- .2. bit = 0:univerzálně přidělená adresa MAC
- 2. bit = 1: lokálně přidělená adresa MAC

7.2 Internetová vrstva

Vrstva IP (Internet Protokol) dopravuje data mezi dvěma sousedními směrovači. Sousední směrovač je nazýván next-hop. Vzájemným propojením směrovačů a předáváním informací o připojených sítích, se uskutečňuje přenos dat (směrování / routování) mezi jednotlivými sítěmi LAN. Podle této vrstvy byla nazvána Globální síť INTERNET.

Internetová vrstva je prezentována IP adresou. Adresa síťového rozhranní (z pohledu lokální sítě) se skládá z adresy sítě, a z adresy počítače. K rozřešení které bity v IP adrese patří síti, a které konkrétnímu počítači, využíváme pomocného údaje tj. masky. Maska se používá pro zjištění adresy sítě z IP adresy. Adresování v IP sítích prošlo také vývojem.

V současné době se nezávisle na sobě používají adresy standardu IP v4 a IPv6. Adresa podle IP v4 je dlouhá 32 bitů. Zapisuje se po 4 oktetech desítkově. Více viz kapitola Adresace v síti IP v4.

7.3 Protokoly IPv4:

- IP – (Internet Protokol) vlastní protokol
- ICMP – (Internet Control Message Protocol) protokol používaný k signalizaci mimořádných stavů v síti.
- IGMP – (Internet Group Management Protocol) protokol používaný pro dopravu adresních oběžníků
- RARP/ARP – (Reverse Address Resolution Protocol / Address Resolution Protocol) samostatné protokoly nepoužívající IP záhlaví, sloužící k identifikaci IP adres příjemce, a odesilatele. Každé zařízení v IP síti má alespoň jednu unikátní adresu, která je nezávislá na hardware, ale je závislá na topologii dané sítě. Tuto adresu používají

aplikační protokoly k identifikaci cíle v LAN. Pro komunikaci síťové vrstvy s vrstvou fyzickou tj. propojení IP adresy s fyzickou adresou MAC se používá protokolu ARP a RARP. Toto mapování se provádí pouze v koncových uzlech LAN sítě a na přilehlém směrovači sítě LAN. Proces je dynamický a zabírá určitou režii sítě. Protokol ARP slouží pro vyhledání MAC adresy fyzického adaptéru podle IP adresy. Počítač v LAN si udržuje při komunikaci svou tabulku ARP cache. Pokud potřebuje komunikovat s počítačem, jehož MAC adresu nezná, zná pouze jeho IP adresu, použije ke zjištění adresy cílového počítače protokol ARP. Vyšle žádost protokolu ARP se svou IP adresou a MAC adresou, a také s cílovou IP adresou. Tuto žádost pošle všem stanicím v síti LAN na tzv. všeobecnou adresu. Všechny počítače v daném segmentu sítě zkontrolují, jestli IP adresa není jejich. Počítač, který spatří shodu, pošle zpět původní stanici doplněnou informaci o jeho MAC adrese. Pokud je daný počítač připojen k jinému segmentu sítě LAN, odpoví místo cílové stanice směrovač daného segmentu LAN. Protokol RARP je analogií ke zjištění IP adresy při znalosti MAC adresy. V operačních systémech na počítačích PC je přímo k dispozici terminálový příkaz arp -a, který vypíše aktuální APR cache daného počítače. U počítače připojeného do sítě LAN minimálně získáme MAC adresu směšovače sítě LAN.

7.4 Transportní vrstva

Transportní vrstva slouží k přepravě dat mezi dvěma konkrétními počítači a aplikacemi běžících na nich. Používají se dva nezáměnné protokoly:

- UDP – (User Datagram Protocol) nepotvrzovaná datagramová služba – její výhoda je v rychlosti, nelze garantovat pořadí přijatých dat
- TCP – (Transmission Control Protocol) potvrzovaná spojovaná služba, na dobu spojení vytváří plně duplexní virtuální okruh. Jednotlivá data jsou číslována. Při jejich ztrátě, nebo poškození dochází k opakovanému přenosu. Samotná integrita dat je zabezpečena proti poruchám technických prostředků kontrolním součtem. Ochrana proti zneužití dat cíleným útokem je řešena speciálními bezpečnostními protokoly v součinnosti s vyšší vrstvou.

7.5 Aplikační vrstva

Aplikační vrstva slouží ke vzájemné komunikaci jednotlivých programů mezi počítači v síti. Množství protokolů používaných na této úrovni se neustále vyvíjí.

Protokoly Aplikační vrstvy:

- TELNET (Telecommunication network protocol). Historie sahá až do roku 1969. Telnet je popsán ve standardu RFC-764 a RFC-854. Protokol slouží k emulaci terminálu v sítích založených na modelu TCP/IP.
- FTP (File Transfer Protokol) – slouží pro přenos souborů. Je popsán ve standardu RFC-959, RFC-2228, RFC-2640.
- SMTP (Simple Mail Transfer protokol) – Přenos elektronické pošty na Internetu. Je popsán v RFC-821, RFC-822. Jde o aplikaci typu Klient/Server.
- POP3 (Post Office Protocol ver. 3) – Jednoduchý protokol umožňující uživateli stáhnout poštovní zprávy ze serveru na lokální poštovní klient v počítači. Popsán je v RFC-1939.
- HTTP (Hypertext Transfer Protokol) – Nejpoužívanější protokol pro vyhledávání a přenos informací na Internetu podporující proxy a tunelování. Je popsán v RFC-2616.
- DNS (Domain Name System) – Protokol sloužící k vyhledávání IP adres a doménových jmen v centrálních databázích jmenných serverů v síti. Popsán v RFC-1035, RFC-1995, RFC-1996, RFC-1034, RFC-2065, RFC-2136, RFC-2181, RFC-2308 v rozšířené verzi RFC-3007.
- DHCP (Domin Host Configuration Protocol) – Protokol sloužící k usnadnění práce síťovým administrátorům, k předávání konfiguračních dat klientům, nutných pro práci s IP protokolem. Nahrazují manuální nastavení síťového adaptéru klienta.
- SNMP (Simple Network Management Protocol) - SNMP se používá ke správě a monitorování prostředků v síti. Popsán v RFC-2578.
- TFTP (Trivial File Transfer Protokol) – Jednoduchý protokol pro přenos souborů. Vznik v roce 1980. Slouží např. k přenosu dat mezi bezdiskovým počítačem a sítí. Využíván také k přenosu X Terminálu (práce na virtuálním grafickém terminálu vzdáleného počítače v síti). Popsán v RFC-1350.
- BOOTP (Bootstrap Protocol) – Historicky využíván k UDP přenosu, k natažení IMAGE operačního systému na bezdiskové pracovní stanici. Je využíván ve spojení s protokolem DHCP. Popsán v RFC-2578.
- RPC (Remote procedure call) – Umožňuje spouštět programový kód v novém adresním prostoru na jiném počítači v síti. Tímto protokolem lze zajistit sdílení objektových programů, výpočetních výkonů počítačů zapojených v síti. Je tak možnost

realizovat aplikace typu klient-server a umožnit distribuované zpracování úloh. Dnešním typickým příkladem používání jsou aplikace založené na apletech v jazyce Java. Popsán v RFC-707, RFC-1057, RFC-1831.

- NFS (Network File Sharing) Protokol pocházející původně od firmy Sun Microsystems z roku 1984, soužící k jednoduchému sdílení dat mezi počítači. Popsán v RFC-1094, RFC-1813, RFC-3530, RFC-3010.

Většina těchto protokolů na aplikační vrstvě má i své „bezpečné“ představitele z pohledu přístupu, přenosu a ochrany datové komunikace. Viz literatura [3].

8 Adresace v prostředí sítí IP v4

Protokol IP verze 4 používá adresu o délce 4 bajty. Adresa prezentuje jednoznačně síťové rozhranní výpočetního systému. Každý systém může mít i více těchto rozhranní, vždy však s jinou IP adresou. Jde o tzv. Unicast adresy. Tato adresa bývá prezentována ve dvojkové soustavě, nebo srozumitelněji desítkově po oktetech oddělených tečkou.

Např.:

- 192.168.0.1 – desítková prezentace
- 11000000 10101000 00000000 00000001 – dvojková prezentace

Adresa síťového rozhranní (z pohledu lokální sítě) se skládá z adresy sítě, a z adresy počítače. K rozřešení které bity v IP adrese patří síti, a které konkrétnímu počítači, využíváme pomocného údaje tj. masky. Maska se používá pro zjištění adresy sítě z IP adresy. Adresování v IP sítích prošlo také vývojem.

8.1 Adresace v síti – historická epocha I.

Jde o období do roku 1993. Podrobnější specifikace je popsána v RFC-796.

V daném období se uvažuje o tzv. Třídách IP adres. Jsou definovány třídy A, B, C, D a E. Rozlišují se prvním oktetem v IP adrese.

třída	1. oktet	2. oktet	3. oktet	4. oktet
A	1 - 127	adresa počítače		
B	128 - 191	síť	adresa počítače	
C	192 - 223	síť	síť	Adresa počítače
D	224 -239	multicast	multicast	multicast
E	> 239			

Tabulka 8.1 Třídy IP adres

Maska sítě – jde opět o čtyřbajtové číslo, prezentované v desítkové soustavě, oddělené tečkou po oktetech v binární soustavě.

Například standardní maska sítě typu C:

- 255.255.255.0 – desítková prezentace
- 11111111 11111111 11111111 00000000 – dvojková prezentace

Prostým bitovým vynásobením IP adresy s IP maskou, získáme adresu sítě.

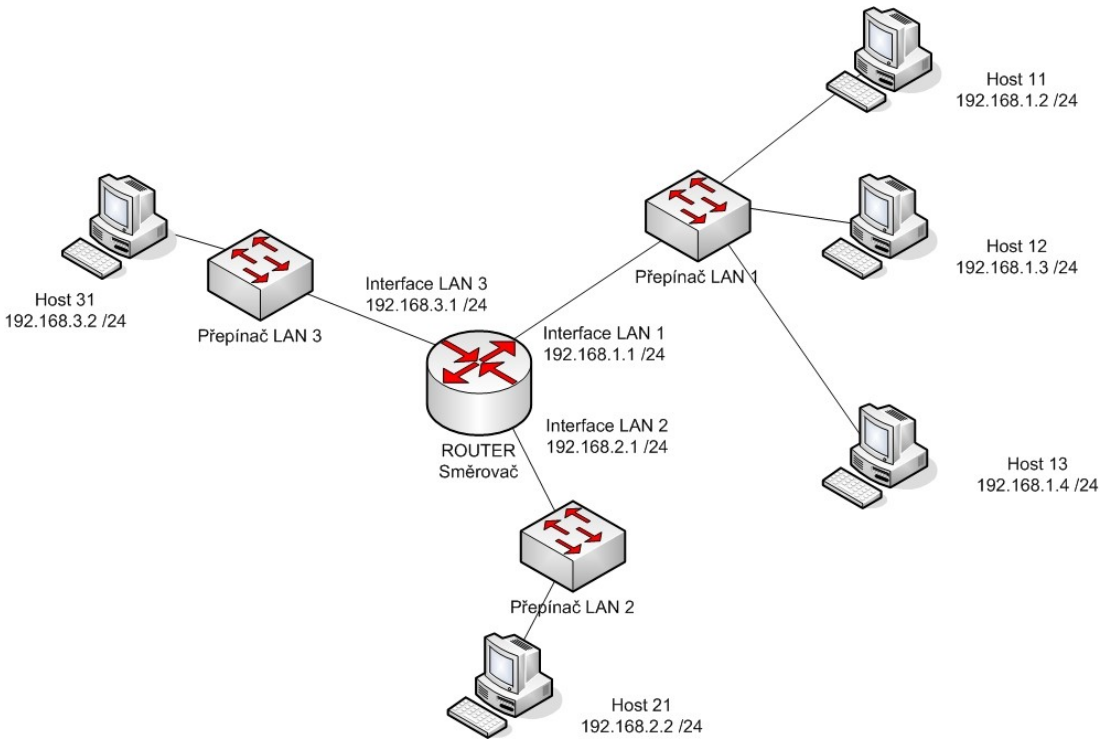
```
                11000000 10101000 00000000 00000001
          X     11111111 11111111 11111111 00000000
-------------------------------------------------------------------------------------------------------
                11000000 10101000 00000000 00000000
```

- Tj. Dostáváme Adresu sítě: 192.168.0.0

Pro shrnutí:

Síťový adaptér zařízení s IP adresou 192.168.0.1, maskou 255.255.255.0 se nachází v síti 192.168.0.0.

Přímo mezi sebou mohou komunikovat počítače (host) se stejnou adresou sítě. S hosty v jiných sítích mohou komunikovat jen v případě existence směrovače (router) spojujících dané sítě.



Obrázek 8.1.1Propojení sítí počítačů pomocí aktivního prvku - routeru

Obecná adresa je ve tvaru -> adresa sítě, adresa počítače

První tři bity adresy udávají typ dané sítě.

síť	adresa počítače	popis	význam
0.0.0.0		všechny nuly	Tento počítač na této síti
00…0	počítač		Počítač na této síti
síť	00…0		Adresa sítě
síť	11…1	samé jedničky	Broadcast - všeobecný oběžník možno směrovat i do dalších sítí
11…1		samé jedničky	Limited Broadcast - všeobecný oběžník - nelze směrovat do dalších sítí
127.x.x.x			Loopback - lokální programová smyčka, nepředává se mimo počítač

Tabulka 8.2 Speciální IP adresy

8.2 Adresace v síti – historická epocha II.

Jde o období od roku 1993. Podrobnější specifikace je popsána v RFC-1517 až RFC-1520. Na problematiku adresace se pohlíží více z pohledu masek, než z pohledu tříd adres sítě – viz epocha I. Kapitola 7.2.

Dochází k rozmělnění adresy sítě na adresu sítě a adresu podsítě (subnetu). Masku sítě můžeme použít konstantní, nebo variabilní. V tomto případě se adresa sítě udává počtem jedniček v binární prezentaci masky. Adresy s maskami mající méně jedniček než standardní maska se nazývají adresami supersítí. Naopak adresy s maskami mající více jedniček než standardní maska se nazývají adresami podsítí.

V lokálních sítích dostáváme obecnou IP adresu ve tvaru:

- adresa sítě, adresa podsítě, adresa počítače

Tak např. síť 192.168.0.0/24 tj. s maskou 255.255.255.0 třídy C, můžeme dále rozdělit na podsítě s konstantní maskou například takto:

- Maska subnetu : 110nnnnn.nnnnnnnn.nnnnnnnn.sssshhhh

- Desítkově: 255.255.255.224
- Subnet bitů v 1 : 27
- Počet bitů pro hosty: 5
- Počet subnetů: 8
- Použitelných adres hostů v subnetu : 30

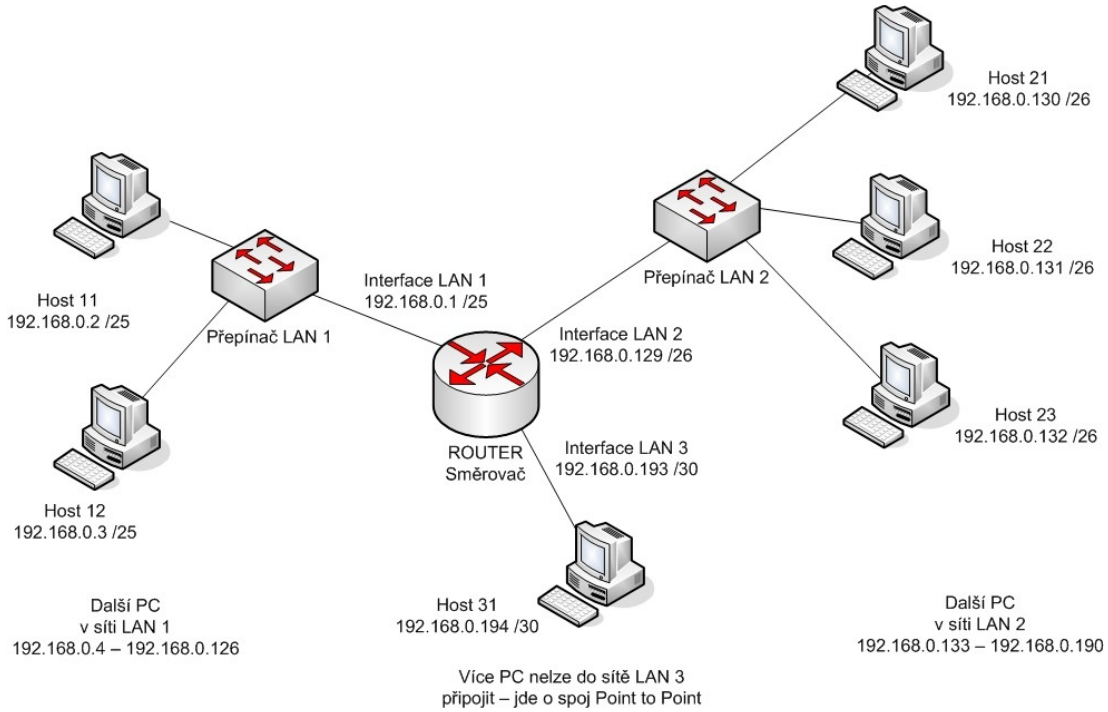
Síť	Maska	Velikost subnetu	IP Rozsah hostů	Broadcast
192.168.0.0	255.255.255.224	30	192.168.0.1 to 192.168.0.30	192.168.0.31
192.168.0.32	255.255.255.224	30	192.168.0.33 to 192.168.0.62	192.168.0.63
192.168.0.64	255.255.255.224	30	192.168.0.65 to 192.168.0.94	192.168.0.95
192.168.0.96	255.255.255.224	30	192.168.0.97 to 192.168.0.126	192.168.0.127
192.168.0.128	255.255.255.224	30	192.168.0.129 to 192.168.0.158	192.168.0.159
192.168.0.160	255.255.255.224	30	192.168.0.161 to 192.168.0.190	192.168.0.191
192.168.0.192	255.255.255.224	30	192.168.0.193 to 192.168.0.222	192.168.0.223
192.168.0.224	255.255.255.224	30	192.168.0.225 to 192.168.0.254	192.168.0.255

Tabulka 8.3 IP adresy sítě C rozdělená do subnetů s konstantní maskou

V praxi často nepotřebujeme rozdělit přidělený IP rozsah sítě na stejně velké podsítě (subnet). Například pro spojovací sítě by byl subnet o velikosti maska /27 plýtváním a pro segment LAN naopak nedostatečný. Proto se zavádí variabilní síťová maska. Například pro síť zobrazenou v tabulce 7.3. bychom mohli připravit adresaci takto:

Síť	Maska	Velikost Subnetu	IP rozsah hostů	Broadcast
192.168.0.0	255.255.255.128	126	192.168.0.1 to 192.168.0.126	192.168.0.127
192.168.0.128	255.255.255.192	62	192.168.0.129 to 192.168.0.190	192.168.0.191
192.168.0.192	255.255.255.252	2	192.168.0.193 to 192.168.0.194	192.168.0.195

Tabulka 8.4 IP adresy sítě C rozdělená do subnetů s variabilní maskou



Obrázek 8.2.1 Propojení sítí počítačů pomocí směšovače, Epocha II

Více viz literatura [4] kapitola 13 a [5] kapitola 8.

9 Moderní sítě

9.1 Klasické pojetí přenosových sítí

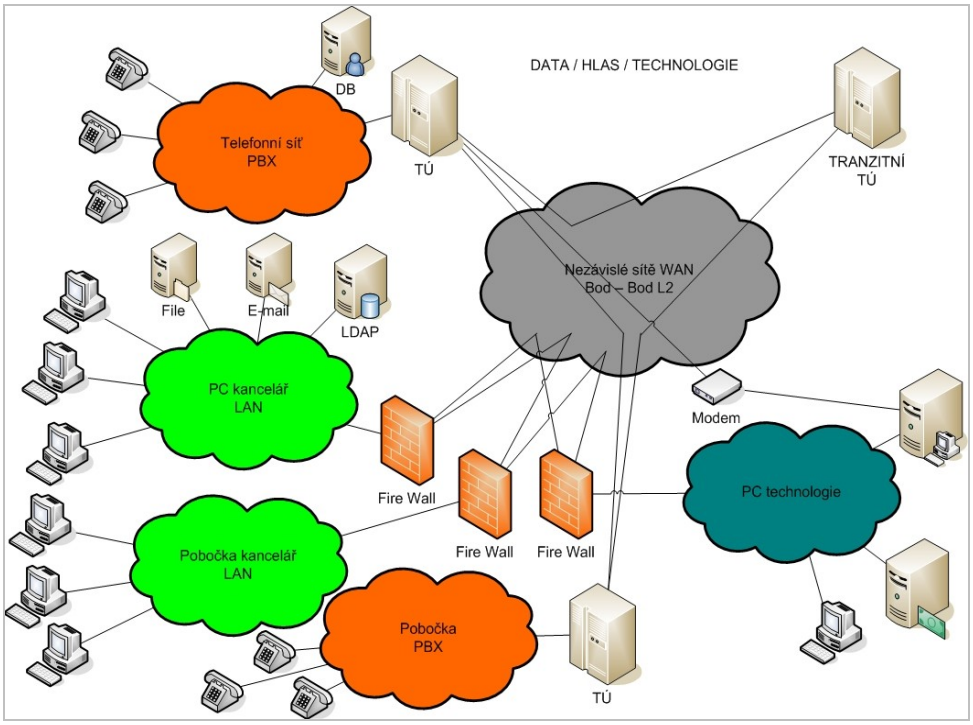
V klasické podobě, jsou sítě budovány odděleně, a to podle účelu přenášených dat. Například rozlišujeme na sítě sloužící k přenosu DAT mezi kancelářskými systémy, odděleně probíhá hlasová (telefonní) komunikace, síť pro sběr technologických dat, síť pro řízení technologických procesů, a další externí sítě (Internet), sítě významných odběratelů/dodavatelů,…

Výhody:

- Jednotlivé sítě jsou oddělené
- Porucha jedné sítě, způsobí výpadek pouze určitého izolovaného systému

Nevýhody:

- Vysoké náklady spojené s budováním a správou oddělených sítí.
- Kompatibilita použitých komponent.
- Udržování velkého množství různorodých systémů mnohdy bez budoucí podpory.
- Spoje mezi sítěmi jsou zranitelné.
- Je potřeba velké množství vysoce kvalifikovaných specialistů, bohužel se znalostí jen určitého systému (neexistuje zastupitelnost na úrovni technologie a aplikací).
- Je nutný N násobný pronájem přenosových kapacit v sítích WAN/MAN/LAN
- V případě přenosu datových sítí, je oddělení pouze adresací v síti, routery
- Bezpečnost musí zastávat další aktivní prvky sítě - firewall
- Špatná škálovatelnost všech systémů
- Nutná koordinace mnoha dodavatelů, servisních smluv a závazků
- Dohled nad několika nestejnorodými systémy vyžaduje zaměstnávat další specialisty
- Různorodé nároky na napájení technologií a jejich zálohy - střídavé systémy 230V, stejnosměrné systémy 48V, 24V, 12V



Obrázek 9.1.1 Klasické sítě

9.2 Konvergentní sítě

V této podobě je vybudována jednotná infrastruktura LAN/WAN umožňující přenos různorodých dat v izolovaných datových rámcích, bez ohledu na jejich množství, a strukturu. Z hlediska univerzálnosti systémů jsou současné technologie založeny nejčastěji na technologii MPLS (Multi Protocol Label Switching, případně na TDM (Time Divising Multiplexing).

Například telefonní sítě byli před příchodem VoIP považovány ryze za spojově orientované sítě, provozované na bázi přepojování okruhů. Příchodem VoIP Voice over Internet Protokol, přechází hlasové sítě přímo do sítí založených na technologiích paketově přepínaných.

9.3 TDM/FDM

- Time division multiplex (TDM) - časový multiplex
- Frequency Division Multiplexing (FDM) – frekvenční multiplex

Pro zpracování datových toků o nestejné přenosové rychlosti je výhodné použít „statistické multiplexování“. Příkladem jsou paketové sítě. Data jsou rozdělena do mnoha fragmentů, paketů, které obsahují kromě užitečných dat také informace o odesílateli

a příjemci, na základě kterých jsou směrovány napříč přenosovou sítí, aniž by byly vázány na konkrétní přenosovou cestu.

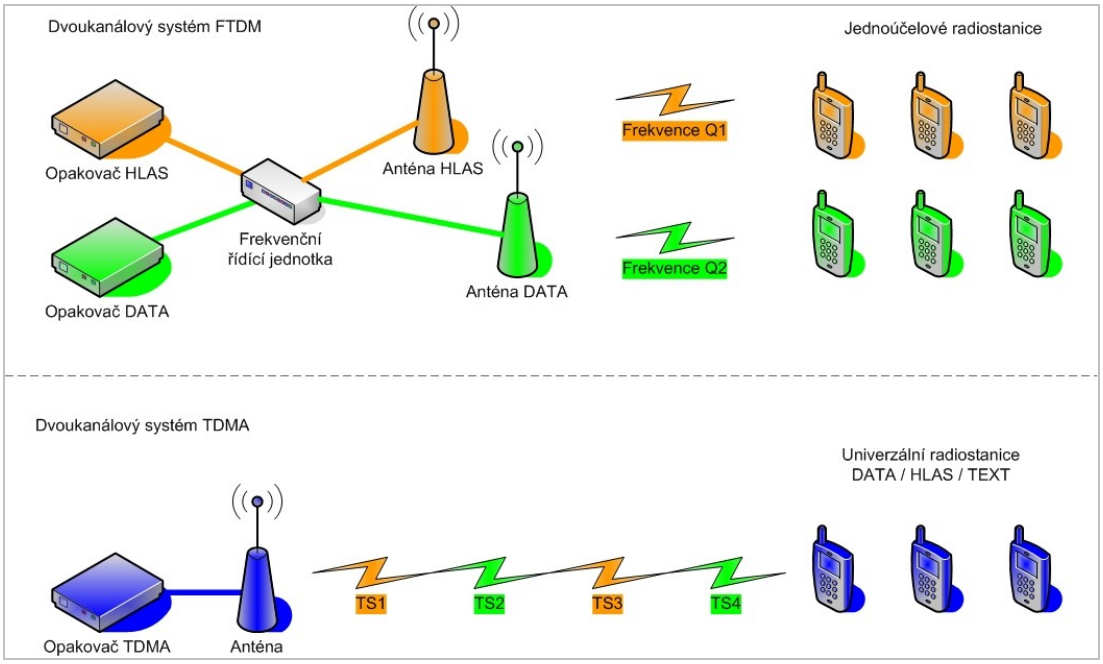
U bezdrátové komunikace lze také využít multiplexování různými polarizacemi signálu.

U digitálního zpracování signálu přichází v úvahu také kódový multiplex (CDMA – Code Division Multiple Access), kde různé signály používají odlišné kódy přenášených informací. Lze také využít ortogonální multiplex s kmitočtovým dělením (OFDM – Orthogonal frequency-division multiplexing).

TDM je princip přenosu více signálů jedním společným přenosovým médiem. Jednotlivé signály jsou odděleny tím, že se každý z nich vysílá (přenáší) pouze krátký pevně definovaný časový úsek. Prakticky ve všech případech se používá rámcové struktury, která je rozdělena na stejně velké time sloty (TS), časové intervaly pro vysílání, pro každý signál jeden. Tento rámec se v čase neustále opakuje, a tedy každý signál se přenáší stále se stejnou pravidelností.

TDM je základní metodou přenosu signálů klasické digitální telefonie. Hlasový signál se pomocí modulace typu PCM digitalizuje a několik hovorových kanálů spolu s pomocnými a řídícími kanály se skládá do časového multiplexu TDM. Tak vznikne např. ISDN BRI (2 hovory + 1 úzký signalizační kanál) nebo ISDN PRI (celkem 32 kanálů, z toho 30 hovorů, jeden signalizační a jeden synchronizační timeslot). Časový multiplex je využíván také uvnitř klasických digitálních ústředen, kde s ním pracuje spojovací pole.

Například u radiových sítí (pro úsporu a nutnost držení licencí na více kmitočtových spekter systému FDM) přecházejí výrobci radiových transpondérů na integraci multiplexu do základnových radiových jednotek. Tedy přechod od FDM k úspornější variantě TDM. FDM si lze představit i jako souběžně vybudované sítě pracujících na různých kmitočtech Q, kde se v jedné síti přenáší hlas a v druhé samostatné síti data pro řízení /ovládání technologie. Přechodem k TDM pracuje již radiový přenos pouze na jedné síti, kde data a hlas jsou vysílány v pravidelně se střídajících time slotech TS viz obrázek 8.3.1 Například firma MOTOROLA, klasický výrobce zařízení na přenos dat a hlasu na kmitočtech v pásmu VHF (136 – 174 MHz) / UHF (403 – 470 MHz), nazývá svůj systém TDMA - MOTOTRBO. Kapacita datového a hlasového kanálu je omezená daná použitou modulací a šířkou přenášeného pásma. Pro systém MOTOROLA MOTOTRBO typicky 12,5 kHz v pásmu VHF. Do jednoho TS se vejde 1 hlasový kanál anebo 1 datový kanál s propustností 2 Kbps.



Obrázek 9.3.1Využití TDM jako náhrada duplicitního pole vysílačů DATA/HLAS

9.4 MPLS

Multi Protocol Label Switching (MPLS) – Přepínané sítě na základě značek paketů.

Síť založená na principech MPLS přesouvá podstatnou část operací nad datovými toky do okrajových částí sítě. Jde o směrování, QoS, administrativní strategie. Vnitřní uzly sítě jsou optimalizovány pro maximální přenosové rychlosti. Jsou jim ponechány jednoduché funkce, implementované přímo do speciálních obvodů ASIC (application-specific integrated circuit).

Přepínání značek odděluje proces směrování od vlastního předávání paketů. Směšovače na okraji sítě opatří při vstupu datgramy daného datového toku značkou. Dál se datagram předává sítí na základě této značky. Tím odpadá nutnost prohledávat směrovací tabulky a urychluje transport datagramů v síti. Díky této technice se datagramy pohybují sítí po cestách, které jsou obdobou okruhů ve veřejných sítích.

Značka obsahuje informace o dalším skoku na cestě. Může také informace o QoS. Značka má pouze lokální význam – je platná pouze pro dva sousední směrovače LSR (Label Switching Router).- nebo také tranzitní router LSR vkládá značku přímo do paketu mezi záhlaví druhé a třetí vrstvy. Příchozí datagram se opatří na LER (Label Edge Router) značkou

L1, Router LSR R1 opatří datagram novou značkou L2 a předá na rozhraní směrovače R2 a takto pokračuje datagram k dalšímu LSR směrovači směrem k cíli. Na cílovém LER je značka z datagramu odstraněna na výstupním rozhraní. Při transportu dochází k výměně značek (label swapping). Všechny datagramy se posílají stejnou cestou LSP (Label Switched Path) RFC 4206 je obdobou PVC v sítích ATM. Na každém směrovači je udržována lokální tabulka značek podle příchozích rozhranní., dále tabulka výstupních značek podle rozhranní. Tabulka značek je udržována v závislosti na IP adresách podle použitého lokálního směrovacího protokolu. Směrování přes celou síť je řízeno pomocí signalizace protokolem LDP (Label Distribution Protokol) a distribuováno mezi jednotlivé LSR. Vstupní LSP bývá také označován jako Ingress Router, a poslední LSP Egress Router.

Značka label stack – nese tyto informace:

- 20 bitovou hodnotu značky
- 3 bitová pole pro QoS a prioritu
- 1 bitovou informaci o dnu zásobníku. Je-li nastaven, je značka poslední v zásobníku.
- 8 bitové pole TTL (Time To Live) – životnost značky

Využití v sítích používaných na úrovni Enterprise (podniků) a Service Provider (poskytovatelé služeb).

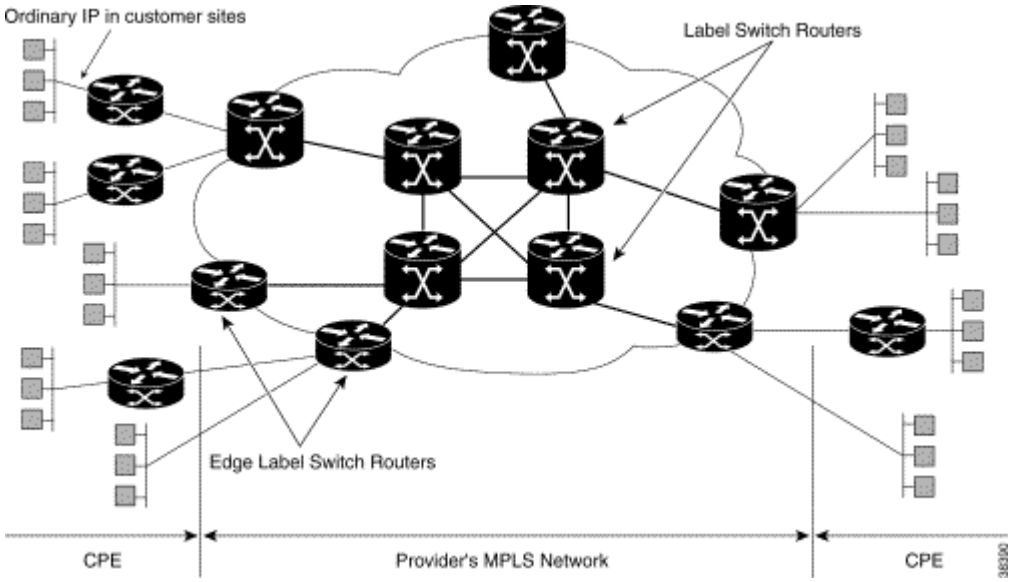
Výhody:

- Jednotlivé sítě jsou oddělené na úrovni přenášených paketů
- Porucha v jedné síti neovlivní síť druhou
- Čas potřebný pro rekonfiguraci LSP shodná s okruhem SONET/SDH pod 50 ms
- Technologické bezpečnosti se dosahuje budováním redundantních uzlů a jejich zakončení. Toto platí z pohledu propojení sítí LAN/WAN, tak i z pohledu připojení serverů s aplikacemi, případně i pro koncové počítače, a návazné technologie.
- Je budován jednotný dohledový systém
- Je potřeba méně zaměstnanců zabývajících se správou sítě
- Stačí podstatně méně dodavatelů technologie, nejznámější např. Cisco Systems, Inc.
- Síť je více transparentní, a nezávislá na specializaci aplikací
- Nativní použití technologie MPLS (Multiprotokol Label Switching) označovaný též vrstvou na úrovni L2,5 modelu TCP/IP

- Přímé podpora L2 VPN
- Přímá podpora L3 VPN
- Přímé podpora multipoint L2 VPN
- Lze provozovat na současné technologii LAN/WAN
- Podpora QoS, GMPLS, IPv6
- Podpora budování sítí s vysokou dostupností služeb – základem podpora routingu na protokolech BGP.
- Možnost nezávisle šifrovat a kódovat jednotlivá spojení, VPN
- Škálovatelnost, jak portů fyzických, tak i logických, transportovaných protokolů
- Je budována jednotná síť, což vede k celkovým úsporám celého životního cyklu technologií sítě.

Nevýhody:

- V případě existujících sítí vybudovaných na řadě aktivních prvků CISCO Systems Inc. - Pořizovací náklady na softwarové vybavení routerů – IOS, podporující MPLS, a zaškolení zaměstnanců – specialistů sítě.



Obrázek 9.4.1Typické zapojení struktury MPLS sítě viz odkaz zdroje

http://www.cisco.com/univercd/illus/3/90/38390.gif (odkaz platný k datu 16. 5. 2009)

Konvergenci v oblasti sítí lze chápat jako postupný proces sbližování odlišných komunikačních technologií, které jsou ve výsledku provozovány na jednotné síťové infrastruktuře. Jedná se tedy o pravý přenos informací (videa, hlasu, dat – společně multimédií) na určitou vzdálenost.

10 Bezdrátové sítě WiFi

Základním způsobem zabezpečení bezdrátových sítí je rozdělení do patřičných skupin oprávnění, na základě pokrytého území, či lokality, nastavení přístupových práv, identifikace uživatele, identifikace připojovaného hardware. Případně pokročilejší technologie založené na analýze instalovaného software na klientské stanici.

Důležitou roli sehrává zabezpečení samotného přenosového kanálu mezi uživatelem a přístupovým bodem bezdrátové sítě.

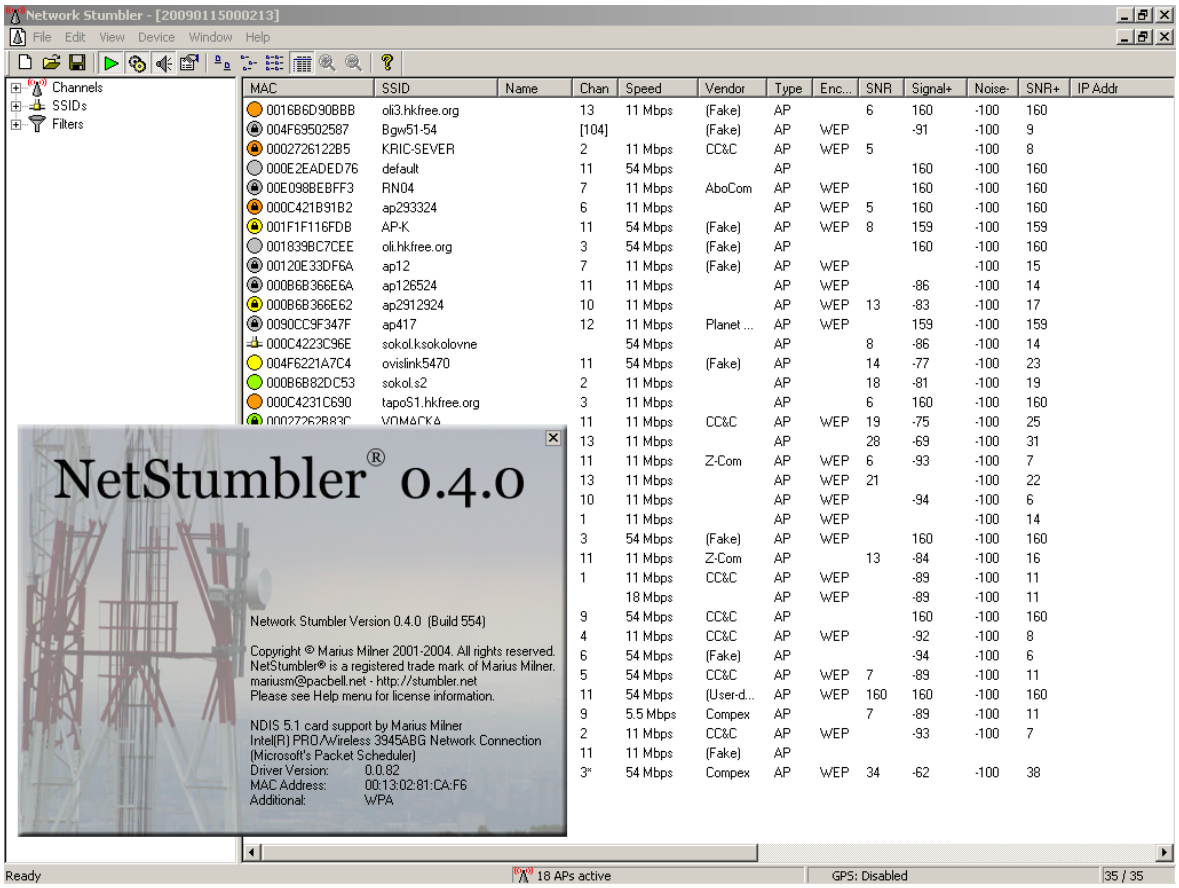
10.1 Spojení Point to point

Jde o topologicky dvoubodové (v případě komunikace pouze dvou zařízení) spojení nezávislé na dalších zařízeních. Při současné komunikaci více koncových stanic jde o polygonální radiové spojení - každý s každým. Omezením zůstává dosah komunikace, danou intenzitou vyzářeného užitečného výkonu anténou daných zařízení, a citlivostí přijímacího systému ostatních stanic. V zařízeních WiFi je tato technika označována Ad-Hoc (dá se přeložit z lat. Jen pro tento případ), k dočasnému použití. Tato technika je často používána při prezentacích ke spojení mezi zařízením na projekci obrazu a přenosným počítačem, případně ke spojení s tiskárnou.

10.2 Spojení distribučním systémem

Jak již bylo napsáno výše, jde o integraci přístupových bodů WiFi do stávajících sítí LAN. Koncová zařízení WiFi se v distribučním systému jmenují stanice. V zařízeních WiFi je tato technika označována Infrastructure Mode u koncových zařízení Station Mode, nebo Client Mode.

Přístupové body spolu s klienty tvoří distribuční systém a jsou logicky svázány prostřednictvím BSS (Basic Service Set) souborem základních služeb. Pro možnost budování hierarchie nezávislých skupin klientů, kteří spolu mohou vzájemně komunikovat (v sítích LAN obdobou VLAN ID) jsou jednotlivé BSS vzájemně rozlišeny SSID (Service Set Identifier).



Obrázek 10.2.1Zobrazení jednotlivých SSID pomocí aplikace NetStumbler

Přístupový bod může SSID skrývat. Jednoznačným identifikátorem v sítích LAN zůstává MAC adresa výrobce adaptéru (jednoznačná adresa zařízení) NIC fyzického rozhranní WiFi.

Každý zařízení pracující se sítí je možné popsat pomocí sedmivrstvého modelu ISO/OSI. Standard 802.11 definuje jako vlastní pouze dvě nejnižší vrstvy – fyzickou a spojovou. Všechny ostatní vrstvy nechává nedotčené.

10.3 Fyzická vrstva

Fyzická vrstva (PHY – physical layer) je fyzickým rozhraním mezi zařízeními v síti. Protože jde o bezdrátové sítě, jedná se o bezdrátovou vrstvu.

Podle prvních ujednání o standardu 802.11 v roce 1997 byly standardizovány tři druhy fyzické vrstvy:

- FH (Frequency hopping spread spectrum radio) frekvenčně rozprostřené spektrum
- DSSS (Direct-sequence spread spectrum radio) kódově rozprostřené spektrum

- IR pulzně-kódová modulace v krátkovlnném infračerveném pásmu

V roce 1999 byly tyto vrstvy při revizi standardu doplněny o další dvě, v roce 2003 pak byla vrstva OFDM použita i pro další revizi standardu IEEE 802.11g.

- 802.11a a 802.11g: OFDM (Orthogonal Frequency Division Multiplexing)
- 802.11b: HR/DS nebo HR/DSSS (High-Rate Direct Sequence)

Rychlost Mbps	Kódování
6	BPSK
9	BPSK
12	4 QAM
18	4 QAM
24	16 QAM
36	16 QAM
48	64 QAM
54	64 QAM

Tabulka 10.1Použité kódování OFDM

10.4 Dostupné rádiové frekvence

V České republice je využití rádiového spektra upraveno koordinátorem ČTÚ (Český telekomunikační úřad) vydanou normou „Všeobecné oprávnění VO-R/10/08.2005-24 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu“. Pro používaná pásma podle IEEE 802.11b, IEEE802.11g (ISM – industry / science / medical) je stanoven maximální výkon 25mW EIRP přibližně -16dBW. Pro přenos signálů může být použito libovolně celé pásmo.

Kanál	Frekvence – střed (GHz)
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484 – není povoleno v ČR

Tabulka 10.2Frekvence kanálů Wifi 802.11 b/g

Pásmo ISM není primárně určeno pro datovou komunikaci, proto může být rušeno z průmyslových i jiných zdrojů (mikrovlnné trouby).

Pásmo 5 GHz je vyhrazeno pouze pro datové přenosy IEEE 802.11a.

Kmitočtové pásmo	Omezení celkového vyzářeného výkonu
5150-5250 MHz	pouze pro vnitřní sítě s max. 200 mW EIRP. Toto pásmo je podporováno standardy IEEE 802.11a a 802.11h.
5250-5350 MHz	pouze pro vnitřní sítě - max. 1 W EIRP (USA) a max. 200 mW EIRP (Evropa). Pro standardy IEEE 802.11a a 802.11h.
5470-5725 MHz	povoleno v Evropě pro venkovní i pro vnitřní sítě s max. výkon 1 W EIRP. Omezeno národním regulátorem.
5725-5825 MHz	povoleno v USA s max. 4 W EIRP, v Evropě včetně ČR jen v rámci nespecifikovaných stanic s maximálním vyzářeným výkonem 25 mW. Omezeno národním regulátorem.
5825-5875 MHz	povoleno v Evropě v rámci nespecifikovaných stanic s maximem 25 mW vyzářeného výkonu. Omezeno národním regulátorem.

Tabulka 10.3 Povolená provozní pásma na 5GHz

11 Zabezpečení přenosu

Zabezpečení bezdrátových sítí, zpočátku nasazování této technologie budilo oprávněnou nedůvěru uživatelů. V zásadě se lze k přístupovému bodu připojit s klientem, pokud známe jeho SSID. Tato komunikace může probíhat se sdíleným klíčem, nebo s otevřenou komunikací. V prvé řadě nebyla výrobci garantována vzájemná kompatibilita zařízení. V původním návrhu IEEE 802.11 se uvažovalo pouze o zabezpečení pomocí protokolu WEP (Wired Equivalent Privacy) – zabezpečení ekvivalentní s připojením pevnou sítí. S možnostmi nasazování bezdrátových sítí postupoval vývoj v zabezpečení sítí dále. Mezi nejpokročilejší metody zabezpečení přístupu lze považovat zabezpečení podle modelu AAA (authentication, authorization and accounting), volně přeloženo - ověření uživatele, přiřazení přístupových práv podle databáze a účtování. Model AAA se využívá v počítačových sítí k zajištění přístupu uživatele jak do sítě samotné, tak i k zabezpečení přístupu do jednotlivých konfiguračních menu jednotlivých zařízení, případně SW aplikací.

11.1 WEP

Režimy provozu:

- bez šifrování
- 40 ti bitové šifrování
- 128 bitové šifrování

V režimu WEP se používá k „utajení“ přenášených paketů na straně vysílače 40 bitový tajný klíč (nebo 128 bitový) generovaný podle algoritmu RC4. Algoritmus RC4 používá pro šifrování 24 bitový náhodný inicializační vektor. Přijímací strana musí znát stejný tajný klíč, kterým data dešifruje. Slabinou je inicializační vektor, který dává 2^{24}=16777216 možných hodnot. Toto vede při odposlechu datové komunikace, k brzkému opakování šifrované sekvence. Stačí zajistit programem pro odposlech paketů dostatečně velký vzorek dat, a pomocí matematických statistických operací, lze hodnotu inicializačního vektoru zjistit.

11.2 Filtrování MAC adres

Opět odposlechem paketů (například volně dostupnou aplikací Ethereal – Network Protocol Analyzer) probíhající komunikace, lze ihned odhalit MAC adresy zúčastněných

zařízení. MAC adresa NIC lze jednoduše změnit. Navíc ve větší síti může nastat problém s distribucí seznamů povolených / zakázaných adres na ostatní přístupové body v síti.

11.3 WPA/TKIP

Oproti WEP je dynamicky měněn. Inicializační vektor je již zvětšen na 48 bitů. Je zde uplatněn princip ověření uživatele na bázi protokolu EAP. Je zde nový algoritmus pro zajištění integrity zasílaných zpráv, který dočasně blokuje komunikaci s útočníkem při detekci pokusu o prolomení TKIP (Temporal Key Integrity Protocol).

11.4 WPA2/AES

Plná implementace podle doporučení IEEE802.11i.AES (Advanced Encryption Standard) Šifra využívá symetrického klíče s délkou 128, 192 nebo 256 bitů. Metoda šifruje data postupně v blocích s pevnou délkou 128 bitů. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). AES je od roku 1997 nástupce prolomeného šifrovacího standardu DES. Zatím není znám případ prolomení této ochrany.

12 Zabezpečení přístupu

12.1 Sdílený klíč

Zabezpečení přístupu na základě sdíleného hesla PSK (Pre Shared Key) jednoduchá varianta zabezpečení. Obě strany přenosového řetězce spolu komunikují, pouze v případě že PSK je shodné. Omezením je právě toto PSK, které je stejné a je nutné jej nastavit na všech zařízeních, která spolu mohou komunikovat v dané skupině. Výhodou je jednoduchá implementace, bez potřeby nasazovat ověřovací server. Hodí se zejména k připojení malého počtu klientů k jednoduchému přístupovému bodu typu Infrastruktura. Také je vhodné použití v kombinaci WPA2/AES + PSK s kombinací filtrování na MAC adresy, k zabezpečení přenosu dat na radiových spojích typu Point to Point, anebo na velice vzdálených lokalitách, které jsou schopny pracovat autonomně.

12.2 Protokol EAP

(Extensible Authentication Protocol) standardizovaný protokol podporovaný podle IEEE 802.1X pro řízení bezpečnosti na hraničních portech. Pro svoji činnost potřebuje aplikační server, kde běží aplikace podle protokolu RADIUS (Remote Authentication Dial In User

Service), RFC-2865. a RFC 2866.[5] Zjednodušeně, pokud uživatel potřebuje přistoupit přes některý port do sítě LAN (přístupový server / port přepínače sítě LAN / WiFi přístupový bod) vyšle uživatel prostřednictvím klientského software (802.1X suplikant) nejprve protokolem UDP žádost serveru RADIUS na Autentizaci (ověření totožnosti klienta). Pokud je v databázi (nebo databázi LDAP na který se RADIUS odkazuje) RADIUS shledán požadavek na přístup jako oprávněný, je uživateli vrácena zpět akceptační informace – uživatel je Autorizován. Teprve poté je uživateli povolen vstup do datové sítě.

12.3 Radius

Tímto názvem je také nazýván server, na kterém samotná služba RADIUS běží.

Typy zpráv využívající protokol RADIUS:

- AccessRequest – klient protokolu RADIUS jím odesílá požadavek na autentizaci serveru RADIUS
- AccessAccepted – server potvrzuje identitu klienta – autorizuje přístup oprávněného uživatele do sítě
- AccessReject – server zamítá přístup do sítě
- AccessChallenge – výzva serveru RADIUS přístupovému rozhranní na doplnění klientovi jednorázové heslo pro komunikaci se serverem.
- Autorizace RADIUS serveru – probíhá na základě sdíleného tajemství mezi serverem a 802.1X suplikantem na klientském počítači.

12.4 TACACS+

TACACS+ (Terminal Access Controller Access-Control Systém), kontrola přístupu k terminálu systém řízení přístupu. Jde o implementaci firmy CISCO k zabezpečení přístupu k síťovým aktivním prvkům. TACACS+ poskytuje AAA služby odděleně.

12.5 Metody Autentizace:

- EAP MD5 nejméně bezpečná verze, generován hash (otisk) MD5 z uživatelova přihlašovacího jména a hesla. Nicméně metoda vhodná k ověření funkce ověřovacího serveru.
- LEAP podobně jako předchozí verze, navíc se pro každé klientské připojení dynamicky generují jednorázové klíče WEP, časová platnost jednorázových klíčů

(během komunikaci dochází automaticky ke změnám klíče), provádí obousměrnou autentizaci mezi přístupovým bodem a klientem. Oficiálně „prolomená“ metoda autentizace, kterou již firma CISCO nedoporučuje používat.

- EAP-TLS autentizace prostřednictvím certifikátů X.509, veřejný klíč PKI se přenáší pomocí zabezpečené transportní vrstvy. Dvojité certifikáty.
- EAP-TTLS klient se musí autentizovat vůči serveru pomocí certifikátu, uživatelé přitom zadávají pouze uživatelské jméno a heslo. Administrátor může předdefinovat způsob ověření uživatele.
- PEAP - Protected EAP, doporučovaná perspektivní metoda autentizace.

12.6 Zabezpečení přístupovým serverem - VPN tunelování

Neméně významným způsobem zabezpečení, je umožnění přístupu uživatelů na základě principů modelu AAA, do podnikové sítě, tunelováním datového provozu (vytvořením bezpečného šifrovaného kanálu dat, nezávislého na okolní adresaci) libovolnou sítí, například nebezpečnou sítí Internet. VPN (Virtual Private Network) tunel se využívá zejména k vytvoření zabezpečeného přístupu klientského počítače pomocí spuštění VPN programového vybavení (například CISCO AnyConnect VPN Client, nebo pro WiFi specializovaný CISCO Secure Services Client 5.1), umožňující navázat IPSec VPN k přístupovému bodu sítě (VPN koncentrátor), kde je AAA model realizován.

Přístup do sítě zprostředkovává většinou samostatný HW, doporučuje se používat přímo firewall. V ucelené a ověřené škále tímto RAS (Remonte Acess Server – vzdálený přístupový server), může být například Cisco ASA řady 5500 s patřičným SW.

Vhodné je také nasazení systému detekce výskytu potenciálně nebezpečných datových vzorků obsažených v paketech datové komunikace. K tomu se nasazují systémy IPS/IDS (Intrusion Prevention Systems / Intrusion Detection Systems) Systémy prevence / detekce vniknutí. V případě zjištění určité datové sekvence (nebezpečný vzorek dat) v datovém toku, (podezření na infiltraci útočníka, zaznamenání virové nákazy), je samočinně na základě předdefinovaných procesů), omezen, nebo zcela uzavřen datový kanál, a jsou zaregistrovány potřebné informace do bezpečnostní databáze systému. Vadná datová sekvence, bývá nejčastěji ihned zahozena, a původce bývá přesměrován do DMZ (Demilitarizovaná zóna).

13 Nasazení izolovaných přístupových bodů

Každý AP nese kompletní informaci o nastavení parametrů jak RF vysílače, bezpečnostní parametry přístupu (protokoly zabezpečení, odkaz na RADIUS, vlastní přístupové filtry na IP adresy, MAC adresy okolních přístupových bodů, případně klientů), spravované účty klientů (přihlašovací jména, hesla). Dále musí být takovýto AP přístupný vzdálené správě (protokolem SNMP), to jsou další informace obsažené přímo v daném AP (IP adresy, přístupové účty, hesla). Z hlediska nasazení autonomního bezdrátového AP a při jeho odcizení získává potenciální útočník na bezdrátovou síť veškeré informace konfigurované v takovémto autonomním přístupovém bodě. Značnou další nevýhodou je v případě požadavku na konfiguraci RF parametrů, či změně parametrů sítě (BSSID, VLAN, přístupových práv), nutnost administrativně se přihlásit do daného AP a provést patřičné změny. Při požadavku na změnu současně na více autonomních AP, přibývá geometricky potřebný čas na administraci daných přístupových bodů.

Za izolované body lze považovat většinu přístupových bodů nasazených na spojích Point to Point, které jsou nasazovány většinou v síti jako mosty s rozhranním Ethernet na straně LAN podle IEEE.802.1D s podporou IEE 802.1p a IEEE 802.1Q pracující na L2 ISO/OSI. K přenosu se využívají zařízení od mnoha výrobců, které spojují pouze standardy TCP/IP (ISO/OSI). Integrace do centrálního managementu sítě bývá dost často omezena pouze na terminálový přístup, u novějších přímá podpora SNMP, s různou úrovní zabezpečení přístupu a přenosů informací.

Bezpečnost je řešena na vyšších úrovních přenosových protokolů, případně tunelováním (šifrováním a nasazením AAA) na straně klienta a zdroje dat, nebo použitím firewallu alespoň na straně zdrojů dat sítě. V obou případech dochází ke snížení propustnosti přenosové kapacity sítě.

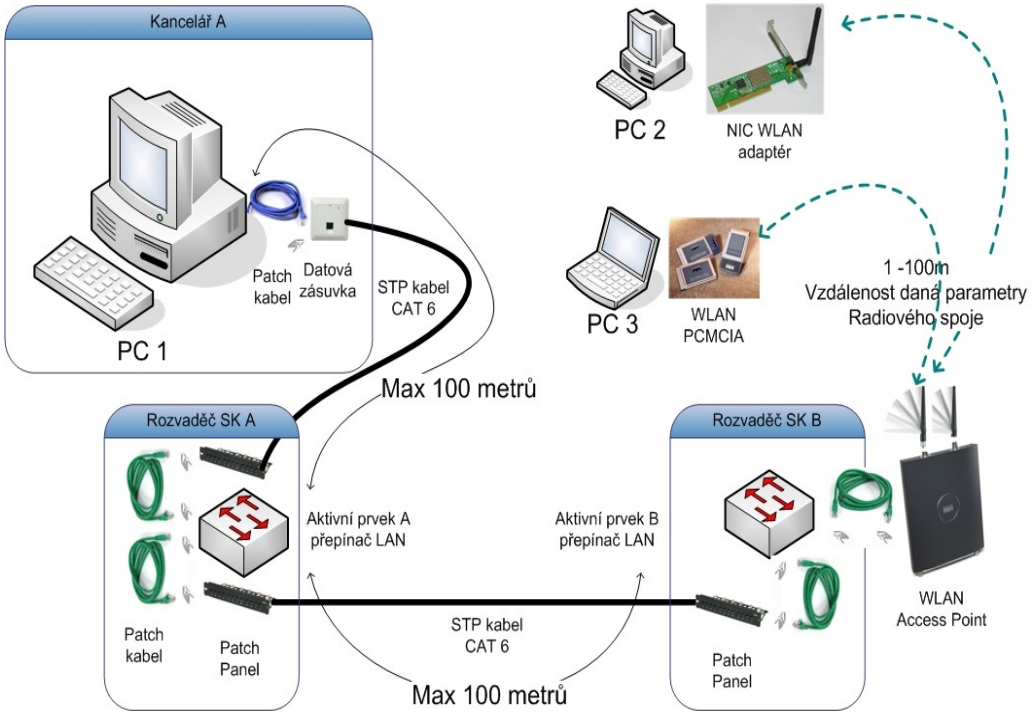
13.1 Nasazení aktivních prvků WiFi

Zařízení využívajících technologií WLAN mohou spolu komunikovat přímo bez použití fyzického spojení. Případně dalších zařízení. Přenos probíhá modulovaným signálem v podobě vysokofrekvenčního elektromagnetického pole, šířeného v okolním prostředí. Zařízení, která chtějí spolu komunikovat musí být pouze vybavena rozhranním umožňující tuto komunikaci. Tímto rozhranním je NIC (Network Interface Card) splňující parametry

použité technologie, například podle IEEE 802.11a,b,g zařízení výrobci označovaná WiFi (WiFi Aliance – sdružení výrobců zařízení). V dnešní době mobility bývá tento interface standardní výbavou přenosných zařízení. Také výrobci tiskáren a video-projekčních zařízení umožňují volitelně použít k přenosu dat WiFi. Toto řešení je vhodné v rámci místnosti na nezbytně nutnou dobu.

Při potřebě nasadit technologii WiFi na pokrytí větších prostor, nebo potřebě současně sdílet určité datové zdroje z LAN, je za tímto účelem třeba instalovat komunikační infrastrukturu s návazností na LAN. Infrastruktura je založena na rozhraních mezi LAN a WiFi, jež zajišťují aktivní prvky Access Point (přístupové body) za WiFi a aktivní prvky přepínače za LAN.

Soudobé WiFi přístupové body přímo podporují nezávislé vyzařování v režimech IEEE802.11b/g a IEEE802.11a, podporují IEEE 802.1q podpora až osmi SSID z jednoho přístupového bodu. Každé SSID lze nezávisle přiřadit způsob AAA podle IEEE802.1X, s návazností na klasické VLAN ID v pevné síti. Podpora IEEE 802.1D zahrnující prioritizaci paketů. Je možné je napájet přímo z přepínače LAN podle standardu IEEE 802.3af napájení z rozhranní Ethernet. Je možné individuálně nastavovat způsob zabezpečení přenosu na radiové části.



Obrázek 13.1.1Připojení Access Pointu do LAN

14 Nasazení centrálně řízených přístupových bodů

Využití v instalacích s velkou hustotou přístupových bodů, nebo s častými změnami konfiguračních parametrů sítě, velkému územnímu pokrytí s jednotnou technickou platformou použitých zařízení. Vhodné k nasazení v prostřední s velkou hustotou nasazených AP, s omezeným počtem zaměstnanců spravujících datové sítě. Nově budované firemní sítě využívají téměř standardizované protokoly LWAP a CAPWAP. Protokol LWAP, nebo CAPWAP slouží k vytvoření virtuálního kanálu mezi přístupovým bodem LWAP (Light Weight Access Point) a řídícím kontrolérem WLC (WLAN Controller).

U implementace některých firem jsou řídící a datové informace šifrovány. Například u firmy CISCO Systems, Inc dochází pouze k šifrování konfiguračních rámců.

Z principu jde o to, že AP již nenesou kompletní konfiguraci o síti a uživatelích. Při jejich ztrátě, útočník získá maximálně informaci o názvu daného AP, jeho MAC adresy radiové sítě a rozhranní Ethernet, případně konfigurační IP adresu AP. Veškerá logika řízení, konfiguračních dat je spravována na speciálních zařízeních – kontrolérech bezdrátové sítě, umístěných v bezpečí serveroven a vyhrazených rozvaděčích sítí. Každé AP navazuje samostatný kanál na daný kontrolér.

KONTROLER WLAN – sdružuje konfigurační data všech LWAP Access Pointů ve skupině, redistribuuje konfigurační informace WLAN, VLAN, BSSID, provádí kontrolu a řízení využití RF pásem, slouží k rychlému roamingu klientů (předávání informací o připojených klientech mezi AP), provádí ověření přístupu podle modelu AAA, sbírá a zasílá informace protokolem SNMP na centrální systém dohledu a správy sítí. Slouží také k rychlé identifikaci klientů, podle MAC adresy, případně podle informací z vyšších vrstev IP adresa, jméno uživatele, jméno počítače. Velice významný je troubleshooting například při navazování relace AAA uživatele. Ihned je k dispozici náhled, ve kterém stavu se uživatel (jeho stanice) nachází, došlo-li ke korektnímu spárování klienta podle pravidel AAA. Dále je umožněno účtování služby, například podle doby připojení. V případě pokusu o detekci zneužití sítě, je možné zpětně dohledat informace podle zaznamenaných logů. Při nasazení AP v módu AP senzor je možné přehledně monitorovat RF signály z okolí tohoto AP. Je tak možné vynucovat novou autentizaci okolních AP, které nepatří do pracovní skupiny dané sítě WLAN, a tím omezit jejich fungování v síti. Užitečná funkce k detekci cizích AP, která by se v centrálně nasazených technologiích firemních aplikací, například budov, neměla nacházet.

15 Implementace bezdrátových sítí v ČEZ ICT Services, a. s.

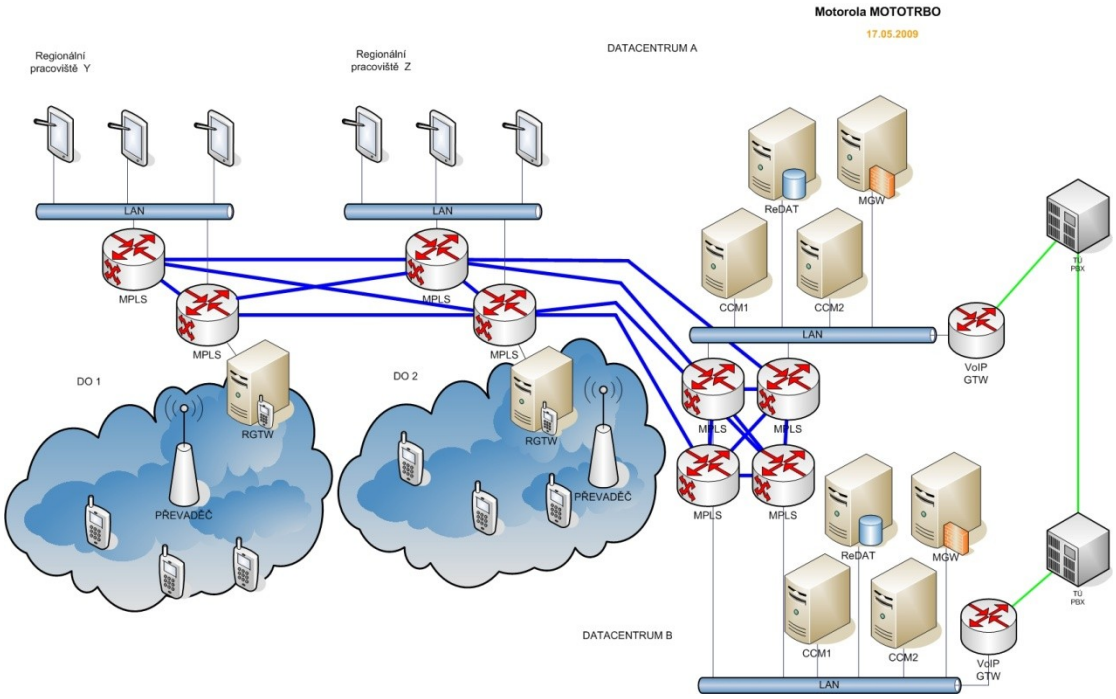
15.1 Relace point to point Datová a Přenosová síť

Dvoubodové spoje slouží k propojení lokalit na větší vzdálenosti. Jsou náhradou pevných optických sítí, kde není z ekonomických důvodů plánována obměna zemního lana na vedeních VN a VVN, případně NN, za KZL (kombinované zemní lano). V KZL se stal již standardem vláknový profil v počtu minimálně 24 vláken s optikou 9/125 μm. V současné době, jen na území východních Čech, jsou využívány systémy Ericsson MiniLink v Licencovaném pásmu 13 GHz, 18GHz a také ve volném pásmu 10 GHz systémy ALCOMA. Výhodou těchto technologií je časem prověřená stabilita, možnost v daném radiovém skoku přenášet data na standardních rozhranních E1/E2 G.703, i FastEthernet, a to až do přenosové kapacity spoje 40 Mbps. Nejnovější technologie umožňují ve volném pásmu 10 GHz dosáhnout kapacity datového spoje až 80 Mbps. Spoje jsou nasazovány převážně s ohledem na požadavky zajištění konektivity soustav automatického (bezobslužného) provozu, zajištění telefonních služeb, a propojení administrativní datové sítě pracovišť firem Skupiny ČEZ, a.s. Striktně je brán zřetel na logické oddělení technologických a kancelářských datových sítí. Některé spoje jsou realizovány účelně, na základě obchodních projektů externích zákazníků k distribuci čistě jen Internetové konektivity ČEZ ICT Services, a.s., dříve ČEZnet, a.s.

15.2 Radiová datová a hlasová síť pro dispečerské řízení

Jedná se od roku 2008 o nově zaváděnou radiovou síť na kmitočtech 146 – 174 MHz s použitím technologie Motorola Mototrbo. Síť sjednocuje data a hlas do samostatné sítě na principu TDM a FDM, s využitím IP telefonie firmy CISCO Systems, Inc. Síť slouží k propojení 5 ti dispečerských pracovišť v lokalitách Plzeň, Ústí nad Labem, Praha, Hradec Králové a Ostrava, s jednotlivými regionálními pracovišti zásahových čet ČEZ Distribuce. Každé dispečerské pracoviště bude připraveno obsluhovat 10 standardních provozních pracovišť zásahových čet, a až 6 pracovišť pro přípraváře, které se dají rekonfigurovat na plnohodnotná pracoviště v době kalamit. Pracoviště zásahových čet využívají k přenosům dat a hlasu vysílačky Motorola Mototrbo v provedení do zásahových vozidel a v ručním provedení. Jsou použity produkty Motorola řady: DP 3600/DM 3400/DM3600 a pevné základnové stanice DR3000. Na dispečerských pracovištích jsou použity komunikační pulty TTC Marconi TouchCall. Přenos dat a hlasu v pevné síti je realizován v samostatné TCP/IP

L3 VPN MPLS na technologii CISCO Systems Inc. Síť obsahuje samostatné VoIP servery Call Managers na protokolu SIP, VoIP Gateway do pevných sítí telefonie a na tranzitní telefonní ústředny. Dále Media Gateway pro řízení sítě Motorola Mototrbo a Radiové Gateway mezi IP sítí LAN/WAN a radiovou sítí Motorola. Z bezpečnostních důvodů je řešeno nahrávání veškerých hovorů protokolem H.323 na osvědčené zařízení ReDAT. Hlasová komunikace se využívá pro přímé řízení v provozu, datová komunikace pro dálkové řízení úsekových spínačů rozvodů NN a VN.



Obrázek 15.2.1

15.3 Datové sítě WiFi v ČEZ ICT Services, a. s.

Datové dítě WiFi jsou používány od roku 2006 a to ve vnitřních prostorách budov, za účelem zajištění jednotného přístupu mobilních uživatelů ke zdrojům kancelářské sítě LAN. V původním projektu dceřiné společnosti ČEZ Data, s.r.o., bylo počítáno s nasazením samostatně konfigurovaných přístupových bodů. Byl stanoven požadavek na zabezpečení WLAN sítě protokolem WPA / TKIP / s využitím RADIUS serverů na Linuxové platformě Radiator od Open Systém Consultants. Na klientských stanicích byl použit 802.1X suplikant v podobě instalace klienta AEGIS Secure Connect Single Sign s platným certifikátem pro radius server. Autentizace protokolem PEAP, s tunelováním GTC. Jako alternativa bylo počítáno s protokolem MSCHAPv2 implementovaného přímo v operačním systému MS Windows XP, používaného na klientských stanicích.

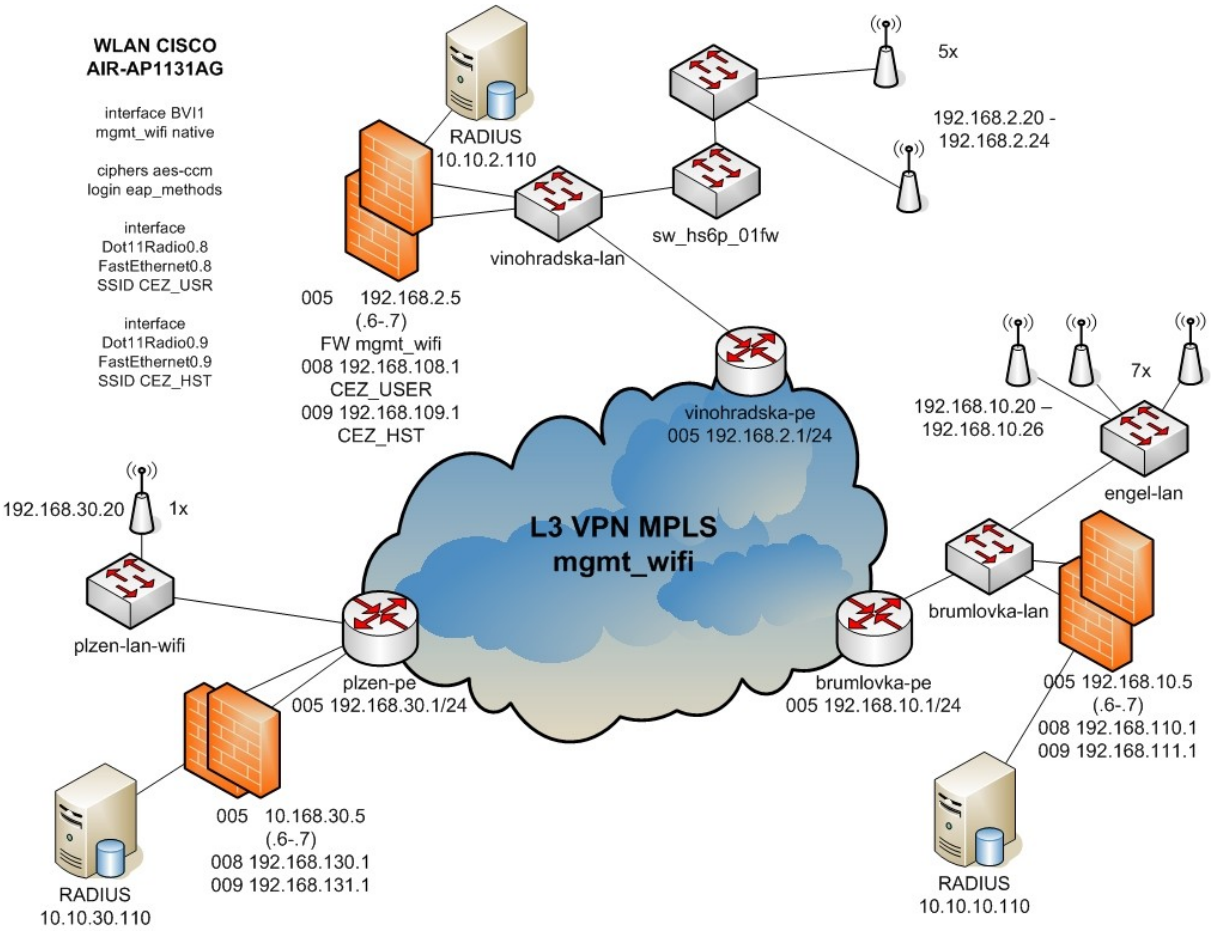
Servery Radius měly být instalovány na dedikovaných serverech v DMZ v perimetru lokálních firewallů lokalit. Servery jsou přímo svázány s certifikační autoritou Lotus Notes, a systémem LDAP.

Za odsouhlasený HW WiFi klientů jsou odsouhlaseny karty standardu 802.11 a/b/g standardně dodávaných v NTB (notebook) podle korporátních standardů. Alternativní způsob připojení, schválený dne 15. 6. 2006 v Praze je připojení kabelem na rozhranní Fast Ethernet.

15.3.1 První etapa – autonomní AP

V první etapě došlo k nasazení autonomních AP AIR-AP1131AG od firmy CISCO. Konkrétně s firmware 12.3-8.JEA a později 12.3-11.JA z 31. s datem publikování srpen 2006. Instalace obnášela pokrytí signálem zasedacích místností v areálu budov:

- Praha Brumlovka, „Engel“ v počtu 7 kusů autonomních AP;
- Praha Vinohradská ul., v počtu 5 kusů autonomních AP;
- Plzeň Guldnerova ul., v počtu 1 kusů autonomních AP;



Obrázek 15.3.1 1. etapa nasazení autonomních AP CISCO

15.3.2 Druhá etapa – centrální řízení

V druhé etapě došlo k nasazení centrálně řízených AP AIR-LAP1131AG od firmy CISCO. K ověření LWAPP technologie v lokalitě Hradec Králové Sladkovského. Kontrolér pro celou lokalitu byl zvolen WiSM WLAN Service Module WS-SVC-WISM-1-K9 do routeru CISCO Catalyst 6509 se Supervisor Engine 720 WS-SUP720-3B. Instalace obnášela pokrytí signálem zasedacích místností ČEZ net, a.s. v areálu budov lokality Hradec Králové, a pomocí kontroléru CISCO 4402, lokalita Praha Fügenerovo nám. s testovacími 5 ks AP. Stejný kontrolér 4402 dále obsluhuje lokalitu Praha Tiskařská ulice a tam instalovaná 3 vzdálená AP. A to mimo korporátní síť ČEZ, a.s. Zde se také provedly v reálném režimu testy WiFi IP telefonie na mobilním telefonu dispečinku.

V testovacím provoze byl použit jediný server TACACS+ od firmy CISCO Systems, Inc. A to na HW serveru HP ProLiant s OS Windows 2003 instalovaný v Hradci Králové. Došlo k ověření funkce přístupu do kancelářské sítě ČEZ net, a.s. AAA bylo nastaveno zjednodušeně, bez nutnosti použití certifikátu zabezpečením komunikačního kanálu WPA2/AES s ověřením na serveru RADIUS pod SW TACACS+ protokolem PEAP, MSCHAPv2. Testovacího provozu se účastnili převážně technici firmy ČEZ net, a.s. a někteří členové managementu. K plné spokojenosti zúčastněných. Zároveň byl v Hradci Králové instalován centrální dohled nad technologií WCS (Cisco Wireless Control Systém) s doplňkovým serverem Cisco Wireless Location Appliance, umožňující mapovat a identifikovat pohyb klientů v síti WiFi WCS. Na klientské straně byl použit originální software dodávaný s NTB Dell k interním kartám WLAN Intel PROSet/Wireless WiFi s interním suplikantem 802.1X. Tyto ovladače plně podporují CISCO rozšíření CCKM (rychlý roaming) a Cisco Compatible Extensions (umožňuje například regulovat na základě síly signálu mezi klientem a AP výkon RF obvodů, případně pokud je povoleno automaticky přelaďovat stávající komunikaci bez výpadku na volný frekvenční kanál). Tím je opět zlepšen komfort zajištění kvality přenosového kanálu. Důležitá je tato podpora při využívání IP telefonie přes WiFi.

Byla také ověřena možnost poskytovat například Internetovou konektivitu na vyžádání. A to za pomoci funkce Lobby Ambasador. Metoda AAA spočívá ve vytvoření „účtu hosta“ vytvořené přímo na samém kontroléru WLC pomocí centrálního dohledu WCS. Uživatel „host“ se může za předem nastavených podmínek připojit do vybrané sítě a provést AAA relaci prostřednictvím zabezpečené stránky v internetovém prohlížeči protokolem HTTPS.

Výhodou technologií WCS je možnost na daných LWAP konfigurovat nezávisle až 16 BSSID a to na sobě nezávislých, oddělených systémech 2,4 a 5 GHz.

Další testovací lokalitou centrálního řízení byla zvolena elektrárna Prunéřov a Guldnerova ul. Plzeň. V elektrárně Prunéřov 2 je nasazen WCS s kontrolérem CISCO 4402-25 a 1 testovací LWAP. A to z důvodu testování nasazení redundantních TACACS+ serverů. V Plzni je nasazen WISM modul v routeru 6509 a také testovací 2 x LWAP, pro účely testování úseku bezpečnosti ČEZ Data, s.r.o.

15.3.3 Třetí etapa – budova „E“ Praha

Další etapou bylo nasazení LWAP AP v nové budově ČEZ v Praze ulice Duhová. V budově „E“ je celkem nasazeno 75 LWAP AP a 2 kontroléry WISM ve dvou redundantně nasazených routerech 6509. Významnou změnou je příprava nasazení dalšího modelu centrální L3 MPLS VLAN pro uživatele korporátních aplikací v ČEZ, a. s. a zakončení v datovém centru v Plzni. Bohužel daný model dosud čeká na schválení úsekem bezpečnosti, a pokud je mi známo, dosud se nepoužívá. Informace platné k 16. 5. 2009.

Systém byl navrhnut s propustností 10 Mbps na klienta při hustotě 20 klientů na 1 AP. V praxi je ověřena možnost práce až 50 klientů na 1 AP, rozložená na pásmo G/A. Zde je však již limitující rychlost rozhranní 100 Mbps FastEthernetu připojení AP do LAN. Nicméně na běžné kancelářské aplikace stále vyhovující. Naprosto nevhodné je připojování technologie WiFi využít pro aplikace náročné na datovou kapacitu (GIS – grafické informační systémy, bez použití tenkého klienta, nebo tiskový post procesing). V těchto případech bude lépe zůstat u využití metalického vedení LAN.

15.3.4 Čtvrtá etapa – plošné nasazení

Jsou nasazovány WLC a LWAP na lokalitách elektráren a administrativních objektech Skupiny ČEZ. Další připojované lokality: Ostrava, Elektrárna Chvaletice, Elektrárna Poříčí, Elektrárna Počerady, Elektrárna Mělník, Vodní dílo Štěchovice. Další lokality Elektrárna Tisová, Elektrárna Dětmarovice, elektrárna Hodonín, Elektrárna Dukovany, Elektrárna Temelín, Elektrárna Tušimice, Elektrárna Ledvice, Středočeská Energetika, Hlavní správa Děčín, Praha Duhová stará budova HSP, Praha Engels. Datová konektivita je zakončena na místních firewallech, a technické komponenty jsou integrovány do centrálního dohledu. Daná

technologie umožňuje během krátké chvíle nakonfigurovat nové BSSID a parametry AAA přístupu na daných lokalitách.

15.4 Instalace BC Varšava a Budapešť

V obou lokalitách je použito shodné technické řešení. Pro zajištění datových a hlasových služeb jsou použity autonomní Call Managery Express, místní Routery MPLS-CE a LAN switches 3560-48-PS. Za WLC byl vybrán malý kontrolér 2006 umožňující připojit maximálně 6 LWAP a přímo může napájet 2 ks AP na standardu IEEE 802.3af . Ve Varšavě jsem instaloval celkem 4 kusy AIR-LAP1131G. V Budapešti pouze 2 kusy AIR-LAP1131G. V Budapešti byla nasazena WiFi VoIP v podobě 3 kusů mobilních WiFi telefonů IP Phone 7921 série. Routery jsou použity 2811. Call Manager Express zajišťuje VoIP telefonii, navazování hovorů, bránu mezi pevnou sítí místního telefonního operátora, a VoIP telefonní z ČR. Bohužel současný IOS nedovolil nasazení jediného routeru pro funkce jak hlasové CCME (Call Manager Express), tak pro funkce datové sítě. V instalovaném voice IOSu chybovala podpora VRF Lite. Z tohoto důvodu je pro funkci směrování sítě WAN a LAN nutný druhý server. Router s CCME plní zároveň funkci hlasové gatewy do sítě LAN. Ve Varšavě byly v Obchodním centru ČEZ požadovány pevné IP telefony. Je zde nasazeno 15 IP telefonů série 7960 napájených pomocí 803.af (napájení po Ethernetu). Z obou lokalit jsou pronajímány kanály WAN s kapacitou 2Mbps do ČR, kde jsou na Telehouse Sitel Praha připojeny k páteřní síti MPLS. K tunelování samostatných VLAN spojovacích sítí pro dohled aktivních prvků LAN, dohled WiFi technologie, Internetovu konektivitu, a hlasové služby slouží protokol FrameRelay nad rozhrnním E1 G.703.

15.5 Demo lab wifi domácí kancelář

Za účelem testování WiFi technologie na standardu IEEE 802.11 v pozici Point to Point WAN spoje v současné době využívám daných technologií k práci z domu. Na vzdálenost cca 3 km vzdušnou čarou, mám nasazenu technologii Motorola Canopy na kmitočtu 5500 Mhz. Radiový skok mám v režimu bridge dle 802.1D, zakončenou přepínačem CISCO Catalyst 2960 a IP telefonem 7960 s expanzním modulem 7914 pro rychlou volbu volaného. Telefon je napájen ze samostatného síťového adaptéru 48V DC. Telefonní služby zabezpečuje Call Manager na centrále. Hovory a data jsou routovány na L3 MPLS routeru protokolem BGP a distribuovány v oddělených sítích L2 VLAN. Přepínač LAN je integrován do centrálního SNMP dohledu a přístup je monitorován podle pravidel AAA třemi centrálními

distribuovanými servery TACACS+. Měl jsem také na daném spoji možnost testovat technologii MikroTik. Také jsem ověřil vhodnost technického řešení radiové relace 2 na 2. K plné spokojenosti, jen mi chyběli volné nezaručené kmitočty v pásmu 802.11a. Bohužel zde je možná slabina dnešních širokopásmových radiových sítí, pracujících v bezlicenčních pásmech. Další otázkou může být časová stabilita a bezporuchovost nasazené technologie.

15.6 Další projekt na WiFi síť Praha

Momentálně se připravuje další projekt na zajištění WiFi technologie v právě stavěné nové budově ČEZ v Praze. Předpokládám s nasazením technologie na budoucím standardu 802.11n Draft 2007, využívající k šíření signálu i odražené vlny, technologie MIMO. Je plánováno s nasazením cca 75 AP Aironet 1140, která jsou opět napájena dle standardu 802.3af, ale již s rozhranním připojením do LAN Gigabit Ethernet. Technologie by měla ještě lépe využít přenosového frekvenčního spektra 2,4 a zároveň 5GHz, a tím umožnit přenosovou rychlost do 300Mbps. Také je plánováno nasazení nových standalone WLC s průchodností 8 až 16 Gbps. Protokol LWAP / CAPWAP již bude umožňovat transport plně šifrovaných dat mezi AP a kontrolérem. Samozřejmá je integrace do stávajícího systému TACACS+ a dohledu WCS.

16 Přístup k sítím a jejím službám z pohledu uživatele

Sjednocením infrastruktury pod jednotný princip distribuce (jednotnou fyzickou infrastrukturu, jednotné metody přístupu, připojení jedním kabelem) dochází z pohledu uživatele k zjednodušení celé problematiky síťové konektivity. Pro uživatele se přenosová technologie, (způsob přenosu informací, adresace, směrování, zabezpečení, kapacita) stává nezajímavou - transparentní. Zajímá jej pouze vstupně výstupní rozhranní nabízených služeb, grafické provedení aplikací, jednoduchost používání a kolik za toto zaplatí.

Další co zákazníka kromě ceny zajímá je „Dohoda o úrovni poskytovaných služeb“, z mezinárodně uváděné zkratky SLA (service level agreement).

Takovýto pohled většiny zákazníků, a vzrůstající konkurence na informačním trhu, vede uživatele k rozhodnutí nákupu služeb od patřičných telekomunikačních / IT firem.

17 Závěr

Z praxe mám odzkoušeny možnosti nasazení mobilních a pevných technologií WiFi a jejich konfigurace od výrobce CISCO Systems, Inc. Dále mám ověřenu kompatibilitu běžně používaných RR spojů ALCOMA, ERICSSON a MOTOROLA Canopy, MikroTik, (Technologie Motorola Mototrbo je stále v testovacím režimu). V zaměstnání každý den pracuji s technologií LAN / WAN MPLS CISCO.

Jistým omezením RR (radio reléových spojů) jsou různé přístupy výrobců k možnostem zabezpečení přenosového kanálu například doplňkovým šifrováním celého přenosového kanálu na bázi AES, možnosti nasazení metody přístupu AAA k jednotlivým API/GUI konfigurace zařízení (konfigurace prostřednictvím terminálu po RS 232), případně IP TELNET, v lepším případě podpora IP SNMP protokolu.

Pro účely vylepšení spolehlivosti stávající vnitřní sítě WiFi ČEZ ICT Services, a. s., bych doporučil náhradu stávajících serverů Radius Radiátor na platformě Linux nahradit za osvědčenou technologii CISCO TACACS+, která se dá velice dobře integrovat do stávajících systémů LDAP, pracujících spolehlivě v redundantním režimu, momentálně využívaných za účelem ověřování přístupu a změn konfigurací v aktivních prvcích sítě LAN/WAN. K připojení uživatelů by bylo vhodné odladit SW CISCO Secure Services Client 5.1. K připojování externích zaměstnanců je možné vyžít funkce Lobby Ambasador, a povolit přístup k síti Internet. Pokud budou tito lidé požadovat přístup k vlastním zdrojům dat, jistě využijí vlastní nástroje na uskutečnění relace VPN.

Pro účely návrhu malých obchodních center se osvědčil model nasazený v zahraničí, viz kapitola 15.4. Pro bezporuchový provoz je dobré oddělit WiFi hlas, a WiFi data do samostatných BSSID, VLAN, MPLS-VRF.

Také by bylo optimální rozšířit řady zaměstnanců o další 2 zaměstnance na plný úvazek, (s tímto bylo v záměru stavby počítáno) kteří by spravovali pouze síť WiFi skrz celou ČR, včetně On-Line podpory uživatelů přenosných PC.

Také by se mohla podstatně zlepšit koordinace či spolupráce s oddělením bezpečnosti, rozvoje a koncových zařízení, vedoucí ke zrychlení nasazování nových technologií.

18 Použitá literatura

[1] F. Kállay, P. Peniak: Počítačové sítě a jejich aplikace: Grada Praha 2003, ISBN 80-247-0545-1;

[2] L. Dostálek, A. Kabelová: Velký průvodce protokoly TCP/IP a systémem DNS, Praha 2002, ISBN: 80-7226-675-6;

[3] L. Dostálek a kolektiv: Velký průvodce protokoly TCP/IP Bezpečnost, Praha 2003, ISBN: 80-7226-849-X;

[4] TJ. Velte, A. T. Velte: Síťové technologie CISCO velký průvodce, Computer Press 2003, ISBN 80-7226-857-0

[5] T. M. Thomas: Zabezpečení počítačových sítí bez předchozích znalostí, CP Books, a.s. 2005, ISBN: 80-251-0417-6;

[6] J. Dobeš, V. Žalud, Moderní Radiotechnika, BEN Praha 2006, ISBN: 80-7300-132-2;

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

[8] Diane Teare: Návrh a realizace sítí Cisco, CP Books, a.s. 2003, ISBN: 80-251-0022-7;

19 Zdroj Internet

http://cs.wikipedia.org/wiki/Local_Area_Network

http://cs.wikipedia.org/wiki/Internet

http://en.wikipedia.org/wiki/Structured_cabling

http://www.svetsiti.cz/default.asp

http://www.ieee802.org/11/

http://www.ietf.org/iesg/1rfc_index.txt

http://www.aspa.cz

http://cs.wikipedia.org/wiki/Referenční_model_ISO/OSI

http://cs.wikipedia.org/wiki/TCP/IP

http://en.wikipedia.org/wiki/Request_for_Comments

http://www.cisco.com/

http://www.convergedigest.com/Bandwidth/archive/010910TUTORIAL-rgallaher1.htm

http://business.motorola.com/mototrbo/UK/index.html

http://www.alcoma.cz/wp/

Odkazy testovány k datu 17. 5. 2009