Komplexní návrh řešení informačního systému ve firmě KPB Intra Bučovice

Comprehensive draft of information system analysis in KPB Intra Bučovice Company

Bc. Robert Santler

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Robert SANTLER**
Osobní číslo:	**A09518**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Komplexní návrh řešení informačního systému ve firmě KPB Intra Bučovice**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Analyzujte stávající síťový provoz a strukturovanou kabeláž ve společnosti KPB Intra.**
3. **Navrhněte optimální řešení rekonstrukce datové sítě včetně strukturované kabeláže, připojení do Internetu, firewallu a směrovače, IP telefonie, IP kamerového systému a GSM bran.**
4. **Doporučte nejvhodnější aplikaci IP telefonie a IP kamerového systému v provozu společnosti KPB Intra.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **SOSINSKY, Barrie. Mistrovství-počítačové sítě. 1.vydání. Brno : Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.**
2. **PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z. 2.vydání. Brno : Computer Press, 2006. 432 s. ISBN 80-251-1278-0.**
3. **HORÁK, Jaroslav; KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. 4.vydání. Brno : Computer Press, 2008. 328 s. ISBN 978-80-251-2073-6.**
4. **LAMMLE, Todd. CCNA Cisco Certified Network Associate : Výukový průvodce přípravou na zkoušku 640-802. 1.vydání. Brno : Computer Press, 2010. 928 s. ISBN 978-80-251-2359-1.**
5. **OREBAUGH, Angela, et al. Wireshark a Ethereal : Kompletní průvodce analýzou a diagnostikou sítí. 1.vydání. Brno : Computer Press, 2008. 448 s. ISBN 978-80-251-2048-4.**
6. **TEARE, Diane. Návrh a realizace sítí Cisco : Autorizovaný výukový průvodce. 1.vydání. Brno : Computer Press, 2003. 758 s. ISBN 80-251-0022-7.**
7. **WALLACE, Kevin. VoIP bez předchozích znalostí. 1.vydání. Brno : Computer Press, 2007. 232 s. ISBN 978-80-251-1458-2.**
8. **MAČEK, Karel. Návrh překryvné VoIP sítě na stávající ISDN síť. Zlín, 2008. 69 s. Diplomová práce na Fakultě aplikované informatiky Univerzity Tomáše Bati ve Zlíně. Vedoucí diplomové práce Ing. Miroslav Matýsek Ph.D.**

Vedoucí diplomové práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **24. února 2011**

Termín odevzdání diplomové práce: **18. května 2011**

Ve Zlíně dne 24. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Záměrem této diplomové práce bylo navrhnout komplexní informační zabezpečení typické pro středně velkou firmu zabývající se elektrotechnickou výrobou.

Práce je zaměřena na analýzu stávajícího stavu informačního zabezpečení ve firmě KPB Intra s.r.o. Prostřednictvím softwarového nástroje se snaží najít slabiny v síťovém provozu a rozborem požadavků zákazníka hledá prostor pro úspory v komunikačním zabezpečení. Pomocí zjištěných poznatků a moderních trendů v informačních technologiích nabízí možné řešení nejen v oblasti komunikace pomocí IP, ale i v oblasti video záznamu jakožto vhodného prostředku pro optimální výrobní proces. Předpoklad Snaha racionálně využívat vložené investiční prostředky do informačních zařízení vede k zavedení video záznamů jako prostředku v hledání optimálního výrobního procesu.

Klíčová slova: LAN, směrovač, přepínač, VoIP, IP, firewall

ABSTRACT

The intent of this thesis was to design complex information security that is typical for midsize company engaged in manufacturing electronic. This thesis is focused on analyzing the current state of information security in the company KPB Intra s. r. o. By means of software it tries to pinpoint weak points in the network operation. Throughout the analysis of requirements it looks for space saving in communication security. Using established knowledge and modern trends in information technology, it offers a possible solution not only in communication with IP but also in the video recording as a suitable medium for the optimal production process. Effort to rationally use the embedded investment funds in information equipment leads to introduction of video recording as means of finding the optimal production process.

Keywords: LAN, router, switch, VoIP, IP, firewall

Využívám možnosti poděkovat vedoucímu mé diplomové práce panu Ing. Miroslavu Matýskovi Ph.D. za jeho cenné rady, vedení a užitečné podměty, ze kterých jsem po celou dobu čerpal a jenž mi po celou dobu pomáhaly překlenout nástrahy spojené s vytvářením této práce.

Zároveň chci poděkovat mé manželce, která měla trpělivost se čtením této práce a korekturou textu.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

…….

podpis diplomanta

OBSAH

ÚVOD

Držet krok s rychlým a nezadržitelným rozvojem informačních technologií, je v současnosti existenční úkol každé moderní firmy, která se chce udržet své místo v ostrém konkurenčním prostředí. Také snaha nepodlehnout iluzi spokojenosti se současným stavem je základním stavebním kamenem rozvoje a prosperity firmy. Nutí nás sledovat moderní trendy ve vývoji a vnášet tyto poznatky do vlastního prostředí. V neposlední řadě je důležité vědomí neudržitelnosti původní infrastruktury a snaha zlepšit současný stav modernizací.

Pojem modernizace informační infrastruktury představuje soubor faktorů neboli zásad, které jsou důležité při samotném návrhu. Tyto zásady jsou nezbytné proto, aby ekonomická návratnost vložených investic byla pro zákazníka uspokojující. Jednotlivé komponenty použité v modernizaci musí být v případě potřeby jednoduše nahraditelné a vyměnitelné a to jak z důvodu nefunkčnosti nebo jejich morální zastaralosti.

Další z rozhodujících faktorů je také to, co vlastní fyzické realizaci předchází. Tedy kvalitní analýza projektu, která se skládá z mapování objektu, analýzy požadavků, určení datových tras, perspektivy vývoje a dalších prvků. V případě realizace na základě nevhodně zpracovaného projektu dochází po velmi krátké ke zjištění, že strukturovaná kabeláž neodpovídá požadované datové propustnosti, nelze na ni uplatnit požadavky na rozšíření provozního zatížení ani snahu na univerzálnost.

Primárním cílem této práce však není jen obvyklý návrh strukturovaných datových linek, ale i hledání možností jak využít informační technologie při zefektivnění výroby, zamezení ztrát v důsledku průniku neoprávněných osob k citlivým informacím a v neposlední řadě také v posílení pozice firmy na poli informačních technologií.

I. TEORETICKÁ ČÁST

1 FILOSOFIE NÁVRHU STRUKTUROVANE KABELÁŽE

Zkušenosti z realizací a provozem lokálních či vzdálených počítačových sítí, postupně celkem jednoznačně demonstrovaly zásadní pravidla, která jsou třeba při budování počítačových sítí dodržovat. Čeho je třeba se naopak vyvarovat a co může být případně na uvážení realizátora sítě - zákazníka.

1.1 Obecné principy návrhu síťové architektury

Principy jsou vyjádřením podniku o tom, jaké cíle mám síť splňovat vzhledem v dlouhodobém měřítku. Poskytují základní spojení mezi obchodními strategiemi a strategií síťové technologie. Jsou základem pro další složky architektury a vychází z podnikových hodnot a cílů [2].

1.1.1 Technologická strategie pro podnikovou síť

Technologická strategie spočívá ve stanovení určitých kroků, které jsou nezbytné pro vytvoření podkladu k návrhu podnikové sítě. Tyto kroky mají z hlediska budoucího vývoje firmy svou důležitost a význam.

1. krok – stanovení věcných omezení – nastavuje hranice související s požadavky na zaměstnance, finančním rozpočtem a časovým průběhem projektu.
2. krok – určení bezpečnostních požadavků – stěžejní krok, jenž nám ve výsledku ohodnocuje bezpečnostní rizika, stanovuje podmínky přístupu k vnitřní síti a udává podmínky pro autentizaci a autorizaci.
3. krok – požadavky na správu sítě – do tohoto kroku spadají požadavky na správu závad, účtování, konfigurace zařízení, výkonu a zabezpečení.
4. krok – zjištění aplikačních požadavků – umožňuje vyhodnotit zátěž, jaká bude kladena na novou síť v závislosti na počtu uživatelů, na nových aplikacích, na nových protokolech a na denní době špičkového zatížení
5. krok – analýza síťového provozu v nových podmínkách – do tohoto kroku spadá charakteristika provozní zátěže, chování síťového provozu a využití systémových síťových nástrojů.

6. krok – zjištění požadavků na výkon sítě – k analýze tohoto kroku se využívají základní síťové veličiny jako je doba odezvy, přesnost, dostupnost, maximální využití sítě, propustnost, efektivita a reakční doba
7. krok – specifikace potřeb uživatele – cílem je popsat stávající síť (v případě, že existuje), určit požadavky a omezující podmínky nové sítě. Specifikace potřeb je také základem písemné smlouvy se zákazníkem [6].

1.1.2 Princip aktualizace síťové strategie podniku

Proces aktualizace doporučuje každých 6 až 12 měsíců provést postup revize návrhu a stávajícího stavu, aby podnikové řešení bylo optimální vzhledem k měnícím se požadavkům na technologický rozvoj a udržení kroku se soudobím rozvojem síťových technologií.

S pojmem aktualizace je úzce spjat i pojem životnost. Životnost souvisí s postupnou degradaci rozvodu, snížení funkčnosti a selhání sítě. Koresponduje s použitými materiály a technologiemi. Životnost běžného stolního počítače je 3 až 5 let, aktivních prvků sítě 5 až 7 let, což v zásadě nesmí ovlivnit relativně drahou výstavbu strukturovaných rozvodů, která musí přežít několik takovýchto vylepšení aktivních prvků sítě. V současné době je metodika budování strukturované kabeláže propracována natolik dobře, že spolu s kvalitními materiály je životnost systému kabeláže 15 až 25 let.

1.1.3 Princip univerzálnosti

Důležitým parametrem pro návrh strukturované kabeláže je její snaha o maximální univerzálnost. Univerzálnost předpokládá, že datové rozvody se využijí jak pro přenos v rámci počítačové sítě, tak pro běžné telefonní rozvody, pro rozvody k zabezpečovacím zařízením a čidlům, bezpečnostním a kamerovým systémům, teplotním regulátorům a mnoha jiným připojitelným zařízením. I proto je v poslední době tendence unifikovat interface těchto zařízení pro bezproblémové připojení na běžnou počítačovou síť realizovanou podle principů strukturované kabeláže, v optimálním případě využít tuto síť k napájení těchto zařízení, bez nutnosti rekonstrukce silových rozvodů.

1.2 Technické řešení a výběr technologie

Pro výběr a vybudování vlastní sítě neexistuje, žádný přesný návod, jehož dodržování by neomylně vedlo k nalezení optimálního řešení. Důvodem pro toto, je velké množství kritérií související jak s celým prostředím, které má být podporováno sítí tak s výhledem do budoucna i s možnostmi nabídky technologií, koncových systémů i propojovacích systémů.

Při počátečním výběru technologií je nutné brát v úvahu aspekty jako je cena, typ prostředí kde bude síť působit, potřeba začlenit do lokální sítě stávající technické prostředky, dostupnost produktu a jejich servis, informační strategie společnosti, podpora managementu správy sítě, ale v neposlední řadě i soulad se stávajícími normami a profily. [2].

2 POČÍTAČOVÉ SÍTĚ

Pojem počítačová síť definuje soubor základních prvků, nutných k reciproční výměně informací mezi dvěma či více aktivními složkami. Přímé propojení dvou počítačů kabelem tvoří nejmenší možnou počítačovou síť. V pracovních skupinách, jež obsahují tak nízký počet prvků nevyžaduje počítačová síť žádnou centrální službu. V opačném případě s centrální službou se jedná o komunikaci typu klient – server.

V závislosti na rozlehlosti se počítačové sítě dělí na lokální LAN (Local Area Network), rozlehlé WAN (Wide Area Network) nebo i univerzitní sítě CAN (Campus Area Network) či metropolitní sítě MAN (Metropolitan Area Network).

Každá počítačová síť se skládá z daných komponent, které umožňují přenos informací mezi odesilatele a příjemcem. Jedná se o:

- propojené systémy
- propojovací software
- fyzická přenosová media
- síťový hardware
- adresní systém pro uvedené komponenty [1].

2.1 Lokální sítě LAN

Jsou charakterizovány omezeným rozsahem, který je do několika kilometrů nebo působí v rámci několika budov. Svým využitím jsou předurčeny pro agregovaný přenos dat, hlasu či obrazu.

Obecně můžou být popsány podle určitých hlavních bodů:

- podle pracovního režimu, který může být bez spojení, což znamená, že navázání, udržování a ukončení spojení není nutný předpoklad pro přenos dat k zamýšlenému příjemci.
- umožňují multiaccess přístup k sdílenému přenosovému médiu, přičemž přístup může být deterministický nebo náhodný.
- přenášejí rámce vysíláním signálu po sdíleném médiu.

Každá lokální síť obsahuje jednu nebo více obslužných stanic se síťovým operačním systémem, zahrnující jak obslužné tak aplikační programy. Každá obslužná stanice se může specializovat na různé funkce. Může to být obslužná stanice souborů, tiskáren, jmenných názvosloví či IP (Internet Protocol) adresního prostoru. Obslužné stanice komunikují s uživatelským koncovým zařízením lokální sítě. K tomu využívají síťové programové vybavení, jehož účelem je poskytovat skupinu společných služeb pro každého uživatele v síti [2].

2.2 Fyzické přenosové médium

Vlastnosti a struktura přenosového média jsou definovány v první fyzické vrstvě modelu OSI (Open Systems Interconnection). Dnešní moderní informační technologie rozeznává tři základní formy síťového přenosového média:

- metalické kabely – měděné pro přenos elektrických signálů
- optické kabely – přenos optických pulsů
- bezdrátové – mikrovlnné signály s různými způsoby modulace

2.2.1 Metalické kabely

Měděná média jsou tvořena kabely, používající měděné vodiče pro přenos datových a řídících signálů mezi síťovými zařízeními. Méně využívaná jsou média na bázi koaxiálního kabelu. Pro zapojení jednotlivých zařízení se používají modulární zástrčky a zásuvky. Nevýhodou metalických kabelů je jejich možné ovlivnění interferencemi či elektromagnetickým šumem.

Nejvyužívanější typy kabelů:

- UTP (Unshielded twisted-pait) - nestíněná kroucená dvojlinka, skládající se zpravidla ze čtyř zkroucených párů vodičů s koncovkou RJ-45 (Registered Jack – 45).
- STP (Shielded Twisted Pair) – stíněná kroucená dvojlinka. Již z názvu je patrné, že její konstrukce je tvořena stíněnými páry.

2.2.2 Optické kabely

Základem moderních vysokorychlostních sítí s vysokou kapacitou jsou optické kabely. Optické kabely využívají k přenosu jednotlivých bitů ze zdroje do cíle světelné impulsy. Přenos světelných impulsů se děje prostřednictvím skleněných nebo plastových vláken. Světelné impulsy jsou vysílány buď pomocí LED (Light Emitting Diode) nebo laserové diody. Na opačné straně jsou přijímány polovodičovými diodami – fotodiodami [9].

Optické kabely v zásadě dělíme podle režimů (módů) na SM (Single Mode) jednovidové kabely a MM (Multi-mode) vícevidové kabely:

- SM kabely obsahují vlákna s velmi tenkými jádry (průměr 9 μm). Světelný paprsek vstupuje do jádra pod velmi malým úhlem, z toho důvodu se pohybuje takřka bez lomu, čímž dosahuje na rozdíl od vícevidových vláken větší vzdálenosti a šířky pásma. Nevýhodou je barevný rozptyl.
- MM kabely mají nízký dosah kvůli modální disperzi, používají se na menší vzdálenosti a to hlavně na přenos širokopásmových aplikací. Výhodou je jejich cena.

K připojování optických kabelů slouží různé druhy konektorů, například LC (Lucent Connector), FC (Fixed Connection), SC (Subscriber Connector), MTRJ (Mechanical Transfer Registered Jack).

Obr. 1. Koncovky optického kabelu MTRJ.

Výhodou optických kabelů je jejich odolnost vůči elektromagnetickému rušení. Jako možnou nevýhodu lze považovat ztráty vznikající při přenosu. Ztráty neboli útlum vznikají působením více jevů. Například materiálovou absorpcí, materiálovým rozptylem, ztráty v ohybech, ve spojích a konektorech [1].

Tab. 1. Fyzické charakteristiky některých médií.

	100Base-TX	100Base-FX	1000Base-T	1000Base-SX	1000Base-ZX
Druh média	CAT 5, UTP 2 páry	50/62,5 µm MMF	CAT 5 a vyšší UTP 4 páry	50/62,5 µm MMF	9 SMF
Max. dosah	100 m	2 km	100 m	do 550 m	cca 70 km

Z důvodu snížení útlumu při průchodu světelného signálu vláknem, se nevyužívá celé světelné spektrum, ale jen tzv. přenosová okna se jmenovitými vlnovými délkami:

- 850 nm - mnohavidová vlákna
- 1300 nm - mnohavidová vlákna (1310 nm - jednovidová vlákna)
- 1550 nm - jednovidová vlákna

2.2.3 Bezdrátové přenosové systémy

Jistou alternativou k pevným sítím jsou sítě bezdrátové. Odstraňují základní nevýhodu pevných sítí spojenou s plánováním, pokládkou a údržbou kabelů. Propojení jednotlivých stanic elektromagnetickými vlnami poskytuje větší pružnost a mobilitu při připojování stanic do sítě. Kromě výhod má toto řešení i nevýhody a to v podobě problému s rušením, překryvu dvou nebo více sítí a v neposlední řadě také s bezpečností.

Bezdrátové sítě jsou běžně označovaný jako WLAN (Wireless LAN). V těchto sítích se přistupuje ke sdílenému médiu pomocí metody CSMA/CA (Carrier Sense Multiple Access/Collision Avoidenace), která využívá pro přístup náhodnou odmlku po kolizi. Tato odmlka velmi snižuje možnost vzniku opakované kolize. Pro ověření úspěšně přijatého rámce využívají potvrzování na linkové vrstvě [9].

Další služby implementované do standardu 802.11 jsou autentizace, asociace a utajení dat šifrováním. Komponenta sítě WLAN, která poskytuje přístup k síti, se nazývá entita přístupu k portu PAE (Port Access Entity).

Tab. 2. Rozdělení standardu 802.11.

Norma	Pásmo (GHz)	Modulace	Propustnost (Mbps)	Teoretická rychlost (Mbps)	Dosah venku (m)
802.11a	2,4	OFDM	23	54	120
802.11b	5,0	DSSS	4,3	11	140
802.11g	2,4	OFDM	19	54	140
802.11n	2,4/5.0	OFDM	74	600	250

Pro navázání autentizační komunikace mezi žadatelem a poskytovatelem se zavádí zvláštní klíč pro každou jednosměrnou relaci s klientem. Rámce, které nejsou kódovány s pomocí relačního klíče, se zahazují. K šifrování se používají tři základní protokoly:

- protokol WEP (Wired Equivalent Privacy) využívá symetrickou šifru RC4 s 40 nebo 104 bitovým klíčem a 24 bitový inicializační vektorem. Jedinou, ale zásadní nevýhodou protokolu WEP je to, že klíč protokolu je otevřený. Aby se zabránilo neoprávněnému získání klíče, musí být tento přes bezdrátový spoj odeslán bezpečně. Toto však protokol WEP neposkytuje.
- protokol WPA (Wireless-Fidelity Protected Access) odstraňuje nedostatky WEP tím, že zavádí generování klíčů mechanismem TKIP (Temporary Key Integrity Protokol). Tento mechanismus je generován klíčem pro každý přenášený paket. Oba koncové body mají stejný předem sdílený klíč PSK (Pre-Shared Key), který nelze odečíst z komunikace.
- protokol WPA2 využívá protokol CCMP (Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol) se silným šifrováním AES (Advanced Encryption Standard), MAC (Message Authentication Code) dynamicky mění 128 bitový klíč a MIC (Message Integrity Code) pro kontrolu integrity. MIC poskytuje ochranu proti útokům snažící se zopakovat předchozí odposlouchanou komunikaci. Existují dva druhy protokolu WPA2 Personal a Enterprise. Režim zabezpečení WPA2 Enterprise používající ověřování standardu IEEE 802.1X a je určen pro

podnikové zabezpečení. Režim zabezpečení WPA2 Personal používající předsdílený klíč (PSK) a slouží pro soukromé zabezpečení [1].

3 SÍŤOVÝ HARDWARE

Pro vytváření síťových okruhů se využívají propojovací zařízení, lišící se podle vrstvy architektury, na níž provádějí komunikaci mezi dvěma síťovými segmenty. Jsou to:

- opakovače, rozbočovače – pracují na první fyzické vrstvě
- mosty a přepínače – využívají druhou spojovou vrstvu
- směrovače – působí na třetí síťové vrstvě
- brány – pracují na sedmé aplikační vrstvě [2].

3.1 Opakovače a rozbočovače

Jedná se o zařízení, které prodlouží dosah sítě pouhým propojením vstupní linky se dvěma, čtyřmi, osmi a více spoji. Rozbočovače mohou být pasivní a pouze předávat signál, anebo mohou signál zesilovat.

Přicházející data rozesílá na všechny výstupní porty. Veškeré zapojené segmenty patří do stejné kolizní domény. V případě kolize rozbočovač odesílá zprávu všem připojeným zařízením, aby přestala vysílat data.

Zesílením a synchronizací signálu před jeho odesláním dále, se zabývají opakovače. Propojit sítě s různou architekturou s nimi však nelze. Nemohou sloužit ani k filtraci paketů. Důležitost opakovačů nabývá na významu v sítích, kde je k přenosu informace použito optického média.

3.2 Mosty a přepínače

Pro zlepšení výkonnosti lokální sítě LAN, se tyto obvykle rozdělují do několika menších segmentů, vzájemně mezi sebou propojených přepínačem sítě LAN nebo mostem. Výhodou takto rozdělené sítě je také rozdělení síťové zátěže, prodloužení efektivního dosahu, urychlení provozu a vznik bezkolizního prostředí. Základem urychlení je transparentnost komunikace. Obě zřízení nemění obsah rámce, pracují na spojové vrstvě a nezabývají se informacemi vrstev vyšších. Úkolem přepínače je vytvořit dočasné dvoubodové spojení mezi zdrojovým a cílovým uzlem. Spojení je vytvořeno pro potřeby přenosu jednoho rámce. Pro přenos je přitom vyhrazena celá šířka pásma a vytváří logický dvoubodový spoj.

Ne vždy je však cílový uzel připraven převzít data. Z toho důvodu se využívá několik metod pro přeposílání rámců:

- store and forward – přepínač ukládá v případě nedostupnosti cíle rámec do vyrovnávací paměti a přeposílá ho, až když je cílový uzel volný.
- cut-through switching – přijatý rámec se odesílá, ještě než jej přepínač přijme kompletní.
- fragment free – přepínač čeká na přijetí prvních 64 bytů a v případě, že v segmentu nevznikla kolize, data odesílá.
- adaptive switching – optimalizuje výkon přepínače tak, že v případě bezchybné komunikace zasílá data metodou cut-through, v opačném případě metodou store and forward [2].

Přenos typu full-duplexu, kdy je cíl volný a bez kolize, přepínač odesílá data bez nadbytečné režie.

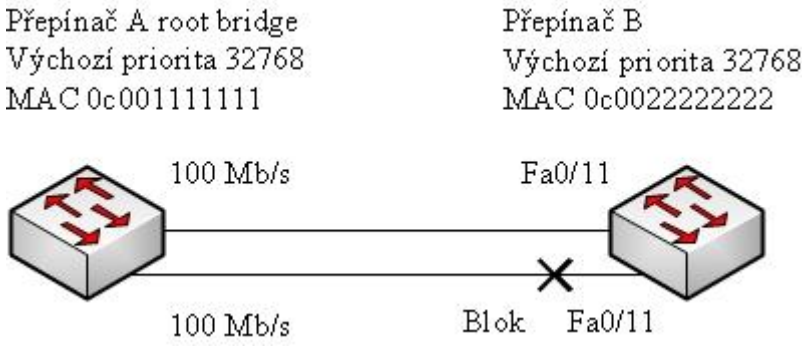
Rozesílání rámců je prováděno na základě MAC (Media Access Control) adresy, kterou přepínač ukládá do obsahu tabulky pomocí Backward Learning algoritmu. Tyto adresy jsou spárované s portem a tudíž i příslušným uzlem. Kromě algoritmu učení sleduje přepínač také stáří záznamu a v případě jeho překročení záznam smaže. Další funkcí přepínače je také kontrola rámců z hlediska jejich nekorektnosti. Oproti směrovači je přepínač rychlejší, naopak přepínače nejsou schopny rozdělit všesměrovou doménu na třetí vrstvě [9].

Rozdíl mezi mostem a přepínačem je v zásadě ten, že most je dvouportové zařízení, určené k propojení dvou segmentů sítě a přepínače je víceportové zařízení. Mosty pracují formou store a forward a jsou založeny na softwaru, kdežto přepínače pracují na hardwarovém principu.

V návrzích počítačových sítí, jako prevenci proti kompletnímu výpadku sítě jsou výhodná uvažovat redundantní spojení mezi přepínači. Toto řešení však neposkytuje jen výhody, ale skrývá i nebezpečí v podobě broadcast storms, či generování vícenásobných kopií rámců v síti.

K potlačení těchto nežádoucích jevů se využívá protokol STP (Spanning Tree Protokol). Tento protokol má za úkol v normálním provozu najít všechny linky v síti a vypnout všechny redundantní. To se děje tak, že se určí ústřední most sítě (root brigde) na základě

nejnižší hodnoty BID (Bridge ID). BID je základní hodnota každého přepínače a skládá se z priority (2B) a MAC adresy přepínače (6B). Všechny ostatní přepínače najdou jediný přidělený kořenový port, což je port, který poskytuje největší šířku pásma směrem k root bridge. Ostatní porty se uvedou do stavu blokovaný. Blokované porty mohou i nadále přijímat datové jednotky, ale neodesílají rámce.



Obr. 2. Přepínaná síť s redundantními přepínanými trasami.

O informování jednotlivých přepínačů se stará BPDU (Bridge Protocol Data Units), který obsahuje konfigurační informace, časové parametry a globální informace o protokolu STP.

Neméně důležitý parametr u přepínaných sítí je čas, než porty přepínačů přejdou ze stavu blokovaných do stavu přeposílaných. Tedy v případě změny topologie sítě, odpojení či připojení přepínače (portu), nebo změny konfigurace STP. V této době síť konverguje.

Nejdůležitější příkazy protokolu STP

portfast – tento příkaz nastaví port tak, že po zapnutí přejde rovnou do stavu předávání. Tudíž nečeká na to, až síť zkonverguje. Příkaz je využíván u portu určeného pro rychlý náběh připojeného na server, uživatelskou stanici či IP telefon.

SWITCH(config-if)#spanning-tree portfast - pro jeden port

SWITCH(config)#spanning-tree portfast default - pro všechny porty

uplinkfast – tento příkaz zkracuje čas konvergence protokolu STP v případě selhání linky. To znamená, že při selhání primárního spojení, se sekundární (dočasně blokované) aktivuje rychleji.

SWITCH(config)#spanning-tree uplinkfast

spanning-tree – protokol zabraňuje, aby v sítích vznikaly smyčky. Na síť nahlíží jako na ohodnocený graf a vyhledává v něm nejkratší cesty mezi dvěma přepínači. Nejkratší cesta je

určena na základě kumulativní ceny linek (cost). Dále je využíván pro vyvažování zátěže VLAN (Virtual LAN) na trunk portech mezi dvěma přepínači. Oba přepínače jsou propojeny dvěma linkami a blokuje se ten port, který má nižší prioritu. Defaultní nastavení je na 128. Validní hodnoty jsou násobky 16 do hodnoty 240. Vyšší prioritu má port s nižší hodnotou.

SWITCH(config-if)#spanning-tree vlan 2 port-priority 64

- port připojený na VLAN 2 má prioritu 64

SWITCH(config-if)#spanning-tree cost 4

- port má cenu s hodnotou 4

bpduguard – ochraňuje port, který je určen pro koncovou stanici. V případě že projde přes tento port paket BPDU, přepínač port vypne.

SWITCH(config-if)#spanning-tree bpduguard enable

bpdufilter – slouží k filtrování STP provozu na portech určených pro koncovou stanici. Zabraňuje přijímání a odesílání BPDU paketů.

SWITCH(config-if)#spanning-tree bpdufilter enable [4].

3.3 Směrovače

Směrovač jako aktivní síťový prvek je zařízení, které propojuje dvě a více různých sítí. Rozděluje kolizní doménu, filtruje síťový provoz, blokuje všesměrové vysílání a optimalizuje směrováním cestu paketů v síti. Směrovač obsahuje dvě oddělené funkční úrovně a to řídící a doručovací.

Úkolem řídící úrovně je udržování aktuální směrovací tabulky. Směrovací tabulka je vytvářena při konfiguraci síťového subsystému. Obsahuje záznamy o dostupných sítích, o odpovídajících portech směrovače a metriku komunikační cesty. Statické záznamy v směrovací tabulce, jsou vytvořeny správcem sítě. Dynamické vytváří démon čili software dlouhodobě skrytě spuštěný na pozadí nějakého směrovacího protokolu.

Doručovací úroveň vyšetřuje vstupní pakety a rozhoduje o jejich předání na správné rozhraní. Při doručování se hledá v tabulce záznam cíle.

3.3.1 Směrovací tabulka

Na každém směrovači se příchozí rámec odpouzdří na paket. V paketu se zmenší TTL (Time To Live) o jedničku. Pokud je TTL rovné 0, paket se zahodí a odesilateli je o tom odeslána zpráva ICMP (Internet Control Messge Protocol) o překročení doby života paketu. Z paketu se separuje cílová IP adresa a ta, je postupně porovnávána s jednotlivými záznamy (řádky) ve směrovací tabulce, dokud není nalezena shoda. Tento řádek se použije pro směrování porovnávaného IP datagramu. Pokud shoda není, následuje porovnání s dalším řádkem tabulky. Poslední řádek tabulky typicky obsahuje takzvanou implicitní bránu. Směrovač následně může paket odeslat na další směrovač, nebo ho může odeslat cílovému hostiteli, případně pokud je cíl nedostupný ho odloží. Příchozí rámec je po určení cesty znovu zapouzdřen.

Při určování cesty se cílová IP adresa datagramu směrovaném sítí nemění, zatím co cílová MAC adresa se mění skok po skoku a odvíjí se od MAC adresy rozhraní následujícího směrovače, či cílové stanice v síti.

Každá směrovací tabulka musí obsahovat několik základních informací, které jsou při zpracování IP datagramů potřeba:

Adresát - za cíl je považována adresa podsítě, cílového počítače nebo implicitní trasa.

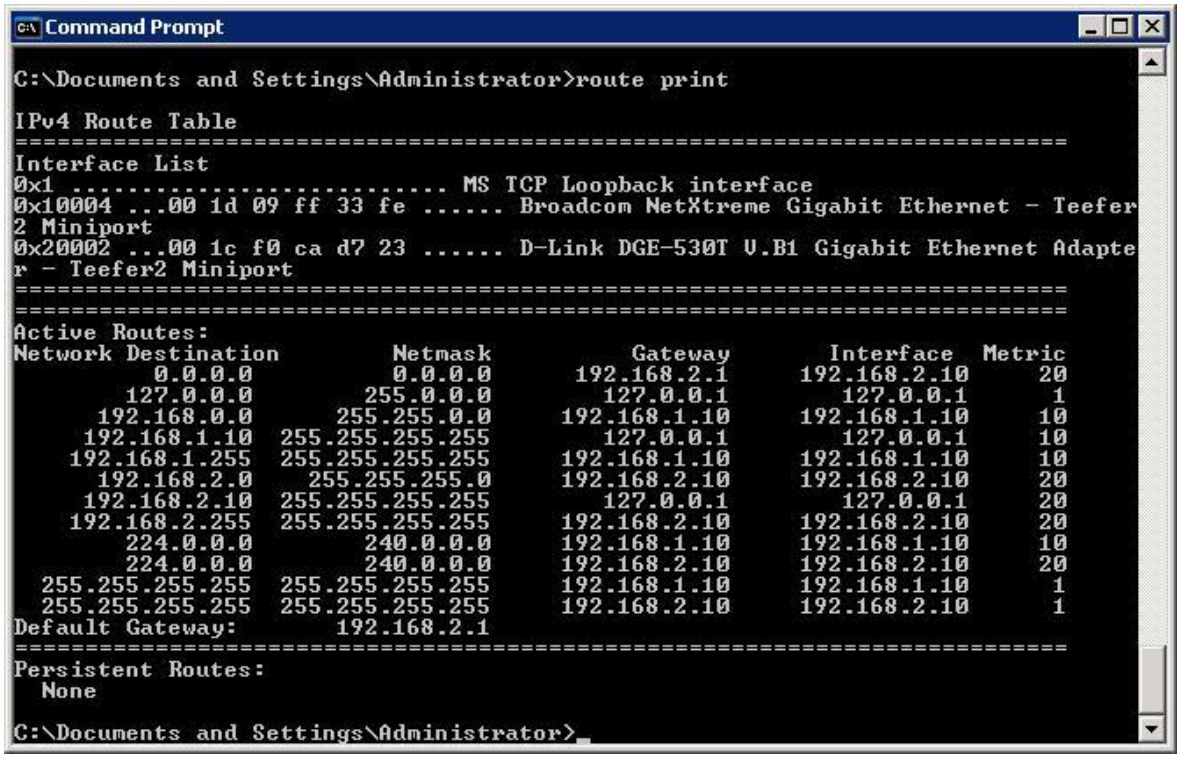
Síťová maska - maska sítě slouží pro určení platného rozsahu IP adres v tabulce.

Brána - hodnota brány udává IP adresu nejbližšího směrovače, na který mají být datagramy předávány.

Rozhraní - je symbolické označení síťového rozhraní nebo IP adresy síťového rozhraní v místním počítači, která má být použita pro předání IP datagramu.

Metrika - vyjádření relativní ceny při použití dané trasy pro přenos dat k danému cíli. AD (Administrative Distance) vyjadřuje cenu, kvalitu nebo důvěryhodnost směrovacího protokolu. Nejlepší protokol má nejmenší AD. Například přímo připojená síť má AD = 0.

Protokol - údaj u protokolu uvádí, jak byly informace o trase získány.



Obr. 3. Směrovací tabulka Windows

3.3.2 Směrování

Je považováno jako výběr nejlepší cesty, pro přeposlání daného paketu mezi sítěmi. Číselné vyjádření ceny cesty se nazývá metrika. Nejlepší cesta je nejlevnější cesta, tady cesta s nejmenší metrikou. V přeposílání mohou nastat tři případy:

- data se dopravují v rámci jedné sítě a není třeba směrování.
- cílová síť je přímo připojená (přilehlá), tudíž jsou data do ní rovnou předávána.
- cílová síť není přímo připojená a cesta se hledá ve směrovací tabulce.

Směrování je důležité z toho důvodu, že není možné vytvořit fyzické spojení pro všechny trasy. Pomocí interních směrovacích protokolů IGP (Interior Gateway Protokols), nebo externích směrovacích protokolů EGP (Externet Gateway Protokols) optimalizuje propojení v rámci jednoho nebo více autonomních systémů.

Vyhledávání optimálního propojení funguje na základě tří výchozích algoritmů:

Algoritmy zahrnující vektor vzdálenosti DV (Distance Vector)

Podkladem pro ohodnocení každého síťového spojení je počet skoků, to znamená síťových segmentů, které je nutno po trase překonat. Podstatou protokolů RIP (Routing Information Protokol) a IGRP (Interior Gateway Routing Protocol) je právě algoritmus vektoru vzdálenosti.

Protokol RIP nachází uplatnění v menších sítích a to především pro svoji nenáročnou konfiguraci a jednoduchost. Jako ochrana proti směrovacím smyčkám je u tohoto protokolu nastaven maximální počet přeskoků stanoven na 15 a životnost jakékoli trasy je 180 vteřin. Pro zamezení zahlcení sítě vysílají směrovače aktualizované směrovací tabulky, v různých časových okamžicích na základě specifických algoritmů.

Směrování na základě stavu linky

Na rozdíl od protokolů založených na vektorech vzdálenosti, je přenášena pouze informace o nejlepších následovnících pro dané trasy, vybraných ze všech sousedů. V podstatě každý směrovač informuje síť jen o svém okolí. Pro kalkulaci nejkratší trasy se pomocí Dijsktrova algoritmu vytvoří topologická mapa či graf sítě v každém směrovači. Tento algoritmus se využívá převážně v rozsáhlých sítích. Dokáže na základě atributů, jako jsou mimo jiné rychlost linky, dostupná šířka pásma, ocenění linky stanovit trasu s nejmenší cenou rychleji, než algoritmus s vektorem vzdálenosti.

Představitel algoritmu směrování podle stavu linky je OSPF (Opne Shortest Path First). Primárním záměrem tohoto protokolu je snížení síťové komunikace a zrychlení procesu nalezení nejkratších tras pro danou oblast. Využívá Dijkstrův algoritmus a k němu přidává systém primárních a záložních směrovačů.

Směrování podle vektoru trasy

Algoritmus vektoru trasy je odvozen od metodiky pracující s vektory vzdálenosti a navíc je zde uvedena celá trasa potřebná k dosažení cíle. Výhodou je možnost detekce cyklů v síti a rychlost reakce na tyto cykly. Jednotlivé uzly si uchovávají dvě tabulky obsahující jak platné trasy k libovolnému cíly, tak tabulku s identifikací následného směrovače pro tyto trasy.

Protokol BGP (Border Gateway Prokol) se využívá ve velké míře pro směrování provozu na Internetu a to ve formě externího BGP nebo interních BGP. Uchovává si atributy jako je cena trasy, následník, původ, cesta do autonomního systému, bod opuštění autonomního systému a další [1].

3.4 Brány

Brána (Gateway) označuje určitý východ ze sítě nebo také uzel, který spojuje dvě sítě s odlišnými protokoly. Brána přijme celou zprávu, která se může skládat z mnoha menších částí. Tuto pak převede do formátu určeného pro cílovou síť a odešle. Může být zakomponována do sítě ve formě hardwarového zařízení nebo programu, tedy softwarové brány. V širším uvažování může být brána implementována do každého směrovače. Důležitým prvkem odlišující jednotlivá zařízení určená k propojování sítí, je schopnost operovat na vyšších vrstvách síťového modelu OSI, tedy až v sedmé aplikační vrstvě, do které směrovače nezasahují [1].

3.5 IP telefonie

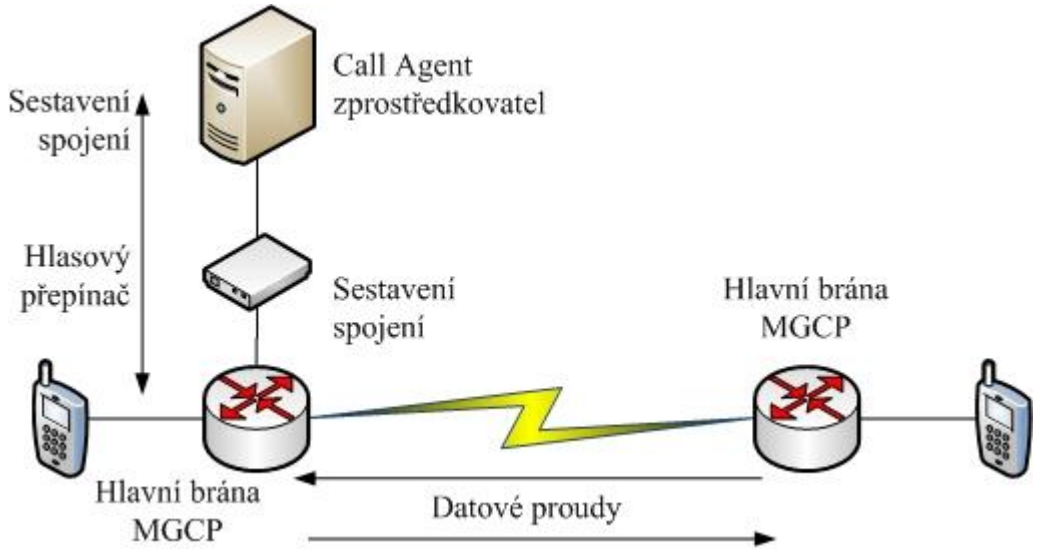
Úspora nákladu se objeví ve formě nižších investic do počtu hardwaru, přenosového média, nižších nákladů za pronajaté telefonní okruhy, hlasového přenosu a dalších. Nespornou výhodou je také využívání jediného úložiště pro hlasovou poštu, faxové zprávy, elektronickou poštu, využívání virtuálního call centra, možnost přenositelnosti čísla či používání videohovorů.

Přenos hlasu v analogové podobě je řešen v sítích VoIP (Voice over Internet Protokol) jeho převodem do binární podoby vzorkováním a kvantováním. Takto zdigitalizovaný signál je dále z důvodu co nejlepšího využití šířky pásma zkomprimován pomocí vhodného kodeku. Jako příklad může být kodek G.711, který využívá pulsně-kódovou modulaci v prostředí vysokorychlostní sítě LAN nebo G.726 jenž používá adaptivní diferenčně pulsně-kódovou modulaci, G. 729 v sítích WAN. Z takto zdigitalizovaného signálu se pro vlastní přenos dat sestavují pakety.

Samotné spojení IP telefonu ze sítě VoIP a telefonu ve veřejné síti zabezpečuje pomocí společného protokolu hlasová brána případně server, na kterém běží vhodná softwarová utilita. Hlasová brána neboli také směrovač, vytváří hranici mezi dvěma prostředími. K telefonní lince se směrovač připojuje pomocí analogového FXS (Foreign Exchange Station), FXO (Foreign Exchange Office) rozhraní, nebo pomocí digitálnímu rozhraní T1, E1 [7].

Hlavní funkcí hlasové brány je podpora přenosu datových protokolů RTP (Realtime Transport Protokol). Protokol je využíván pro přenos údajů související s hovorem a

navázání spojení. Například jsou to informace o stavu a účtování nebo informace o IP adresách a portech koncových bodů.



Obr. 4. Inicializace hovoru MGCP [7].

Sítě založené na komunikačním protokolu MGCP (Media Control Gateway Protocol) využívají ke spojení zprostředkovatele volání. V tomto případě hlasové brány přeposílají vytáčená čísla tomuto zprostředkovateli, jenž se stará o další směrování. Po sestavení spojení probíhá hovor již bez tohoto zprostředkovatele, prostřednictvím datového proudu RTP mezi MGCP zařízeními.

Další komunikační protokol využívaný ve VoIP je H.323. Nejedná se o samostatný protokol, ale o množinu protokolů používaných pro zahájení a ukončení hovoru, pro kódování video přenosů nebo pro kódování hlasových přenosů. Tento protokol definuje také hardwarovou architekturu, která se obecně skládá z koncových bodů neboli terminálů, zařízeních pro převod zvuku mezi jednotlivými formáty, řadičem pro řízení plynulosti přenosu, jednotek pro správu konferenčních hovorů a zprostředkovatelů volání.

Velmi jednoduchý, ale univerzální je protokol SIP (Session Initiation Protocol). Slouží k výměně informací nutných ke spojení ve formě relací. Komunikace probíhá pomocí protokolu RTP, který se přenáší v těle SIP paketů. Samotný hovor je realizován jako stream UDP (User Datagram Protocol) datagramů posílaný na IP adresu příjemce. SIP pracuje na principu klient-server. Mezi koncové body (uživatelské agenty) patří uživatelská zařízení jako SIP telefony, PC s klientským softwarem a brány do jiných sítí (zejména brány pro IP telefonii) [7].

Obr. 5. IP telefon Cisco SPA962 VoIP.

Technologie VoIP a jejich signalizační a řídící protokoly neposkytují odpovídající ověření volajících účastníků, ochranu integrity ani důvěrnost volání. Informace obsažené v těchto protokolech mohou být tedy snadno zachyceny díky použití takzvaných snifferů, tedy nástrojů pro sběr informací o provozu v sítích LAN nebo bezdrátových LAN. Z tohoto důvodu poskytují softwarový zprostředkovatelé hovorů tři úrovně zabezpečení VoIP spojení:

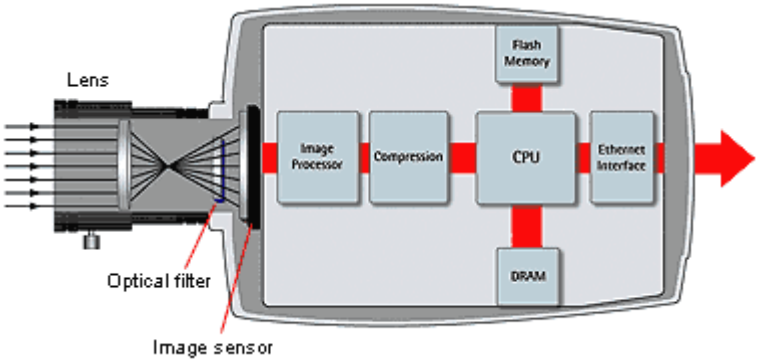
- **identita** představuje ověření uživatele na základě určitého certifikátu, za který se zaručí certifikační autorita.
- **integrita** potvrzuje, že data nebyla během přenosu změněna. Ověření se děje prostřednictvím kontroly pravosti firmware telefonu, obsahu konfiguračního souboru telefonu, a zda nedošlo ke změně paketů signalizace volání.
- **soukromí** představuje šifrování obsahu rámce pomocí 3DES (Triple Data Encryption Standard) nebo AES [7].

3.6 IP kamerový systém

IP kameru můžeme popsat jako kameru a počítač v jednom. Má vlastní IP adresu, je připojena k síti, má vestavěný webový server, FTP server a FTP klienta. Nemusí být připojena k počítači, funguje nezávisle a umístění IP kamery je omezeno jen připojením k počítačové síti. Zachycuje a vysílá živé záběry přímo přes IP síť a umožňuje tak

autorizovaným uživatelům lokálně nebo na dálku sledovat, ukládat a spravovat video záběry pomocí standardní síťové infrastruktury založené na IP.

Nachází uplatnění v širokém spektru oblasti. Využívá se ke sledování střežených objektů, při identifikaci osob, v oborech automatizace nebo v ochraně lidského zdraví v nebezpečných prostorech.



Obr. 6. Blokové schéma IP kamery [11].

Poskytuje nám nespočet výhod, jenž by využitím klasických analogových kamer, bylo jen obtížné. Umožňuje přístup na dálku, pružnost v umístění, cenově výhodné řešení, možnost ukládání záznamu do síťového úložiště, snadnou instalaci a škálovatelnost.

V obecném pohledu se IP kamera jeví jako zařízení skládající se ze specializovaného počítače, video kamery a síťového rozhraní. Video kamera zachycuje obraz pomocí obrazového senzoru, jako světlo o různých vlnových délkách a přeměňuje jej na elektrické signály. Tyto signály jsou pak převedeny z analogového na digitální formát a přeneseny do počítače, kde je obraz komprimován. Komprimace probíhá na základě komprimačních algoritmů, z kterých je nejznámější JPEG (Joint Photographic Experts Group) , Motion JPEG nebo MPEG-4.

Pro napájení IP kamer se využívá technologie PoE (Power over Ethernet), jenž umožňuje, aby bylo napájení síťového zařízení, jako je IP kamera nebo také IP telefon, poskytováno přes stejný kabel, který je použit pro jeho připojení do sítě.

Pro ukládání dat na síti slouží úložiště, která můžeme dělit podle přístupu v ukládání dat na záznamová média (pevné disky):

- První způsob je případ, kdy pevný disk je umístěn ve stejném počítači kde běží software pro správu video záběru neboli aplikační server.

– Druhý způsob aplikuje oddělení datového úložiště od serveru pomocí ukládacího prostoru připojeného k síti NAS (Network Attached Storage) nebo sítě ukládacích prostorů SAN (Storage Area Network).

Tab. 3. Síťové protokoly a porty běžně využívané při přenosu video dat [11].

Protokol	Přenosový protokol	Port	Běžné použití	Použití v síťovém videu
FTP	TCP	20/21	Přenos souborů	Přenos videa ze síťových kamer
SMPT	TCP	25	Odesílání emailů	Zasílání upozornění IP kamery
HTTP	TCP	80	Webové stránek	IP kamera jako webový server
HTTPS	TCP	443	Přístup k webovým stránkám	Zabezpečený přenos videa
RTP	TCP/UDP	554/6970 - 9999	Streamování, videokonference	Běžný způsob přenosu MPEG videa

NAS

Ukládací prostor připojený k síti tvoří jedno ukládací zařízení, které je přímo připojeno k síti a nabízí společný ukládací prostor všem uživatelům sítě. Zařízení typu NAS se jednoduše instaluje a spravuje, poskytuje levné řešení požadavků na ukládací prostor, ale má omezenou propustnost pro příchozí data.

SAN

Síť ukládacích prostorů je vysokorychlostní síť, která je určena pro ukládání video dat. Je propojena s jedním nebo více servery pomocí optického vlákna. Centralizované úložiště snižuje nároky na administrační čas a poskytuje výkonný, flexibilní ukládací prostor pro použití v prostředí více serverů [11].

Tab. 4. Celkové nároky na úložiště pro 3 kamery a 30 dní archivace [11].

Kamera	Rozlišení	Bit rate (kbps)	Počet snímků za sekundu	MB/hod	Hodin denně, kdy natáčí	GB/den
č. 1	CIF	170	5	76,5	8	0,6
č. 2	CIF	400	15	180	8	1,4
č. 3	4CIF	880	15	396	12	5

Z důvodu omezených možností v ukládání dat v datovém úložišti musí být zohledněny takové parametry jako je celkový počet kamer, dobu po kterou budou kamery nahrávat, doba po jakou se mají data uchovávat a zdali se bude jednat o nepřetržitý záznam. Dále parametry související se záznamem videa jako je počet snímků za sekundu, komprese a kvalita obrazu případně složitost scény.

4 BEZPEČNOSTNÍ STRÁNKY POČÍTAČOVÉ SÍTĚ

Bezpečnost počítačové sítě je souhrn mnoha aspektů, které slouží k ochraně našich dat přenášených pomocí informačních technologií, před vnitřními či vnějšími útoky.

Mezi útoky zvenčí se řadí přetížení sítě všesměrovým vysíláním ICMP paketů, zahlcení služby sítě požadavky útočníka, podvržením autentizačních údajů, nebo koordinovaným útokem většího množství systémů.

Do vnitřních útoků se řadí napadení pomocí různého nebezpečného softwaru, jako jsou červi, trojské koně, zadních vrátek, nebo pomocí MITN (Man-In-The-Middle) útoku, který odposlouchává provoz, mění pakety a ty odesílá na určené místo.

Tyto útoky mohou být úmyslné nebo neúmyslné a podle toho jak působí na naše data aktivní či pasivní.

Zabezpečení počítačové sítě dělíme na kategorie podle toho, co má být chráněno:

- informace a data
- služby přenosu a zpracování dat
- zařízení
- uživatelé

Mechanismus ochrany sítě souvisí jak s fyzickým a logickým návrhem sítě, tak se specializovanými protokoly. Neméně důležitým prvkem zabezpečení sítě je také správně implementovaná podniková bezpečnostní politika, jež ohodnocuje rizika, působí preventivně, detekuje hrozby a včasně reaguje na incidenty.

Ochrana před vnitřními útoky je z velké části založená v preventivním působení na uživatele, používáním antivirových ochran a softwaru určeného ke sledování a analýze síťového provozu. Je z velké části ovlivnitelná chováním uživatelů a správců sítě. Před útoky z vnějšího prostředí je nutné použít prostředků, jež můžeme rozdělit na využívání bezpečnostních protokolů, hardwarových bezpečnostních prvků a zabezpečených datových spojů.

4.1 Bezpečnostní protokoly

Bezpečnostní komunikační protokoly vznikly za účelem ochrany přenášených dat pomocí mezinárodní sítě Internet.

4.1.1 IPSec

Těchto protokolů v dnešní době existuje celá řada, přičemž mezi dnes nejrozšířenější soubor mechanismů pro poskytování bezpečnostních služeb patří IPSec (Internet Protocol Security Architeture). Princip IPSec je v zavedení kryptografického mechanismu jednoznačné identifikace mezi koncovými uzly spojení.

IPSec rozeznává dva druhy spojení a to:

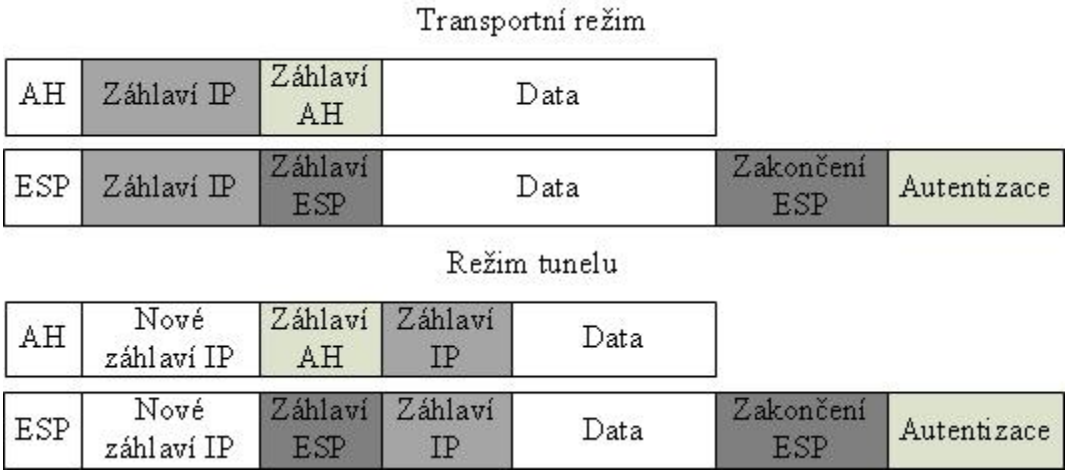
- transportní režim, jenž se používá pro spojení mezi dvěma uzly navzájem a kódují se jen data.
- režim tunelu šifruje a zapouzdřuje celé původní pakety. Využívá se pro vytvoření VPN (Virtual Private Network) mezi dvěma sítěmi, mezi hostem a sítí nebo mezi dvěma hosty [1].

Pro autentizaci a kontrole integrity dat, je v IPSec využíváno autentizační záhlaví AH (Autentication Header), které je vloženo za původní IP záhlaví. AH se šifruje pomocí algoritmu MD5 a provádí se před fragmentací datagramu. Autentizace probíhá pomocí hashovacího algoritmu, který generuje kontrolní hodnotu ICV (Integrity Check Value). Na základě porovnání těchto hodnot se po přijetí paketu rozhoduje o tom, zda jsou nebo nejsou data autentická.

Protokol ESP (Encapsulation Security Payload) zajišťuje utajení zprávy šifrováním datového obsahu i záhlaví. Struktura paketů ESP obsahuje:

- záhlaví ESP, ve kterém se nachází, SPI (Security Parametr Index) pro určení správného přidružení zabezpečení k zaslanému paketu a sekvenční číslo, jenž označuje jedinečné číslo odeslaného paketu v dané platnosti přidružení zabezpečení.
- koncovou část s výplní, délkou výplně pro zajištění správné délky dat a dalšího záhlaví k identifikaci typu dat.
- ověřovací část obsahuje hodnotu ICV k ověření zprávy a kontroly integrity [10].

Pro dohodu mezi komunikujícími stranami o způsobu šifrování, autentizace, použitých bezpečnostních protokolech, parametrech a klíčích, slouží protokol IKE (Internet Key Exchange). Adresy IP v novém záhlaví protokolu IP jsou koncovými body tunelového propojení a adresy IP zapouzdřené hlavičky protokolu IP jsou adresami původního zdroje a cíle (Obr. 7).



Obr. 7. Struktura záhlaví paketů v protokolech AH a ESP [1].

4.1.2 Protokol TLS

TLS (Transport Layer Security) rozšiřuje protokol SSL (Secure Sockets Layer) a využívá se pro šifrovanou a autentizovanou výměnu dat mezi webovými servery a klienty.

Navázání spojení se děje ve třech krocích:

1. Sjednání podporovaného protokolu na základě dohody mezi TLS serverem a klientem o druhu šifrovacích a hashovacích funkcí k zabezpečení spojení.
2. Výměna klíčů a jednoduchá autentizace pomocí digitálního certifikátu.
3. Výměna veřejného klíče mezi klientem a serverem pro vytváření relací.

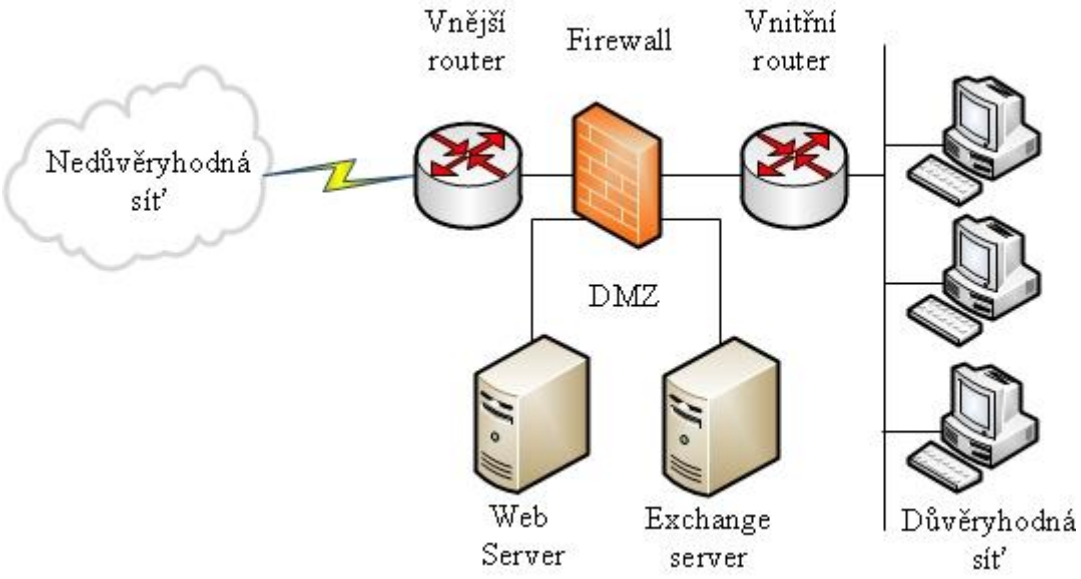
4.1.3 Protokol HTTPS (Hypertext Transfer Protocol Secure)

HTTPS je nadstavba síťového protokolu HTTP (Hypertext Transfer Protocol), která umožňuje zabezpečit spojení mezi webovým serverem a klientem. HTTP funguje způsobem dotaz-odpověď. Klient zasílá serveru dotazy ve formě čistého textu, obsahujícího označení

požadovaného dokumentu, informace o schopnostech prohlížeče apod. Server poté odpoví pomocí několika řádků textu popisujících výsledek dotazu, za kterými následují data samotného požadovaného dokumentu. Na takto vzniklou komunikací je aplikováno šifrování pomocí SSL nebo TLS.

4.2 Hardwarové bezpečnostní prvky

Principem tohoto zabezpečení je oddělení sítí pomocí fyzických síťových rozhraní a tím izoluje a chrání důvěryhodnou část sítě před vnějším napadením. Takovéto zařízení se nazývá firewall a představuje filtr, jenž může pracovat v závislosti na konkrétní potřebě od síťové (druhé) až po aplikační (sedmou) vrstvu modelu OSI.



Obr. 8. Typicky zabezpečená síť [4].

Firewall se také přeneseně říká službě operačního systému, která chrání server či stanici tím, že filtruje jejich síťovou komunikaci a neumožňuje aplikacím nestandardní či neschválené chování vůči systémovým prostředkům. Výhodou tohoto řešení je flexibilita, programovatelnost a možnost dalších služeb. Nevýhodou je nižší výkon oproti hardwarovému firewallu.

Obecně firewall zjišťuje, zda parametry přijatých síťových dat vyhovují pravidlům definovaných správcem sítě. Tyto pravidla dále určují akci, která se má s danými daty provést. Data mohou být předána dál, zahozena, případně jiným způsobem upravena.

Firewally se podle jejich činnosti člení na několik kategorií:

Paketové filtry – řízením těchto filtru se neovlivňuje obsah předávaných dat. Paketové filtry mají pravidla utvořená na základě příchozí a odchozí adresy a typu služby. Při této činnosti firewall čte data ze záhlaví paketů, bez jakéhokoliv kontextu a tudíž není schopen chránit síť před komunikací, používající podvržené informace. Paketové filtry spadají do bezstavových firewallů využívající technologie síťové vrstvy.

Stavové filtry – ke své činnosti využívá stavovou tabulku, do které ukládají informace o povolených spojeních. Jedná se o technologii dynamické filtrace, která se přizpůsobuje spojením či relacím a mění chování v závislosti na vzájemném působení komunikujících systémů. Stavový filtr využívá procesu nazývaného stavová inspekce paketů, který probíhá na síťové vrstvě.

Stavová tabulka spojení obsahuje hlavní atributy každé relace, zejména zdrojovou a cílovou IP adresu, čísla portů a sekvenční čísla, která odečítá z paketů. Tyto informace využívá při testování přicházejících paketů a na základě rozhodovacího procesu povoluje nebo naopak zamítne přístup do chráněné zóny. Položky ve stavové tabulce se pro danou relaci vyskytují jen po dobu, než tato skončí. Poté je položka vymazána.

Nevýhodou těchto filtrů je, že jsou pomalejší než paketové filtry na základě vyšších režijních nákladů a mají malou odolnost vůči útokům typu odmítnutí služby.

Stavové paketové filtry s kontrolou protokolu – implementující technologii IDS (Intrusion Detection Systems). Filtry tohoto typu jsou schopny kontrolovat pakety až na úroveň korektnosti procházejících dat známých protokolu a aplikaci. Firewally využívající IDS pracují podobně jako antiviry a pomocí databáze signatur a heuristické analýzy jsou schopny odhalit vzorce útoků i ve zdánlivě nesouvisejících pokusech o spojení, např. skenování adresního rozsahu, rozsahu portů, známé signatury útoků uvnitř povolených spojení apod.

Výhodou těchto systémů je vysoká úroveň bezpečnosti kontroly procházejících protokolů při zachování relativně snadné konfigurace, poměrně vysoká rychlost kontroly ve srovnání s aplikačními branami, nicméně je znát významné zpomalení proti stavovým paketovým filtrům.

Nevýhodou je jejich složitost a tudíž možnost, že ve vnitřním kódu firewallu se vyskytne zneužitelná chyba, vedoucí ke kompromitaci celého filtru.

Aplikační brány – nazývané také proxy firewally. Podrobně sledují obsah daného komunikačního protokolu a data předávají nepřímo po analýze a sestavení. Jedná se o nejkomplexnější, ale také zároveň o nejpomalejší filtrovací techniku.

Firewally oddělují oblasti sítě do zón s různými úrovněmi důvěryhodnosti. Zóna bez důvěryhodnosti je obvykle přímo dostupná z Internetu. Pakety přicházející do této oblasti jsou vysoce podezřelé a musí být náležitě prozkoumány. Za zónou bez důvěryhodnosti se nachází DMZ demilitarizovaná zóna, která je od vnější oddělena směrovačem a hraničním firewallem.

Směrovač, jehož hlavní úlohou je určování cest v počítačových sítích, může také překládat veřejné síťové adresy, prostřednictvím mapovací tabulky, na adresy v privátním rozsahu. Hraniční firewall pak poskytuje komunikaci s DMZ, která má již střední úroveň důvěryhodnosti a v níž se nacházejí prvky, jako jsou webové servery, FTP (File Transfer Protocol) servery nebo poštovní servery. Za DMZ se může nacházet ještě interní firewall a směrovač, jenž oddělují interní důvěryhodnou síť.

4.3 Zabezpečené datové spoje

Základním stavebním prvkem pro vytvoření zabezpečených datových spojů je virtuální privátní síť. VPN vytvářejí bezpečné linky na nezabezpečených spojích a propojují klienty prostřednictvím veřejné sítě s pomocí tunelovacích a šifrovacích protokolů. K založení sítí VPN se využívá kombinace protokolů druhé a třetí vrstvy modelu OSI.

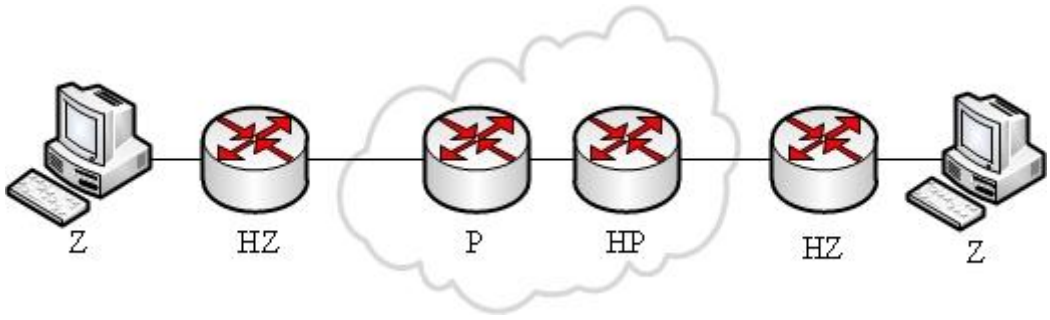
Pro zašifrovaný přenos dat se využívají různé druhy šifrovacích protokolů, které mají za úkol vkládat do směrovaných paketů zašifrované datové bloky. Mezi nejznámější šifrovací protokoly využívající se při zakládání VPN jsou IPSec, SSL, L2TP a další.

V širším pohledu poskytují VPN sítě spojení mezi jednotlivými klienty nebo mezi různými sítěmi navzájem. Ne vždy se spojení sestavuje v rozlehlých sítích WAN, ale VPN technologie se může využít i na menší vzdálenost při spojení v rámci jedné LAN.

Z hlediska topologie síť VPN zahrnuje (Obr. 9):

Zařízení zákazníka (Z) a poskytovatele (P) – jedná se o všechny místní síťové zdroje, jako jsou počítače, směrovače, přepínače ve zdrojové či cílové oblasti propojené VPN linkou.

Hraniční systémy pro zákazníka (HZ) a pro poskytovatele (HP) – vytváří WAN spoj mezi hraničními prvky. Zařízení HZ dokáže rozluštit VPN komunikaci, ale hraniční zařízení poskytovatele tuto možnost nemá. Jako hraniční prvek zákazníka HZ se obvykle využívá brána nebo koncetrátor. Toto zařízení může být koncovým bodem jednoho nebo více VPN spojení.



Obr. 9. Páteřní VPN síť poskytovatele [1].

Mezi další prvky zabezpečující VPN spojení může patřit server přístupu k síti NAS (Network Access Server), který poskytuje rozhraní mezi veřejnou sítí a páteří IP sítě a zajišťuje autentizaci a vyřizování požadavků a servery AAA (Authentication, Authorization, Accounting) sloužící k účtovací, autentizační a autorizační funkci.

Největší množství zařízení je určeno k budování VPN topologií, propojující sítě navzájem prostřednictvím VPN páteře.

II. PRAKTICKÁ ČÁST

5 ANALÝZA STÁVAJÍCÍHO STAVU

Analýza současného stavu byla prvotním úkonem, který předcházel návrhu nové počítačové sítě. Návrh musí odpovídat v maximální míře požadavkům klienta a zároveň splňovat kritéria daná současným vývojem v oblasti informačních technologií.

5.1 Popis firmy

Společnost KPB INTRA s.r.o. se sídlem v Bučovicích, byla založena v roce 1995. Od počátku se zaměřuje na výrobu, prodej, ale také na vývoj přístrojových transformátorů vysokého napětí. Přestože jde o malou společnost, zastává v regionu střední a východní Evropy v tomto oboru významné postavení.

Pro dosažení maximální kvality podléhají veškeré výrobky firmy kusovým zkouškám, které zajištěny přímo ve výrobě zkušebním a kontrolním oddělením. Vysoká kvalita, dobrý management a marketing stojí také za udělením standardů ISO 9001:2008, ISO 14001:2004 a ČSN OHSAS 18001:2008.

Od svého vzniku zaznamenává společnost stále rostoucí tendenci rozvoje. Během velmi krátké doby se firma vypracovala ve strukturovanou jednotku s vlastním vývojovým oddělením. Nárůst výroby sebou přináší potřebu nahradit stávající provozní prostory za nové, s vyšší kapacitou.

5.2 Charakteristika informačního zabezpečení

Stávající informační zabezpečení se vztahuje k administrativní části areálu firmy, nezasahuje do výrobních provozů a z velké části slouží k přenosu dat mezi jednotlivými kancelářemi. Kromě administrativních prostor se v areálu firmy nachází ještě tři průmyslové objekty vzdálené od sebe do 100 metrů, ve kterých se nachází hlavní výrobní provozy.

5.2.1 Hardwarové vybavení

Do současné sítě je zapojeno 42 stolních počítačů a tři servery. Všechny počítače a servery jsou připojeny do místní sítě LAN prostřednictvím dvou přepínačů v datové místnosti. Současná struktura sítě je uvedena v příloze č. **Chyba! Nenalezen zdroj odkazů.**. Přehled hardwarové konfigurace uvádějí následující tabulky:

Tab. 5. Stávající hardwarové konfigurace serveru01.

HP ProLiant ML350 G4	
Operační systém	Windows SBS 2003 R2 Premium Edition
Procesor	Intel Xeon 3.00 GHz
Operační paměť	4 GB PC2-5300 DDR2-667 MHz
Pevné disky	6 x 72.8G 10K RPM, 3 x RAID 1 svazky
Síťová karta	2 x NC7170 1 Gb se systémem TOE (TCP/IP Offload Engine)
DHCP	Služba běžící na serveru
DNS	Služba běžící na serveru
Firewall/Web proxy	Microsoft ISA (Internet Security and Acceleration Server) 2004

Tab. 6. Stávající hardwarové konfigurace serveru02.

HP ProLiant ML350 G5	
Operační systém	Windows Server 2003 R2 Premium Edition
Procesor	Intel Xeon 5110, 1,6GHz
Operační paměť	4 GB
Čipová sada	Intel 5000Z
Pevné disky	2 x 72.8 GB, 2 x 146 GB – 2 x RAID 1 svazky
Síťová karta	HP NC373i a HP NC320T PCIe 1Gb se systémem TOE (TCP/IP Offload Engine)
Aplikační vybavení	MS Exchange 2003
Antivir	Nod 32

Tab. 7 Stávající hardwarové konfigurace serveru03.

HP ProLiant ML350 G4	
Operační systém	Windows Server Standard 2008 SP2 64bit
Procesor	Intel Xeon E5620, 2.4 GHz
Operační paměť	12 GB
Čipová sada	Intel 5000Z
Pevné disky	4 x 146 GB SAS, 2 x 146 GB RAOD 1 svazky
Síťová karta	Broadcom NetXtreme Gigabit Ethernet
Aplikační vybavení	SQL Server 2008 64bit
Antivir	Microsoft Essentials

Tab. 8 Typická hardwarové konfigurace uživatelské stanice.

Stolní počítač	
Operační systém	MS Windows XP
Procesor	Intel Core 2 Duo 2,8 GHz
Operační paměť	2 GB
Čipová sada	Intel PCH 3450
Pevné disky	250 GB
Síťová karta	Realtek 10/100 MB
Aplikační vybavení	MS Office 2003, IS Helios Orange, Autolan, Docházka
Antivir	Avast 4.0

5.2.2 Současná struktura a adresování

Všechny síťové karty počítačů o rychlosti 100 Mbps jsou propojeny pomocí stromové topologie s centrálními přepínači umístěnými v 19“ datovém rozvaděči 24U. K propojení se využívá kabel UTP CAT 5a a koncovek RJ-45. Datová síť nevyužívá redundance a prakticky při poruše hlavního přepínače dojde k výpadku celé sítě. V datovém rozvaděči jsou umístěny taktéž všechny servery, pobočková ústředna ATEUS Omega a směrovač. Směrovač umožňuje přístupu do sítě Internet, funguje jako překlad adres NAT (Network Address Translation) a vykonává funkci firewallu. Privátní rozsah adres vychází z třídy A se síťovou maskou 255.255.255.0, která umožňuje vytvořit $2^{16} = 65536$ podsítí. V každé podsíti může být $2^8 - 2 = 254$ platných hostitelů. Adresa sítě je v tomto případě 10.0.0.0. Adresa směrovače je 10.0.0.254 (Tab. 9).

Dynamické přidělování jedinečných IP adres v daném rozsahu je zajištěno službou DHCP, která pracuje na serveru01. Stejný server a služba DNS (Domain Name Systém) zabezpečuje také vzájemné převody IP adres uzlů sítě a doménových jmen.

Tab. 9. Adresace.

Stávající adresace	
Adresní prostor	10.0.0.1 - 10.0.0.253
Síťová maska	255.255.255.0
Brána	10.0.0.254

5.2.3 Použité systémové a aplikační vybavení

Pro administrativní činnost na stolních počítačích je využíván operační systém Microsoft Windows XP. Běh samotných serverů zabezpečuje operační systém Microsoft Windows SBS 2003 R2 Premium Edition a v případě databázového serveru Windows Server Standard 2008 SP2 64bit.

Aplikační software z velké části je zabezpečován kancelářským balíčkem Microsoft Office 2003. Pro samotnou počítačovou síť představuje největší zátěž Microsoft Exchange 2003,

Internet Explorer verze 8, SQL Server 2008 – IS Helios Orange, Autolan, Docházka a další.

5.2.4 Aktivní prvky stávající počítačové sítě

Aktivní část počítačové sítě se skládá ze tří hlavních prvků. Je to směrovač ZyWALL 5 a přepínači 3com BaseLine Plus Switch 2226 a 3com BaseLine Switch 2250 Plus.

Směrovač je svou konstrukcí určen pro malé kanceláře. Obsahuje server DHCP (Dynamic Host Configuration Protokol), čtyři porty LAN s možností vytvořit demilitarizovanou zónu a jeden port WAN. K administraci směrovače je určené konzolové rozhraní RS-232. Pomocí něho a webového rozhraní nebo příkazové řádky lze nastavovat vnitřní parametry směrovače.

Přepínače 3com BaseLine Plus Switch 2226 a 3com BaseLine Switch 2250 Plus jsou určené pro přepínání ethernetových linek v malých až středně velkých organizacích. Pro přepínání využívají druhé vrstvy modelu OSI a porty o rychlosti 10/100 Mbps.

Tab. 10. Směrovač ZyWALL 5.

ZyWALL 5	
Síťové protokoly	RIP I/RIP II, ICMP, SNMP v1 & v2c + MIB II (RFC 1213), IP Multicasting IGMP v1, v2, IGMP Proxy
VPN	IPSec NAT, IKE, PKI maximální propustnost 25 Mbps
Firewall	Stavový SPI, ochrana před DoS a DDoS
Řízení provozu	Optimalizace šířky pásma
Filtrování obsahu	Blokování Java, Active X, Cookie, Proxy, URL
Síťové služby	DHCP, PPPoE, PPTP
Správa	Webové rozhraní, CLI (Command-Line Interface), Telnet, SSH
Rozhraní	1 x WAN, 4 x LAN, 2 x RS-232

K propojení přepínačů mezi sebou, nebo propojeni přepínače a směrovače, slouží dva účelové duální gigabitové uplinky uzpůsobené pro připojení UTP kabelu, nebo SFP (Small Form-Factor Pluggable) modulu a optické linky. Jsou připraveny pro podporu hlasových sítí VLAN, IGMP (Internet Group Management Protocol) snooping a SNMP (Simple Network Management Protocol) management. Optimální škálovatelnost a dostupnost je zabezpečeno použitím protokolu RSTP (Rapid Spanning Tree Protocol Rapid). Webový management umožňuje snadnou změnu konfigurace.

Tab. 11. Směrovač 3com BaseLine Plus Switch 2226.

3com BaseLine Plus Switch 2226	
Rozhraní	24 x 10/100Base-TX, 2 x COMBO Gigabit SFP
Konfigurace	Web management, CLI, SNMP v.1 a v.2, port miroring, RMON
Síťové služby	IGMP, QoS, RCST, VoIP, OSPF, RIP
Max. počet VLAN	256
Bezpečnost	ACL, TACACS+, RADA, EAP, PAP

Tab. 12. Směrovač 3com BaseLine Plus Switch 2250

3com BaseLine Plus Switch 2250	
Rozhraní	48 x 10/100Base-T, 2 x Gigabit SFP
Konfigurace	Web management, CLI, SNMP v. 3, port miroring, RMON
Síťové služby	IGMP, QoS, RCST, VoIP, OSPF, RIP
Max. počet VLAN	256
Bezpečnost	ACL,TACACS+, RADA, EAP, PAP

5.2.5 Bezpečnost informací a připojení k síti Internet

Směrovač ZyWALL 5 je prezentován jako bezpečnostní internetová brána s podporou IPSec VPN, ochranou před útoky typu odmítnutí služby a filtrování webového obsahu a

dat. Obsahuje stavový firewall s podporou SPI (Stateful Packet Inspection). Tento firewall je schopný sledovat všechny navázané TCP (Transport Control Protocol)/UDP relace a propouštět jen ty, které jsou povolené.

Kontrola přístupu u přepínačů 3com BaseLine Plus je zabezpečena autorizačními protokoly založenými na bázi TACAS+ (Terminal Access Controller Access-Control System) a RADA (Radius Authenticated Device Access). K prokazování totožnosti při použití protokolu point-to-point slouží protokoly CHAP (Challenge Handshake Authentication Protocol), PAP (Password Authentication Protocol) a EAP (Extensible Authentication Protocol). Přepínač 3com BaseLine Plus Switch 2226 podporuje šifrovaný přenos dat protokolem SSH (Secure Shell). Přestože tyto přepínače umožňují zabezpečený přístup, není této možnosti v současné době využíváno.

Připojení počítačové sítě k veřejné síti Internet je realizováno firmou Infos, která poskytuje veřejnou IP adresu a rychlost připojení 4Mbps.

5.3 PRTG Network Monitor

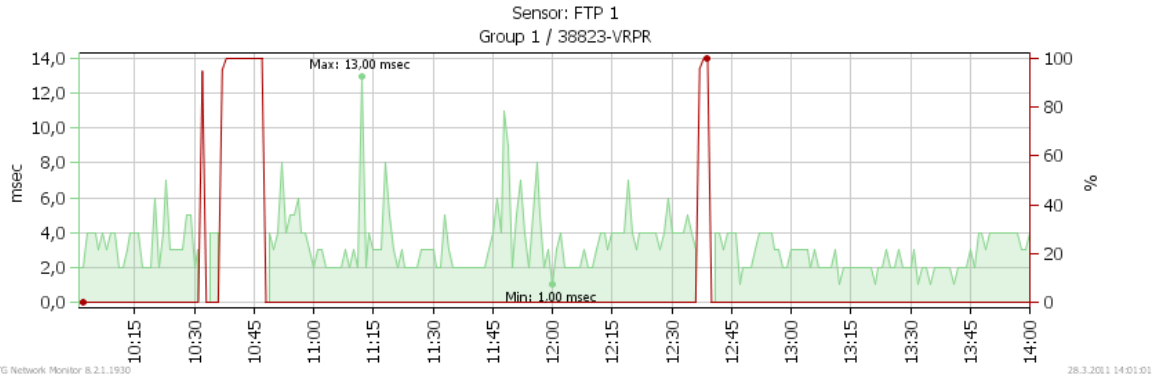
Program PRTG Network Monitor je výkonné a snadno použitelné řešení pro centrální monitorování sítě pomocí jediného nástroje. PRTG Network Monitor je výsledkem vývoje německé firmy Paessler AG, která je uznávána jako Cisco Technology Developer Partner a VMware Technology Alliance Partner. Tento sofistikovaný softwarový produkt slouží jako východisko pro firmy menší a střední velikosti.

Program PRTG pomáhá optimalizovat šířku pásma, zlepšuje kvalitu služeb a minimalizuje prostoje v síti. Může běžet nepřetržitě a zaznamenává data do databáze pro pozdější analýzu. Pro konfiguraci zařízení a čidel využívá webové uživatelské rozhraní. Vytvořené výstupy lze následně prezentovat zákazníkům pomocí grafů a tabulek. Pro sledování využití datové sítě a šířky pásma využívá protokol SNMP. Analýza jednotlivých paketů se děje prostřednictvím procedury Packet Sniffing. PRTG může sledovat pakety procházející síťovou kartou nebo portem přepínače. Technologii je možné využívat i pro bezdrátové sítě WLAN.

5.3.1 Zátěžové testy

Zátěžový test databázového serveru03

Při měření výkonnosti sítě je vhodné se zaměřit na nejvíce zatížená místa. Tyto se obvykle nachází na přístupových uzlech serverů, nebo na rozhraních přepínačů. K měření vytížení serveru je vhodné zvolit protokol FTP a měřit dobu odezvy. Z obrázku je patrné, že v době měření od 10:00 hodin dopoledne do 14:00 hodin odpoledne v normální pracovní den došlo ke třem výpadkům sítě. Tyto výpadky se projevily nedostupností serveru do úhrnné doby 20 minut.



Obr. 10. Sensor FTP PRTG.

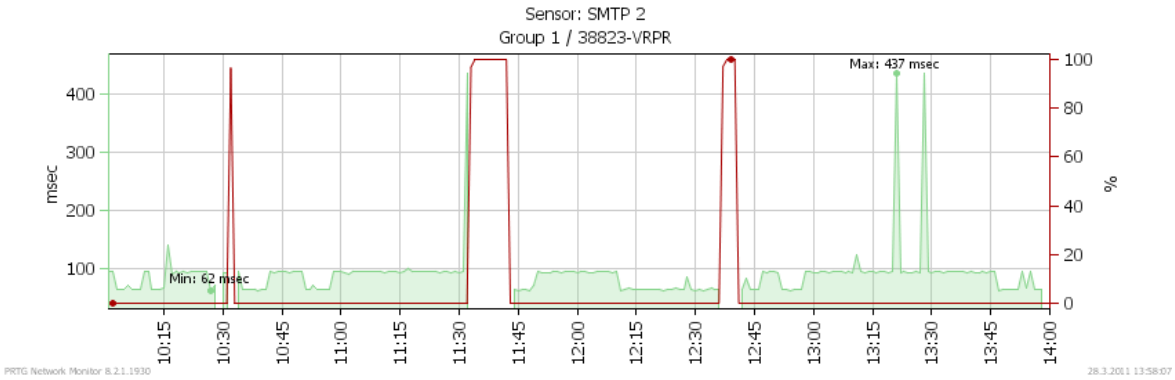
Zátěžový test poštovního serveru02

K testování SMTP (Simple Mail Transfer Protocol) se využívá Email Round Trip technologie, pomocí které se sleduje dostupnost a výkon v procesu doručování e-mailů. Testování se děje prostřednictvím dvou snímačů:

SMTP&POP3 Round Trip Sensor

SMTP&IMAP Round Trip Sensor

Oba na začátku zasílají testovací zprávu na poštovní server pomocí protokolu SMTP. Poštovní server doručuje testovací zprávu na POP3 (Post Office Protocol version 3)/IMAP (Internet Message Access) server. Nato se PRTG v krátkých intervalech připojuje na POP3/IMAP server, dokud mu neumožní stáhnutí testovacího emailu. Vyhodnocuje se čas nutný k doručení zprávy.

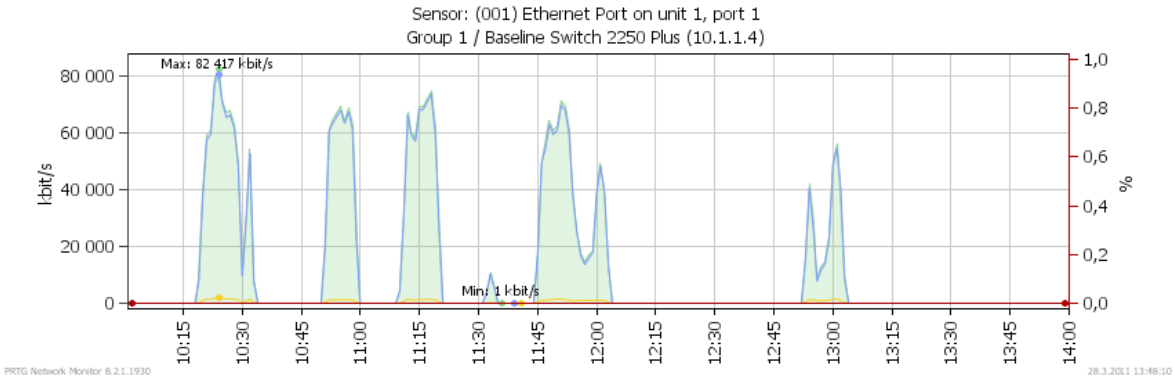


Obr. 11. Sensor SMTP PRTG.

Kromě času nutného k doručení nás PRTG informuje o funkčnosti protokolu SMTP, konektivitě a správného nastavení poštovního spojení. I zde je možné vysledovat nedostupnost serveru.

5.3.2 Provozní parametry aktivních prvků

Kromě parametrů provozních stanic a serverů lze programem PRTG sledovat provozní zátěž na rozhraních přepínačů a směrovačů implementovaných do sledované sítě. Ke sledování provozní zátěže ve firmě KPB Intra s.r.o. je využit port číslo 1 u přepínače 3Com Baseline Switch 2250 Plus. Z grafu na obrázku (Obr. 16) je patrné, že maximální zátěž tohoto rozhraní v pracovní době od 10:00 hodin do 14:00 hodin je 82,417 Mbps. V případě využití teoretické přenosové rychlosti tohoto přepínače, která je 100 Mbps, dosahuje tato hodnota více než dvou třetin.



Obr. 12. Provozní zátěž na portu Ethernet 1/1.

Sledováním naměřených hodnot je patrné, že síťový provoz, jeho propustnost a rychlost, odpovídá stávající infrastruktuře. Výpadky provozu serverů činí statisticky přibližně 6,5 hodiny měsíčně, z čehož plyne i nehospodárné využití pracovní doby.

Budeme-li uvažovat budoucí další rozvoj firmy, je informační zabezpečení z pohledu síťové struktury nedostatečné a nevyhovující. K těmto poznatkům je nutné přihlédnout při návrhu nové počítačové sítě.

6 POŽADAVKY ZÁKAZNÍKA

Nevyhovující stav současné počítačové sítě je znám jak informačnímu specialistovi pracujícím pro firmu KPB Intra s.r.o., tak i vedení společnosti, která je k rekonstrukci počítačové sítě nakloněna. Potřebu výstavby nové sítě podtrhují také časté výpadky provozu. Ty zapříčiňují nižší výkonnost firmy a z toho plynoucí ekonomické dopady.

6.1 Věcné omezení

Vedení firmy požaduje, aby nově vytvořená síť pokrývala celý areál podniku a centrum počítačové sítě bylo umístěno v administrativní budově, ve které je umístěno i centrum stávající sítě. Taktéž požaduje maximální využití stávající infrastruktury. Na tuto bude navazovat nová tak, aby byly uspokojeny požadavky pokrytí celého areálu. Aktivní prvky budou nahrazeny novými kvalitnějšími poskytujícími záruku bezproblémového chodu.

Při návrhu nové počítačové sítě však musí být brán zřetel i na finanční stránku. Ta musí být nastavena tak, aby návratnost vložených investic byla v souladu s rychlým vývojem informačních technologií.

6.2 Bezpečnostní požadavky

Bezpečnostní rizika plynoucí z využívání mezinárodní sítě Internet jsou vedení firmy známa. Přístup k využívání sítě Internet bude povolen jen pro určené pracovníky. Webové stránky firmy jsou umístěny na pronajatém serveru, který poskytuje kompletní hostingové služby. Z tohoto důvodu, nejsou kladeny požadavky na umístění webových stránek firmy na vlastní server. Přístup k datům z vnější strany bude omezen pouze ke komunikaci s poštovním serverem02.

6.3 Správa sítě

Jelikož je areál firmy rozlehlý, je potřeba správy sítě z jednoho místa více než aktuální. To bude zajištěno pomocí monitorovacího software od dodavatele firmy Cisco.

Jak bylo zmíněno ve firmě KPB Intra s.r.o. již pracuje informační specialista a jeho odborné znalosti nevyžadují další zaškolení v případě využití nových technologií.

6.4 Provozní zátěž

Pro komunikaci vedení firmy se zaměstnanci vyžaduje firma zavedení bezdrátových telefonů, které budou využívat nově vybudované rozvody. Tyto rozvody budou sloužit i ke kontrole výroby prostřednictvím kamerových systémů. Zpětnou analýzou videozáznamu výroby povede ke snížení produkce vadných výrobků. Tomu odpovídají požadavky kladené na šířku pásma, úroveň služeb a zabezpečení kvality QoS (Quality of Service).

6.5 Požadavky na výkon sítě

Rozšíření počítačové sítě o IP telefonii a IP kamerové systémy, nesmí mít dopad na již provozované informační systémy a aplikační software IS Helios Orange, Autolan a Docházka. Síť musí být také schopna zabezpečit provoz případného rozšíření tohoto aplikačního softwaru. IP telefonie bude využívána prioritně pro komunikaci v areálu společnosti.

Pro budoucí využití informačních technologií s vyššími rychlostmi budou páteřní rozvody dimenzovány pro rychlost přenosu 10 Gbps. Propojení přístupové vrstvy bude realizováno propojením s rychlostí 1 Gbps. Aktivní prvky vzhledem k vysokým investičním nákladům budou projektovány na rychlost o řád nižší.

7 NÁVRH STRUKTURY NOVÉ SÍTĚ

Problematika návrhu základní topologie je velmi rozsáhlá, variabilní a do velké míry se odvíjí od parametrů jaké má konečná síť splňovat. Nároky kladené na architekturu jsou rozdílné pro jednotlivé firmy a liší se nejen rozsahem počítačové sítě, geografickým rozmístěním, ale také typem podniku. Jisté je, že průmyslový závod, IT firma nebo bankovní subjekt, mají diametrálně rozdílné požadavky na celkové pojetí počítačové sítě.

7.1 Návrh topologie

U síťové topologie ve firmě KPB Intra s.r.o. z hlediska nákladů, snadnějšího budoucího rozvoje, dobré administrace a lepšího izolování závad lze využít kombinaci hybridní a bezpečnostní topologie. Samotná implementace tohoto modelu bude v tomto případě řešena prostřednictvím stromové topologie, která spojuje jednotlivé výrobní provozy s ústředím firmy, datového centra a serverů. Hierarchický model z pohledu aktivních prvků se dělí na tři vrstvy a to vrstvu jádra, distribuční vrstvu a přístupovou vrstvu. V případně menších a středních firem se využívá lépe dvouvrstvý model, skládající se z vrstvy jádra a přístupové vrstvy, který je i v tomto případě dostačující.

Vrstvu jádra tvoří páteřní přepínač Cisco Catalyst WS-C3750G-12S-S, který poskytuje vysokou spolehlivost, odolnost vůči chybám, malé zpoždění a snadnou správu. Tento bude propojen pomocí optických kabelů s přístupovými přepínači.

Rovněž připojení serveru01 a databázového serveru03 bude z důvodu zajištění vysokorychlostního a bezchybného přenosu dat realizováno k páteřnímu přepínači.

Druhá vrstva je přístupová a zabezpečuje propojení přepínačů Cisco Catalyst 2960-48PST-L, jednotlivých počítačů, IP telefonů a IP kamer.

Bezpečnostní část topologie představuje ochrana vnitřní sítě LAN, před nedůvěryhodnou síti v našem případě sítí Internet. Ideální řešením pro umístění hostitelských systémů je v tomto případě firewallový systém s demilitarizovanou zónou.

7.2 Přenosové médium

Při výběru přenosových médií nelze vycházet z krátkozrakého řešení v podobě sice mnoha lety prověřené, ale v dnešní době již nevyhovující megabitové technologii. Vzhledem

k velmi rychlému rozvoji informačních technologií je logicky výhodné použití gigabitových rychlostí pro připojení samostatných počítačů, IP telefonů a kamer. Z této rychlosti dále vyplývá nutnost snížení rizika vzniku úzkých hrdel na páteřních linkách. Toho lze dosáhnout propojením přepínačů pomocí uplink portů s přenosovou rychlosti až 10 Gbps. Jinou alternativou je použití agregace více gigabitových portů.

Neopomenutelným faktem, je i prostředí, ve kterém se bude přenosové médium nacházet. Jiné požadavky kladou administrativní budovy a jiné provozní průmyslové objekty. Vliv elektromagnetického rušení je značný v provozních prostorech s vysokým napětím, nebo velkým magnetickým polem. Toto je případ i firmy KPB Intra s.r.o., která využívá při výrobě přístrojových transformátorů vysoko indukční pece.

Výše uvedené zásady jsou rozhodující při volbě přenosového média a typu konektorů. Pro přenosovou rychlost 1 Gbps, je výhodné použít metalický kabel S/FTP s kategorií kabeláže CAT 6, který má výhodný poměr ceny a výkonu. Tento kabel poskytuje stíněním PiMF (Paar in Metallfolie) spolehlivou ochranu před elektromagnetickým zářením a zároveň umožňuje přenos protokolů 1000Base-T/TX s pracovní frekvencí do šířky pásma 250 MHz do vzdálenosti až 100m. Jednotlivé měděné páry jsou stíněny folií a všechny páry jsou dále stíněny opletením. Kabelem prochází neizolovaný zemnící vodič pro snadnější uzemnění. Materiál pláště je z PVC nebo LSOH (Low Smoke Of Halogen) pro omezení tvorby kouře v případě požáru.

Alternativou pro kabeláž kategorie CAT 6 je kategorie CAT 6a, která poskytuje dvojnásobnou šířku pásma 500 MHz, plnohodnotný přenos protokolu 10GBase-T s přenosovou rychlostí 10 Gbps do vzdálenosti 100 m. Cenové znevýhodnění je oproti nižší verzi přibližně třetinové.

Keystony – konektory pro připojení stíněných kabelů CAT 6 a CAT 6a jsou osazeny duální zařezávací svorkovnicí typu 110/Krone. Stínění těchto konektorů je provedeno oplechováním těla konektoru stříbrnou kovovou částí. Pro bezchybné spojení jsou kontakty konektoru pozlaceny. Modulární datové zásuvky ve stíněné verzi CAT6 STP RJ-45 jsou v celokovovém provedení s odpovídajícím propojovacím konektorem.

Páteřní propojení je realizováno vícevidovým optickým kabelem 50/125 μm kategorie OM3 standardu 10GBase-SR, který na vzdálenost 300 m garantuje přenosovou rychlost až 10 Gbps v přenosovém okně 850 nm, při šířce pásma 2000 MHz. Jako vysílač využívá laser

VCSEL (Vertical-Cavity Surface-Emitting Laser), díky čemuž vyniká nízkou cenou. Nevýhodou je omezená vzdálenost přenosu. Použití vícevidového optického vlákna optimalizované pro laser LOMMF (Laser optimized multi-mode fiber) 850 nm lze dosáhnout vzdálenosti až 550 m kategorie OM4. Velkou výhodou vícevidových kabelů je jejich nízká cena.

V případě páteřního propojení dvou přepínačů v duplexním módu, je nutné použít dvě vlákna pro jeden spoj. Pro budoucí redundantní spoje či zálohování je vhodné použít 24 vláken v jednom kabelu.

Způsob instalace je s ohledem na budoucí snadnější výměnu realizovat formou mikrotrubiček a optický kabel do takto připravených mikrotrubiček zafouknout.

Jako jinou volbu páteřního propojení lze využít také jednovidový kabel 9/125 μm, standardu 10GBase-LX4 pracující se čtyřmi lasery, každý s odlišnou vlnovou délkou se středem 1310 nm. Další vhodný jednovidový kabel je standardu 10GBase-LR. Má již jen jeden laser tudíž je levnější a provoz s ním vykazuje nižší spotřebu energie. V obou případech je dosah těchto kabelů až 10 km.

Optické kabely jsou ukončené standardními optickými konektory FOCIS (Fiber Optic Connector Intermateability Standard).

7.3 Síťový hardware

Navrhované aktivní prvky vychází z posouzení jednotlivých požadavků zákazníka. Dále je zde zohledněna investiční stránka realizace a v neposlední míře také budoucí vývoj jak na straně firmy, tak na straně vývoje informačních technologií. Návrh topologie sítě spolu s aktivními prvky a přenosovým médiem je představen v příloze č. **Chyba! Nenalezen zdroj odkazů.**. Rozmístění aktivních prvků v jednotlivých datových rozvaděčích je uvedeno v příloze č. P I.

7.3.1 Směrovač

Návrh směrovače patří mezi nejdůležitější kroky při tvorbě struktury funkční, bezpečné a spolehlivé sítě. Moderní přepínač musí být optimalizován pro bezpečné směrování a zabezpečení kvalitního přenosu dat, hlasu a videa. V struktuře směrovače je nutné

implementovat odolný systém pro rychlé a škálovatelné obsloužení kritických podnikových aplikací.

Jako optimální se v případě firmy KPB Intra s.r.o. jeví směrovač Cisco 2821 z řady Cisco 2800. Tento směrovač je určen pro pobočkové kanceláře a středně velké podniky. Je souhrnně označován jako směrovač integrovaných služeb ISR (Integrated Services Routers).

Obr. 13. Směrovač Cisco 2821.

Zahrnuje v sobě kromě směrování datového provozu funkce bezpečnostní (firewall, IPS (Intrusion Protection Systems), koncentrátorVPN / SSL) a funkce pro podporu hlasových služeb jako jsou hlasová brána, softwarová ústředna a SRST (Survivable Remote Site Telephony). Hlasové služby ve formě IP telefonie jsou u směrovače Cisco 2821 podporovány pomocí softwarových produktů Call Manager Express a Cisco Unity.

Bezpečnostní aspekty v sobě zahrnuje hardwarová podpora šifrování, stavový firewall a podpora IPS.

Univerzálnost a škálovatelnost je zastoupena pomocí rozšiřujících, síťových a hlasových modulů:

- AIM (Advanced Interface Module) kompresní modul do interního slotu AIM, který redukuje potřebu drahého širokého WAN pásma.
- HWIC (High-Speed WAN Interface Card) vysokorychlostních modul k propojení se sítí typu WAN.
- VIC (Voice Interface Card) hlasový modul umožňující přímé připojení do jednotné telefonní sítě JTS, nebo k pobočkové ústředně. Hovory mohou být díky tomuto rozhraní směrovány do IP sítě a zpět do JTS.
- VWIC modul do rozhraní pro sítě typu WAN (WIC) a hlasového rozhraní (VIC). Podporuje jak hlasové i datové služby.

- NME (Network Module Ethernet)/NM (Network Module) rozšiřující síťový modul.
- PVDM (Packet Voice Digital Module) modul poskytující pomocí digitálnímu procesoru konektivitu o vysoké hustotě pro hlas, videokonference a překódování v Cisco IP komunikacích.
- EVM (Extension Voice Module) analogově digitální modul pro hlas a fax.
- IPS modul sloužící k monitoringu sítě a ochraně před útoky vedeným proti koncovým zařízením, síťové infrastruktuře a službám sítě.
- WLAN Controller modul k řízení centralizovaných bezdrátových sítí.
- NAM (Network Analysis Modul) modul pro podporu síťových aplikací.

Tab. 13. Přehled vlastností směrovačů řady Cisco 2800.

Vlastnost	**Cisco 2801**	**Cisco 2811**	**Cisco 2821**	**Cisco 2851**
Ethernet WAN	2 FE	2 FE	2 GE	2 GE
LAN Ethernet portů (na NME)	max. 16	max. 32	max. 40	max. 64
HWIC / WIC / VIC / VWIC slot	4	4	4	4
NME / NM slot	-	1	1	1
EVM slot	-	-	1	1
AIM slot	2	2	2	2
IPSec VPN tunelů (AIM)	800	1800	1800	1800
DSP slotů na zákl. jednotce	2	2	3	3
Call Manager Express (uživ.)	24	36	48	96
Počet současných hovorů[4]	32 / 32	55 / 80	100 / 128	150 / 192
PoE	120 W	160 W	240 W	360 W

7.3.2 Přepínače

Přepínač páteře je volen s ohledem na spolehlivost a cenu. Vysokou odolnost, snadnou použitelnost a výbornou provozní efektivitu nabízí přepínač Cisco Catalyst WS-C3750G-12S-S. Tento přepínač s IP Base image nabízí pokročilou správu QoS, statické směrování, RIP a EIGRP. Přepínač podporuje stohování až devíti samostatných přepínačů do jednoho logického celku bez přerušení provozu.

Nová technologie Cisco StackWise podporuje multicastové aplikace jako jsou video a hlas. Tomu odpovídá podpora Jumbo Frames pro pokročilé datové a video aplikace, vyžadující velké snímky. Z bezpečnostního hlediska podporuje přepínač sadu zabezpečovacích funkcí ACL (Access Control List), autentizace, zabezpečení na úrovni portu, základní a rozšířené síťové služby standardu IEEE 802.1x. Pro utajenou komunikaci přepínač využívá protokoly SSH/SSL a funkcí filtrování MAC adres znesnadňuje neautorizovaný přístup.

Pro dostatečnou šířku pásma je u tohoto přepínače zajištěna podpora desetigigabitového ethernetu a plně duplexního režimu v podobě dvou X2-Based 10 Gbps Ethernet portů, který lze nahradit v případě potřeby pomocí Cisco TwingGig adaptéru, na čtyři 1 Gbps Ethernet SFP porty.

Konfigurace a management se provádí pomocí CLI, nebo webového nástroje Cisco Network Assistant Software.

Mezi další rozšířené funkce patří DHCP klient a server, IGMP snooping, kontrola broadcast storms, podpora protokolů STP, SNMP, RMON (Remote Network MONitoring), Telnet a HTTP.

Obr. 14. Cisco TwinGig Adapter.

Pro připojení je možné využít dvanáct SFP 1 Gbps Ethernet portů a dvanáct rozšiřujících SFP (mini-GBIC) rozhraní pro LC optické konektory.

Propojení páteře a přístupové vrstvy se děje za pomocí optických kabelů. Přístupová vrstva obsahuje vysokou hustotu portů, připojuje klienty a zajišťuje bezpečnost na úrovni portu. Do této vrstvy patří přístupové body bezdrátové sítě, ale i připojení serverů v datovém centru, jenž je však výkonnější. Do páteře je zaimplementováno propojení přepínačů vysokorychlostním médiem, rozdělení sítě na segmenty VLAN, routování mezi nimi a kontrola provozu.

Jako vhodný přepínač určený pro přístupovou vrstvu je Cisco Ctatalyst 2960-48PST-L. Může podporovat až 48 Ethernet 10/100 Mbps PoE portů s celkovou kapacitou PoE výkonu až 370W dle normy IEEE 802.3af.

Obr. 15. Cisco Catalyst 2960.

Využitím Cisco Catalyst Intelligent Power Managament se může výkon rozdělit na všech 48 portů a tím připojovat zařízení jako je IP telefon, či IP kamera. Všech 48 portů přepínače Cisco Catalyst 2960-48PST-L pracuje s rychlostmi 10 a 100 Mbps. Rozhraní Uplink je realizováno dvěma 1 Gbps Ethernet SFP porty a dvěma pevnými Ethernet 10/100/1000 Mbps porty. K rozhraní lze tedy připojit metalický kabel s konektorem RJ-45, nebo optický kabel s konektorem LP, v závislosti na typu zásuvného mini-modulu. Přepínač podporuje až 255 sítí VLAN, přičemž každá může obsahovat až 4094 zařízení.

Přepínače Cisco Catalyst 2960 podporují stohování přepínačů pomocí Cisco FlexStack Stacking. Umožňuje, aby všechny přepínače umístěné do stohovacího zásobníku vystupovaly jako jedna spínací jednotka.

Velká výhoda tohoto uspořádání spočívá v možnosti konfigurovat tuto skupinu, pomocí managementu z jedné IP adresy. Poskytuje též vyšší dostupnost, jednodušší řízení a nižší celkové náklady.

Přepínače řady Cisco Catalyst 2960 pomáhají snížit provozní náklady prostřednictvím komplexní sady funkcí Cisco Catalyst Smart, které zjednodušují nasazení LAN, usnadňují konfiguraci a řešení problémů.

Tab. 14. Porovnání parametrů přepínačů řady Cisco Catalyst 2960.

Funkce nastavení	**Model**	**10/100 Eth porty**	**Uplinky**	**Napájení**
LAN Base Layer 2	WS-C2960-48TT-L	48	2 x 1000BT	45 W
LAN Lite Entry Layer 2	WS-C2960-48TC-S	48	2 Dual Purpose	45 W
	WS-C2960-48PST-L	48 PoE	2 x 1000BT 2 x SFP	370 W
LAN Base Layer 2	WS-C2960-48PST-S	48 PoE	2 x 1000BT 2 x SFP	370 W

Některé užitné vlastnosti přepínačů Cisco Catalyst 2960

- Automatický QoS zjednodušuje konfiguraci autodetekcí IP telefonů.
- DHCP autokonfigurace více přepínačů přes boot server.
- Auto-negotiation na všech portech automaticky vybírá poloviční nebo plný duplex.
- DTP (Dynamická Trunking Protocol) a VTP (VLAN Trunkig Protokol) usnadňuje konfiguraci dynamických linek napříč všemi porty přepínače v sítích LAN a VLAN.
- MDIX (Automatic Media-Dependent Interface Crossover) automaticky přenastavuje vysílací a přijímací páry při zapojení nevhodného kabelu.
- ARP (Address Resolution Protocol) funguje ve spojení s Private VLAN Edge na minimalizaci všesměrového vysílání a dosažení maximální dostupné šířky pásma.
- IGMP Snooping pro IPv4 umožňují vyčlenění šířky pásma pro žadatele multicast streamů.

- Voice VLAN usnadňuje správu a řešení potíží u telefonních zařízení tím, že udržuje hlasový provoz na samostatné VLAN.
- RSPAN (Remote Switch Port Analyzer) umožňuje správcům vzdáleně monitorovat porty přepínačů sítě z jakéhokoli jiného přepínače ve stejné síti.
- Vestavěný RMON softwarový agent zlepšuje řízení provozu, sledování a analýzu pomocí čtyř RMON skupin (historie, statistika, alarmy a události).

Nástroje pro rozšířený inteligentní management

Pro detailní konfiguraci nabízí přepínače Cisco Catalyst 2960 CLI a Cisco Network Assistant Software což je nástroj pro rychlou konfiguraci, na základě předem nastavených šablon. Kromě toho, podporují tyto přepínače LMS (LAN Management Solution) pro celosíťový management, který je založen na osvědčeném designu a doporučeních získaných monitorováním a řešením problémů.

Bezpečnostní funkce

- Port Security zajišťuje přístup portům na základě MAC adresy.
- DHCP snooping zabraňuje falšování DHCP serveru a vysílání falešné adresy.
- DAI (Dynamic ARP Inspection) pomáhá zajistit integritu dat zabezpečením protokolu ARP.
- IP Source Guard brání vložení falešného obsahu, nebo převzetí IP adresy uživatele vytvořením tabulky mezi klientovou IP adresou a MAC adresou, portem, a VLAN.
- TrustSec zajišťuje přístup k síti, prosazením zásad zabezpečení a nabízí standardní bezpečnostní řešení jako je IEEE 802.1X.

Další pokročilé funkce zabezpečení

- Port-Based ACL umožňuje zavedení bezpečnostní politiky na jednotlivé porty přepínače.
- SSH Protokol, Kerberos a SNMPv3.
- SPAN (Switched Port Analyzer) monitoruje provoz pomocí funkce zrcadlení portů.
- TACACS + a RADIUS autentizace umožňuje centralizované řízení přepínače a omezuje neoprávněným uživatelům měnit nastavení.

- MAC Address Notification umožňuje administrátorům, aby byli informování, která MAC adresa byla přidána, nebo odstraněna ze sítě.
- Multilevel Security on Console Access zabraňuje neoprávněným uživatelům měnit konfiguraci přepínače.
- Aktivace BPDU Guard eliminuje nedovolené šíření BPDU zpráv s cílem změnit topologii sítě.

Redundance

Důležitou funkcí při použití redundance je FlexLink, který při výpadku sítě poskytuje konvergenci s dobou kratší než 100 ms. K tomu využívá RSTP a MSTP (Multiple Spanning Tree Protocol).

Zabezpečení Quality of Service

Plánování, klasifikace a značení paketů je zahrnuto do více služeb za účelem poskytnutí vhodného výkonu pro přenos dat, hlasu a videa. Mezi tyto služby patří:

- Class of Service (CoS) je způsob, jak třídit a upřednostnit pakety na základě typu aplikace (hlas, video, přenos souborů, zpracování transakcí), typu uživatele (CEO, sekretářka), nebo jiné nastavení.
- Cisco Control Plane Policing slouží ke zvýšení bezpečnosti. Cílem je snaha zabránit zpracování nechtěných nebo potenciálně nebezpečných dat procesorem zařízení. K tomuto účelu obsahuje filtr, který dovoluje spravovat tok dat control plane paketů k zajištění kvality služeb.
- SRR (Shaped Round Robin) plánovač front. Pomáhá zajistit řízení toku paketů při průchodu výstupní a vstupní frontou. Každé frontě nastavuje váhu, pomocí níž upřednostňuje tok paketů.
- WTD (Weighted Tail Drop) poskytuje ochranu před zahlcením fronty. Na základě nastavení vah zahazuje pakety přicházející do fronty a předchází zahlcení, dokud toto nebezpečí nepomine.
- SPQ (Strict Priority Queuing) rozděluje provoz na pakety s vyšší a nižší prioritou a zajišťuje to, že pakety s nejvyšší prioritou jsou obsluhovány přednostně.

- Rate Limiting omezuje rychlost na základě zdrojové a cílové adresy IP, zdrojové a cílové MAC adresy.

7.3.3 VoIP

Ucelenou a zároveň otevřenou soustavu představuje komunikace pomocí IP telefonie, IP kamerových systémů nebo GSM modulů. Tato soustava se skládá z infrastruktury na bázi směrovačů, přepínačů, firewallu, přenosových médií, systému řízení hovoru například Cisco CallManager Expres, dále koncových přístrojů a aplikačního vybavení.

Použitím IP telefonie dochází k redukci investic, snížení nákladů pro implementaci nových služeb a centrální správu systému.

U firmy KPB Intra s.r.o. je telefonní spojení v dnešní době zabezpečeno centrálním komunikačním prvkem. Tento prvek je pobočková ústředna ATEUS Omega, která již v dnešní době nesplňuje náročné požadavky rozvíjející se společnosti.

Výhodou směrovače Cisco 2821 je, že obsahuje mimo jiné i zabudované DSP moduly pro paketový přenos hlasu. Tento model přichází s volitelnou zcela nezávislou verzí CME (CallManager Express), což je podmnožina VoIP platformy CallManager. Jedná se o jednoduchou aplikaci pro zpracování hovorů s funkčností pobočkové ústředny.

Rovněž modul hlasové pošty CUE (Cisco Unity Express) obsahuje grafické prostředí pro nastavení uživatelů, hlasových schránek, hlasové pošty s funkcemi přesměrování hovoru a automatické spojovatelky. Nespornými výhodami jsou tedy integrované zpracování digitálního signálu, grafický správce konfigurace, monitor rozhraní a podpora existujících karet WIC, VIC a síťových modulů.

Nevýhodu lze spatřit ve využívání příkazového řádku při zpracování určitých úloh.

Další aplikace rozšiřující IP telefonii ve směrovači Cisco 2821 jsou:

Cisco Unity Express, sjednocuje messaging se zlepšenou škálovatelností až do 250 poštovních schránek a novou funkcí VoiceView Express, umožňuje uživatelům procházet jejich hlasové poštovní záznamy z prostředí PDA, e-mailové schránky, nebo z displeje IP telefonu.

Cisco IP Communicator, umožňující realizovat bezpečné hlasové a video IP hovory přes desktop nebo notebook.

Unified Video Advantage, který zákazníkům poskytuje efektivní možnosti videotelefonie.

IP telefony jsou zahrnovány do skupiny jednoúčelových telefonů. Pomocí integrovaného Ethernet přepínače se mohou vkládat mezi stávající připojený počítač a aktivní prvek LAN a tudíž neomezují připojení počítače do sítě. Uživateli stačí k připojení počítače a IP telefonu jedna přípojka a tudíž není nutné navyšovat kapacitu sítě. Pomocí standardů IEEE 802.1q podporují VLAN, takže počítačová a telefonní síť mohou být od sebe z bezpečnostních důvodů částečně odděleny. V dnešní době nespornou výhodou IP telefon je jejich možnost napájení přes Ethernet centrálně pomocí PoE IEEE 802.3af . Možnost IP telefonů zobrazovat krátké zprávy, jednoduchou grafiku či doplňkové funkce, nabízí grafický display spolu s jednoduchým XML (Extensible Markup Language) prohlížečem.

Jedná se například o:

extension mobility - možnost přihlášení se k přístroji, získání odpovídající linky, oprávnění k volání a dalších parametrů. Linka tak může cestovat po síti s uživatelem do jakékoli lokality bez nutnosti centrální změny parametrů přístroje.

telefonní seznam - nejen interní seznam firmy, ale i externí seznamy, které jsou k dispozici na Internetu. V ČR tak mohou mít uživatelé k dispozici kompletní telefonní seznam osob a organizací nabízený společností Telefónica O2 Czech Republic, a.s. prostřednictvím stránek O2 Active.

integrace s intranet aplikacemi - pokud jsou založeny na www službách, IP telefon je pouze speciálním typem www prohlížeče.

IP telefonů je nepřeberné množství, z nichž si je možné vybrat. Z pohledu kompatibility při použit aktivních prvků firmy Cisco, je vhodné využít i IP telefony této značky.

Jako vhodný telefonní přístroj do administrativních prostorů lze použít Cisco SPA962. Je osazen dvěma zásuvkami RJ-45 pro připojení PC a konektorem k připojení náhlavní soupravy. Pracuje na základě protokolu 100Base-TX s podporou PoE. IP telefon podporuje celou řadu síťových protokolů jako například TCP/IP, UDP, RTP, DHCP, ICMP a další. Přenos hlasu je zabezpečen pomocí inteligentního QoS a kodeků G.711, G.726, G.726A, G.723. Administrace je provedena přes webové rozhraní chráněné heslem. Přenos hovoru může být chráněn pomocí šifrování a to až 256bitového AES, nebo MD5.

Obr. 16. Cisco - Linksys WIP330 Wireless-G.

Jako příklad přenosného IP telefonu vhodného pro využití ve firmě KPB Intra s.r.o. se jeví telefon Cisco - Linksys WIP330 Wireless-G, jenž představuje kvalitní přenos hlasu pomocí IP (VoIP) prostřednictvím bezdrátové sítě standardu IEEE 802.11g. Telefon pracuje v pásmu 2.4GHz, podporuje 802.11g a řadu síťových protokolů. Velký plně barevný display s vysokým rozlišením usnadňuje pohyb uživatele v telefonu i v nastavení.

Mezi další rozšiřující funkce paří zobrazení čísla volajícího, přesměrování hovorů, přepojení hovoru, historie volání a uložení až 250 kontaktů.

Telefon je určen pro mobilní pracovníky v provozech. Jeho dosah ve vnitřním prostředí při vhodném umístění AP bodu je až 75m ve venkovním ideální pro prostředí až 300 m.

Pro přenos hlasu v síti využívá řadu protokolů jako například: TCP/UDP/IP, DNS, ARP, ICMP, DHCP a další. Dále hlasové kodeky G.711, G.729 A. Kvalita přenosu je podpořena funkcemi G.168 Echo Cancellation, Jitter Buffer Control nebo Comfortable Noise Generation.

Pro konfiguraci využívá webové aplikační rozhraní součástí, kterého je i nastavení hovoru v šifrovaném módu pomocí AES nebo SSL Encryption.

7.3.4 IP kamery

IP kamery nabízí mnoho výhod oproti standardním uzavřeným televizním okruhům CCTV (Closed Circuit Television). Nejznámější výhodami IP kamery je možnost zobrazení živého videa přes Internet odkudkoli ve světě, detekce pohybu, možnost ukládání záznamu, vzdálené ovládání a další. Významným kritériem při výběru IP kamery je skutečnost, že

umístění IP kamer bude v průmyslových objektech, tedy v prostředí se zvýšenou prašností, vlhkostí, nízkém osvětlení a dalšími omezujícími faktory. Těmto parametrům nejlépe vyhovuje IP kamera Vivotek IP8332.

VIVOTEK IP8332 je zapouzdřena do odolného krytu s IP66 a je vhodná pro různé venkovní aplikace. Je vybavena snímačem umožňující snímat rychlostí 30 fps při rozlišení 1280x800 pixelů. S cílem přizpůsobit se měnícím se světelným podmínkám je IP kamera vybavena odnímatelným IR filtrem a IR osvětlovačem účinným až do 15m.

Obr. 17. VIVOTEK IP8332.

Vivotek IP8332 podporuje průmyslový standard H.264 a kodeky MPEG-4, MJPEG, čímž se výrazně sníží velikost souborů za účelem zachování šířky pásma sítě. Kodeky jsou kompatibilní a umožňují zasílání streamů v různých formátech a rozlišeních.

IP kamera VIVOTEK IP8332 obsahující řadu dalších pokročilých funkcí jako je detekce pohybu, včetně detekce sabotáže dále podporu napájení IEEE 802.3af PoE, podporu SDHC (Secure Digital High Kapacity) paměťových karet, ukládání videa na video rekordér a další.

Pro záznam videostreamu je vhodné použít IPCorder KNR-410 firmy Koukaam, které nabízí záznamové řešení pro systémy IP kamer. Tento rekorder se vyznačuje snadnou obsluhou, stabilním chodem, nízkou spotřebou a kompaktními rozměry.

Veškerou administraci a prohlížení záznamů provádí uživatel ze svého počítače pomocí webového prohlížeče a to jak na platformě Windows tak Linux, či Apple MacOS bez nutnosti nákupu dalšího software. Systém rekorderu je založen na bázi OS Linuč a dokáže spravovat, sledovat a nahrávat videostream, až z 24 IP kamer.

Obr. 18. IPCorder KNR-410.

Tento datový proud se ukládá na 4 x SATA a 2 x eSATA pevné disky s kapacitou do 8 TB. Pro síťové připojení využívá port o rychlosti 10/100/1000 Mbps.

7.3.5 GSM gateway

GSM brána je zařízení využívající k přenosu dat mobilní síť. Prvotní předpokladem pro její funkci musí být SIM karta, která zabezpečuje komunikaci poskytovatele mobilních služeb a uživatele. V zásadě se GSM brány používají pro komunikaci bezpečnostních zařízení, k dálkovému ovládání zařízení nebo pro využívání pevných telefonu jako mobilů.

Typy GSM bran:

- analogové brány – využívají analogový výstup pobočkové telefonní ústředny. Výrazným způsobem šetří hovory finanční náklady na hovory z klasických telefonů na mobilní
- ISDN brány – jsou připojené pomocí rozhraní digitálního rozhraní ISDN
- VoIP brány – umožňuje přímé volání z IP telefonu do sítě GSM.

VoIP GSM brány

VoIP GSM brány jsou IP systémy využívající LCR (Least Cost Routing) k nákladově efektivnímu volání z IP telefonu do GSM sítě. Podmínkou pro úspěšnou funkci je také podpora signalizačního protokolu SIP nebo H.323.

Jako vhodné řešení ve firmě KPB Intra s.r.o. je využít navrhovaný směrovač Cisco 2821 ve formě SIP proxy serveru, na kterém běží softwarová verze PBX (Private Branch Exchange) a optimální přídavnou VoIP GSM brány podporující Cisco CallManagerem.

2N® VoiceBlue Lite je GSM/UMTS brána navržená s cílem co nejvyšší úspory nákladů. Kromě hlasu, odesílání a přijímání SMS zpráv, uchovávání záznamů o hovorech má řadu dalších pokročilých funkcí.

Obr. 19. 2N® VoiceBlue Lite

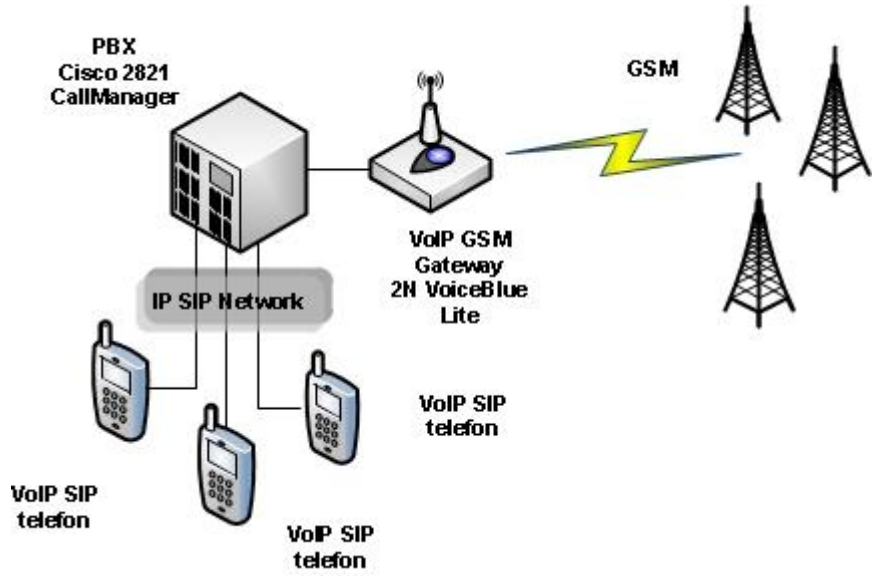
Pro komunikaci využívá 4 hlasové kanály a síťové protokoly TCP, UDP, IP, RTP.

Kódování hlasu se děje prostřednictvím kodeků G.711, G.729 a G.723.

Modul podporuje pásma 850/900/1800/1900 MHz pro GSM služby a pásma 1900/2100 MHz pro UMTS služby.

Připojení k LAN je realizováno konektorem RJ-45 10Base-T a pro konfiguraci se využívá konektor RS 232 – AT rozhraní a rozhraní USB 1.1 typ B. K maximálnímu využití frekvenčního pásma a zaručení kvality hovoru slouží externí anténa připojená do antenního konektoru SMA. Spolu s tímto konektorem se zde nachází i čtyři sloty na SIM karty.

2N VoiceBlue Lite GSM brána je možné využívat v režimu Point-to-Point nebo v režimu Point-to-Multipoint se SIP Proxy serverem.



Obr. 20. Režim Point-to-Multipoint [12].

V režimu Point-to-Point může VoiceBlue Lite komunikovat pouze s jedním SIP VoIP telefonem nebo jiným SIP VoIP zařízením. V tomto režimu má VoiceBlue Lite nastavenu jako IP adresu Proxy serveru vždy IP adresu protější strany.

V Point-to-Multipoint režimu může být SIP proxy serverů (softwarová verze PBX) více. Je možné využít více zdrojových (například VoIP telefony) a stejně tak více cílových zařízení (například VoiceBlue Lite). Schéma distribuované VoIP sítě s jedním (Obr. 20) nebo více SIP Proxy servery odpovídá režimu Point-to-Multipoint. Na těchto serverech běží softwarová verze PBX, která se stará o veškerou signalizaci v VoIP. Pro směrování hovorů se využívá vnitřního směrovacího algoritmu LCR. SIP proxy server udržuje databázi klientů, sestavení, ukončování a udržování spojení a směrování hovorů. VoIP GSM brána 2N VoiceBlue Lite se chová jako koncové zařízení SIP sítě a přijímá požadavky na hovory a na základě vnitřní tabulky LCR směruje do GSM sítě [12].

Blízká budoucnost

Dalším možným řešení VoIP přístupu do GSM je hybridní technologie, která umožňuje využívat GSM telefon jako přístupové zařízení pro spojení s bezdrátovým přístupovým bodem WiFi. V případě, že je telefon mimo dosah bezdrátového přístupového bodu WiFi dojde k přesměrování na GSM síť.

Tato technologie musí mít zabudovanou podporu UMA (Unlicensed Mobile Access). Základní myšlenka UMA spočívá v tom, že se do jednoho přístroje integruje telefon

umožňující volání v síti GSM a zařízení, které umožňuje bezplatné telefonování v rámci budovy přes VoIP. UMA je řešení 3GPP, které realizuje mobilní přístup prostřednictvím místní WLAN. Tato technologie propojuje mobilní telefon, IP přístupovou síť a MSC (Mobile Switching Centre) daného operátora mobilní sítě. Hlasová signalizace i vlastní provoz GSM se přenáší prostřednictvím tunelů přes IP síť do domény mobilního provozovatele. Při pohybu uživatele mezi oblastmi pokrytí WiFi a GSM se síť sama postará o bezproblémové předávání uživatele.

Nevýhodou jsou koncová mobilní zařízení, které musí být speciální, nestačí obecně jakýkoli GSM mobil podporující současně WiFi.

Nutnost používat speciální mobil je největším nedostatkem uvedené metody poskytování mobilních služeb na bázi konceptu UMA. Existuje řešení, které umožňuje využít obecně jakýkoli GSM mobil. V tomto případě se domácí základnová stanice (femto buňka) chová jako základnová stanice sítě GSM v tom smyslu, že používá stejná licenční pásma a stejné přenosové protokoly a techniky, jen je menší než klasická BTS (Base Transceiver Station). Domácí základnová stanice je připojena k počítačové síti a jejím prostřednictvím s MSC. Mobilní telefon buňku automaticky rozpozná a bude ji preferovat před klasickou BTS.

8 ADRESACE A BEZPEČNOST

8.1 Adresace

Pro připojení k veřejné síti Internet bude využíván překlad adres NAT a to jak z důvodu zajištění vyšší bezpečnosti, tak z důvodu šetření veřejných IP adres. Poskytuje též základní sdílení zátěže pomocí funkce distribuce zátěže TCP. NAT umožňuje připojit do sítě Internet i privátní internetové sítě, které používají neregistrované IP adresy. Na druhou stranu nevýhodami převodu adres NAT je nefunkčnost některých aplikací, nemožnost sledovat IP adresu mezi koncovými zařízeními a zpoždění v cestě směrování.

V případě firmy KPB Intra s.r.o. lze využít rozsah privátních IP adres třídy A 10.0.0.0 až 10.255.255.255. Z návrhu masky podsítě 255.255.255.0 je možné následně získat

$2^{16} = 65536$ podsítí a $2^8 - 2 = 254$ platných hostitelů v každé podsíti.

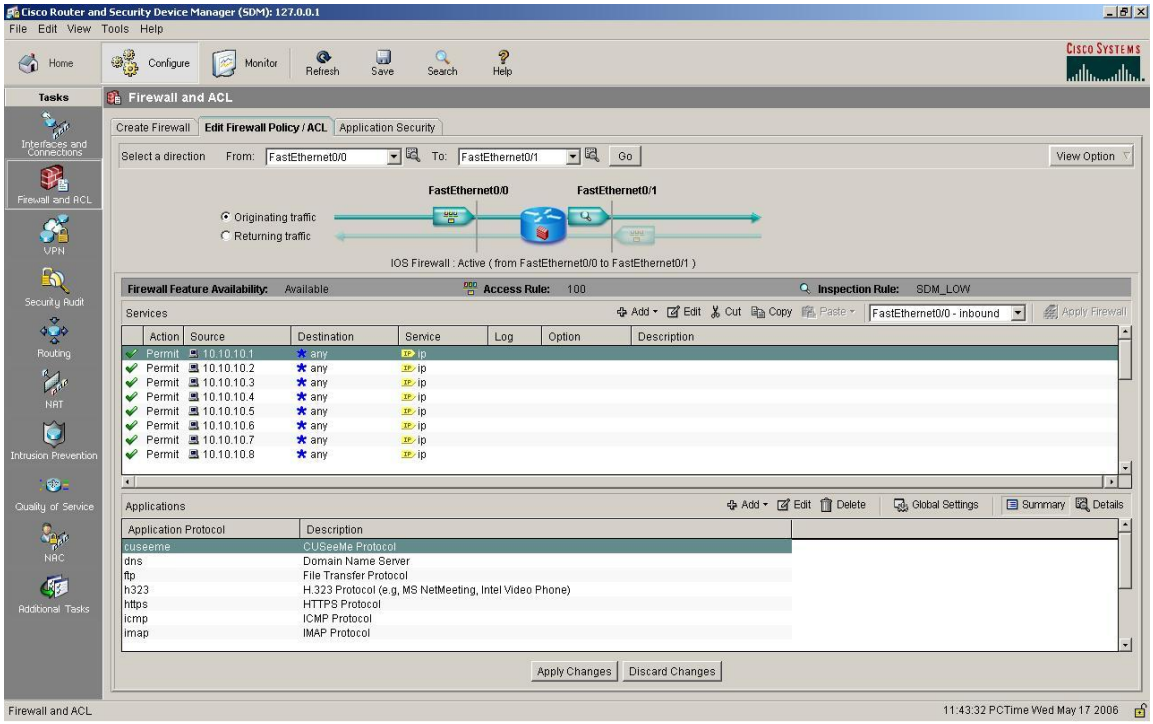
Tab. 15. Adresní prostor.

	Subnet01	**Subnet02**	**Subnet03**	**...**
Adresa podsítě	10.1.0.0	10.1.1.0	10.1.2.0	...
První hostitel	10.1.0.1	10.1.1.1	10.1.2.1	...
Poslední hostitel	10.1.0.254	10.1.1.254	10.1.2.254	...
Broadcast	10.1.0.255	10.1.1.255	10.1.2.255	...

8.2 Bezpečnost

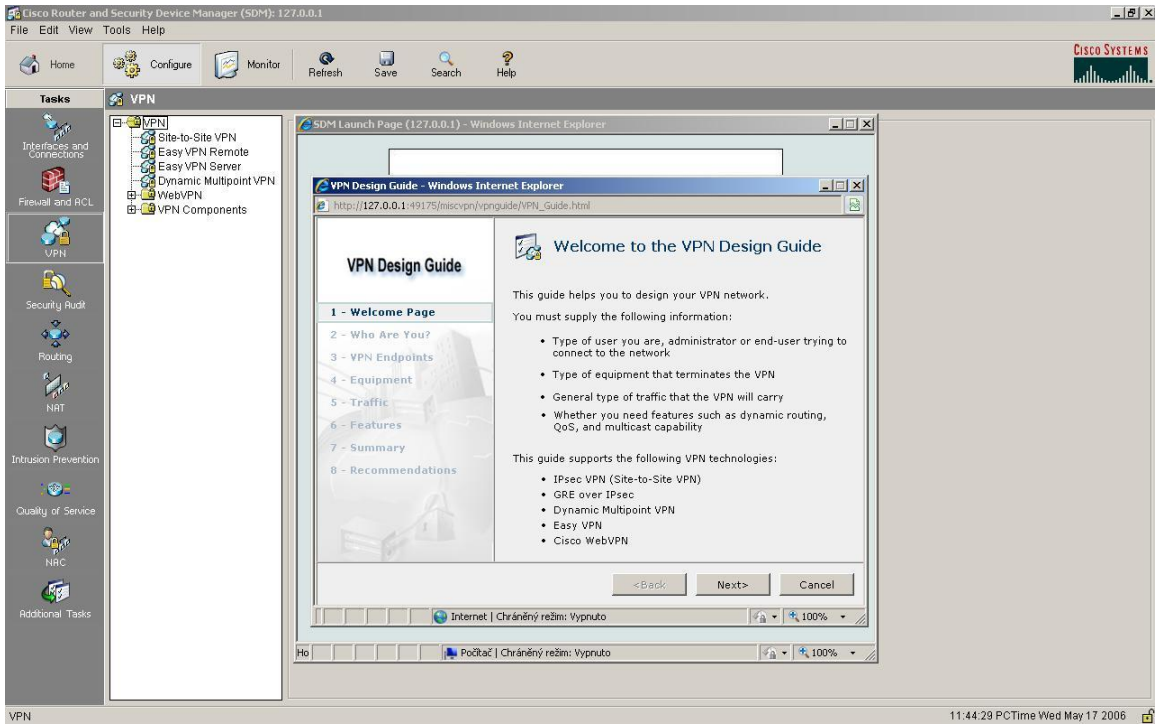
Pro uživatelsky přátelskou konfiguraci směrovačů bez nutnosti využívat CLI, nabízí Cisco nástroj SDM (Secure Device Manager). Tento webový nástroj zjednodušuje nastavení prostřednictvím inteligentních průvodců, umožňuje implementovat a monitorovat přístup k Cisco směrovačům.

Kromě konfigurace jednotlivých rozhraní, lze pomocí tohoto nástroje nastavit veškeré bezpečnostní prvky včetně QoS, VPN, IPS, NAT firewallu, demilitarizované zóny a ACL.



Obr. 21. Nastavení DMZ a ACL pomocí nástroje SDM.

Cisco SDM umožňuje konfigurovat a monitorovat směrovač ze vzdálených míst pomocí protokolu SSL a vytvořit tak zabezpečené připojení prostřednictvím Internetu, mezi uživatelem, prohlížečem a směrovačem.



Obr. 22. Nastavení VPN pomocí nástroje SDM.

9 KONFIGURACE AKTIVNÍCH PRVKŮ

Pro konkrétní nastavení jednotlivých portů, firewallu, přístupových tabulek, překladačů NAT, bezpečnostních a monitorovacích funkcí přepínačů a směrovačů můžeme také využívat CLI. Příkazový řádek nám v některých případech poskytuje detailnější možnost nastavení než sofistikované webové nástroje.

9.1 Konfigurace přepínačů

Jádro směrovačů a většiny přepínačů společnosti Cisco tvoří operační systém Cisco IOS (Internetwork Operation System). Samotná konfigurace je realizována připojením přes konzoli směrovače, pomocný port modemu, protokolem Telnet či zabezpečený komunikační protokol SSH. Přístup k CLI se označuje jako relace EXEC.

Konfigurace Cisco směrovačů a přepínačů můžeme provádět v několika uživatelských režimech:

Tab. 16. Hlavní módy přepínačů a směrovačů Cisco.

Režim	**Zobrazení**	**Definice**
Uživatelský režim (EXEC)	SWITCH>	Omezen na základní příkazy pro sledování, je k dispozici ihned po přihlášení.
Privilegovaný režim (EXEC)	SWITCH#	Výchozí mód pro přístup do dalších konfigurací.
Režim globální konfigurace	SWITCH(config)#	V tomto režimu se konfigurují funkce, které ovlivňují celý systém
Režim konkrétní konfigurace	SWITCH(config-if)#	V tomto módu konfigurujeme vlastnosti určitého konkrétního interface
Instalační režim		Interaktivní konfigurační dialog, ke vstupu slouží příkaz *setup*, ukončení CTRL+C

9.1.1 Základní nastavení přepínače Cisco Catalyst 2960-48PST-L

– nastavení lokálního jména přepínače.

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#hostname vyroba01
SWITCH(config)#end
SWITCH#write memory
```

Nastavení lokálního jména přepínače „terminal“

– nastavení vstupní zprávy.

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#banner motd x Neautorizovany pristup x
SWITCH(config)#end
SWITCH#write memory
```

Vstupní zpráva pro uživatele, jenž se snaží připojit k přepínači je označována jako banner. Nejčastěji se využívá vstupní zpráva se zprávou dne MOTD (Message Of The Day)

– nastavení vstupní hesla.

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#enable secret terminal
SWITCH(config)#end
SWITCH#write memory
```

Nastavení hesla „terminal“ v privilegovaném režimu.

– nastavení uživatelského hesla.

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#line aux 0  [console 0, vty 0]
SWITCH(config-line)#password terminal
SWITCH(config-line)#login
SWITCH(config)#end
SWITCH#write memory
```

Nastavení hesla „terminal“ pro přístup v uživatelském režimu přes port konzoly, pomocný port nebo Telnet.

– nastavení SSH šifrované komunikace.

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#ip domain-name kpb.com
SWITCH(config)#crypto key generate rsa generel – keys modulus 1024
SWITCH(config)#ip ssh time-out 60
SWITCH(config)#ip ssh authentication-retries 2
SWITCH(config)#line vty 0
SWITCH(config-line)#transport input ssh
SWITCH(config-line)#end
SWITCH(config)#end
SWITCH#write memory
```

Připojení pomocí šifrované komunikace SSH a nastavení doménového serveru.

Generování šifrovacího klíče o délce 1024bitů.

Nastavení doby vypršení session a počtu pokusů o přihlášení.

Připojení k lince směrovače a povolení vstupu SSH.

– nastavení IP adres.

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#ip default-gateway 10.1.1.1
SWITCH(config)#interface vlan 10
SWITCH(config-if)#ip address 10.1.2.2 255.255.255.0
SWITCH(config)#end
SWITCH#write memory
```

Nastavení IP adresy brány, čísla VLAN a IP adresy přepínače.

Nastavení portu Cisco Catalyst 2960-48PST-L 10/100 Ethernet

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#interface f0/1
```

Přepnutí přepínače do privilegovaného módu a režimu konfigurace portu 0/1.

```
SWITCH(config-if)#switchport mode access
SWITCH(config-if)#switchport access vlan 10
SWITCH(config-if)#description 3.14
```

```
SWITCH(config-if)#mls qos trust device cisco-phone
```

Zapnutí portu do přístupového módu

Zařazení do patřičné VLAN

Povolení globálního QoS

Nastavení prioritního provozu pro připojené Cisco telefony.

```
SWITCH(config-if)#switchport voice vlan none
```

```
SWITCH(config-if)#switchport priority extend cos
SWITCH(config-if)#spanning-tree portfast
```

Nastavení odesílání paketů z telefonu.

Telefon používá svoje nastavení a priorita portu je na nejvyšší úrovni

Do portu je zapojeno koncové zařízení pro rychlý náběh.

```
SWITCH(config-if)#power inline auto max
SWITCH(config-if)#power inline police
SWITCH(config-if)#end
SWITCH#write memory
```

Nastavení automatického PoE.

V případě překročení výkonového limitu dojde k vypnutí portu.

Návrat do privilegovaného EXEC módu a uložení konfigurace.

Nastavení portu Cisco Catalyst 2960-48PST-L 10/100 Ethernet do režimu Access

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#interface f0/1
```

Přepnutí přepínače do privilegovaného módu a režimu konfigurace portu 0/1.

```
SWITCH(config-if)#switchport mode access
SWITCH(config-if)#switchport port-security
SWITCH(config-if)#switchport port-security mac-address 0023.8B1B.09BF
SWITCH(config-if)#switchport port-security violation shutdown
```

Nastavení portu do režimu Access.

Nastavení povolené MAC adresy.

Vypnutí portu při porušení podmínky a zaslání syslog zprávy.

```
SWITCH(config-if)#end
```

```
SWITCH#write memory
```

Nastavení portu Cisco Catalyst 2960-48PST-L 10/100 Ethernet - analýza síťového provozu pomoci protokolu SPAN

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)# no monitor session 1
SWITCH(config)# monitor session 1 source interface gigabitethernet0/1
SWITCH(config)# monitor session 1 destination interface
gigabitethernet0/2 encapsulation replicate
SWITCH(config)# end
SWITCH#write memory
```

Odebrání existujících SPAN konfigurací.

Specifikace nové SPAN session a monitorovaných portů.

Specifikace SPAN session a nastavení cílového portu.

Nastavení dual-purpose uplink port Cisco Catalyst 2960-48PST-L 10/100/1000 Ethernet - UDLD

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#interface g0/1
SWITCH(config-if)#udld port aggressive
SWITCH(config-if)#end
SWITCH#write memory
```

Sledování konektivity u Fiber Optic pomocí UDLD.

Nastavení podmínky - při přerušení je port vypnut.

Nastavení dual-purpose uplink port Cisco Catalyst 2960-48PST-L 10/100/1000 Ethernet

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#interface g0/1
SWITCH(config-if)#media-type sfp
SWITCH(config-if)#speed nonegotiate
SWITCH(config-if)#duplex full
SWITCH(config-if)#end
```

```
SWITCH#write memory
```

Nastavení typu připojeného modulu, rychlosti a duplexního přenosu.

9.1.2 Nastavení přepínače Cisco Catalyst WS-3750G-12S-S

Základní nastavení přepínače je shodné s Cisco Catalyst 2960-48PST-L. Pro přístup ke konfiguraci je vhodné použít distribuovaný přístupový systém RADIUS. Tento klient/server systém zajišťuje sítě proti neoprávněnému přístupu. RADIUS klienti běží, na podporovaných Cisco směrovačích a přepínačích. Klienti posílat požadavky na ověření na centrální RADIUS server, který obsahuje všechny ověřovací informace uživatelů a síťových služeb. RADIUS hostitel je obvykle víceuživatelský systém běžící na RADIUS serveru jako software od společnosti Cisco (Cisco Secure Access Control Server verze 3.0), Livingston, Microsoft, nebo jiného poskytovatele softwaru.

Pro ověřování v oblasti počítačové bezpečnosti využíváme AAA (Authentication, Authorization and Accounting protocol), autentizační, autorizační a účtovací protokol.

Základní bezpečnostní nastavení Cisco Catalyst WS-3750G-12S-S

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#username admin secret kpb
SWITCH(config)#username admin privilege 15 secret 5
$1$VdJx$jU4LU/TtOsJjd2iHS/gAh0
SWITCH(config)#radius-server host 10.1.2.3 auth-port 1645 acct-port 1646
key 981230167820
SWITCH(config)#aaa new-model
SWITCH(config)#aaa authentication login kpb local group radius
SWITCH(config)#line vty 0
SWITCH(config-line)#login authentication kpb
SWITCH(config-line)#end
SWITCH(config)#end
SWITCH#write memory

SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#aaa authorization exec kpb local group radius
SWITCH(config)#line vty 0
SWITCH(config-line)#authorization exec kpb
SWITCH(config-line)#end
```

```
SWITCH(config)#end
SWITCH#write memory
```

Nastavení lokálního hesla do uživatelského módu šifrovaného pomocí MD5 hash. Nastavení hesla do privilegovaného módu.

Nastavení RADIUS serveru a zapnutí AAA.

Vytvoření přístupové skupiny „kpb“.

Nastavení linky a aplikace autentizačního seznamu.

Konfigurace webové autentizace Cisco Catalyst WS-3750G-12S-S

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#ip admission name accesskpb proxy http
SWITCH(config)#interface f0/1
SWITCH(config-if)#ip admission accesskpb
SWITCH(config)#end
SWITCH(config)#ip device tracking
SWITCH(config)#end
SWITCH#write
```

Konfigurace autentizační role.

Určení rozhraní a konfigurace autentizace na rozhraní.

Zapnutí zařízení ke sledování tabulky.

Konfigurace AAA

```
SWITCH>enable
SWITCH#configure terminal
SWITCH(config)#aaa new-model
SWITCH(config)#aaa authentication login default group radius
SWITCH(config)#aaa authorization auth-proxy default group radius
```

Zapnutí AAA autentizace.

Definování autentizační přístupové metody.

Vytvoření autentizační metody pro webovou autorizaci

Konfigurace RADIUS serveru

```
SWITCH(config)#ip radius source-interface Vlan80
SWITCH(config)#radius-server host 10.1.2.3
```

```
SWITCH(config)#radius-server key rad123
SWITCH(config)#radius-server dead-criteria tries 2
```

Specifikace RADIUS paketů, které mají IP adresu z daného rozhraní.

IP adresa vzdáleného RADIUS serveru.

Nastavení autorizačního a šifrovacího klíče.

Zadání počtu dotazů na RADIUS server před označením, že je nedostupný.

Konfigurace HTTP server

```
SWITCH(config)#ip http server //zapnutí HTTP serveru
SWITCH(config)#ip admission proxy http login page file flash:login.htm
SWITCH(config)#ip admission proxy http fail page file flash:fail.htm
SWITCH(config)#ip admission proxy http login expired page flash
flash:expired.htm
SWITCH(config)#ip admission name AAA_FAIL_POLICY proxy http event timeout
aaa policy identity GLOBAL_POLICY1
SWITCH(config)#ip admission max-login-attempts 10
SWITCH(config)#end
SWITCH#write
```

Zapnutí HTTP serveru a určení výchozí přihlašovací stránky.

Určení náhradní výchozí přihlašovací stránky v případě nedostupnosti.

Určení stránky zobrazené po vypršení timeoutu.

Vytvoření AAA pravidlo v případě selhání AAA serveru.

Nastavení maximálního počtu neúspěšných pokusů o přihlášení.

Konfigurace rozhraní a nastavení VLAN

```
SWITCH>enable
SWITCH# configure terminal
SWITCH(config)#interface t0/2
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.1.1.2 255.255.255.0
SWITCH(config)#end
SWITCH#write memory
```

Nastavení IP adresy a zapnutí rozhraní.

Vytvoření VLAN a statické přiřazení portu

```
SWITCH>enable
```

```
SWITCH#configure terminal
SWITCH(config)#vlan 20
SWITCH(config-vlan)#name test20
SWITCH(config-vlan)#end
SWITCH(config)# interface t0/2
SWITCH(config-if)#switchport mode access
SWITCH(config-if)#switchport access vlan 20
SWITCH(config-if)#end
SWITCH(config)#vtp mode transparent
SWITCH(config)#end
SWITCH#write memory
```

Nastavení ID VLAN.

Nastavení jména VLAN.

Určení portu a nastavení přístupu na port.

Přiřazení portu VLAN.

Nastavení módu VLAN Trunking Protocol.

Konfigurace trunku

```
SWITCH# configure terminal
SWITCH(config)#interface t0/2
SWITCH(config-if)#switchport trunk encapsulation dot1q
SWITCH(config-if)#switchport trunk allowed vlan 20
SWITCH(config-if)#switchport trunk mative vlan 20
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport nonegotiate
SWITCH(config-if)#end
SWITCH(config)#end
SWITCH#write
```

Specifikace Trunk portu.

Nastavení rozlišovací metody VLAN.

Určení nativních a přenášených VLAN.

Nastavení portu do trunku a zrušení automatického vyjednávání pro daný trunk.

Konfigurace ARP

```
SWITCH>enable
```

```
SWITCH#configure terminal
SWITCH(config)#ip igmp snooping
SWITCH(config)#arp access-list host2
SWITCH(config-arp-acl)#permit ip host 10.1.2.3
SWITCH(config-arp-acl)#exit
SWITCH(config)#ip arp inspection filter host2 vlan 1
SWITCH(config)#interface t0/1
```

Zapnutí IGMP na všechny VLAN.

Definování ARP ACL a přepnutí do konfiguračního módu.

Povolení ARP hostitele, aplikace ARP ACL na VLAN.

Ve výchozím nastavení nejsou definovány žádné ARP ACL na žádný VLAN - „host2“ název ALC, vlan 1 číslo VLAN.

Specifikace propojeného rozhraní.

```
SWITCH(config-if)#no ip arp inspection trust
SWITCH(config-if)#ip arp inspection limit rate 1024
SWITCH(config-if)#end
SWITCH(config)#end
SWITCH#write
```

Konfigurace rozhraní jako nedůvěryhodné. Omezení počtu ARP dotazů na 1024.

Konfigurace Port-Based Traffic Control

```
SWITCH#configure terminal
SWITCH(config)#interface t0/1
SWITCH(config-if)#storm-control broadcast unicast level 87.65
SWITCH(config-if)#end
SWITCH(config)#end
SWITCH#write
```

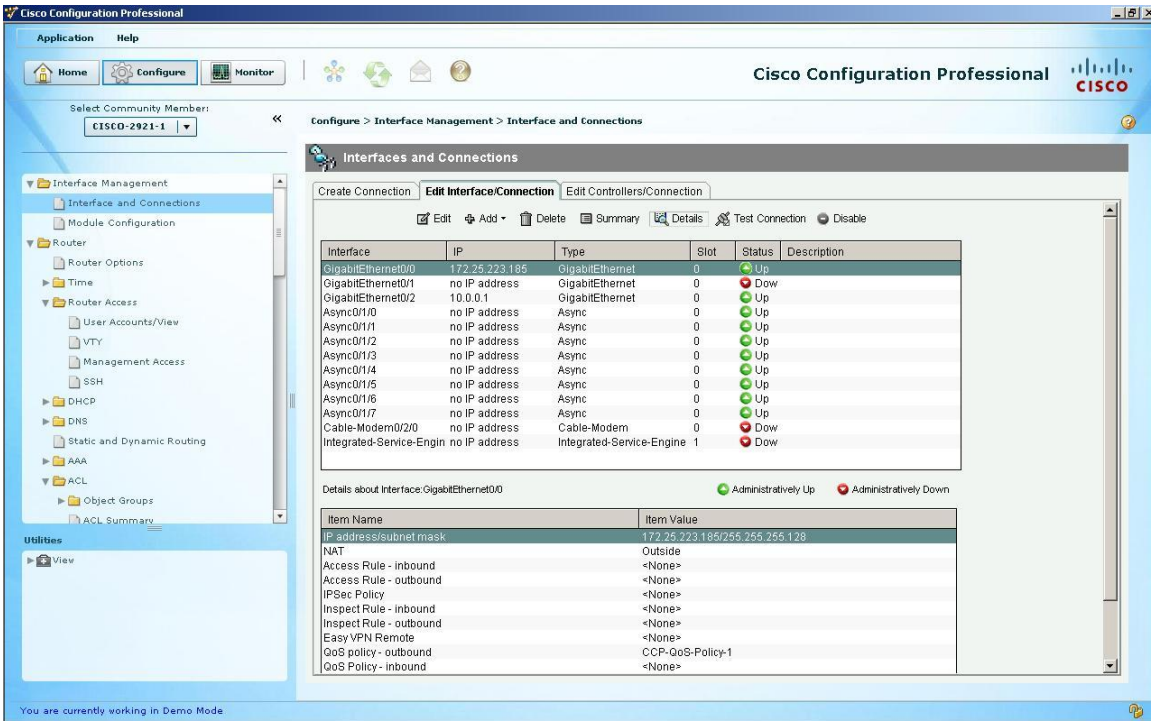
Nastavení kontrolovaných rozhraní.

Nastavení druhu kontroly – broadcast a prahové hodnoty šířky pásma v procentech.

9.2 Konfigurace směrovače

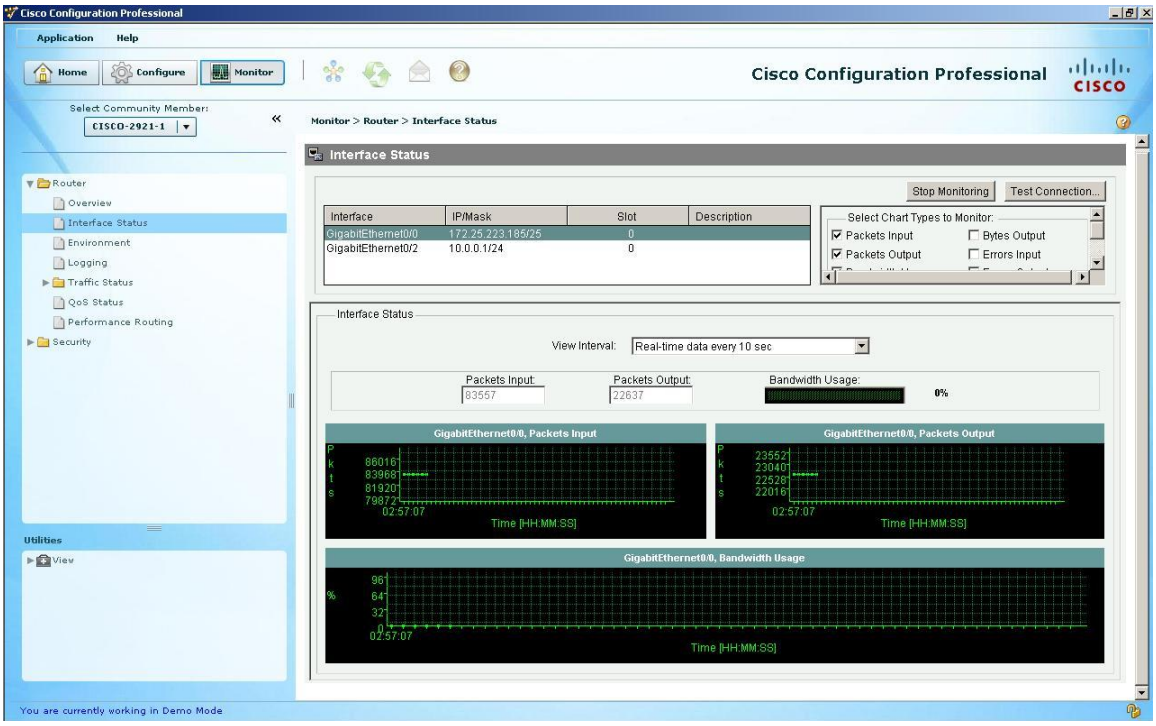
V současné době využívá společnost Cisco k profesionálnímu nastavení směrovačů kvalitní nástroj Cisco Configuration Professional.

Cisco Configuration Professional je GUI (Graphical User Interface) prostředek pro správu, konfiguraci a vzdálené sledování směrovačů Cisco bez použití Cisco IOS CLI. Zjednodušuje nastavení směrovače, firewall, IPS, VPN, WAN, LAN a základní konfiguraci bezdrátových sítí prostřednictvím snadno použitelných průvodců. Jeví se jako vhodný hlavně pro středně velké podniky a pobočky firem. Cisco Configuration Professional má do konfigurace zabudovaný inteligentní systém kontroly nastavení ke snížení počtu chyb z důvodu nesprávné konfigurace.



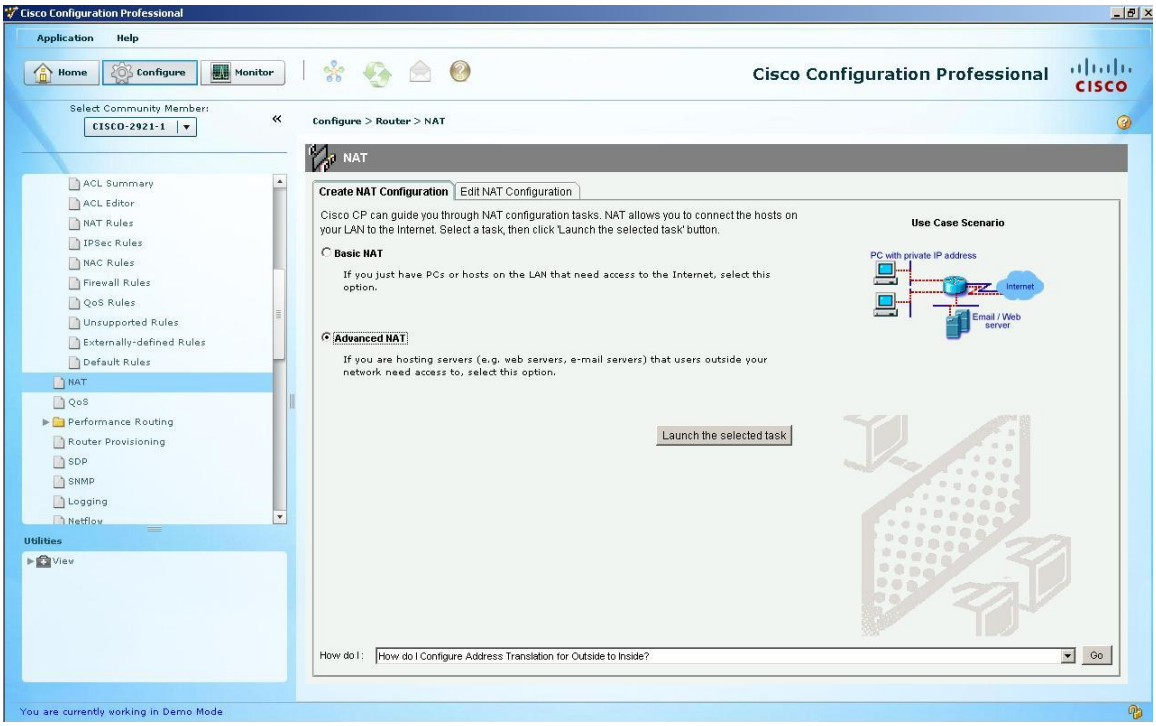
Obr. 23. Konfigurace rozhraní pomocí nástroje Cisco Configuration Professional.

Tento nový správce zařízení Cisco směrovačů s integrovanými službami by měl postupem času nahradit starší nástroje, jako jsou Cisco router nebo SDM.



Obr. 24. Monitorování rozhraní pomocí nástroje Cisco Configuration Professional.

Stejně jako SDM, Cisco Configuration Professional předpokládá obecnou znalost síťových technologií a podmínek. Zcela nenahrazuje CLI, ale je jeho vhodným doplňkem.



Obr. 25. Konfigurace NAT s nástrojem Cisco Configuration Professional.

Důležitou funkcí tohoto konfiguračního nástroje je možnost snadno nastavit Cisco IP telefonii pomocí vzdálené konfigurace Cisco Unified Communications Manager Express pro zpracování hovorů a Cisco Unity Express pro podporu hlasové schránky.

Systém IP telefonie pomocí aplikace Cisco Configuration Professional, lze nakonfigurovat jako samostatnou telefonní pobočku nebo jako vstupní bránu.

Součástí je nastavení vlastnosti potřebných pro nasazení IP telefonie, včetně uživatelů, jednotlivých telefonů, číselných plánů, sdružených skupin, paging skupin, konferencí, interkomu, analogové a digitální linek.

ZÁVĚR

Cílem této práce bylo vytvoření komplexního návrhu informačního systému pro společnost KPB Intra s.r.o.

Při jednání se stávajícím správcem počítačové sítě a vedoucím manažerem firmy, byly stanoveny základní požadavky na novou počítačovou síť, s ohledem na výrobní zaměření společnosti.

Součástí tohoto návrhu bylo i testování stávajícího síťového zabezpečení pomocí softwarového analyzátoru PRTG. Provedené testování ukázalo problémy, se kterými se současná síť potýká. Množina takto získaných informací tvoří jádro konceptu, ze kterého jsem vycházel při tvorbě návrhu.

Výběr aktivních prvků byl omezen finančními možnostmi zadavatele. Proto jsem jako základní stavební prvky sítě, s ohledem také na spolehlivost a informační podporu, navrhl použít přepínače a směrovač firmy Cisco.

V celé síti je plně implementována podpora přenosu hlasu pomocí VoIP. Nastavení přepínačů je optimalizováno také pro přenos videa a jeho ukládání do datového úložiště.

Ochrana počítačové sítě je tvořena směrovačem s firewallem. Přístup k poštovnímu serveru je řešen umístěním do DMZ. Ostatní servery jsou z hlediska vysokorychlostního přístupu připojeny k jádru sítě.

Jako přenosové médium mezi jednotlivými přepínači využívám optické spoje, které jsou svými parametry dimenzovány na rychlost až 10 Gbps. Rovněž metalické propoje je možné použít pro rychlosti vyšší, což umožní i další informační rozvoj firmy.

Požadavky pro budoucí vývoj a navýšení rychlosti přenosu, je možné splnit pouhou výměnou aktivních prvků, při zachování stávající kabeláže.

Takto navržená síť plně vyhovuje stanoveným požadavkům ze strany zákazníka a současně umožňuje svou koncepcí i její další rozšiřování.

CONCLUSION

The aim of this thesis was to develop a comprehensive information system for company KPB Intra s. r. o.

Basic requirements for a new computer network have been established when dealing with the current computer network administrator and the head manager with respect to company´s production.

Part of this proposal was testing network security using a software analyzer PRTG. Testing showed the problems which current network is facing. Set of information thus obtained forms the core of concept in which I relied on when formulating the draft.

Selection of the components was limited due to submitter´s financial possibilities. Therefore, I proposed to use the switch and router of company Cisco as the basic structural element of network with regard to reliability and information support.

There is fully implemented support for voice transport by force of VoIP. Switch settings are also optimized for video transmission and for data stacking in data storage.

Protection of computer network consists of router with firewall. Access to the mail server is solved by placing it into DMZ. In terms of high speed access the other servers are connected to the network core.

As the transmission medium between the switches I use the optical links which are designed with the parameters to speed up to 10 Gbps. It is also possible to use metallic interconnection for higher speed which will allow further development of the company.

Requirements for future development and increase of transmission speed can be achieved by changing the active components while maintaining current wiring.

In this manner proposed network fully meets the stated requirements specified by the costumer and also allows further expansion.

SEZNAM POUŽITÉ LITERATURY

[1] SOSINSKY, Barrie. *Mistrovství-počítačové sítě.* 1.vydání. Brno: Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.

[2] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z.* 2. vydání. Brno: Computer Press, 2006. 432 s. ISBN 80-251-1278-0.

[3] HORÁK, Jaroslav; KERŠLÁGER, Milan. *Počítačové sítě pro začínající správce.* 4. vydání. Brno: Computer Press, 2008. 328s. ISBN 978-80-251-2073-6.

[4] LAMMLE, Todd. *CCNA Cisco Certified Network Associate: Výukový průvodce přípravou na zkoušku 640-802.* 1. vydání. Brno: Computer Press, 2010. 928 s. ISBN 978-80-251-2359-1.

[5] OREBAUGH, Angela, et al. *Wireshark a Ethereal: Kompletní průvodce analýzou a diagnostikou sítí.* 1. vydání. Brno: Computer Press, 2008. 448 s. ISBN 978-80-251-2048-4.

[6] TEARE, Diane. *Návrh a realizace sítí Cisco: Autorizovaný výukový průvodce.* 1. vydání. Brno: Computer Press, 2003. 758 s. ISBN 80-251-0022-7.

[7] WALLACE, Kevin. *VoIP bez předchozích znalostí.* 1. vydání. Brno: Computer Press, 2007. 232 s. ISBN 978-80-251-1458-2.

[8] MAČEK, Karel. *Návrh překryvné VoIP sítě na stávající ISDN síť.* Zlín, 2008. 69s. Diplomová práce na Fakultě aplikované informatiky Univerzity Tomáše Bati ve Zlíně. Vedoucí diplomové práce Ing. Miroslav Matýsek Ph.D.

[9] PÁV, Miroslav; SYŘÍNEK, Jan; HOŠKOVÁ, Jana. *CCNA Exploration - Základy sítí* [online]. Plzeň: VOŠ a SPŠE Plzeň, 2010 [cit. 2011-02-27]. Dostupné z WWW: <http://download.fw.sk/up/knihy/CCNA_Exploration_1_0.pdf>.

[10] *Microsoft TechNet: Resource for IT Professional* [online]. c2011 [cit. 2011-02-27]. Transportní režim. Dostupné z WWW: <http://technet.microsoft.com/cs-cz/library/cc739674(WS.10).aspx>.

[11] *IP kamery pro zabezpečovací a dohledové systémy: netcam.cz* [online]. c2007 [cit. 2011-02-27]. Dostupné z WWW: <http://www.netcam.cz>.

[12] *2N-Telekomunikační řešení na míru pro firmy i operátory po celém světě* [online]. 2010 [cit. 2011-03-26]. Dostupné z WWW: <http://www.2n.cz/cz/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization, Accounting
ACL	Access Control List
AD	Administrative Distance
AES	Advanced Encryption Standard
AES	Advanced Encryption Standard
AH	Autentication Header
AIM	Advanced Interface Module
ARP	Address Resolution Protocol
BGP	Border Gateway Prokol
BID	Bridge ID
BPDU	Bridge Protocol Data Units
BTS	Base Transceiver Station
CAN	Campus Area Network.
CCMP	Counter Cipher Block Chaining Message Authentication Code Protocol
CCTV	Closed Circuit Television
Cisco IOS	Internetwork Operation System
CLI	Command-Line Interface
CME	CallManager Express
CoS	Class of Service
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance.
CUE	Cisco Unity Express
DAI	Dynamic ARP Inspection
DHCP	Dynamic Host Configuration Protocol

DMZ	Demilitarized Zone
DNS	Domain Name System
DTP	Dynamická Trunking Protocol
DV	Distance Vector
EAP	Extensible Authentication Protocol
EGP	Externet Gateway Protokols
ESP	Encapsulation Security Payload
EVM	Extension Voice Module
FC	Fixed Connection
FOCIS	Fiber Optic Connector Intermateability Standard
FTP	File Transfer Protocol
FXS	Foreign Exchange Station
FXO	Foreign Exchange Office
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
HWIC	High-Speed WAN Interface Card
CHAP	Challenge Handshake Authentication Protocol
ICMP	Internet Control Messge Protocol
ICV	Integrity Check Value
IDS	Intrusion Detection Systems
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protokols
IGRP	Interior Gateway Routing Protocol
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol

IP	Internet Protokol.
IPS	Intrusion Protection Systems
IPSec	Internet Protocol Security Architekture
ISR	Integrated Service Router
JPEG	Joint Photographic Experts Group
LAN	Local Area Network.
LC	Lucent Connector
LCR	Least Cost Routing
LED	Light Emitting Diode.
LMS	LAN Management Solution
LOMMF	Laser optimized multi-mode fiber
LSOH	Low Smoke Of Halogen
MAC	Media Access Control.
MAN	Metropolitan Area Network.
MCGP	Media Control Gateway Protocol
MDIX	Automatic Media-Dependent Interface Crossover
MIC	Message Integrity Code
MITM	Man-In-The-Middle
MM	Multi Mode
MSTP	Multiple Spanning Tree Protocol
MSC	Mobile Switching Center
MTRJ	Mechanical Transfer Registered Jack
NAM	Network Analysis Modul
NAS	Network Attached Storage
NAS	Network Access Server

NAT	Network Address Translation
NME	Network Module Ethernet
OSI	Open Systems Interconnection
OSPF	Opne Shortest Path First
PAE	Port Access Entity
PAP	Password Authentication Protocol
PBX	Private Branch Exchange
PiMF	Paar in MetallFolie
PoE	Power over Ethernet
POP3	Post Office Protocol version 3
PSK	Pre-Shared Key
PVDM	Packet Voice Digital Module
QoS	Quality of Service.
RADA	Radius Authenticated Device Access
RIP	Routing Information Protokol
RJ-45	Registered Jack – 45.
RMON	Remote Network MONitoring
RSPAN	Remote Switch Port Analyzer
RSTP	Rapid Spanning Tree Protocol
RTP	Realtime Transport Protokol
SAN	Storage Area Network
SC	Subscriber Connector
SDHC	Secure Digital High Capacity
SDM	Secure Device Manager
SFP	Small Form-Factor Pluggable

SIP	Session Initiation Protocol
SM	Single Mode
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPA	Switched Port Analyzer
SPI	Security Parametr Index
SPI	Stateful Packet Inspection
SPQ	Strict Priority Queuing
SRR	Shaped Round Robin
SRST	Survivable Remote Site Telephony
SSL	Secure Sockets Layer
SSH	Secure Shell
STP	Shielded Twisted Pair.
STP	Spanning Tree Protokol
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protokol.
TKIP	Temporary Key Integrity Protokol
TLS	Transport Layer Security
TTL	Time To Live
UDP	User Datagram Protokol
UMA	Unlicensed Mobile Access
UTP	Unshielded twisted-pait.
VCSEL	Vertical-Cavity Surface-Emitting Laser
VIC	Voice Interface Card
VLAN	Virtual LAN

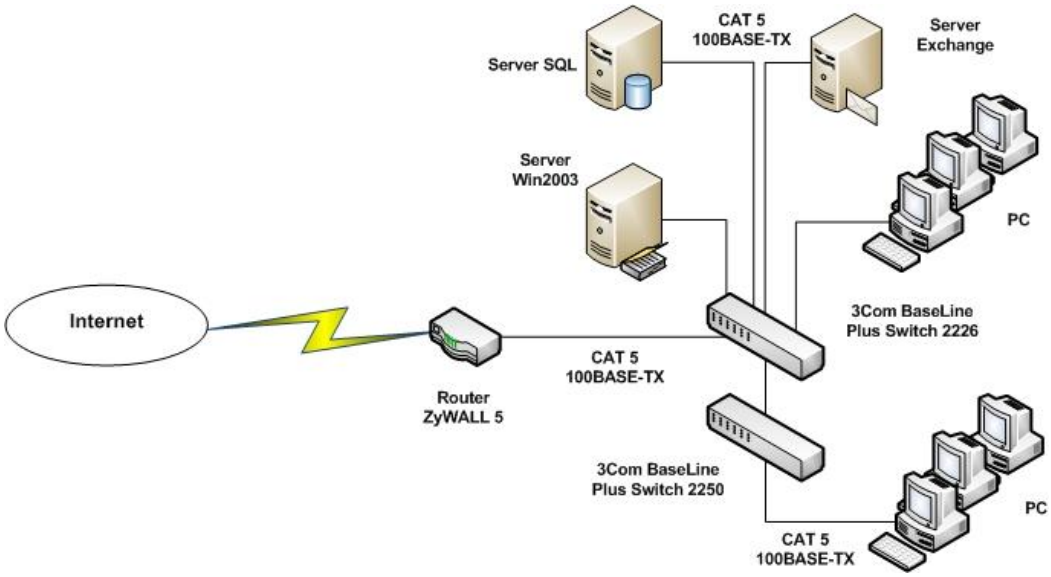
VoIP	Voice over Internet Protokol
VPN	Virtual Private Network
VTP	VLAN Trunkig Protokol
WAN	Wide Area Network.
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
Wi-Fi	Wireless-Fidelity Protected Access
WLAN	Wireless LAN
WTD	Weighted Tail Drop
XML	Extensible Markup Language

SEZNAM OBRÁZKŮ

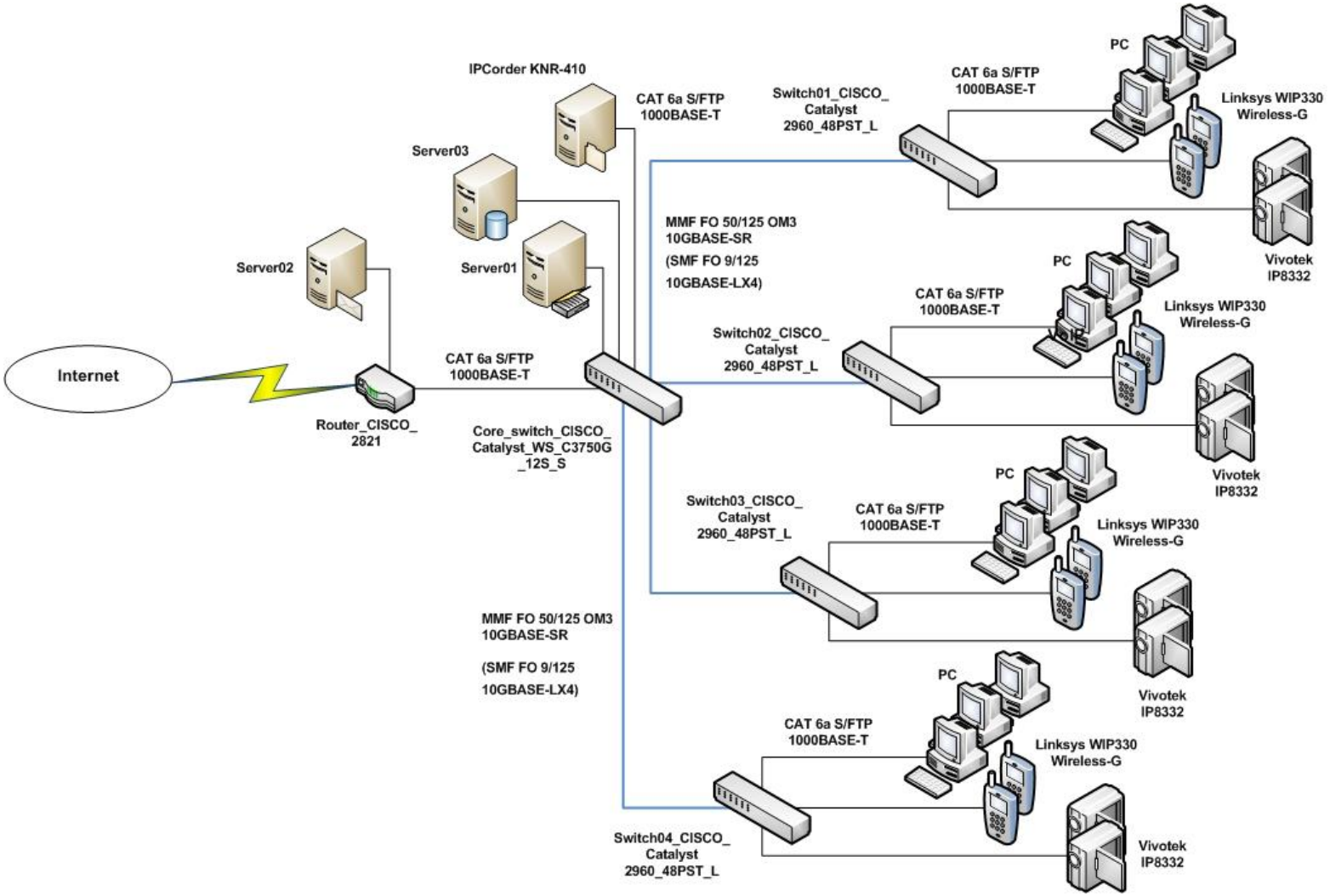
SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: SOUČASTNÁ STRUKTURA POČÍTAČOVÉ SÍTĚ FIRMY KPB INTRA S.R.O.



PŘÍLOHA P II: NOVĚ NAVRŽENÁ STRUKTURA POČÍTAČOVÉ SÍTĚ FIRMY KPB INTRA S.R.O.



PŘÍLOHA P III: SCHÉMA DATOVÝCH ROZVADĚČŮ FIRMY KPB INTRA S.R.O.