

Inovácia firemnej počítačovej siete

Corporate computer network innovation

Bc. Michal Mikula

Diplomová práca
2013



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Michal Mikula**
Osobní číslo: **A11494**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Informační technologie**
Forma studia: **kombinovaná**

Téma práce: **Inovace firemní počítačové sítě**

Zásady pro vypracování:

1. Zpracujte literární rešerši na dané téma.
2. Navrhnete výkonnější strukturu sítě a nakonfigurujete nové aktivní prvky sítě od firmy Cisco, včetně Firewallu.
3. Porovnejte strukturu staré a nové sítě, včetně použitých aktivních prvků.
4. Navrhnete zabezpečení Vámi inovované sítě, včetně způsobu monitorování intranetu.
5. Konfiguraci aktivních prvků inovované sítě ověřte na Cisco zařízeních Cisco Akademie FAI.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. CISCO. Cisco Systems [online]. 2013 [cit. 2013-02-02]. Dostupné z: <http://www.cisco.com/en/US/hmpgs/index.html>
2. NORTH CUTT, Stephen a Lenny ZELTSER. Bezpečnost sítí: velká kniha. Vyd. 1. Brno: CP Books, 2005, 589 s. ISBN 80-251-0697-7.
3. DONAHUE, Gary A. Kompletní průvodce síťového experta. Vyd. 1. Brno: Computer Press, 2009, 528 s. ISBN 978-80-251-2247-1.
4. FRAHIM, Jazib a Omar SANTOS. Cisco ASA: all-in-one firewall, IPS, Anti-X, and VPN adaptive security appliance. 2nd ed. Indianapolis: Cisco Press, 2010, 1119 p. ISBN 15-870-5819-7.
5. KÁLLAY, Fedor a Peter PENIAK. Počítačové siete a ich aplikácie. Žilina: EDIS, 1998. ISBN 80-7100-380-8.
6. SOSINSKY, Barrie. Mistrovství počítačové sítě. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.
7. THOMAS, Thomas M. Zabezpečení počítačových sítí bez předchozích znalostí. Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.
8. TRULOVE, James. Síť LAN: hardware, instalace a zapojení. Vyd. 1. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.

Vedoucí diplomové práce:

Ing. Miroslav Matýsek, Ph.D.

Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce:

22. února 2013

Termín odevzdání diplomové práce:

22. května 2013

Ve Zlíně dne 22. února 2013

prof. Ing. Vladimír Vašek, CSc.
děkan



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

ABSTRAKT

Cieľom práce bolo inovovať počítačovú sieť podniku, tak aby zohľadňovala moderné trendy z oblasti počítačových sietí.

V práci sa kladie dôraz na kvalitu služieb poskytovaných sieťou a jej dostupnosti aj v prípade nečakaných okolností. Firma pre ktorú je inovácia siete vykonávaná, požaduje také riešenie, ktoré v prípade potreby umožní firemnú sieť kedykoľvek jednoducho rozšíriť. Použitie bezdrôtových technológií je vyžadované aj v procese výroby a preto sa počítalo s rozšírením podnikovej Wifi siete aj do týchto priestorov. Pri procese inovácie sa museli do návrhu zapracovať aj spôsoby pripojenia druhej budovy a jej implementácia do podnikovej siete. Zabezpečiť vnútornú sieť podniku a zároveň umožniť prístup na verejne dostupný webový server bolo tiež súčasťou novo navrhutej sieťovej štruktúry. Monitorovanie siete spolu s možnosťou vzdialeného prístupu určite napĺňa aj tie najvyššie požiadavky na modernú počítačovú sieť.

Kľúčové slová: LAN, WIFI, Firewall, VPN, DMZ

ABSTRACT

This thesis focus on the innovation of corporate computer network so that it will make provision for the new trends of computer networking.

This proposal focus on quality of services what network offers to end user during unexpected circumstances. The company which network is innovated need solution when they are able to extend their layout in anytime when they need. Wireless technology is important during production process and then company WIFI must be extended to this area, too. The innovation have to cover of connection method of the second building directly to company network. The network protection and externall access to company web server is one part of this thesis. Network monitoring and remote access are last important parts what all modern networks should have.

Keywords: LAN, WIFI, Firewall, VPN, DMZ

Touto cestou by som sa chcel poďakovať svojmu vedúcemu diplomovej práce pánovi Ing. Miroslavovi Matýskovi, Ph.D. za jeho odborné, pomocné a iné rady vďaka ktorým som mohol úspešne dokončiť tvorbu tejto diplomovej práce. Ďalej ďakujem môjmu zamestnávateľovi, ktorý ma poveril prestavbou firemnej počítačovej siete a zároveň mi umožnil túto realizáciu popísať do tejto práce. Zároveň ďakujem svojej rodine a kolegom v práci za podporu a vytvorenie podmienok vďaka ktorým som sa mohol venovať štúdiu na FAI.

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	10
I. TEORETICKÁ ČASŤ	11
1 FYZICKÉ PRVKY SIETE	12
1.1 KRÚTENÁ DVOJLINKA.....	12
1.1.1 Zakončenie kabeláže	13
1.2 OPTICKÝ KÁBEL	14
1.2.1 Stavba optického kábla.....	14
1.2.2 Prenos dát po optickom kábli	16
1.2.3 Optické konektory	17
1.3 PASÍVNY A AKTÍVNY ROZBOČOVAČ.....	18
1.4 PREPÍNAČ	18
1.5 SMEROVAČ.....	19
1.6 VIACVRSTVOVÉ PREPÍNAČE.....	20
1.7 BEZDRÔTOVÉ PRÍSTUPOVÉ BODY.....	21
1.8 FIREWALL.....	22
2 REFERENČNÝ MODEL OSI	23
2.1 POPIS JEDNOTLIVÝCH VRSTIEV OSI.....	24
2.1.1 Aplikačná vrstva.....	24
2.1.2 Prezentačná vrstva.....	24
2.1.3 Relačná vrstva	24
2.1.4 Transportná vrstva.....	25
2.1.5 Sieťová vrstva	25
2.1.6 Spojová vrstva.....	26
2.1.7 Fyzická vrstva.....	26
3 REFERENČNÝ MODEL TCP/IP	27
3.1 POPIS JEDNOTLIVÝCH VRSTIEV TCP/IP.....	28
3.1.1 Aplikačná vrstva TCP/IP.....	28
3.1.2 Transportná vrstva TCP/IP.....	28
3.1.3 Sieťová vrstva TCP/IP	29
3.1.4 Fyzická vrstva TCP/IP.....	29
3.2 PROTOKOL IP	29
3.2.1 Protokol IP verzia 4.....	30
3.2.2 Adresovanie v IPv4	30
3.3 POTOKOL TCP.....	32
3.3.1 Štruktúra protokolu TCP.....	32
3.3.2 Prenos dát pomocou TCP protokolu	33
3.4 PROTOKOL UDP.....	33
3.4.1 Prenos dát pomocou protokolu UDP.....	34

3.5	PROTOKOL IPV6	34
4	LOKÁLNA POČÍTAČOVÁ SIĚŤ	35
4.1	ŠTANDARD 802.3	35
4.1.1	Ethernet rámec.....	37
4.2	VIRTUÁLNA LOKÁLNA SIĚŤ.....	38
4.2.1	Trunk	38
4.3	SPANNING TREE PROTOKOL.....	39
4.4	PREPÍNACIE METÓDY RÁMCOV	41
4.5	SMEROVANIE V LOKÁLNEJ POČÍTAČOVEJ SIETI	41
4.6	PRENOS HLASU POMOCOU INTERNET PROTOKOLU	42
4.7	KVALITA SLUŽIEB.....	43
5	BEZDRÔTOVÉ SIETE.....	45
5.1	KOMUNIKÁCIA PO BEZDRÔTOVEJ SIETI	45
5.2	RÁMEC 802.11	47
5.3	ŠTANDARDY	47
5.4	OCHRANA BEZDRÔTOVÝCH SIETÍ.....	49
5.4.1	Autentifikácia 802.1X.....	50
5.4.2	Šifrovanie komunikácie v bezdrôtových sieťach	51
5.4.3	Generovanie kľúčov	52
6	ZABEZPEČENIE POČÍTAČOVÝCH SIETÍ.....	53
6.1	FIREWALL.....	53
6.2	PRÍSTUPOVÉ ZOZNAMY	55
6.3	DEMILITARIZOVANÁ ZÓNA	56
6.4	VPN.....	57
6.5	PREKLAD SIEŤOVÝCH ADRES	58
II.	PRAKTICÁ ČASŤ	59
7	PÔVODNÝ STAV FIREMNEJ SIETE	60
7.1	ZARIADENIA NACHÁDZAJÚCE SA NA SIETI	60
7.2	POŽIADAVKY NA NOVÚ POČÍTAČOVÚ SIĚŤ	61
8	NOVÝ STAV FIREMNEJ SIETE.....	63
8.1	ADRESOVANIE VO VNÚTORNEJ SIETI.....	63
8.2	ZÁSADY PRE POMENOVANIE ZARIADENÍ NA SIETI	64
8.3	NÁVRH TOPOLOGIE LAN.....	65
8.3.1	Prenosové média	65
8.3.2	Aktívne prvky siete	65
8.3.3	Základné ovládanie zariadení Catalyst.....	68

8.4	TOPOLÓGIA BUDOVY A	69
8.4.1	Základné nastavenie prepínačov	70
8.5	TOPOLÓGIA BUDOVY B.....	74
8.6	VZÁJOMNÉ PREPOJENIE BUDOV	75
8.7	SMEROVANIE V SIETI	75
8.7.1	Smerovanie v rámci budovy.....	75
8.7.2	Smerovanie medzi budovami	76
8.8	BEZDRÔTOVÁ SIEŤ.....	77
8.8.1	Prístupový bod.....	77
8.8.2	Požiadavky na bezdrôtovú sieť	78
8.8.3	Realizácia bezdrôtovej siete	79
8.8.4	Konfigurácia prístupových bodov	81
8.9	OCHRANA SIETE	85
8.9.1	Ochrana vo vnútornej sieti	85
8.9.2	Ochrana vnútornej siete.....	85
8.10	PRÍSTUP DO DMZ.....	88
8.11	VPN.....	91
9	MONITOROVANIE SIETE	94
9.1	APLIKÁCIA OPENNMS	94
9.2	APLIKÁCIA CISCO NETWORK ASSISTANT	95
	ZÁVER	97
	CONCLUSION	98
	ZOZNAM POUŽITEJ LITERATÚRY	99
	ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK.....	101
	ZOZNAM OBRÁZKOV	104
	ZOZNAM TABULIEK	105
	ZOZNAM PRÍLOH.....	106

ÚVOD

Predtým než začnú zariadenia navzájom komunikovať musia si dohodnúť pravidlá, na základe ktorých bude uskutočňovaná vzájomná výmena informácií. Komunikáciu možno chápať za úspešnú, ak správa bude doručená a príjemca správne pochopí to, čo odosielateľ posielal. Problém môže nastať ak máme v sieti nejaký faktor, ktorý môže brániť úspešnej komunikácii. Tieto faktory môžu byť vonkajšie ako počet zariadení cez ktoré musí správa prejsť kým sa dostane do cieľa. Ďalej to môže byť počet naraz prenášaných správ v danej sieti. Okrem toho ešte existujú vnútorné faktory, ktoré sa zameriavajú na formát posielanej správy. Po sieti sú prenášané rôzne typy správ, ktorých štruktúra môže byť viac aj menej zložitá. Dôležitá komunikácia potrebuje viac prostriedkov na zabezpečenie doručenia ako napríklad správy, ktoré sú prenášané ako čistý text. Medzi hlavné interné faktory patrí veľkosť, zložitosť a dôležitosť prenášanej správy. Napríklad veľkosť správy má veľký význam pre prenos informácie, pretože táto správa môže byť v rôznych bodoch siete prenášaná rôznym spôsobom. Štandardizácia týchto faktorov môže výrazne pomôcť prenášať dáta spoľahlivo, rýchlo a bezpečne.

V dnešnej dobe Internetu nie je problém prenášať rôzne typy dát z jednej strany zeme na jej opačnú stranu. Počítačové siete musia podporovať širokú paletu aplikácií a služieb, ktoré sú prenášané na rôznych typoch fyzickej infraštruktúry. Dôležitým predpokladom je, že Internet je odolný proti chybám. Predpokladáme, že je vždy dostupný pre milióny používateľov a jeho architektúra umožňuje pri výpadku jednej cesty vytvoriť inú cestu a dáta po nej úspešne preniesť. Túto vlastnosť spôsobujú redundantné cesty medzi zdrojom a cieľom komunikácie. Dobre navrhnutá sieť umožňuje jednoduché a rýchle rozšírenie, či už pridaním nového zariadenia, rozšírením služieb, alebo umožnením prístupu pre nových používateľov. Takéto rozšírenie by malo nastať bez prerušenia u zvyšku siete a teda bez obmedzenia pre používateľov. Aplikácie dostupné pre používateľa, majú veľké požiadavky na kvalitu prenášania a doručovania informácií. Hlas a video prenos vyžadujú taký prenos, kde nebude nastávať prerušovanie, ktoré potom obmedzuje alebo úplne znemožňuje využívanie takejto služby. Internet sa vyvinul z malej a kontrolovanej počítačovej siete, ktorá spájala vzdelávacie a vládne inštitúcie, pre ktoré zaistovala vzájomnú komunikáciu. Bezpečnosť a ochrana súkromia sú nevyhnutným dôsledkom prenášania a výmeny citlivých osobných, alebo firemných informácií vo svete Internetu. Neustály nárast komunikácie je potrebné chrániť a ochranné metódy implementovať priamo do sieťovej architektúry.

I. TEORETICKÁ ČASŤ

1 FYZICKÉ PRVKY SIETE

Komunikácia začína správou, ktorá musí byť doručená do svojho cieľa. Prenos správy obsahuje tri základné elementy. Prvým je zdroj správy, teda odosielateľ, ktorým môže byť človek odosielajúci dáta z počítača. Druhým elementom je príjemca, ktorý predstavuje cieľ doručenia správy. Tretím elementom je médium tvoriace trasu, po ktorej sa správa prenáša od zdroja do svojho cieľa.

Všetky správy prenášané pomocou počítačovej siete sú prevedené do binárnych čísiel nazývaných bity a tie sú kódované do signálov, ktoré dokážu byť prenášané cez dané médium. V počítačových sieťach to môžu byť vodivé káble, optické káble, alebo bezdrôtové siete. V tejto práci bude sieť predstavuje priestor, ktorý bude schopný prenášať komunikáciu rôzneho druhu po rôznych typoch prenosového média, prípadne ich kombináciou.

1.1 Krútená dvojlinka

Najčastejšie používanou kabelážou pre počítačové siete je krútená dvojlinka. Môže slúžiť pre prenos analógového, ale aj digitálneho signálu. V starej telefónnej linke sa používali dva krútené páry, kde sa využil iba jeden kábel z páru. Prirodzenou vlastnosťou krúteného kábla je, že znižuje vplyv externých magnetických a elektrických polí a tým bráni interferenciám signálov medzi jednotlivými drôťmi. Zakrútené káble majú zvýšenú odolnosť voči súhlasnému typu rušenia, pretože vplyvom opačnej fázy sa rušenie eliminuje. Krútená dvojlinka sa najčastejšie používa pri ethernetových počítačových sieťach. Krútená dvojlinka sa skladá z jedného alebo viacerých párov izolovaných vodičov, ktoré sú skrútené dohromady a obalené plášťom. Hlavnými parametrami sú priemer vodiča, typ vodiča, počet závitov, typ izolácie, charakteristická impedancia a typ plášťa. Vodič môže byť lanko alebo plný drôt, ktorý sa používa pre káble zakončené do nejakej zásuvky, alebo zárezového bloku. Lanko sa používa pre koncové a prepojovacie káble. Zakončenie môže byť šesťpinový, alebo osempinový modulárny konektor. Najviac používané rozdelenie krútenej dvojlinky je nasledovné:

- Netienená krútená dvojlinka.
- Tienená krútená dvojlinka.

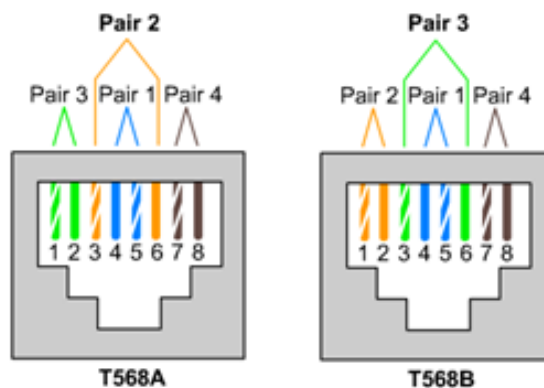
Netienená krútená dvojlinka označovaná ako UTP (Unshielded Twisted Pair) je kábel, ktorý nemá dodatočné tienenie. Tieto káble sú veľmi obľúbené v rôznych typoch sietí a sú štandardom asociácie EIA/TIA (Electronic Industries Alliance / Telecommunications Industry Association).

Tienená krútená dvojlinka ScTP (Screened Twisted Pair) je označovaná viacerými skratkami v závislosti od spôsobu tienenia. Pokiaľ je kábel tienový jednoduchou fóliou, označuje sa ako FTP (Foil Twisted Pair), alebo opletaním STP (Shield Twisted Pair). Obe tienenia musia byť na konci uzemnené. Samotná krútená dvojlinka redukuje rušenie signálu po celej svojej dĺžke. Tienené káble trpia rušením a degradáciou signálu spôsobenou elektromagnetickou interferenciou na koncoch kábla. Čím je kábel viac obtočený na jednotku svojej dĺžky, tým je viac odolnejší voči rušeniu. Najčastejšie sa ako izolácia používa polyvinylchlorid (PVC), ktorý je dostatočne ohybný. Ďalším materiálom je propylén (FEP), ktorý je menej ohybný, ale splňuje požiadavku nízkej horľavosti, vďaka ktorej je možné tieto káble použiť napríklad vo ventilačných systémoch.

Ďalším typom krútenej dvojlinky sú prepojovacie a užívateľské káble. Najčastejšie to je kus ohybného kábla, ktorý má na oboch koncoch osempinovú koncovku. Niekedy sa prepojovací kábel nazýva patch kábel, pretože sa používa na prepojenie dvoch patch panelov, alebo na prepojenie patch panela a rozdeľovača. Tieto káble môžu byť tienené, ale aj netienené. Užívateľské káble sú vlastne koncové káble určené pre pripojenie počítača alebo sieťového zariadenia. Rozdiel medzi prepojovacím káblom a užívateľským káblom je iba v jeho dĺžke. Označenia jednotlivých častí kabeláže je dôležité pri testovaní siete. Ich presnú definíciu je možné nájsť v štandarde TIA-568-C.1 oddiel 11. Dĺžka kábla je rôzna, pretože závisí od použitia a umiestnenia kábla.

1.1.1 Zakončenie kabeláže

Sieťová kabeláž môže byť zakončená viacerými spôsobmi. Na stole, alebo v stene budeme mať modulárne zásuvkové kryty. V serverovni, alebo v racku bude kabeláž zakončená patch panelom, alebo zárezovým blokom. Štandard TIA-568-C popisuje dva rôzne spôsoby zapojenia a to TIA-568-A a TIA-568-B. Líšia sa len umiestnením druhého a tretieho páru. Nie je žiaden rozdiel medzi verziami A a B, pokiaľ sú obe strany zapojené rovnako.



Obr. 1. Schéma zapojenia podľa TIA [1].

Obe schémy zapojenia podľa TIA sa dajú považovať za univerzálne, pretože zahŕňajú všetkých osem pinov a dajú sa použiť pre Ethernet, Token Ring, ISDN, T1 a ATM-PMD. Pre dátové siete sa používajú modulárne konektory, ktoré najčastejšie obsahujú od štyroch do osem pozícií a od dvoch do osem pinov. Označujú sa USOC (Universal Service Order Code) kódom RJ, pomlčka číslo špecifikujúce rozmer konektora. Osempinová modulárna zástrčka je popísaná v štandarde IEC 603-7 a predpis je v TIA-568-C, ISO/IES IS-11801. Modulárny pin je plochý kontakt s hrotom, ktorý prepichne izoláciu vodiča a elektricky sa spojí s jeho vodivým stredom.

1.2 Optický kábel

Je prenosové médium vyrobené z oxidu kremíka, plastu, alebo skla. Optický prenos pozostáva zo zdroja svetla, detektora, kábla zloženého z optického vlákna. Zdroj musí vysielat' svetelné pulzy (signály), ktoré keď sú zachytené, predstavujú hodnotu jedna a tiež zapnuté. Absencia signálu je hodnota nula a aj vypnuté. Čím rýchlejšie je možné zdrojom generovať svetelné pulzy, tým viac dát je možné optickým vláknom preniesť. Optické káble nie sú ovplyvnené rádiovým a elektromagnetickým rušením. Dôležitým problémom pri optických vláknoch oproti medeným káblom je ich krehkosť. Existujú dva zdroje generujúce svetelné pulzy. Prvým je LED (Light Emitting Diode) a polovodičová dióda.

1.2.1 Stavba optického kábla

Jadro je extrudovaný materiál o šírke 50 alebo 62,5 μm (mikrometrov). Svetelný vodič je potiahnutý refrakčným povlakom s nižším indexom lomu ako má samotné jadro. Povlak

obsahujú všetky optické vlákna a niekedy sa mu hovorí aj plášť. Úlohou plášťa je udržať svetlo v jadre a po celej dĺžke kábla ho odrážať späť. Vláknó a plášť majú spoločne 125 mikrometrov. Podľa TIA/EIA-568-C má mať vlákno rozmer 62,5/125 μm a typ 50/125 μm sa nachádza v TIA/EIA-568-B. Medzi ďalšie používané rozmery patria 85/125 μm a 100/245 μm . V rámci jednej siete je vhodné používať jeden typ vlákna, aby prechody medzi vláknami rôzneho typu nespôsobovali zbytočné straty. Dokonca aj zdroje a detektory svetla bývajú optimalizované pre vlákno konkrétnej veľkosti a typu. Ak by sme použili vlákno inej veľkosti, môžeme časť signálu stratiť, alebo kvôli zlému spojeniu môže komunikácia úplne zlyhať.

U nás sa používajú jednovidové (single-mode) a viacvidové vlákna (multi-mode). Rozdiel je v tom ako sa vo vlákne šíri svetelný lúč. Jednovidové vlákno má úzke jadro do ktorého sa dostane iba úzky zväzok svetla. Širšie jadro má viacvidové vlákno a tým sa do neho zmestí akoby niekoľko vidov svetla. Tieto sa potom šíria na základe už spomínaného odrazu od steny jadra. Jednovidové vlákno má jadro o priemere 4 až 8 μm a plášť s priemerom 125 μm . Okrem toho sa viacvidové vlákna delia podľa indexu lomu svetla a to na vlákna s plynulou zmenou indexu lomu a na vlákna so skokovou zmenou indexu lomu. Pri skokovej zmene sa lúče svetla na rozhraní plášťa a jadra prudko odrazia späť. U plynulej zmene sa index lomu mení plynulejšie a lúče sa skôr ohýbajú. Jednovidové vlákno má obrovskú šírku pásma, ale kvalita signálu je akceptovateľná na kratšie vzdialenosti. Okrem TIA mnohovidové optické vlákna konkrétne štandardizuje ITU-T a to dokumentom G.651.1 pre 50/125 μm . ITU neštandardizuje vlákno 62,5/125 μm a konkrétny štandard nájdeme v dokumentácii 492AAA-A od TIA. Jednovidové vlákno popisuje štandard G.652 od ITU-T. Dosah viacvidového vlákna pri rýchlosti 1Gbit/s je 600 metrov a pri jednovidovom vlákne môžeme počítať s dosahom až niekoľko kilometrov. Útlm v jednovidovom vlákne spôsobuje farebný rozptyl, kde pre rôzne vlnové dĺžky dochádza k inému lomu svetla. Viacvidové vlákna ovplyvňuje modálny rozptyl, kde pri ceste signálu po vlákne sa postupom času rýchlosť rôznych módov svetla mení a so zvyšujúcou sa vzdialenosťou sa tieto módy stretávajú. Kvôli tomu sa optické káble vyrábajú tak, že index lomu sa vo vlákne postupne mení a práve preto existujú vlákna so skokovou a krokovou zmenou indexu lomu, ale iba jednovidové vlákno používa len krokovú zmenu indexu lomu. Duplexný režim je pri optických kábloch zabezpečený združením vláknien do dvojíc. Tieto dvojice môžu byť potom spojené s ostatnými optickými

káblami umiestnenými v jednej trubici. Samotný kábel môže byť pevný, alebo ohybný. Trubice s pevnými káblami sa používajú mimo budovy na prepojenie väčšej vzdialenosti. Ako izolácia sa používajú materiály podobné s izoláciou pre metalické káble. Poznáme dva druhy optických káblov s ohľadom na ich ochranu.

Prvý typ sú káble s tesnou sekundárnou ochranou, je to plastová vrstva, ktorá optické vlákno oddeľuje od ostatných vrstiev a chráni vlákno po ich odstránení. Ak majú káble viacej vlákien, tak každé vlákno má svoju vlastnú tesnú sekundárnu. Ak by sme takýto kábel chceli zakončiť, musíme odstrániť vonkajší obal až po tenké ohybné vlákno, ktoré pozostáva z jadra, obalu, primárnej ochrany a tesnej sekundárnej ochrany. Pre odstránenie tesnej sekundárnej ochrany sa používajú špeciálne nástroje, ktoré ju dokážu odstrániť tak, aby nedošlo k poškodeniu optického vlákna. Pred skrátením a napojením optického konektora sa vlákno očistí vhodným rozpúšťadlom.

Posledným typom sú káble s voľnou sekundárnou ochranou, kde sú holé vlákna potiahnuté primárnou ochranou a uložené voľne vo vnútri plastovej trubky. V trubke môže byť jeden až dvanásť vlákien. Niekoľko takýchto trubiek môže byť osadených do jedného plášťa. Ak kábel naraz obsahuje jednovidové a viacvidové vlákna, ale každý typ v samostatnej trubke, tak hovoríme o hybridných kábloch. O odľahčenie ťahu a uloženie prebytočného kábla sa stará špeciálny box určený na zakončovanie optických káblov.

1.2.2 Prenos dát po optickom kábli

Kvalitne vyrobené optické vlákna dokážu svetlo prenášať na veľké vzdialenosti s veľmi malými stratami. Optické rozhrania sú väčšinou simplexné, teda jednosmerné, pretože dokážu buď iba vysielať, alebo iba prijímať, ale nie oboje naraz. Obojsmerné duplexné spojenie vyžaduje dva spoje. Optické vlákna sa kvôli tomu používajú v pároch a sú označené podľa toho, či slúžia na posielanie, alebo prijímanie dát. Vysielací je označený ako Tx (transmit) a prijímajúci je označený Rx (receive). Existuje spôsob ako na jednom vlákne zabezpečiť duplexné spojenie, ak pre prijímajúci a vysielací lúč použijeme inú vlnovú dĺžku a oddeľujeme ich pomocou špeciálnej optiky. Táto metóda sa nazýva multiplexovanie delením vlny (WDM). Pre prenos dát je kritická aj presnosť prepojenia optických zariadení. Kvalitu prenosu vyjadruje efektívna šírka pásma konkrétneho kábla a počíta sa ako šírka pásma na kilometer deleno skutočná dĺžka kábla v km.

Tab. 1. Šírka pásma pre viacvidové vlákna [2].

priemer vlákna / obal [μm]	použitá vlnová dĺžka [nm]	Šírka pásma [MHz]
50/125	850	500
50/125	1300	500
62,5/125	850	160
62,5/125	1300	500

Použité materiály prepúšťajú signál s malými stratami, ktoré sa nazývajú útlm. Je výsledkom odchýlky a absorpcie. Odchýlka je vychýlenie dráhy svetla od ideálnej dráhy a absorpcia je spôsobená prímiesami a nečistotami v použitom materiály. Svetlo sa prenáša jadrom kábla z jedného konca na druhý a pritom sa odráža od hraníc medzi vrstvami s rozdielnym indexom lomu. Úroveň ohybu závisí od indexu lomu. Ak uhol pri ktorom lúč vstupuje do prostredia prekročí medznú hodnotu, tak lúč svetla sa namiesto ohnutia odrazí naspäť. Jednovidové vlákno prepúšťá malý rozsah vlnovej dĺžky, ale pre viacvidové vlákna existuje viacero ciest, kde je každá určená svojím uhlom lomu, alebo módom, odborne vidom. Pri zväčšujúcej sa vzdialenosti jednotlivé vidi spolu inreferujú, pretože rozdiel medzi indexami lomu sa ostro mení na pomerne krátkej vzdialenosti nazývanej krokový index.

1.2.3 Optické konektory

Pre optické káble existujú rôzne typy konektorov a najčastejšie používané pre lokálne siete sa označujú SMA, ktorý je šrobovací a má dva podtypy 905 a 906. Druhý je konektor s priamym dotykom ST (straight tip), tretí je SC (subscriber connector) a posledným typom konektoru je LC (Lucent connector). Konektory SMA a ST sa zapojujú samostatne a tým môže nastať prehodenie prijímacieho a vysielacieho vlákna. Podobne ako konektor SMA aj konektor ST sa kvôli bajonetovej konštrukcií musí po nasunutí pootočiť. Aby nedošlo k prehodeniu vlákien, vynikol ďalší typ konektoru SC ako štandard IEC 61754-4 a TIA/EIA-568. Výhodou je zapojenie zasunutím a odpojenie vytiahnutím konektora a kvôli tomu, že nie je potrebné nič pootočiť, tak je možné zapojiť dva konektory súčasne. Dva konektory SC sú buď ako dva samostatné konektory, alebo sú spojené duplexnou sponkou a označujú sa ako 568SC. Úplne novým typom optických konektorov sú takzvané

kompaktné konektory SFF (Small Form Factor) a tie mali vyriešiť problém SC konektora, ktorý bol veľký a zaberol veľa miesta. Štandard TIA-568-C.3 definoval základné požiadavky pre kompaktné konektory. Zarovnanie optických častí musí vyhovovať príslušnému dokumentu FOCIS (Fiber Optic Connector Standard) a konektor musí dodržať orientáciu A/B. Okrem toho majú kompaktné konektory zámok, ktorý zabezpečí správne nasadenie konektora a následne ho drží na mieste. Ak z nejakého dôvodu potrebujeme previesť optický signál na signál prenášaný metalickým vedením alebo naopak, môžeme použiť média konvertor, teda optický prevodník.

1.3 Pasívny a aktívny rozbočovač

Rozbočovač (HUB) predstavuje spôsob vzájomného prepojenia sieťových káblov a to tak, aby ho bolo možné zopakovať na všetky ostatné pripojené káble rozbočovača. Sú to veľmi jednoduché zariadenia, ktoré prijatý signál na ľubovoľnom porte zopakuje na všetky ostatné porty. Rozbočovače sú transparentné zariadenia, ktoré nemedia rámce a ostatné zariadenia na sieti o ich prítomnosti nevedia. Pracujú na prvej vrstve a všetky zariadenia pripojené do rozbočovača patria do jeden kolíznej domény. Pasívny rozbočovač je taký, ktorý nijako nezosilňuje signál ktorý ním prechádza. Jedinou výhodou rozbočovača je jeho schopnosť kopírovať dáta všesmerovo, čo prepínače emulujú funkciou zrkadlenia portov (port mirroring). Aktívny rozbočovač je zariadenie fyzickej vrstvy a zväčšuje dosah pomocou zosilnenia a synchronizácie signálu predtým, než ho pošle ďalej. Pri veľkej vzdialenosti môže signál strácať kvalitu a opakovač signál prepošle ďalej s opravenou fázou a frekvenciou. Používanie opakovača v sieti má za následok mierne zdržanie signálu, ktorému sa hovorí propagačné zdržanie. Dnes už sa rozbočovače používajú iba ak je to naozaj nevyhnutné.

1.4 Prepínač

Prepínač (switch) je aktívne zariadenie pracujúce na fyzickej, dátovej a v niektorých prípadoch aj na sieťovej vrstve OSI modelu. Kvôli minimalizovaniu kolízií prepínač pracuje tak, že každý sieťový segment má svoju vlastnú kolíznú doménu a šírku pásma, čím je bez kolízie s inými portami prepínača a pri tom pracuje v plne duplexnom režime. Určiť kam sa má prenášaný rámec v sieti preniesť, prepínač určí na základe informácie uloženej v prenášanom rámci. Ethernet rámec obsahuje zdrojovú a cieľovú MAC (Media

Access Control address) adresu. Prepínač dokáže rámec otvoriť a prečítať cieľovú adresu, ktorú potom porovná so svojou tabuľkou adres. Pokiaľ sa daná adresa v tabuľke nenachádza, prepínač si ju do nej pridá. Táto tabuľka MAC adres obsahuje aj výstupný port smerovača, cez ktorý sa dá dostať k cieľovej adrese. Pokiaľ prepínač nevie cez ktorý port sa k cieľovej MAC dostane, rámec sa odošle cez všetky porty okrem toho, cez ktorý bol rámec prijatý. Ak chce nejaké zariadenie používajúce IP protokol poslať paket na IP adresu z rovnakého rozsahu, tak ako prvé musí zistiť MAC adresu cieľa. Toto sa uskutoční odoslaním požiadavky ARP (Address Resolution Protocol), ktorý je všesmerový a odoslaný na všetky porty prepínača. ARP paket potom obsahuje informáciu o MAC adrese a prepínač už potom vie, ktorým smerom sa majú dáta posielat'. CISCO prepínače môžeme rozdeliť na dva typy. Prvým typom sú prepínače s pevnou konfiguráciou a štandardne obsahujú len Ethernet porty. Druhým typom sú prepínače pracujúce aj na vyšších sieťových vrstvách. Najpoužívanejšie sú prepínače Cisco Catalyst 2950, 2960, 3650 a 3750. Posledné dva prepínače sa dajú stohovať, to znamená spojenie viacerých prepínačov dohromady a tým by tvorili jeden logický celok ovládaný ako jedno zariadenie. Výhodou modulárnych prepínačov Cisco je ich väčšia rozšíriteľnosť. Jedným z takých prepínačov je Cisco Catalyst séria 6500, pre ktoré existuje veľké množstvo spolupracujúcich modulov. Moduly môžu obsahovať buď len Ethernet porty, alebo poskytovať iné služby ako modul FWSM, slúžiaci na poskytovanie firewallových služieb a iných, ktoré sú mimo rozsah obvyčajného prepínača.

1.5 Smerovač

Smerovač (router) je zariadenie, ktoré prepája minimálne dve siete s rôznym sieťovým rozsahom. Funguje na tretej sieťovej vrstve a rozdeľuje kolízne domény, filtruje vysielanie a zabezpečuje smerovanie paketov do cieľa. V smerovačoch sa používajú veľmi zložité algoritmy, ktoré optimalizujú výkon siete a preto smerovač pozostáva z dvoch oddelených funkčných systémov, nazývaných riadiaca úroveň a doručovacia úroveň. Tieto úrovne sa starajú o výber portu a odoslanie dát na správne výstupné rozhranie. Riadiaca úroveň spolupracuje s inými sieťovými zariadeniami a jej výsledkom je smerovacia tabuľka spolu s trasami pre doručovanie. Obsahuje aj funkcie blokovania, kvality služieb a filtrovania. Smerovacia tabuľka je skupina adres určujúcich jednosmernú komunikáciu s koncovými bodmi siete. Manuálne je možné smerovaciu tabuľku doplniť pridaním statickej cesty,

alebo doplniť pravidlá pre používanie týchto statických ciest. Smerovacia tabuľka sa nazýva aj база smerovacích informácií RIB (Routing Information Base). Navyše niektoré smerovače obsahujú aj базу informácií o doručovaní FIB (Forwarding Information Base), ktorá je uložená v rýchlo dostupnej pamäti. Druhou variantou sú takzvané plávajúce statické adresy (floating static routes). Najčastejšie ale smerovače fungujú v dynamickom režime, kde si viacero smerovačov navzájom vymieňa informácie o logickej úrovni siete. Vďaka tomu môžu uprednostňovať určité trasy v sieti. Smerovače dokážu ešte jednu často využívanú funkcionálnu a to sú logické rozhrania priradené tým fyzickým, pričom sa s nimi pracuje úplne rovnako ako s fyzickými. Doručovacia úroveň preveruje pakety na vstupnom rozhraní a prenáša ich na správne výstupné rozhranie. Aby sa dáta mohli preposielať súčasne, tak viacero doručovacích úrovní smerovača je prepojených do kríža. Pri doručovaní sa v tabuľke hľadá záznam obsahujúci sieťový identifikátor, alebo MAC adresu výstupného rozhrania. Pre väčšiu bezpečnosť smerovače obsahujú pravidlá, ktoré určujú aké pakety majú byť smerované a aké nie. Tie, ktoré sa odfiltrujú, budú zahodené a ich zdroju sa neposiela žiadna informácia o vykonaní tejto akcie. Existuje niekoľko algoritmov, podľa ktorých sa smerovač riadi pri zahadzovaní paketov. Najčastejšie algoritmy sú:

- Algoritmus RED (Random Early Detection) – Monitorovanie veľkosti fronty a zahadzovanie paketov nastáva na základe štatistickej pravdepodobnosti. Ak zdroj generuje veľké množstvo dát, tak má väčšiu pravdepodobnosť zahodenia paketov.
- Adaptívny algoritmus RED – Obsahuje premenlivú štatistickú pravdepodobnosť zahrňujúcu prioritu paketov.
- Algoritmus Tail Drop – Meria obsah vyrovnávajúcej pamäte a ak prekračuje maximálnu úroveň, tak prichádzajúce pakety zahodí.

Smerovač dokáže vykonávať segmentáciu paketov, ktorá ale môže ovplyvniť výkonnosť siete.

1.6 Viacvrstvé prepínače

Tradičný prepínač pracuje na druhej vrstve OSI modelu. V dnešnej dobe už tieto prepínače skoro dokážu to čo smerovače. Dokážu spracovávať protokoly až po siedmu vrstvu a aj ich testovanie. Najväčšou výhodou viacvrstvého prepínača MLS (Multi-Layer Switch) je

smerovanie medzi virtuálnymi sieťami. Po pridaní virtuálneho rozhrania, ktoré je viazané na danú virtuálnu sieť, vznikne prepínané virtuálne rozhranie SVI (Switched Virtual Interface). V takomto prepínači už od výroby existuje jedno prepínacie rozhranie pre virtuálnu sieť číslo jedna, ktoré sa nedá vymazať. MLS smerovače Cisco fungujú tak, že najprv sa musí vytvoriť virtuálnu sieť, ktorej priradíme nejaké číslo. Ďalej musíme vytvoriť virtuálny interfejs s číslom virtuálnej siete. Teraz už máme vytvorené virtuálne prepínané rozhranie fungujúce na druhej vrstve, kde ešte prepínač medzi nimi nesmeruje. Na to, aby smerovač začal medzi nimi smerovať v zmysle smerovania, na tretej vrstve musíme virtuálnemu rozhraniu prideliť IP adresu. Často sa ešte pridávajú fyzické porty na prepínači do požadovanej virtuálnej siete. Najznámejšie modely prepínačov sú Catalyst série 3500, 3700 a veľmi výkonné určené pre datacentra sú série 4500, 6500.

1.7 Bezdrôtové prístupové body

Bezdrôtový prístupový bod AP (Access Point) je kombináciou prijímacieho a odosielacieho zariadenia. Umožňuje pripojenia používateľov do počítačovej siete bez nutnosti používania káblov. Je to bod, kde končí metalické vedenie a začína bezdrôtový prenos. Prenos dát vzduchom sa vykonáva za pomoci rádiových vln, ktoré sa vhodne namodulujú. Rádiové vysielanie sa uskutočňuje na určitej frekvencii, ktorá sa nazýva nosná. Nosné frekvencie sú rôznymi zákonmi rozdelené do pásiem a každé pásmo je určené pre konkrétnu službu. Niektoré pásma sú licencované a niektoré sú voľne využiteľné, pokiaľ sa používajú schválené vysielacie s obmedzeným výkonom. Nelicencované pásmo využívajú lokálne bezdrôtové siete. Najdôležitejšie pásma sú 902-928 MHz, 2400-2483 MHz známe ako 2,4 GHz, 5150-5350 MHz a 5725-5825 MHz označované za 5 GHz pásmo. O vzájomnú koordináciu nosných frekvencií v rôznych krajinách sa stará Medzinárodný Telekomunikačný Zväz ITU (International Telecommunication Union). Väčšina bezdrôtových lokálnych sietí fungujúcich podľa štandardu 802.11 vytvoreného organizáciou IEEE (Institute of Electrical and Electronics Engineers) využíva pásmo 2,4 a 5 GHz.

Najdôležitejším faktorom ovplyvňujúcim kvalitu bezdrôtových sietí pri prenose signálu vzduchom je, že prenos by mal prebiehať pokiaľ možno bez prekážok v smere prenosu. Ideálne je, keď sa zariadenia navzájom vidia a potom už výkon siete obmedzuje len výkon vysielacza. Elektromagnetické vlny sa všeobecne zle dostávajú cez pevné prekážky. Každý

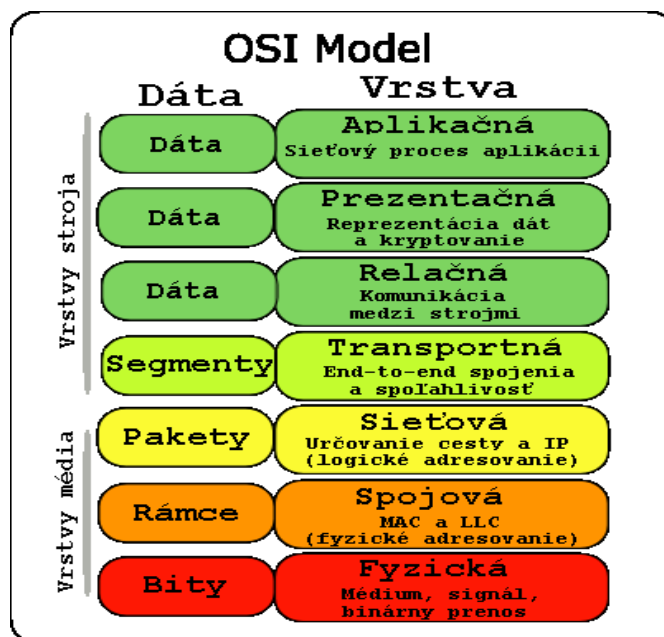
materiál spôsobí útlm signálu a vodivé predmety v blízkosti prijímača, alebo vysielča môžu spôsobovať odrazy signálu. Pokiaľ signál príde k prijímaču priamo a ešte aj odrazom a pri tom sú oba signály približne rovnako silné, dôjde k rušeniu viacnásobným prijatím signálu.

1.8 Firewall

Je zariadenie, ktoré pomocou nastavených pravidiel definuje, čo môže a čo nemôže byť povolené pri prechode týmto zariadením. Firewall začína tam kde končí smerovač a filtrovanie premávky je v ňom dôkladnejšie. Najčastejšie sa používajú na fyzické oddelenie dvoch sietí, napríklad firewall chrániaci vnútornú sieť pred Internetom. Existuje veľké množstvo firewallov, ktoré sa implementujú softvérovo, alebo hardvérovo. Dôležitým výkonnostným faktorom je priepustnosť firewallu. Nech už je charakter použitia firewallu akýkoľvek, vždy funguje na základe nastavenia pravidiel kontrolujúcich prevádzku, ktorá cez neho prechádza. Filtrovanie môže pracovať od druhej až po siedmu vrstvu OSI modelu. V dnešnej dobe používané firewally okrem ochrany vnútornej siete slúžia napríklad aj na sprístupňovanie služieb Internetového webového servera za pomoci presmerovania portov a umožnenia tak vstupu do akejsi polochránenej siete, nazývanej demilitarizovaná zóna.

2 REFERENČNÝ MODEL OSI

Model OSI (Open Systems Interconnection) je akýsi balík protokolov, ktorý bol vytvorený ako štandard pre zabezpečenie komunikácie medzi zariadeniami od rôznych výrobcov. Ako medzinárodná norma bola prijatá organizáciou ISO a ITU-T a preto sa niekedy používa označenie Referenčný model ISO/OSI. Tento model rozdeľuje komunikáciu do siedmych vrstiev a tiež používanie týchto vrstiev v procese výmeny dát. Pri procese odosielania každá vrstva obaluje dáta ďalšími informáciami a pri prijímaní dát sa tieto informácie používajú a odoberajú [3]. To znamená, že každá z týchto vrstiev využíva služby vrstvy pod ňou. Jednotlivé vrstvy majú svoje poradie, pričom prvá je Fyzická vrstva, po nej nasleduje Spojová vrstva, Sieťová vrstva, Transportná vrstva, Relačná vrstva, Prezentačná vrstva a posledná je Aplikačná vrstva.



Obr. 2. Referenčný model OSI [4].

Ako vidíme na obrázku 1 celkovo je definovaných sedem vrstiev a v prípade zahájenia komunikácie sa začína od poslednej siedmej vrstvy smerom k vrstve Fyzickej. Pri prechode jednotlivými vrstvami každá z nich pridá informáciu prislúchajúcu práve pre daný protokol a vrstvu popisujúcu obsah dát a ich použitie. Každé takéto pridanie informácie sa nazýva zapuzdrenie (encapsulation). Okrem toho druhá Spojová vrstva pridá kontrolné údaje pre overenie správnosti prenesených dát. Po prijatí rámca prebieha presne opačná postupnosť

prechodu od prvej vrstvy až po poslednú. Počas prechodu cez vrstvy sa informácie prislúchajúcej vrstvy odoberú a až na konci procesu zostanú samotné dáta. Proces odoberania sa nazýva odpúzdrenie (decapsulation). Výsledkom každého zapuzdrenia je dátový blok nazývaný PDU (Protocol Dáta Unit), ale kvôli zrozumiteľnosti a rýchlej identifikácii má PDU vždy svoj názov s ohľadom na vrstvu, ktorá vykonala zapuzdrenie.

2.1 Popis jednotlivých vrstiev OSI

2.1.1 Aplikačná vrstva

Posledná vrstva OSI modelu je najbližšie ku používateľovi, pretože používateľ a Aplikačná vrstva spolu komunikujú pomocou nejakej softvérovej aplikácie. Táto vrstva zahŕňa rozoznávanie komunikačného partnera, určuje dostupné zdroje a synchronizuje komunikáciu. Pre úpravu dát do požadovanej podoby Aplikačná vrstva komunikuje s príslušným protokolom. Protokol špecifikuje vnútornú štruktúru dát a typ posielanej správy. Touto správou môže byť žiadosť o službu, potvrdenie, samotné dáta, stavová, alebo chybová správa. Protokoly definujú aj komunikačné dialógy zaisťujúce to, že správa bola poslaná a správne služby boli spustené v čase keď odosielanie dát začalo. Na Aplikačnej vrstve nájdeme veľké množstvo protokolov, kde každý protokol poskytuje inú službu, má iné požiadavky na prenos a nesie iný druh dát.

2.1.2 Prezentačná vrstva

Služby tejto vrstvy sú definované v štandarde ISO 8822 a sú aj ako odporúčanie ITU-T X.216. Samotná špecifikácia protokolu je v odporúčaní ITU-T X.226. Samotná vrstva zabezpečuje šifrovanie a formátovanie dát z aplikačnej vrstvy. Aplikačná vrstva predáva dáta v rôznom formáte ako znaky, alebo binárne dáta a Prezentačná vrstva ich transformuje do podoby, v ktorej môžu byť predané ďalej v štandardizovanom kódovacom formáte [3]. Vrstva sa zaoberá len štruktúrou dát a to tak, aby prenášané dáta boli pochopené opačnou stranou nezávisle na operačnom systéme.

2.1.3 Relačná vrstva

Pozostáva z protokolov zabezpečujúcich založenie, ovládanie a ukončovanie spojenia - relácie (session). Komunikácia medzi dvoma aplikáciami na rôznych sieťových

zariadeniach pozostáva zo žiadosti o spojenie a odpovede na žiadosť. Tento proces je ovládaný protokolmi implementovanými v Relačnej vrstve. Ak je relácia v polo duplexnom režime, tak si relačné vrstvy medzi sebou predávajú token a v tom prípade vysielateľ môže len vlastník tokenu. Okrem toho Relačná vrstva značkuje komunikáciu a v prípade straty spojenia je možné reláciu obnoviť.

2.1.4 Transportná vrstva

Segmentácia a teda rozdelenie dát z Relačnej vrstvy, prebieha práve na Transportnej vrstve. PDU vzniknuté na tejto vrstve sa nazýva segment. Všeobecne je zodpovedná za bezchybné doručovanie a dohliada aj na jeho správne poradie. Okrem toho musí prijaté dáta v správnom poradí zložiť a poslať odosielateľovi potvrdenie o prijatí. OSI pre transportnú vrstvu definuje dva typy komunikácie. Prvým typom je spojová komunikácia, kde sa najprv nadviaže spojenie s opačnou stranou a potom sa začnú vymieňať samotné dáta a pritom sa stále potvrdzuje doručenie. Druhým typom je nespojová komunikácia, pri ktorej sa bez nadviazania spojenia dáta jednoducho pošlú a neočakáva sa ani potvrdenie prenosu. OSI definuje päť tried transportného protokolu označovaných TP0 až TP4. Trieda TP4 poskytuje spoľahlivú službu pre spojovú a nespojovú komunikáciu.

2.1.5 Sieťová vrstva

Sieťová vrstva je zodpovedná za smerovanie a výber najlepšej trasy medzi sieťami. Po pridaní hlavičky počas zapuzdrovania PDU vznikne paket. Sieťová vrstva zabezpečuje mechanizmus adresovania zariadení pomocou unikátnych adries. Zapuzdrením sa do paketu dostanú dve adresy identifikujúce zdrojovú adresu a cieľovú adresu. Ďalšou dôležitou službou je smerovanie, to znamená doručenie paketu do svojho cieľa. Odosielajúce zariadenie nemusí byť v tej istej sieti ako príjemca a práve informácia uložená v pakete pomôže smerovaču v prípade nepotvrdenia prenosu nasledujúcim smerovačom vybrať inú trasu do cieľa. Počas prenosu sa informácia v pakete nemení, pretože smerovač má svoju smerovaciu tabuľku, na základe ktorej vyberá nasledujúci bod v sieti na ktorý paket pošle. Po prijatí je v pakete preskúmaná cieľová adresa a ak súhlasí, paket je poslaný Transportnej vrstve.

2.1.6 Spojová vrstva

Druhá vrstva zabezpečuje komunikáciu cez lokálne fyzické médium. Umožňuje vyšším vrstvám prístup na prenosové médium, kontroluje prevádzku na médiu a dokáže určiť ktorým smerom sa budú prenášané dáta posielat'. PDU pozmenené touto vrstvou sa nazýva rámec. Pre riadenie na Spojovej vrstve je potrebné označiť začiatok a koniec úseku dát. Tie sa potom rozdeľujú na rámce o určitých veľkostiach. Ich veľkosť závisí od použitej technológie, alebo nastavením používateľa. Spojová vrstva má spôsob regulácie rýchlosti prenášaných dát pomocou vyrovnávajúcej pamäte (buffer), do ktorej prichádzajú prijaté rámce. IEEE rozdelilo vrstvu na dve podvrstvy LLC (Logical Link Control) a MAC (Media Access Control).

2.1.7 Fyzická vrstva

Prvá vrstva definuje elektrické, mechanické a iné špecifikácie pre aktivovanie, ovládanie a vypnutie fyzického média pri komunikácii medzi dvoma sieťovými zariadeniami. Celé to predstavuje prenos rámcov pomocou bitov transformovaných na signál prenášaný lokálnym médium. Zariadenie Fyzickej vrstvy musí obsahovať mechanizmy ako prenášať rámce pomocou rôznych prenosových médií, či už metalickým vedením, optikou, alebo rádiovou komunikáciou.

3 REFERENČNÝ MODEL TCP/IP

Okrem modelu OSI existuje ďalší referenčný model nazývaný TCP/IP. V porovnaní s modelom OSI pozostáva len zo štyroch vrstiev, to znamená, že jednotlivé vrstvy TCP/IP reprezentujú jednu, alebo viac vrstiev modelu OSI. V modeli TCP/IP poznáme tri rôzne protokoly definujúce spôsob prenosu a dát. Protokol TCP (Transmission Control Protocol) sa zaoberá založením a fungovaním spojenia medzi systémami na Internete. Nespojovú komunikáciu popisuje protokol UDP (User Datagram Protocol) a tretí je protokol IP (Internet Protocol), definujúci formát paketov pri prechode sieťou. Protokoly TCP a UDP operujú na transportnej vrstve a protokol IP je na úrovni sieťovej vrstvy [3].

OSI	TCP/IP
Aplikačná	Aplikačná
Prezentačná	
Relačná	Transportná
Transportná	Sieťová
Sieťová	
Spojová	Fyzická
Fyzická	

Obr. 3. Porovnanie referenčných modelov.

Na obrázku 3 je vidieť, že štvrtá vrstva TCP/IP je ekvivalent siedmej a šiestej vrstvy modelu OSI. Podobne to platí aj pre tretiu transportnú a prvú fyzickú vrstvu TCP/IP. Jedine druhá Sieťová vrstva odpovedá tretej vrstve OSI. Členenie vrstiev modelu TCP/IP nie je voči modelu OSI zjednotené, pretože služby poskytované jednotlivými vrstvami sa prelínajú. Protokoly aj model TCP/IP je spravovaný organizáciou IETF a princíp smerovania jeho IP datagramu popisuje RFC 1180. Rovnako ako pri modeli OSI, aj pri modeli TCP/IP sa počas prechodu dát medzi vrstvami pridávajú informácie typické pre danú vrstvu. To znamená, že po zapuzdrení dát musí prijímajúca strana tieto informácie odstrániť odpúzdrením.

3.1 Popis jednotlivých vrstiev TCP/IP

3.1.1 Aplikačná vrstva TCP/IP

Aplikačná vrstva je najvyššia vrstva pomyselného TCP/IP modelu. Nachádzajú sa tu aplikácie komunikujúce s nižšími vrstvami cez TCP a UDP porty. Aj keď tieto porty nie sú priradené tejto úrovni, Aplikačná vrstva musí o týchto portoch vedieť, pretože posiela a prijíma informácie z týchto portov. Aj keď je táto vrstva najbližšie k používateľovi, neslúži výlučne len jemu. Niektoré aplikácie fungujúce na Aplikačnej vrstve iba zbierajú informácie o konfigurácii siete. Okrem toho existujú aplikácie poskytujúce služby pre sieť, ako napríklad súborové a tlačové služby, alebo služba prekladu mien. Aplikačná vrstva modelu TCP/IP v sebe obsahuje niekoľko vrstiev modelu OSI. Siedma a šiesta vrstva modelu OSI je zahrnutá, ale nie je zjednotené do akej miery Aplikačná vrstva TCP/IP obsahuje Relačnú vrstvu OSI modelu.

3.1.2 Transportná vrstva TCP/IP

Tretia vrstva je rozhranie pre sieťové aplikácie, kde prebieha kontrola chýb, kontrola toku a potvrdzovanie sieťovej komunikácie. Zmyslom tejto vrstvy je poslať dáta do cieľového počítača a do konkrétnej aplikácie bežiackej na danom počítači. Transportná vrstva obsahuje mechanizmus multiplexovania v zmysle spracovania dát od viacerých aplikácií a súčasne riadiť tok dát do nižšej vrstvy. Na strane prijemcu Transportná vrstva musí dáta prijať z nižšej vrstvy a nasmerovať ich do správnych aplikácií. Toto sa nazýva demultiplexovanie a vďaka tomu je možné, aby zariadenie naraz podporovalo viacero aplikácií. Kontrola chýb je schopnosť overiť, či prenos bol úspešný a či boli prenesené všetky dáta. Práve na transportnej vrstve sú definované už dva spomínané protokoly TCP a UDP. Aby mohlo byť doručenie vykonávané pre konkrétnu aplikáciu, zaviedlo sa používanie portov. Port je preddefinované číslo reprezentujúci akúsi adresu, pomocou ktorej sa dáta dostanú z Transportnej vrstvy do požadovanej aplikácie. Po prijatí dát sa preskúma zdrojová adresa, zdrojový port a cieľová adresa s cieľovým portom. Existuje zoznam portov spravovaných organizáciou IANA (Internet Assigned Numbers Authority), podľa ktorého má každá aplikácia pridelené číslo portu na ktorom prijíma dáta pre ňu určené. Existujú tri dôležité rozsahy portov.

- Dobré známe porty – ich číselné rozpätie je od 0 až 1023 a sú priamo spravované organizáciou IANA. Tieto porty sú používané štandardnými protokolmi.
- Registrované porty – rôzne aplikácie môžu pre prenos a prijímanie dát používať svoje porty v rozsahu 1024 až 49150, ktoré sú vyhradené pre tento účel. Aj tento rozsah je spravovaný organizáciou IANA, ktorá aj preň vykonáva registráciu.
- Dynamické a privátne porty – Toto je neriadený rozsah od 49152 až po 65535 a je voľne použiteľný. Takéto čísla portov sa často používajú aj počas aktívneho spojenia.

Samotná komunikácia pomocou portov je spoľahlivé riešenie ako doručovať dáta do správnej aplikácie. Zariadenie počúva na danom cieľovom porte z rozsahu dobre známych portov. Odpoveď je potom posielaná na číslo portu, ktoré si žiadajúca aplikácia náhodne vygenerovala. Štandardne je to port z rozsahu dynamických a privátnych portov.

3.1.3 Sieťová vrstva TCP/IP

TCP/IP spravilo fyzickú adresu neviditeľnú a namiesto toho začalo pre proces objavovania zariadení v sieti používať logickú adresnú schému. Logickú adresnú schému si zariadenia udržiavajú pomocou IP protokolu využívajúceho logickú adresu nazývu IP adresa. Iný protokol na tejto vrstve priradzuje IP adresu fyzickej adrese. Takto vznikne tabuľka spájajúca fyzické adresy s logickými adresami, ktoré sa potom zapisujú do sieťovej karty [5].

3.1.4 Fyzická vrstva TCP/IP

Prvá vrstva tohto modelu zabezpečuje prípravu dát na prenos po prenosovom médiu. Spolupracuje so sieťovou kartou pri prenose za pomoci potrebných prístupových metód. Dáta konvertuje na formát prenositeľný pomocou elektrických pulzov. Kontroluje chyby pri prijímaní dát, pretože pri odosielaní pridáva informáciu pre kontrolu chýb a tak môže príjemca vykonať kontrolu. Fyzická vrstva modelu TCP/IP korešponduje s prvými dvoma vrstvami OSI modelu. Okrem samotného prenosu po lokálnom médiu táto vrstva zabezpečuje aj adresovanie pridaním logickej adresy druhej vrstvy do hlavičky paketu.

3.2 Protokol IP

Svoje služby poskytuje na druhej Sieťovej vrstve TCP/IP modelu. Používa sa na doručovanie paketov medzi zariadenia v TCP/IP sieťach a zdokumentovaný v RFC 791.

Obsahuje adresu a iné informácie, ktoré mu umožňujú prechádzať a teda byť smerovaný cez rôzne sieťové rozsahy. Protokoly vyšších vrstiev ako TCP a UDP sa prepravujú pomocou tohto protokolu. Umožňuje fragmentáciu a znovuposkladanie rozdelených fragmentov do pôvodného celku, ale je nespojovo orientovaný. Každý IP paket pozostáva z hlavičky (header), ktorá obsahuje informácie o IP pakete a užívateľské dáta (payload). Existujú dve používané verzie IP protokolu, ktoré majú odlišný spôsob adresácie. Výhodou tohto protokolu je, že mu nezáleží na druhu spojenia a preto môže byť doručovanie paketov rôzne smerované a tiež sa dokáže prispôbiť aktuálnym podmienkam na sieti.

3.2.1 Protokol IP verzia 4

IPv4 je štvrtá verzia IP protokolu a je popísaný v RFC 791. Posielanie IPv4 paketov je vykonávané bez oznámenia cieľu, že mu ideme niečo poselať. Zapuzdrenie segmentu, alebo datagramu z vyššej vrstvy znamená pridať IPv4 hlavičku obsahujúcu rôzne informácie potrebné na prenos po prenosovom médií. Takzvaný IP datagram je vlastne paket, ktorý sa vytvára na tretej Sieťovej vrstve TCP/IP modelu. Datagram obsahuje 13 častí a povinne sa musí vyplniť dvanásť a za vyplnenou hlavičkou nasledujú samotné dáta. Obmedzujúcim problémom pri prenose je maximálna veľkosť paketu MTU (Maximum Transmission Unit). Ak pošleme paket o určitej veľkosti a on po ceste bude fragmentovaný, tak to predĺži čas prenosu, alebo v určitom prípade ani nemusí fragment doraziť. V sieti typu Ethernet sa používa MTU=1500 bytov. To znamená, ak na smerovač príde paket o veľkosti väčšej ako je MTU na ceste za prepínačom, paket sa musí fragmentovať. Tieto fragmenty sa skadajú až v cieľi a to aj v prípade, ak niektorá ďalšia vetva siete po fragmentácií umožňuje prenos paketu v pôvodnej veľkosti.

3.2.2 Adresovanie v IPv4

Adresa v IPv4 sa skladá z 32 bitov a pre lepšiu orientáciu sa používa zápis ako štyri osembitové čísla. To znamená, že každých osem bitov môže reprezentovať hodnotu od nula po 255, to je 2^8 hodnôt. V ľudskej podobe sa IP adresa zapisuje v desiatkovej sústave pozostávajúcej zo štyroch častí – oktetov, ktoré sú oddelené bodkami. Každé zariadenie pripojené do počítačovej siete má vlastnú logickú adresu známu ako IP adresa. Táto adresa je pre danú oblasť jedinečná a na sieti by sa nemali vyskytovať dve zariadenia s rovnakou IP adresou. Samotná IP adresa pozostáva z dvoch častí, ktoré spolu tvoria celok

informujúci o adrese zariadenia a adrese siete. Keď vieme adresu siete, vieme určiť aj maximálny počet zariadení v danej sieti. S pribúdajúcou potrebou nových zariadení bolo potrebné zmeniť adresnú schému tak, aby bolo jasné, čo predstavuje sieť a čo predstavuje samotné zariadenie na danej sieti. Na to sa používa sieťová maska, ktorá udáva sieťový prefix. Sieťovú masku môžeme vyjadriť v binárnom tvare, ale aj v desiatkovom za pomoci použitia lomky '/'. Pretože niektoré siete sú relatívne malé a iné sú rozľahlé, začali sa adresné bloky zaradzovať do tried od A po C.

Tab. 2. Adresné bloky podľa triedy.

adresná trieda	začiatok	koniec	max. sietí
A	0.0.0.0	127.255.255.255	128
B	128.0.0.0	191.255.255.255	16 384
C	192.0.0.0	223.255.255.255	2 097 152



Existuje aj trieda D, slúžiaca na určenie multicast skupiny a trieda E, ktorá sa používa na experimentálne účely. Problém pri takto roztriedených adresách je ich plytvanie prípadne má organizácia pridelený adresný priestor, ale v skutočnosti nemá taký počet zariadení, ktorý pokrýva daná. Momentálne sa na hospodárnejšie využívanie IP adres používa schéma CIDR (Classless Inter-Domain Routing), popísaná v RFC 1517, ktorá ruší nevýhody sieťových tried. Vymedzenie sieťového rozsahu pre danú sieť nám pomáha premenlivá dĺžka masky podsiete VLSM (Variable Length Subnet Masking). Všetky podsiete je možné spojiť do väčších supersietí. To má okrem efektívnejšieho využívania IP adres aj zväčšenie rýchlosti smerovania na smerovačoch. CIDR nám umožňuje rozdeliť adresný priestor na bloky, ktorý sa potom prideliť používateľovi.

Existuje skupina IPv4 adres ktoré sa neprideliť a ich hodnota má určitý popisný charakter pre danú sieť. Samotný Internet je rozdelený do niekoľkých regiónov s prideleným veľkým rozsahom adres. Tieto rozsahy sú prideliť lokálnym internetovým registrátorom RIR, ktorý ich následne rozdeľuje medzi jednotlivých lokálnych záujemcov. Registrátor pre Európu, Blízky východ a Strednú Áziu je sieťové koordinačné centrum RIPE NCC. O prideliť IP adres pre RIR sa stará organizácia IANA.

3.3 Potokol TCP

TCP je spojovo orientovaný protokol poskytujúci spoľahlivé služby v nespoľahlivom Internete a je zdokumentovaný v IETF RFC 793. Obsahuje sadu riadiacich príznakov, ktoré ovplyvňujú všetky aspekty odosielania a prijímania dát. Pri prenose existuje mechanizmus riadiaci tok paketov zaručujúci, že ak pakety dorazia v rôznych časoch a v rôznom poradí, vždy sa na konci prenosu zostaví správa identická so svojim originálom u odosielateľa. TCP je protokol tretej vrstvy a odosielané dáta sa zapuzdrujú do TCP segmentov. Každý segment obsahuje hlavičku a telo s dátami. Predtým ako sú dáta poslané pomocou TCP protokolu, transportná vrstva začne proces vytvárania spojenia s cieľom pomocou riadiacich príznakov. To zaručí, že každé prijímajúce zariadenie si je vedomé pripravovaného prenosu.

3.3.1 Štruktúra protokolu TCP

Prvá položka segmentu je zdrojový port a hneď po nej je cieľový port vyjadrujúci typ odosielaných dát. Pokiaľ aplikácia prijme segment s hodnotou cieľového portu na ktorom počúva, pristúpi k spracovaniu dát a odpoveď pošle na hodnotu portu, ktorá bola zapísaná v poličku zdrojový port. Poradové číslo odosielaného bytu je informácia k riadeniu prenosu fungujúca spolu s riadiacimi príznakmi SYN, ACK a FIN. Pokiaľ je v riadiacom príznaku SYN nastavená hodnota jedna, tak poradové číslo reprezentuje začiatok dát. Ak je SYN nula, reprezentuje to prvý dátový byte segmentu pre dané spojenie. Poradové číslo prijatého bytu má zmysel v prípade nastaveného príznaku ACK na jedna. To potom ukazuje na prvý očakávaný byte pre danú sekvenciu. Toto dovoľuje prijaté dáta zostaviť v správnom poradí od prvého až po posledný segment. Príznak FIN sa nastaví na jedna, ak odosielateľ už nemá dáta na posielanie. Dĺžka záhlavia vyjadruje veľkosť hlavičky v bytoch. Poradové číslo odosielaného bytu SEQ (sequence number) a poradové číslo prijatého bytu ACK (acknowledgment number) slúžia pri spoľahlivom prenose dát. Kontrolný súčet slúži na identifikovanie správneho doručenia paketu. Jeho hodnota zahŕňa hlavičku aj telo TCP paketu. Priamo za hlavičkou TCP paketu sa nachádza dátové pole obsahujúce prenášané dáta pomocou TCP paketu. Ani tieto dáta nie sú presne to čo vidí používateľ, ale majú charakter vlastný práve používaného protokolu Aplikačnej vrstvy. Samotná veľkosť dátového poľa nemá určenú veľkosť, ale protokol TCP má mechanizmus ovplyvňovania veľkosti dát s ohľadom na určité aktuálne podmienky na sieti.

3.3.2 Prenos dát pomocou TCP protokolu

Spojenie medzi dvoma zariadeniami, nazývanými aj soket (socket), môže nastať iba za predpokladu, ak takéto spojenie medzi soketmi ešte neexistuje. Oboje zariadenia musia súhlasiť so spojením a musia mať dostatočné zdroje na obsluhu takéhoto spojenia. V prípade nesplnenia nejakej podmienky spojenie nemôže nastať. Pred akoukoľvek transakciou za použitia TCP protokolu musí najskôr nastať k inicializácia spojenia pomocou procesu trojcestného zahájeniu spojenia (three-way handshake). Klasický spôsob nadviazania spojenia je, že klient sa dotazuje na port služby bežiackej na serveri. Po úspešnom nadviazaní spojenia nasleduje prenos dát. Na ukončenie spojenia sa pri protokole TCP používa nastavenie príznaku FIN. Okrem toho musí opačná strana potvrdiť prijatie segmentu s nastavenou hodnotou ukončenia komunikácie. Ukončiť spojenie môže hocikto odoslaním príznaku FIN a tento proces vyžaduje až štyri kroky. Existuje možnosť ukončenia spojenia, kedy odosielateľ pošle FIN a prijímateľ odpovie ACK a FIN v jednom segmente. Odosielateľ to len potvrdí poslaním ACK. Iný prípad ukončenia spojenia môže nastať ak vypadne jedna strana prenosu, napríklad z dôvodu prerušenia elektrického napájania a podobne. Aktívna strana zistí prerušenie až keď prestane dostávať odpovede. Na udržanie všetkých TCP spojení sa používa tabuľka spojení, ktorá pre každé spojenie obsahuje informácie o stave spojenia, lokálnej adrese, lokálneho portu, cieľovej adrese a cieľového portu.

3.4 Protokol UDP

Je to jednoduchý protokol poskytujúci bezstavový prenos dát. Protokol UDP (User Datagram Protocol) nie je spojovo orientovaný a to znamená, že nepodporuje spoľahlivé doručovanie dát. Tento protokol nijako neinformuje odosielateľa o úspešnom doručení, to ale neznamená že prenášané dáta nedorazia do cieľa. Ak by aj niečo chýbalo, tak žiadosť o preposlanie musí zabezpečiť iný mechanizmus, napríklad aplikácia na aplikačnej vrstve. UDP protokol má menšie nároky na prenos a tiež nepodporuje riadenie toku dát. Toto má za následok, že prenos dát pomocou protokolu UDP je omnoho rýchlejší ako prenos za pomoci protokolu TCP. Hlavná myšlienka je v tom, že niektoré aplikácie dokážu tolerovať určité množstvo nedoručených dát bez vplyvu na kvalitu poskytovanú pre používateľa. Napríklad strata malého množstva dát pri prenose videa je pre obyčajného človeka

zvyčajne nepostrehnuteľná a nijako nekazí dojem zo sledovaného videa. Samotný protokol UDP je popísaný v RFC 768.

3.4.1 Prenos dát pomocou protokolu UDP

Medzi dvoma komunikujúcimi bodmi sa vymieňajú datgrami a princíp fungovania je založený na základe portov. Hlavička protokolu UDP je jednoduchá a nachádzajú sa v nej len zdrojový a cieľový port, kontrolný súčet a dĺžka prenášaných dát. Kontrolný súčet slúži na odhalenie chýb pri prenose. Posielanie dát pomocou protokolu UDP neznamena najprv nadviazať spojenie, potom preniesť dáta a nakoniec spojenie ukončiť, tak ako to je pri protokole TCP. Tu sa jednoducho dáta začnú posielat' a nezáleží na tom, či je prijímateľ schopný dáta v tomto čase prijať.

3.5 Protokol IPv6

Niekedy je označovaný aj ako protokol nasledujúcej generácie IPng (Internet Protocol next generation). Je to posledná verzia IP protokolu, je zdokumentovaná v RFC 2460. Zmyslom tohto protokolu je nahradiť doteraz používaný protokol IPv4 a tým vyriešiť problémy s ním spojené. Najväčšie výhody sú väčší adresný priestor, vytvorenia troch skupín adries, zvýšenie bezpečnosti, zvýšenie kvality služieb a automatická konfigurácia. Preklad adries už nie je potrebný a pre veľký adresný priestor už nemusíme používať podsiete. Pomocou IPv6 môžeme objavovať susedov, alebo automaticky nakonfigurovať svoju vlastnú IPv6 adresu bez potreby zariadenia, ktoré takúto službu poskytuje. Oproti svojmu predchodcovi má IPv6 v hlavičke omnoho menej častí. Kontrolný súčet je vynechaný z dôvodu jeho poskytovania nižšou vrstvou. Fragmentácia, ak je vôbec potrebná, je presunutá do rozširujúcich volieb, alebo častejšie sa používa metóda kedy smerovač zahodí IPv6 paket pre jeho veľkosť a pošle správu odosielateľovi, aby poslal menší paket. Zreťazenie hlavičiek umožňuje pripojiť jednu, alebo viac hlavičiek, ktoré nesú informácie o rozširujúcich voľbách ako sú fragmentácia, udanie kadiaľ sa má smerovať, šifrovanie obsahu, autentifikácia a podobne. Adresy sú v tomto protokole štyri krát dlhšie a majú 128 bitov, čo je šesťnásť bytov. Ich zápis je vo forme ôsmich dvojbytových slov oddelených dvojbodkou a hodnoty sú reprezentované v šesťnásťkovej sústave. V IPv6 sa na identifikáciu zariadenia používa vždy posledných 64 bitov adresy na rozdiel od IPv4 adresy, kde nám maska oddeľuje sieť od adresy zariadenia.

4 LOKÁLNÁ POČÍTAČOVÁ SIĚŤ

Lokálna počítačová sieť je uzavretá sieťová oblasť, v ktorej sa nachádzajú zariadenia určené pre poskytovanie služieb určených výhradne len pre používateľov nachádzajúcich sa v tejto sieti. Zariadenia a používatelia vo firemných, alebo domácich sieťach sa nachádzajú a spolu komunikujú práve v sieti LAN (Local Area Network). Lokálne siete môžu mať rôzny charakter a topológiu. Najmenšia počítačová sieť je tvorená dvoma navzájom prepojenými počítačmi. Zariadenia vo väčších počítačových sieťach potrebujú na vzájomnú komunikáciu dodatočné zariadenia a komponenty v podobe prenosových médií a sieťového hardvéru. Ďalej môžeme zariadenia rozdeliť na aktívne a pasívne prvky siete.

4.1 Štandard 802.3

Veľmi používanou metódou budovania počítačových sietí je Ethernet. Tento štandard definuje všesmerové vysielanie rámcov na médiu fyzickej vrstvy spolu s signalizačnými metódami spojovej vrstvy pomocou metódy počúvania nosného signálu s viacnásobným prístupom a detekciou kolízie pomocou metódy CSMA/CD (Carrier Sence Multiple Access with Collision) [3]. Je to poloduplexná komunikácia používaná napríklad pri zapojení rozbočovača. Plne duplexné prepínače túto metódu nepoužívajú. Ethernet je popísaný štandardom IEEE 802.3. Existuje niekoľko typov Ethernetu:

- 10BASE - ktorý poskytuje rýchlosť 10Mbps a má ešte niekoľko kategórií v závislosti od typu prenosového média.
 - 10BASE-5 : nazývaný aj Hrubý Ethernet. Jeho základom je hrubý koaxiálny kábel do vzdialenosti 500 metrov.
 - 10BASE-2 : Tenký Ethernet, používal sa tenký koaxiálny kábel do vzdialenosti 185 metrov.
 - 10BASE-T : Používanie krútenej dvojlinky. Písmeno T znamená twisted, ako krútený.
 - 10BASE-F : Predstavuje použitie optických káblov.
- 100BASE – nazývaný aj ako Fast Ethernet, a podporuje prenos až do rýchlosti 100Mbps. Je definovaný ako štandard IEEE 802.3u a tiež má niekoľko typov.
 - 100BASE-T : Štandard využívajúci krútenú dvojlinku.

- 100BASE-T4 : Používa sa pre kabeláž kategórie 3 a to pomocou štyroch krútených párov.
- 100BASE-TX : Prenos pomocou dvoch párov tienenej, alebo netienenej krútenej dvojlinky kategórie 5 a maximálnym dosahom 100 metrov.
- 100BASE-FX : Je určený pre používanie dvoch optických vlákien. Pre plne duplexný režim poskytujú dosah až 2 km a používajú sa viacvidové vlákna.
- 100BASE-BX : Ako optický kábel je použité jednovidové vlákno a dosah je až 40 km.
- 100BASE-SX : Používa sa viacvidový optický kábel a vlnová dĺžka 850 nm. Dosah je až 550 metrov.
- 100BASE-LX10 : Pri použití vlnovej dĺžky 1310 nm a dvoch jednovidových káblov môžeme dosiahnuť dosah až 10 km.

Model 100BASE-X bol navrhnutý na podporovanie prenosu pomocou dvoch párov krútenej dvojlinky kategórie 5, alebo dvoch vlákien optického kábla.

Gigabitový Ethernet popisuje technológiu prenosu rámcov o rýchlosti 1Gbps. Pozostáva z dvoch štandardov 802.3z pre optické vlákna a 802.3ab pre krútenú dvojlinku.

- 1000BASE – Je všeobecné označenie pre Gigabitový Ethernet.
 - 1000BASE-T : ponúka plne duplexný prenos pomocou štyroch párov kábla kategórie Cat 5e.
 - 1000BASE-TX : je to štandard TIA/EIA 854 a používa iba dva páry krútenej dvojlinky a môže sa používať iba s kabelážou kategórie 6 a viac. 1000BASE-T a 1000BASE-TX sú dva úplne odlišné štandardy. Dosah má rovnako 100 metrov.
 - 1000BASE-X : Má označovať prenos cez optický kábel.
 - 1000BASE-SX : Používa viacvidové vlákno pri vlnovej dĺžke 850 nm. Písmeno S ako 'short' má reprezentovať použitie krátkej vlnovej dĺžky. Dosah je do 550 metrov.
 - 1000BASE-LX : Môže používať jedno a viacvidové vlákno. Funguje pri vlnovej dĺžke 1300 nm, čo má reprezentovať písmeno L 'long'. Dosah pri použití viacvidového kábla je 550 metrov a pri jednovidovom vlákne je až do 10 km.

Gigabitový Ethernet nie je poslednou verziou Ethernetu. Existujú aj rýchlejšie verzie, ktorých nasadenie vo firemných sieťach musí mať svoje opodstatnenie. V naozaj veľkých firmách môžeme ešte použiť 10 Gigabitový Ethernet ktorý poskytuje prenos o rýchlosti 10Gbps. Jeho prvý štandard má označenie IEEE 802.3ae-2002. Začlenením optických a metalických prenosových médií vznikol štandard s označením IEEE Std 802.3-2008. Dosah 10 GigE pri použití jednovidového optického kábla sú desiatky kilometrov, viacvidové vlákno 300 metrov a krútená dvojlinka do 300 metrov.

4.1.1 Ethernet rámec

Ak zoberieme v úvahu referenčný model OSI, tak prvá a druhá vrstva sa rozčlení na niekoľko podvrstiev na ktorých Ethernet pracuje. Rozdiel je len na fyzickej vrstve, kde sú protokoly závislé od použitého prenosového média. Spojová vrstva modelu OSI je rozdelená na dve podvrstvy.

- Klient vrstvy MAC – slúži na logické riadenie linky a má označenie LLC .
- MAC vrstva – je určená na riadenie prístupu k médiu. Vrstva MAC má na starosti zapúzdrenie do rámcov.

LLC vrstva sa uplatňuje na koncových zariadeniach, pretože priamo nad ňou sú už protokoly vyšších vrstiev. MAC vrstva podporuje detekciu chýb, zahájenie prenosu rámcov a opätovný prenos rámcov. V prostredí, kde sa používa Ethernet, existujú dva typy sieťových zariadení. Komunikačné dátové zariadenie DCE (Data Communications Equipment) je to, čo Ethernetové rámce prijíma a následne ďalej preposiela. Patrí tam aj sieťová karta počítača [3]. Koncové dátové zariadenie DTE (Data Terminal Equipment) zahŕňa všetko čo predstavuje zdrojové, alebo cieľové zariadenie. V Ethernete sa ako cieľová a zdrojová adresa spojovej vrstvy používa MAC adresa. To znamená, že každé zariadenie musí mať svoj jedinečný identifikátor pozostávajúci z dvanásť znakov hexadecimálnej sústavy. MAC adresa má veľkosť 48 bitov a má niekoľko možných zápisov. MAC adresu 0abc.234b.c6a3 môžeme zapísať nasledujúcimi spôsobmi: 0a:bc:23:4b:c6:a3, alebo aj 0a-bc-23-4b-c6-a3. Túto adresu kontrolujú sieťové karty pri prijatom rámci. MAC adresa je pridelovaná výrobcom sieťovej karty. Pozostáva z dvoch častí. Prvá časť sa nazýva OUI (Organizationally Unique Identifier) a slúži na identifikáciu výrobcu sieťovej karty. Druhá časť je pridelovaná výrobcom a to takým spôsobom, aby

dodržel jej jedinečnosť. Ak by sme chceli adresovať všesmerovú broadcastovú adresu, tak tá pozostáva iba z rovnakých písmenok ff:ff:ff:ff:ff:ff.

4.2 Virtuálna lokálna sieť

Lokálnu sieť je možné rozdeliť na virtuálne lokálne siete, ktoré v konečnom zmysle reprezentujú vnútornú sieť podniku. VLAN (Virtual Local Area Network) pomáha vytvoriť zaradenie jednotlivých zariadení do logického spoločenstva. Pomocou VLAN môžeme sieť rozdeliť do geografických celkov, napríklad podľa služieb poskytovaných pre danú sieť. VLAN umožňuje viacero IP sietí združovať na jednej prepínanej sieti. Každý prepínač nachádzajúci sa v tejto sieti musí byť nakonfigurovaný pre dané virtuálne siete a každý port na prepínači musí patriť do nejakej VLAN. Takéto delenie siete prebieha na úrovni druhej vrstvy OSI modelu. Zariadenia umiestnené v jednotlivých virtuálnych sieťach nedokážu medzi sebou komunikovať a dokonca ani nevedia o vzájomnej prítomnosti vo firemnej sieti. Virtuálne siete sa rozdeľujú na určité rozsahy v ktorých môžu mať svoje číslo.

- Normálny rozsah od 1 do 1005.
 - 1 je vždy prednastavená a nedá sa odstrániť.
 - 1002 až 1005 sú rezervované.
- Rozšírený rozsah od 1006 až 4092 – pre firemné siete sa nevyužívajú.

Aj keď je možné VLAN pomenovať, jednotlivé zariadenia používajú iba ich číslo.

4.2.1 Trunk

Trunk je spojenie medzi dvoma sieťovými zariadeniami a umožňuje prepravovať komunikáciu viacerých VLAN po jednom prenosovom médiu. Trunk je najčastejšie zostavený medzi dvoma prepínačmi, ale je možné pripojiť aj smerovač. Trunk nepatrí do žiadnej VLAN a slúži len na prenos rámcov patriacich do rôznych VLAN. Trunk pracuje na druhej vrstve modelu OSI a prepínače pre preposielanie používajú informácie obsiahnuté v hlavičke Ethernet rámca. Preto, aby prepínač vedel do akej VLAN rámec patrí, musí byť pred prenosom cez Trunk označovaný (tagging). Rámec prijatý od počítača štandardne nie je značkový, pretože až port na prepínači je zaradený do niektorej VLAN. Predtým ako sa začnú rámce “tagovať“, musí sa najskôr dohodnúť protokol.

- Protokol ISL (Cisco Inter-Switch Link) – je to Cisco proprietárny protokol, ktorý rámec zapuzdri do nového rámca. Na začiatok pridá hlavičku, v ktorej sa nachádza informácia o VLAN, do ktorej rámec patrí. Na koniec pridá kontrolný súčet. Celkovo sa Ethernetový rámec zväčší o 30 bajtov.
- Protokol 802.1Q – niekedy nazývaný aj dot1q. Namiesto vytvorenia nového rámca vloží informácie do už existujúceho Ethernet rámca. To znamená pridanie 4 bajty medzi pole zdrojová adresa a typ. Pretože sa týmto rámec zmenil, musí sa nanovo prepočítať kontrolný súčet.

V rámci trunku existuje jedna VLAN, ktorá sa nazýva Natívna VLAN. Táto VLAN sa pri prechode trunkom neznačkuje. Niektoré zariadenia umožňujú značkovanie, ale v prípade 802.1Q trunku bude takýto rámec zahodený. Ak prepínač prijme na trunk port neznačkový rámec, tak ho zaradí do Natívnej VLAN. Prenos rámcov z jednotlivých VLAN cez trunk sa vykonáva pomocou multiplexovania. Zariadenia od Cisca podporujú automatické zostavenie trunku pomocou protokolu DTP (Dynamic Trunk Protocol). Na to aby to fungovalo, musia obidve strany podporovať DTP. V prípade, ak máme v našej sieti veľké množstvo VLAN, Cisco vyvinulo protokol VTP (VLAN Trunking Protocol), ktorý dokáže spravovať jednotlivé VLAN na prepínačoch v sieti. Obmedzenie je len v použití normálneho rozsahu VLAN. Na umožnenie vzájomnej komunikácie sa musí použiť smerovač obsahujúci rozhranie, na ktoré sa jednotlivé VLANy pripájajú. Vzájomná komunikácia medzi virtuálnymi sieťami sa nazýva Inter-VLAN smerovanie.

4.3 Spaning Tree Protokol

Tento protokol je špecifikovaný štandardom 802.1D. STP (Spaning Tree Protocol) pre jednu sieť použitím adaptívneho a dynamického smerovania dokáže riešiť problém sieťových slučiek. Protokol nerieši smerovanie medzi dvoma sieťami, ale pomocou tohto protokolu sa vytvárajú virtuálne okruhy eliminujúce slučky na sieti. Slučky predstavujú problém počas všesmerového vysielania. Prepínač reaguje na všesmerové vysielanie takým spôsobom, že ho replikuje na všetky svoje porty okrem toho, odkiaľ toto vysielanie prijal. Všesmerové vysielanie sa opakuje do nekonečna v prípade, ak sa na sieti nachádzajú slučky. Takto vzniknutá všesmerová búrka (broadcast storm) spôsobí kolaps siete. STP funguje na druhej vrstve modelu OSI. V sieti, v ktorej sa využíva STP, sa jednotlivé prepínače nazývajú mostami. Ako prvé sa musí v sieti vybrať koreňový most. Výsledkom

je, že všetky mosty v sieti môžu koreňový most dosiahnuť pomocou cesty s najmenšou cenou a ostatné cesty budú prerušené. Informácie o jednotlivých mostoch sa každé dve sekundy prenášajú pomocou protokolu BPDU (Bridge Protocol Data Unit.), ktorý je vysielaný ako multicast. Obsahuje informácie o ceste a o aktuálnych cenách jednotlivých segmentov. Pomocou týchto informácií dokážeme vykonávať nasledujúce funkcie:

- Výber koreňového mostu – RB (root bridge).
- Určenie najlepšej cesty do RB.
 - Určenie koreňového portu pre každý most – RP (root port), má najlepšiu cenu.
 - Určenie vyhradeného portu pre každý segment – DP (designated port), má druhú najlepšiu cenu do RB.
- Blokovanie ostatných portov.

V rámci STP protokolu sú odosielané tri typy správ. Konfiguračne BPDU, informácia o zmene a potvrdenie informácie o zmene. Každý most sa identifikuje pomocou svojho BID (Bridge ID), ktoré je kombináciu priority mostu a jeho MAC adresy. Ak most prijme BPDU s nižšou hodnotou BID ako má on sám, tak tento most bude RB a jeho BID bude následne posielat' vo svojich BPDU. Ak prijme na viacerých portoch BPDU, znamená to, že existuje viacero ciest do RB a najlepšia cesta bude tá, ktorá má z nich najmenšiu cenu.

Tab. 3 Cena jednotlivých portov.

Rýchlosť linky	Cena 802.1D
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

Cena cesty je súčet všetkých priorit portov na ceste k RB. Port, na ktorom bolo prijaté najlepšie BPDU a súčet jeho priority portu bude menší ako výsledná cena na ostatných portoch, tak sa stane RP. DP sa stane ten port, ktorý má najlepšiu cenu do RB v rámci daného segmentu. Spravidla je to druhá najlepšia cena do RB. Samotný RB neobsahuje RP, ale všetky jeho porty sú DP. Ostatné porty ktoré prijali BPDU, sa uvedú do stavu

blokovania komunikácie. Na prepínači sú porty stále aktívne, pretože preposielajú niektoré riadiace a informačné rámce v rámci BPDU. Okrem STP existuje aj protokol RSTP (Rapid Spanning Tree Protokol), urýchľujúci zostavovanie novej cesty do koreňového prepínača. Cisco do svojich zariadení implementuje svoju verziu STP, zameranú na prácu s virtuálnymi lokálnymi sieťami. Nazvali ho PVST (Per VLAN Spanning Tree) a vytvára bezslučkovú topológiu pre každú virtuálnu sieť zvlášť. IEEE vyvinulo podobný protokol MSTP (Multiple Spanning Tree Protokol).

4.4 Prepínacie metódy rámcov

Prepínače pracujúce na druhej vrstve pracujú s dvoma základnými metódami prepínania rámcov. Každá metóda určitým spôsobom ovplyvňuje výkonnosť siete a preto je vždy na zvážení, ktorú metódu použiť.

- Metóda Store-and-Forward - Prepínač prijme celý rámec a uloží ho do svojej pamäte. Skontroluje veľkosť a ak je menší ako 64 bytov (Runt Frame), alebo väčší ako 1518 bytov (Giant Frame), tak rámec zahodí.
- Metóda Cut-through - Rámec sa prepne na výstupné rozhranie skôr ako sa celý prijme. Táto metóda má dve varianty.
 - Fast forward - rámec sa prepne v momente ako sa prečíta cieľová MAC adresa.
 - Fragment free – rámce menšie ako 64 byte sú pokladané za chybné a označujú sa za kolízne. Ak sa prijme viac ako 64 byte predpokladá sa, že nie je kolízny.

Store-and-Forward okrem veľkosti rámcov vykonáva aj kontrolu chybovosti pomocou CRC obsiahnutého v prenášanom rámci. Ak je detekovaná chyba, rámec sa zahodí. Cut nekontroluje CRC a ani veľkosť rámca.

4.5 Smerovanie v lokálnej počítačovej sieti

Smerovanie paketov v počítačovej sieti je jednou z najdôležitejších funkčných operácií. Na to, aby sme mohli posielat' dáta medzi rôznymi sieťami, potrebujeme smerovač. Smerovač posielá pakety na základe vybudovanej smerovacej tabuľky. Smerovanie môže prebiehať

rýchlou cestou, pokiaľ sa pri prenose používa rovnaký smerovací protokol tretej vrstvy OSI. Pomalá cesta je, ak smerovač prijme protokol jedného typu a musí ho dodatočne spracovať na protokol fungujúci na výstupnom rozhraní. Smerovacia tabuľka môže byť riadená viacerými spôsobmi. Manuálne môžeme pridať, alebo odobrať statické cesty. Dynamickým spôsobom sa cesty spravujú pomocou smerovacích protokolov, kde si smerovače navzájom vymieňajú informácie o cestách do rôznych sietí. Existuje niekoľko spôsobov ako svoje dáta smerovať:

- Jednosmerové vysielanie- unicast, jedno zariadenie odosiela pre jedno konkrétne zariadenie.
- Všesmerové vysielanie – broadcast, jedno zariadenie odosiela pre všetky ostatné zariadenia.
- Viacsmerové vysielanie – multicast, jedno zariadenie odosiela pre špecifickú skupinu zariadení.
- Výberové vysielanie – anycast, jedno zariadenie odosiela pre špecifickú skupinu zariadení a zariadenie je schopné na ňu reagovať. V prípade, ak hociktoré zariadenie odpovie, tak komunikácia sa ukončí.

V prípade, ak sa pre smerovanie používajú viaceré protokoly, smerovač najlepšiu cestu vyberie na základe dopredu definovaného poradia. Administratívna vzdialenosť AD je hodnota priradená každému smerovaciemu protokolu. Uprednostňuje sa protokol s nižšou administratívnou vzdialenosťou. Manuálne nastavené cesty majú $AD = 1$ a priamo pripojené siete majú $AD = 0$.

4.6 Prenos hlasu pomocou Internet protokolu

VoIP sa používa v sieťach s prepínaním paketov. Hlas je zaznamenaný klasickým spôsobom pomocou mikrofónu, následne je zapuzdrený a potom je pomocou internetového protokolu odoslaný do svojho cieľa. Okrem náročnosti na prenosové podmienky musí byť zabezpečená aj signalizácia medzi zariadeniami využívajúcich VoIP. Uskutočnenie komunikácie prebieha v dvoch fázach. To, ako sa koncové zariadenia prepoja a aký kódex použijú, sa dohodne v prvej signalizačnej fáze. V druhej fáze sa stanice prepoja pomocou nejakého protokolu. SIP (Session Initiation Protocol) je protokol typu bod-bod a používa sa na prenos vide a zvuku. Okrem toho ešte riadi adresovanie a priradenie portov, ale nevie

nič o detailoch prenášaných dát. RTP (Real-Time Transport Protocol) komunikácia pozostáva z dvoch častí. Samotné RTP doručuje zvuk aj video v reálnom čase. Umožňuje identifikovať obsah, pridať časové pečiatky, sekvenčne číslovať a kontrolovať doručenie. Na prenos sa môže použiť TCP, ale UDP je lepšie z pohľadu oneskorenia, ktoré by mohlo nastať pri potvrdzovaní prenosu TCP. Používanie portov nie je štandardizované, ale vyžaduje sa, aby pre RTP bol na párnom porte a najbližší voľný vyšší bude priradený pre protokol RTCP (RTP Control Protocol). Práve RTCP je druhá časť komunikácie RTP kontrolujúca doručovanie dát a poskytuje informácie o kvalite linky. Štandard ITU-T H.323 podporuje audiovizuálny prenos, signalizáciu a spravovanie šírky pásma. H.323 je celý rad protokolov, kde každý zabezpečuje iné služby.

4.7 Kvalita služieb

QoS (Quality of Services) vo svojej podstate zabraňuje zahlteniu linky až do bodu, kedy iné dáta nebudú mať prístup na danú linku. QoS umožňuje ohodnotiť určitý typ komunikácie pomocou priorít a tým umožniť uprednostnený prístup na linku. Ostatné dáta sa zaradia do fronty, v ktorej čakajú na odoslanie. Ak by sa na preťaženej linke všetky pakety ukladali do fronty ktorá má obmedzenú pamäť, tak dáta ktoré sa už nevmestia, budú zahodené. Toto je stav neprípustný pre niektoré dátové prenosy, ktoré sú citlivé na výpadok paketov, nesprávne doručenie, alebo vzájomnú časovú závislosť. QoS je len jeden spôsob ako riešiť kvalitu prenosu v sieti. Tieto a iné riešenia sa vyskytujú pod súhrnným názvom CoS (Class of Service), čo je niečo ako klasifikácia služieb. Najväčší prínos QoS predstavuje pre VoIP, ktoré na prenos využíva nespoľahlivé UDP. Existujú tri modely poskytujúce rozdielne úrovne služieb:

- BE – Best-Effort služba, v princípe ide o doručovanie prevádzky s najmenším úsilím. Nemá žiadne nástroje na reakcie sieťových rozhraní pre jednotlivé druhy prenášaných dát.
- IntServ – Integrated service, úlohou je poskytnúť a zarezervovať potrebné sieťové prostriedky po celej trase medzi zdrojom a cieľom komunikácie.
- DiffServ – Differentiated service, je množina nástrojov pracujúca s frontami a ich klasifikáciami. Smerovače na hranici rozlišujú pakety a podľa toho ich zaradzujú do tried. Takto zaradeným paketom je priradená hodnota DSCP informujúca ostatné

zariadenia v sieti, ako majú narábať s týmito dátami. Reakcie zariadení na túto hodnotu je treba vždy definovať.

Štandardný postup je označovanie paketov priradením ich priority. Obmedzenie šírky pásma je krok vykonaný na základe priority paketu. To znamená, že označenému paketu sa pre uprednostnený prenos vyhradí určitá nastavená časť prenosového kanála. Je dôležité uviesť si, že QoS sa uplatní iba v prípade, ak nastane zahltenie linky [6]. To znamená, že ak pomocou QoS nastavíme dvadsať percent linky pre VoIP, neznamená to, že bude celý čas využívať iba nastavených dvadsať percent. QoS iba zaručujú týchto dvadsať percent v prípade ak bude linka zahltená.

5 BEZDRÔTOVÉ SIETE

Sú druhou najvyužívanjšou technológiou pre pripojenie koncových zariadení do lokálnych sietí. Bezdrôtové siete používané doma, alebo vo firme, majú označenie WLAN (Wireless Local Area Network) a štandardne pracujú s protokolmi zo skupiny protokolov 802.11X. Bezdrôtové siete umožňujú rýchle rozšírenie klasických metalických sietí LAN. Medzi verejnosťou je pre bezdrôtové siete rozšírený názov Wi-Fi (Wireless Fidelity), ktorý je obchodnou značkou Wi-Fi Aliancie. Táto aliancia udeľuje certifikáty pre bezdrôtové zariadenia určené na prevádzku v nelicencovanom pásme. Certifikované zariadenie znamená, že prešlo testovaním a je schopné spolupracovať s ostatnými certifikovanými produktmi určenými pre tento typ použitia. Kvalita prenosu je silno ovplyvnená prostredím cez ktoré sa signál musí šíriť. Wifi zariadenia sa nepoužívajú len pre pripojenie koncových zariadení, ale aj na premostenie sietí napríklad dvoch budov, kde z nejakého dôvodu nie je možné natiahnuť fyzický kábel.

5.1 Komunikácia po bezdrôtovej sieti

Pripojenie používateľa do siete zabezpečuje zariadenie kombinujúce vysielateľ a prijímač. Takýto bod na sieti sa nazýva prístupový bod AP (Access Point), ktorý je potom káblom pripojený do fyzickej siete. Každé AP má určitý konečný dosah, kedy je schopné komunikovať a prenášať dáta na pripojené zariadenie. Existuje niekoľko typov bezdrôtových sietí v závislosti od spôsobu prepojenia klientov. Všetky bezdrôtové siete využívajú jeden sieťový objekt identifikujúci sadu služieb SSID (Service Set Identifier), tvoriaci niečo ako sieťovú doménu, kde reprezentuje názov bezdrôtovej siete.

- IBSS (Independent Basic Service Set) vznikne, ak sa spolu prepoja dve a viac zariadení bez centrálného prístupového bodu. IBSS poskytuje základnú sadu služieb primárne určených na komunikáciu len medzi pripojenými zariadeniami. Táto sieť je typu peer-to-peer a nazýva sa aj Ad-hoc sieť.
- BSS (Basic Service Set) poskytuje základnú sadu služieb a tvoria ju klienti a jeden prístupový bod, ktorý sa identifikuje pomocou BSSID. Takejto sieti sa už hovorí infraštruktúrna sieť.
- ESS (Extended Service Set) je tiež infraštruktúrna sieť poskytujúca rozšírenú sadu služieb. Takáto sieť sa identifikuje indetifikátorom ESSID. Tento typ siete hovorí

o tom, že máme dva a viac prístupových bodov, ktoré spolu komunikujú a navyše sú aj v jednej podsieti.

Komunikácia medzi prístupovými bodmi v infraštruktúrálnej sieti môže byť vykonávaná pomocou prekrývajúcich sa prístupových bodov, alebo cez klasickú káblovú sieť. Takáto sieť sa potom nazýva distribučný systém a poskytuje rôzne výhody pre klienta. Tu už sa potom kombinuje bezdrôtový systém a káblová sieť. AP v pravidelných časových intervaloch vysiela SSID a pomocou neho oznamuje svoju prítomnosť pre klientov ktorý sa chcú pripojiť. Zariadenia pripojené do bezdrôtovej siete nekomunikujú spolu priamo, ale len prostredníctvom prístupového bodu. AP je zariadenie pracujúce na druhej vrstve, ktoré neustále počúva rádiovú prevádzku. Bezdrôtové zariadenia nevykonávajú detekciu kolízií a namiesto nej sa snažia kolízií vyhnúť. Komunikácia je poloduplexná a v jednom okamihu je možné dáta posielat', alebo len prijímať. Jedna metóda sa nazýva CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), využíva funkciu DFC (Distributed Coordination Function). Klient, ktorý chce prenášať dáta, najprv čaká a počúva sieť. Ak zistí, že je sieť voľná na prenos, počká ešte nejaký čas a následne odošle dáta. Po odoslaní očakáva potvrdenie o prijatí. V prípade ak iné zariadenie prenáša dáta, musíme počkať kým prenos skončí a plus ešte náhodný čas. Nevýhodou takéhoto prenosu je fakt, že ak je vzdialenosť medzi klientom a AP veľká, môže prísť k oneskoreniu potvrdenia o doručení. A práve vtedy môžu ostaný klienti začať odosielať svoje dáta. Druhou metódou a možným riešením popísaného problému je vylepšené CSMA/CA popísané štandardom IEEE 802.11 RTS/CTS. Táto metóda funguje na princípe PCF (Point coordination function), kde komunikáciu riadi iba prístupový bod. Klient, ktorý chce posielat' dáta, musí rovnako ako v predchádzajúcom prípade počkať kým sa sieť uvoľní. Potom pošle prístupovému bodu RTS (Request To Send) rámec reprezentujúci žiadosť o prenos s informáciou o predpokladanej dobe prenosu dát. Ak je prenosové médium voľné AP odošle potvrdenie CTS (Clear To Send) povoľujúci klientovi prenos. CTS rámec prijímajú aj ostatný klienti, pre ktorých to znamená obsadenie siete na určitú dobu. Po dokončení prenosu AP pošle rámec ACK, potvrdenie o prijatí a zároveň tým informuje ostatných klientov o ukončení prenosu a uvoľnení siete pre ďalší prenos.

5.2 Rámec 802.11

Siete WLAN sú definované štandardom IEEE 802.11, ktorý vyjadruje zapuzdrenie ethernetového rámca a následne jeho bezdrôtový prenos. Tento protokol určuje charakter takto zapuzdrených rámcov. Samotný rámec sa skladá z troch častí:

- Preambula.
- Hlavička PLCP.
- MAC PDU.

Preambula slúži na synchronizáciu prijímača, obsahuje postupnosť jednotiek a núl. Hlavička PLCP (Physical Layer Convergence Protocol) je súčasťou fyzickej vrstvy. MAC PDU obsahuje samotné dáta protokolu. Tieto dáta nie sú len užívateľské, ale aj informačné. MAC PDU sa skladá z nasledujúcich troch častí: hlavičky, užívateľské dáta a CRC kontrolný súčet. Hlavička obsahuje ďalšie informácie, medzi ktorými sú najvýraznejšie štyri políčka pre adresy. Oproti Ethernet rámcu sa ďalšie dve políčka používajú v závislosti na type prevádzkovanvej bezdrôtovej siete. Dve adresy sú štandardné, odosielateľ a príjemca. Tretia je fyzická adresa prístupového bodu kadiaľ bude rámec cestovať. Štvrtá adresa sa použije, ak prenášame dáta medzi počítačmi na priamo bez AP, adresa reprezentuje zariadenie, ktoré ako prvé odoslalo signálny rámec.

5.3 Štandardy

Ako už bolo spomenuté, bezdrôtové siete fungujú v bezlicenčnom pásme 2,4 GHz a 5 GHz. Štandard 802.11 bol nahradený novými štandardmi poskytujúce mnoho vylepšení. IEEE vydalo normy 802.11x, kde za x ide písmeno vyjadrujúce príslušnosť a typ normy použitej pre danú bezdrôtovú sieť. Samotný štandard 802.11 pri optimálnych podmienkach dosahuje rýchlosť prenosu 2 Mbps. Na prenos má vplyv aj typ použitej modulácie.

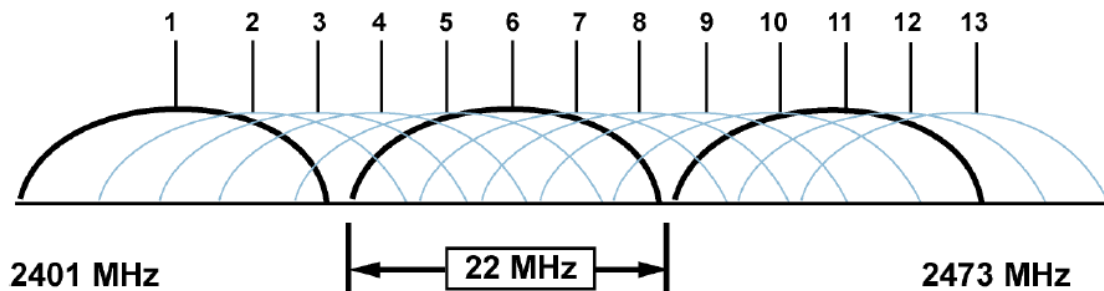
Tab. 4. Prehľad štandardov 802.11.

Štandard	Frekvenčné pásmo	Priepustnosť	Modulácia
802.11	5 MHz	2 Mbps	FHSS
802.11a	2,4 MHz	54 Mbps	OFDM
802.11b	2,4 MHz	11 Mbps	DSSS
802.11g	2,4 MHz	54 Mbps	OFDM
802.11n	2,4 MHz	248 Mbps	MIMO

Každý z týchto štandardov okrem svojej maximálnej prenosovej rýchlosti pri teoretickom sto percentnom využití prenosového kanála, poskytuje aj záložné rýchlosti použité v prípade, ak nie je možné využiť celú kapacitu kanála. Toto sa potom nazýva ako fallback.

802.11a využíva frekvenciu 5 MHz, kvôli ktorej má najväčší problém so stratou kvality signálu pri prechode cez prekážky a preto je dosah siete postavenej na tomto štandarde oproti ostatným normám menší. Teoretická maximálna rýchlosť je 54 Mbps. Fallback je 48, 36, 24, 18, 12, 9 a 6 Mbps. Šírka kanála je 20 MHz rozdelených na podkanály v počte 64 a o šírke 312,5 kHz. 12 kanálov je nevyužitých a 4 sú pilotné.

802.11b už pracuje na frekvencií 2,4 GHz. Maximálna rýchlosť 11 Mbps má fallback o rýchlosti 5,5, 2 1 Mbps. Každý kanál má šírku 22 MHz a v Európskej Únii je povolené používať kanály 1 až 13. Oproti 802.11a má väčší dosah a menšiu absorpciu pri prechode cez prekážky.



Obr. 4. Zobrazenie kanálov pre 802.1b a 802.1g [7].

802.11g jeho maximálna prenosová rýchlosť je 54 Mbps čo je porovnateľné so štandardom 802.11a, ale na rozdiel od neho funguje na frekvencií 2,4 GHz. Rozdelenie frekvencií je rovnaké ako u 802.11b, ale fallback je ovplyvnený moduláciou. Fallback o rýchlosti 54, 48, 36, 24, 28, 12, 9 a 6 Mbps používa OFDM. Pre rýchlosti 12, 5,5, 2 a 1 Mbps používa moduláciu DSSS, teda rovnako ako 802.11b a preto je aj s ním spätne kompatibilný, ale len pre tieto rýchlosti prenosu.

802.11n zvyšuje prenosovú rýchlosť na oboch frekvenciách využívaných 802.11a a 802.11g. Za ideálnych podmienok podľa dokumentácie IEEE môže dosiahnuť rýchlosť až 600 Mbps. Takéhoto výkonu je možné dosiahnuť pomocou modulácie MIMO, ktorá používa viacero antén pre vysielanie a príjem signálu.

5.4 Ochrana bezdrôtových sietí

Ochrániť tak veľký systém akým je bezdrôtová sieť pred neoprávneným použitím, je komplikovaná, ale veľmi dôležitá časť návrhu bezdrôtovej siete. Entita prístupu k sieti PAE (Port Access Entity) je komponent poskytujúci prístup k sieti a je to niečo ako logický port. Môže predstavovať žiadateľa o prístup na sieť (supplicant), autentifikátora predstavujúceho poskytovateľa prístupu, alebo oboje naraz. Existujú dva spôsoby prístupu na bezdrôtovú sieť: nezabezpečený a zabezpečený. Pri nezabezpečenej sieti sa každý, kto sa chce pripojiť, jednoducho pripojí a môže začať využívať služby poskytované touto sieťou. Proces umožnenia prístupu do zabezpečenej WLAN má tri fázy:

- Neautentifikovaný, Neasociovaný - anglicky Unauthenticated, Unassociate, toto je prvotný stav klienta pred prístupom na sieť.
- Autentifikovaný, Neasociovaný - anglicky Authenticated, Unassociated, preukázanie identity klienta voči sieti. Ešte ale nie je asociovaný s AP.
- Autentifikovaný, Asociovaný – anglicky Authenticated, Associated, po úspešnom overení identity klienta je asociovaný na AP a môže začať používať bezdrôtovú sieť.

Na to, aby sme mohli riadiť prístup na sieť, musíme mať autentizačný server. Tento server uchováva prístupové oprávnenia pre žiadateľov a odpovedá na žiadosti o autentifikáciu klientov. Takýto server je buď súčasťou prístupového bodu, alebo sa nachádza niekde na sieti. Žiadateľ požiada o prístup na sieť a posiela svoje identifikačné a prihlasovacie údaje autentifikátoru, ktorý ich následne pošle serveru na overenie. Server odpovie a na základe toho mu je prístup povolený, alebo zamietnutý. Overovanie so serverom najčastejšie prebieha pomocou protokolu RADIUS (Remote Authentication Dial In User Service). Okrem overovania identity klienta je veľmi dôležité zabezpečiť komunikáciu prenášanú medzi klientom a AP. Šifrovanie komunikácie zabezpečí súkromie prenášaných dát. Medzi základné metódy zabezpečenia bezdrôtových sietí je identifikátor SSID. Klient musí poznať SSID siete, do ktorej sa chce pripojiť. Pokiaľ AP vysiela SSID verejne a nemáme dodatočné metódy zabezpečenia, tak klient nemá problém s prístupom. Tomu sa hovorí otvorený systém (open system), ale ak jeho vysielenie skryjeme, klient bude musieť poznať názov siete a pokiaľ by ho nepoznal, nebol by schopný sa do siete pripojiť. Ďalším spôsobom je použitie zdieľaného kľúča, ktorý pozná klient aj AP. Ak obaja majú nastavené

rovnaké heslo a správy dokážu úspešne šifrovať a dešifrovať, tak v tom prípade klienta pripojí do siete. Toto heslo sa volá statický wep kľúč (Static WEP key). Treťou metódou je filtrovanie MAC adres a teda povoliť prístup len zariadeniu s povolenou fyzickou adresou MAC. Ak ale máme v sieti veľa prístupových bodov, je veľmi náročné spravovať jednotlivé AP osobitne. Na nastavovanie AP, riadenie prístupov a mnoho iného existuje centralizované riešenie. Spoločnosť Cisco ponúka zariadenie na správu bezdrôtových sietí WLC (Wireless LAN Controller). WLC kontroluje takzvané LWAP (Lightweight Access Point), sú to odľahčené AP, na ktorých sa nemusia robiť nastavenia priamo, ale komunikujú s kontrolórom WLC pomocou protokolu LWAPP (Lightweight Access Point Protocol) a ten už zabezpečí všetko potrebné. Roaming je prenos asociácie klienta z jedného AP na iné.

5.4.1 Autentifikácia 802.1X

Protokol 802.1X umožňuje zabezpečenie fyzického prístupu na sieť. Ak sa klient pripojuje na zabezpečenú bezdrôtovú sieť, tak na začiatku má zablokovanú inú komunikáciu, okrem komunikácie súvisiacej s overovaním klienta.

Protokol EAP je definovaný v RFC 3748 a samotný EAP (Extensible Authentication Protocol) pracuje na druhej vrstve. Služi na prenos autentifikačných dialógov medzi klientom v zastúpení suplikantom a napríklad Rádus serverom. Nie je to konkrétny spôsob autentifikácie a AP nemusí prenášanej komunikácií rozumieť, pretože ju len prenáša, ale nekontroluje. Pôvodne bol EAP určený pre LAN, ale je vhodný aj pre bezdrôtové siete na základe špecifikácie RFC 4017. Pre EAP existujú aj iné metódy využívajúce rôzne spôsoby autentifikácie.

EAP-MD5 je autentifikácia využívajúca heš, vytvorený z mena a hesla. Tento heš je odoslaný na server Radius a vyžaduje statický WEP kľúč. Nevyužívanie dynamicky generovaných kľúčov neznamená vyššie zabezpečenie oproti protokolu WEP. Klient si nedokáže žiadnym spôsobom overiť pravosť prístupového bodu a preto môže komunikovať aj s kompromitujúcim AP.

LEAP (Lightweight Extensible Authentication Protocol) je ďalšia metóda a protokol bol vyvinutý spoločnosťou Cisco Systems. K overovaniu sa používa meno a heslo, ale na rozdiel od EAP-MD5 sa pre každé pripojenie klienta jednorazovo dynamicky vygeneruje WEP kľúč. Z toho vyplýva, že každé zariadenie používa iný kľúč, ktorý nikto nepozná.

Pretože existujú časové limity pre spojenie, musí sa klient vždy nanovo prihlásiť. K zvýšeniu bezpečnosti sa musí aj AP autentifikovať voči klientovi.

PEAP (Protected Extensible Authentication Protocol) je v podstate zabezpečený EAP. Tento protokol vytvorí bezpečný tunel medzi klientom a Radius serverom. Overovanie je dvojfázové. V prvej fáze sa vytvorí šifrované spojenie a overí sa server pomocou TLS certifikátu. V druhej fáze sa voliteľným spôsobom overí klient. Existuje niekoľko verzií protokolu PEAP a sú vyvíjané spoločnosťami Microsoft a Cisco.

EAP-TLS používa na overovanie namiesto mena a hesla certifikát. TLS (Transport Layer Security) vytvorí zabezpečené spojenie medzi klientom a Radius serverom. Metóda zabezpečuje dynamické generovanie WEP kľúčov a vzájomné overenie klienta a servera pomocou svojich certifikátov.

5.4.2 Šifrovanie komunikácie v bezdrôtových sieťach

Protokol WEP (Wired Equivalent Privacy) vykonáva šifrovanie dát pomocou simetrickej šifry RC4. Používa sa 104 bitová fráza a náhodne vygenerovaný inicializačný vektor o veľkosti 24 bitov. Dohromady to predstavuje 128 bitové šifrovanie. Fráza predstavujúca naše heslo je spolu s inicializačným vektorom IV vložená do generátora pseudonáhodných čísiel. Výstupom bude postupnosť bitov, z ktorých sa vyberie sekvencia rovnakej dĺžky, ako je hodnota fráza plus inicializačný vektor. Táto sekvencia sa potom použije ako šifrovací kľúč, ktorý sa operáciu XOR skombinuje s dátami a ich kontrolným súčtom. Výsledkom je zostavený rámec 802.11, v ktorom sa ešte pred zašifrované dáta pridá inicializačný vektor. Proces dešifrovania je opakom šifrovania. Protokol WEP obsahuje slabiny, ktoré z neho robia menej bezpečný protokol.

WPA (Wi-Fi Protected Access) protokol je nástupcom WEP. Pretože je použitá šifrovacia metóda RC4, tak WPA je spätne kompatibilné s WEP. Vylepšenie spočíva vo využívaní protokola TKIP (Temporal Key Integrity Protocol), ktorý podporuje dynamicky sa meniace kľúče pre každý prenášaný paket. Pre overovanie integrity dát MIC (Message Integrity Code). je namiesto CRC použitý algoritmus, nazývaný Michael. WPA ponúka dve možnosti zabezpečenia:

- WPA-PSK nazývaný WPA Personal, kde sa používa zdieľaný kľúč tzv. master key. Táto možnosť je najčastejšie využívaná v domácnostiach.

- WPA bez přípony označuje nasazení v podnicích a velkých sítích. WPA Enterprise potřebuje autentizační server.

WPA2 je standard IEEE 802.11i a na rozdíl od WPA je jeho šifrovací mechanismus úplně odlišný a není schopen fungovat na slabších zařízeních, kde WEP a WPA nemají žádný problém. Na samotné šifrování se používá protokol CCMP, který implementuje šifrovací metodu AES (Advanced Encryption Standard). Umožňuje i kontrolu integrity přenášených dat. Rovnako jako WPA i WPA2 podporuje i stejné dvě metody zabezpečení. CCM vyžaduje pro každý rámec novou dočasnou hodnotu. CCM je autentizační šifrování pomocí algoritmu AES. AES je symetrická bloková šifra, která v CCMP používá 128 bitový klíč a 128 bitovou délku bloků.

5.4.3 Generování klíčů

Generování klíčů všeobecně závisí na zvoleném způsobu autentifikace. Nejprve se musí odvodit hlavní klíč PMK (Pairwise Master Key). To může znamenat dvě věci a to jak používáme sdílený klíč, tak $PMK = \text{sdílený klíč}$. Pokud používáme například Radius, tak PMK se odvodí z MSK (Master Session Key), který je závislý na zvoleném typu protokolu EAP. Samotné šifrování se nevykonává za použití PMK, ale pouze se z něj odvodzují klíče používané na šifrování. Klíč používaný právě pro aktuální spojení se nazývá PTK (Pairwise Transient Key). V případě broadcast, nebo multicast správ přístupový bod náhodně vygeneruje tzv. GTK (Group Transient Key), které vznikne z náhodně generovaného GMK (Group Master Key). Každému klientovi je potom GTK doručeno a používáno na šifrování a dešifrování přenášených dat. Výměna dočasných klíčů se nazývá 4-Way Handshake a umožňuje i rámce EAPOL klíče (EAPOL-Key Frames). V WPA a WPA2 se někdy dopočítava klíč do potřebné velikosti, protože ne vždy je na vstupu požadovaná délka dostupná. Používá se na to PRF (Pseudo-Random Function).

6 ZABEZPEČENIE POČÍTAČOVÝCH SIETÍ

6.1 Firewall

Každú sieť môžeme zaradiť do určitej skupiny sietí, kde každá skupina predstavuje určitú úroveň bezpečnosti pre používateľa. Lokálne siete môžeme prehlásiť za dôveryhodné. Tieto siete sa z pohľadu firewallu javia ako vnútorná sieť. Internet môžeme označiť za nedôveryhodnú sieť a z pohľadu firewallu je to vonkajšia sieť. Bez ohľadu na nasadenie firewallu, je jeho fungovanie založené na filtrovaní sieťovej komunikácie, ktorá cez neho prechádza. Firewall zabraňuje neoprávnenému vstupu do internej siete a dokáže obmedziť aj komunikáciu smerom von z tejto siete. Moderné firewally okrem filtrovania komunikácie umožňujú aj jej kontrolu. Existuje niekoľko typov firewallov vykonávajúcich kontrolu na rôznych úrovniach:

- Bezstavový firewall – je zariadenie vykonávajúce základnú funkcionality pri ochrane siete. Pri príchode paketu na rozhranie firewallu sa kontroluje zdrojová a cieľová adresa, prípadne aj cieľový port. Tieto informácie sa následne porovnávajú nastavenými pravidlami a podľa toho sa paket pustí ďalej, alebo sa zahodí.
- Stavové firewally – vyššia verzia firewallov, ktoré okrem paketového filtru kontrolujú aj každé spojenie prislúchajúce danému paketu.
- Aplikačný firewall – pod týmto pojmom si môžeme predstaviť proxy server, ktorý slúži ako prostredník medzi klientom a požadovaným serverom. Proxy kontroluje informácie na aplikačnej vrstve a vďaka tomu dokáže kontrolovať a prebrať služby poskytované protokolmi HTTP, FTP, ICMP, POP a podobne.

Bezstavová kontrola kontroluje len informácie tretej vrstvy a preto nie je schopná dostatočne ochrániť vnútornú sieť pred falošnými paketmi. Pri stavovej kontrole sa berú do úvahy informácie obsiahnuté na štvrtej vrstve OSI modelu. Paket sa kontroluje, či patrí do už aktívneho spojenia, alebo sa musí založiť nové. Na aplikačnej vrstve sa kontroluje len paket zahajujúci nové spojenie. Aktívne spojenia sa nachádzajú v takzvanej stavovej tabuľke. Ak sa kontrolovaný paket radí do už aktívneho spojenia, tak je mu umožnené prejsť. Ak tento paket zakladá nové spojenie, musí sa porovnať s príslušnými pravidlami a ak im nevyhovuje, bude zahodený. Táto metóda kontroly všeobecne urýchľuje činnosť

firewallu. Stav je aktuálna podoba danej komunikačnej relácie. Avšak definícia sa pre daného klienta, alebo komunikačnú reláciu môže meniť podľa aplikácie, ktorú využívajú na vzájomnú komunikáciu a protokolu, ktorý ju prenáša. Každá položka stavovej tabuľky obsahuje určité informácie, ktoré jednoznačne identifikujú danú reláciu. Položka v stavovej tabuľke sa vytvorí v okamihu zahájenia spojenia prechádzajúce cez stavové zariadenie. Pri návrate sa potom porovnávajú informácie v pakete s informáciami nachádzajúcimi sa v stavovej tabuľke a tým zistí, či patrí do platnej komunikačnej relácie. Ak sa paket zhoduje, tak je mu umožnené prejsť. Preto musia byť informácie uložené v stavovej tabuľke čo najpodrobnejšie [8]. U rôznych protokolov sa ich stavy kontrolujú na základe rôznych atribútov. Aplikačné firewally sa pre klienta javia ako žiadaný server, ktorý v skutočnosti prevezme klientovu žiadosť o nadviazanie spojenia a vo svojom mene ju preniesie na skutočne požadovaný server. Tento server odpovie nášmu proxy serveru a ten následne tieto dáta preniesie klientovi. Výhodou takéhoto riešenia je fakt, že celá komunikácia prebieha cez proxy server, ktorý kontroluje informácie obsiahnuté v jednotlivých paketoch. Istou formou filtrovania komunikácie je kontrolovať oprávnenia používateľa, ktorý chce využívať nejaké služby siete. Preto môže byť pred spustením komunikácie požadované nejakým spôsobom sa na server proxy prihlásiť. Nedostatkom proxy serverov je ich problém so spracovaním šifrovanej komunikácie, kde nemôže kontrolovať obsah prenášaných dát. Niektoré firewally ponúkajú funkciu detekcie sieťového napadnutia IDS (Intrusion Detection System), ktorý kontroluje dátové prenosy a identifikuje prípadné hrozby pomocou určitých signatúr a následne môžu aj adekvátne reagovať. Systém IDS štandardne nezasahuje do prenosov a väčšinou slúži len na sledovanie komunikácie. Signatúra predstavuje určitý vzor, ktorý sa hľadá v sieťových prenosoch. Nadstavbou IDS je IPS (Intrusion Prevention Systems), ktorý okrem informovaní o prieniku je schopný voči nemu konať, zmierňovať jeho prejavy, alebo ho úplne zastaviť. Existuje veľké množstvo signatúr, pomocou ktorých sa môže kontrolovať premávka. Nevýhodou tohto systému je, že ak používame špecifikované signatúry, tak po zmene spôsobu vykonania útoku už detekcia nemusí byť úspešná. Všeobecnejšie signatúry zas môžu oznamovať väčšie množstvo falošných poplachov a bude nutné signatúry doladiť.

6.2 Prístupové zoznamy

Počas prechodu dát firewallom sa každý paket kontroluje a porovnáva s pravidlami nastavenými vo firewalle. Základné porovnávajúce kritéria sa nazývajú zoznamy riadenia pístupu ACL (Access Control List). Pomocu ACL sa dajú nakonfigurovať pravidlá, pomocou ktorých sa kontroluje zdrojová a cieľová adresa a port. Pri štandardnom zápise ACL sa používa zápis pomocou inverznej masky, ktorá je binárnym opakom masky podsiete. Každé ACL sa vždy musí umiestniť na dané rozhranie a pre určitý smer. Existujú dva rôzne smery, vstupný a výstupný.



Obr. 5. Logika použitia ACL.

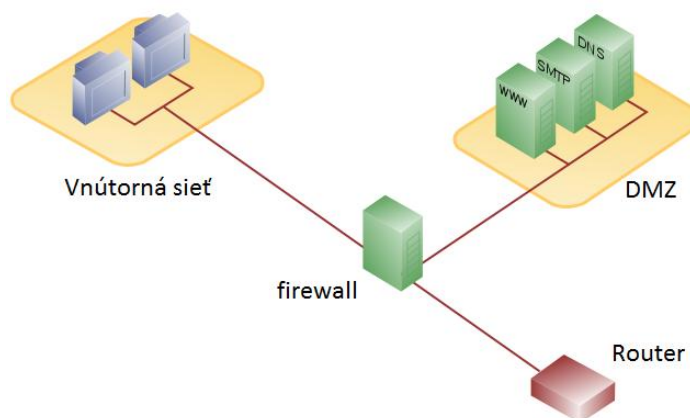
Rozhodnutie, na ktorý smer ACL nastaviť, musí byť urobené z pohľadu zariadenia. Nesprávne umiestnené ACL spôsobí čiastočnú, alebo úplnú nefunkčnosť komunikácie.

- Štandardné ACL – kontroluje sa len zdrojová adresa. Povoľujem, alebo zakazujem celú skupinu protokolov.
- Rozšírené ACL – kontroluje sa zdrojová aj cieľová adresa spolu s definovaným portom.
- Číslované a pomenované ACL – uľahčuje identifikáciu.
- Komplexné ACL – pozostáva z dynamických, reflexívnych a časových zoznamov.

Princíp pracovania ACL je, že firewall kontroluje definované pravidlá po riadkoch smerom od vrchu dole. Ak nastane zhoda, porovnávanie sa ukončí a paket je následne preposlaný, alebo zahodený. Na konci zoznamu je vždy riadok, ktorý zakáže všetku komunikáciu. Z toho vyplýva, že na začiatku je všetko zakázané a pokiaľ to nebude povolené, tak sa to nakoniec aj tak zahodí.

6.3 Demilitarizovaná zóna

DMZ (demilitarized zone) je z pohľadu bezpečnosti logická, alebo fyzická sieť. Ak by sme vnútornú sieť označili za dôveryhodnú a Internet za nedôveryhodnú, tak DMZ by bola niečo ako polodôveryhodná sieť. Zariadenia umiestnené v demilitarizovanej zóne sú dostupné z Internetu a tiež aj z internej siete podniku. Úroveň prístupu pre používateľov týchto sietí je rôzna. Pri vytváraní DMZ je vždy potrebné zvážiť, či zariadenia v nej umiestnené budú môcť pristupovať do vnútornej siete podniku. DMZ je nezávislá a teda má úplne iný adresný rozsah ako vnútorná sieť a je oddelená od Internetu aj vnútornej siete firewallom. V demilitarizovanej zóne môžeme používať privátne a aj verejné IP adresy. Všetko záleží na architektúre a konfigurácii firewallu.



Obr. 6. Model DMZ [9].

Ak máme firewall s tromi a viac sieťovými rozhraniami (three legged firewall), tak jeden firewall môže obsluhovať všetky siete. Použitie architektúry jedného firewallu sa nazýva trihomed DMZ. Existuje niekoľko dôležitých pravidiel, ktoré by sa mali kontrolovať pri používaní demilitarizovanej zóny:

- prichádzajúca prevádzka z Internetu do DMZ,
- prichádzajúca prevádzka z DMZ do vnútornej siete,
- prichádzajúca prevádzka z Internetu do vnútornej siete,
- odchádzajúca prevádzka z vnútornej siete do DMZ,
- odchádzajúca prevádzka z vnútornej siete do Internetu,
- odchádzajúca prevádzka z DMZ do Internetu.

Okrem jedného firewallu je možné použiť dva, ktoré nám spoločne zvyšujú úroveň zabezpečenia. Takéto riešenie sa nazýva back to back DMZ. Prvý firewall (front-end firewall) bude tzv. Internet edge a teda prepojuje Internet do DMZ. Druhý firewall (back-end firewall) bude predstavovať zvýšené zabezpečenie pre vnútornú sieť a bude slúžiť na prepojenie tejto siete s demilitarizovanou zónou.

6.4 VPN

Technológia VPN (Virtual Private Network) sa najčastejšie používa na prepojenie dvoch bodov cez Internet, ktoré sú za normálnych okolností medzi sebou nedostupné. VPN poskytuje rôzne úrovne bezpečnosti tak aby posielané dáta zostali ochránené a izolované od ostatných počítačov v Internete. Spolu môžeme prepojiť jednotlivých užívateľov, alebo viaceré siete tak ako keby sme sa nachádzali v jednej lokálnej sieti. Pomocou VPN sme schopný využívať zdroje vzdialenej siete ako sú zdieľané súbory, tlačiarne, databázy, alebo interný webservice. Takýto typ spojenia sa vytvára medzi počítačmi, ktoré sú pripojené k Internetu. Pre pripojenie do firemnej siete sa musí najprv spustiť VPN server, ktorý plní funkciu brány a zabezpečuje pripojenie, zabezpečenie a šifrovanie celej komunikácie. VPN zabezpečuje nasledovné funkcie:

- vzdialený prístup – pripojenie samotného počítača k vnútornej sieti,
- site-to-site – prepojenie dvoch geograficky oddelených vnútorných sietí,
- 6in4 tunel – prepojenie dvoch IPv6 sietí cez IPv4 sieť.

Niektoré protokoly pre prenos VPN:

- IPSec (Internet Protocol Security): vyvinutý IETF ako štandard bezpečnostného protokolu. Zabezpečuje autentifikáciu a šifrovanie prenášaných dát. Dešifrovanie informácie prebieha na konci tunela odkiaľ je následne smerovaný do svojho cieľa.
- SSL/TLS (Secure Sockets Layer/Transport Layer Security): môže tunelovať celú sieťovú prevádzku, alebo jednotlivé spojenia.

Pomocou SSL (Secure Sockets Layer) sa veľmi často vytvára zabezpečený prenosový tunel pomocou webovo orientovaného SSL bežiacom nad portom 443. Okrem šifrovania web komunikácie dokáže šifrovať aj prenos iných protokolov. Zostavenie spojenia je založené na používaní verejného a súkromného kľúča. Každá strana vlastní túto dvojicu kľúčov. Pri

komunikácií IPsec susedov je dôležitým krokom dohodnúť parametre spojenia. Toto dohadovanie sa nazýva Security Association (SA). Vytváranie a spravovanie SA má na starosti protokol ISAKMP resp. IKE. Pomocou procesu výmeny kľúčov. Vytvorenie spojenia má dve fázy. V prvej fáze sa dohodne politika a bezpečnostné parametre potrebné k vytvoreniu bezpečnému spojeniu. Druhá fáza výmeny kľúčov využíva zostavený tunel z prvej fázy. Vymieňajú sa ďalšie parametre, ktoré budú používané pri prenose používateľských dát. Pred prvotnou komunikáciou pomocou IPsec si každá strana musí overiť totožnosť tej druhej strany a pomocou zdieľaného kľúča, alebo pomocou certifikátu. Rozdiel medzi protokolom IPsec a SSL je v tom, že IPsec vytvorí jeden tunel pomocou ktorého prenáša všetky dáta. Protokol SSL musí pre každú aplikáciu zaviesť samostatné spojenie a tunel [8].

6.5 Preklad sieťových adries

Dobre nastavený hraničný firewall by ani nemal odpovedať na požiadavky protokolu ICMP. Firewall nesmie umožniť priamu komunikáciu zariadeniu v Internete so zariadením vo vnútornej sieti. IP adresy určené pre vnútorné siete sa nemôžu v Internete používať a takáto komunikácia je firewallom implicitne blokována. Na to aby zariadenie z vnútornej siete mohlo komunikovať so zariadeniami umiestnenými mimo vnútornej siete je potrebné použiť preklad sieťových adries.

- NAT (Network Address Translation) – je preklad interných adries na verejné.
 - Statický NAT - Štandardne je preklad vykonávaný 1:1.
 - Dynamický NAT – prekladá na verejnú IP adresu vybranú zo zoznamu pridelených verejných adries.
- PAT (Port Address Translation) – niekedy nazývaný aj preťažený NAT. Prekladá vnútorné IP adresy na jedinou verejnú adresu. Preložené adresy rozlišuje pomocou rôznych portov. Ak je to možné PAT sa snaží zachovať pôvodný port.

Pomocou prekladu sieťových adries sa vyriešil problém s nedostatkom verejných adries IPv4. Preklad sieťových adries je najčastejšie vykonávaný práve na firewalloch. Server umiestnený v Internete nevidí klienta a pozná iba verejnú adresu registrovanú pre daný firewall. Preklad sieťových adries môže spôsobovať problémy pre niektoré protokoly a aplikácie ktoré vkladajú IP adresu priamo do paketu.

II. PRAKTICKÁ ČASŤ

7 PŮVODNÝ STAV FIREMNEJ SÍTE

Firma, v ktorej sa inovácia počítačovej siete realizuje, sa zaoberá elektrotechnickou výrobou pre rôzne svetové spoločnosti. Ako stabilný a strategický partner si plne uvedomuje potrebu inovácie svojej súčasnej informačnej infraštruktúry. Spoločnosť zamestnáva množstvo ľudí a pre každého z nich sa snaží zabezpečiť čo najlepšie pracovné podmienky. Svojim zamestnancom ponúka najvyšší komfort a poskytuje im kvalitnú výpočtovú a inú techniku, potrebnú pre dosahovanie najvyššej kvality pre svoje výrobky.

7.1 Zariadenia nachádzajúce sa na sieti

Vo firemnej sieti sa nachádzajú rozličné typy zariadení slúžiace v procese výroby, ale aj v administratívnej časti budovy. V súčasnosti sa do siete pripájajú aj inteligentné zariadenia uľahčujúce komunikáciu a výmenu informácií medzi zamestnancami firmy. Ako štandardné zariadenia pripojené do internej siete podniku môžeme vymenovať nasledujúce produkty:

- Stolové počítače.
 - Operačný systém Windows XP, Windows 7, Linux.
 - Rýchlosť pripojenia sieťových kariet je 10, 100 a 1 Gbps.
 - Nemajú pripojenie na bezdrôtovú sieť.
- Prenosné počítače.
 - Operačný systém Windows XP, Windows 7, Linux.
 - Rýchlosť pripojenia sieťových kariet je 10, 100 a 1 Gbps.
 - Pripojenie do bezdrôtovej siete.
- Počítače All-in-One.
 - Rýchlosť pripojenia sieťových kariet je 100 Mbps.
 - Pripojenie do bezdrôtovej siete rýchlosťou 54 Mbps.
- Inteligentné zariadenia.
 - Operačný systém Android a iOS.
 - Pripojenie do bezdrôtovej siete.
- Servery.
 - Operačný systém Windows Server 2003, 2008 a 2012.
 - Pripojenie do lokálnej siete o rýchlosti 1 Gbps.

- Sieťové tlačiarne.
 - pripojené sieťovou kartou o rýchlosti 100 Mbps.
- IP telefóny.
- Diskové pole Netapp.
- Pásková knižnica.
- Aktívne sieťové prvky.
 - Firewall PIX505 a 515, ASA 5505 a ASA5510.
 - Catalyst switch 2950, 3560, 3750.
 - AP Cisco Aironet.

Tieto zariadenia sú pripojené do lokálnej siete, ktorá ma relatívne vhodne navrhnutú fyzickú architektúru, ale jej logické členenie predstavuje problematickú správu pre správcu siete. Pretože firma má narastajúce požiadavky na efektivitu práce, ktorá je priamo závislá na informačných prostriedkoch spoločnosti, je potrebné vykonať určité zmeny reflektujúce na nové trendy a súčasný stav sieťovej infraštruktúry

7.2 Požiadavky na novú počítačovú sieť

V súčasnej sieti je pripojených približne 500 zariadení rôzneho druhu. Každý typ zariadenia má určené svoje použitie. Firemná politika zaručuje jednotnosť pri nákupe nových zariadení a tak by nemala nastať nekompatibilita systémového riešenia so zariadeniami prístupujúcimi k sieti. V prípade potreby zmeny špecifikácie pre tieto zariadenia, je táto požiadavka najskôr konzultovaná s príslušným IT oddelením. Spoločnosť plánuje a pokračuje vo výmene starých zariadení nespĺňajúcich nové štandardy a trendy v oblasti výpočtovej techniky. Preto bola stanovená minimálna rýchlosť prístupu k sieti pre všetky nové zariadenia:

- 100 Mbps pre zariadenia pripájajúce sa pomocou sieťovej karty LAN.
- 54 Mbps pre bezdrôtovú sieť a kompatibilita so štandardom 802.11N.

Avšak v terajšej sieti sa stále nachádzajú zariadenia pracujúce pomocou starých štandardov a pre tieto je potrebné prispôbiť prístupovú vrstvu minimálne na mieste, kde sa takéto zariadenie nachádza. Nová požiadavka bola okrem kancelárskych priestorov zabezpečiť pokrytie bezdrôtovou sieťou aj výrobnú halu. Tým sa naskytla možnosť niektoré zariadenia

používané v procese výroby pripojiť do podnikovej siete a to aj v prípade, ak nie je možnosť toto spraviť pomocou ethernetových káblov.

- Každý používateľ v administratívnej časti musí mať prístup na sieť. To platí aj pre budúcich zamestnancov.
- Každý zamestnanec v administratívnej časti má jeden stolový telefón. To neplatí pre niektorých mobilných zamestnancov administratívy.
- Vybraní zamestnanci vo výrobe majú stolové počítače a telefóny.
- Pre administrátorov siete je potrebné zabezpečiť prístup do všetkých podnikových podsietí.
- Jednotlivé siete je potrebné s ohľadom na ich používanie od seba oddeliť, alebo aspoň obmedziť do nich prístup.
- Pre administrátorov je potrebné zabezpečiť možnosť externého pripojenia do firemnej podnikovej siete.
- Návštevníci by nemali mať prístup do vnútornej siete určenej pre zamestnancov.

Okrem toho bolo potrebné sieť rozdeliť na niekoľko samostatných celkov prispôbených pre určité služby poskytované sieťou. Pre firmu je veľmi dôležité chrániť svoje záujmy a informácie kvalitnými bezpečnostnými prvkami. Hraničné zariadenia bolo potrebné vymeniť za nové a pretože firma chce poskytovať pre svojich zákazníkov niektoré služby, ktoré si vyžadujú istý stupeň zabezpečenia, musia byť splnené okrem bezpečnostných aj výkonnostné parametre. Nesmieme zabúdať ani na bezpečnosť vo vnútornej sieti pomocou aktívnych prvkov siete a bezpečnostného softvéru na koncových zariadeniach.

Ako posledná požiadavka bolo pripojiť do firemnej siete novú budovu. V tomto momente sa v novej budove nenachádzajú koncové zariadenia a zatiaľ je potrebné len umiestniť kontaktné body pre prípadnú, alebo plánovanú požiadavku pripojenia do firemnej siete. Predpokladaná maximálna kapacita siete v novej budove je porovnateľná so starou budovou.

8 NOVÝ STAV FIREMNEJ SIETE

8.1 Adresovanie vo vnútornej sieti

Návrh adresovania a rozdelenia podnikovej siete musel vychádzať z jednotlivých požiadaviek zameraných na funkcionality určenú pre danú sieť. Vo veľkých spoločnostiach je vhodné logicky oddeliť jednotlivé časti siete a tým zvýšiť bezpečnosť prenášaných dát. Logická segmentácia siete umožňuje administrátorom lepšie sieť spravovať a obmedziť nechcenú komunikáciu na miesta, kde nie je potrebná.

Tab. 5. Adresovanie v sieti.

VLAN	SSID	číslo VLAN	sieťový rozsah
KancelVL	Kancelarie	31	172.30.31.0 /22
NavstevaVL	Navsteva	32	192.168.32.0 /24
PushVL	Push	33	192.168.35.0 /24
VyrobaVL	Vyroba	34	172.30.34.0 /22
NativVL	N/A	40	N/A
ManazmentVL	N/A	44	172.30.44.0/24
BmanazmentVL	N/A	45	172.30.45.0/24
BkancelVL	Bkancel	61	172.30.61.0 /22
BvyrobaVL	Bvyroba	64	172.30.64.0 /22
MPLS	N/A	101	10.100.10.5 /26
DMZ	N/A	150	192.168.150.0 /24

Podniková sieť bola rozdelená na niekoľko virtuálnych sietí. Nasadenie každej podsiete bolo špecifikované pre dané účely využitia. Základom pre každú podsieť je trieda, z ktorej bol odvodený sieťový rozsah. Virtuálne siete určené pre zamestnancov pozostávali z triedy B. Návšteve bol určený sieťový rozsah z triedy C.

- KancelVL – sieť určená pre zariadenia pripájajúce sa do firemnej siete. Zariadenia v tejto sieti majú prístup na Internet, používajú E-mail a iné služby poskytované sieťou.
- NavstevaVL – určená pre návštevníkov, ktorý prídu do firmy a požadujú prístup na Internet. Táto sieť je úplne oddelená od ostatných vnútorných sietí.
- PushVL – niektorí zamestnanci využívajú služby Push Email na svojich inteligentných telefónoch. Okrem toho využívajú aj iné služby prevádzkované cez Internet. Aj táto sieť je oddelená od ostatných vnútorných sietí.

- VýrobaVL – výrobné stroje a zariadenia používané v procese výroby sa pripájajú do tejto siete. Táto VLAN nemá prístup do Internetu a do iných vnútorných sietí nemá žiaden, alebo obmedzený prístup.
- NativVL – natívna VLAN, používaná pri prepojení prepínačov a smerovačov pomocou Trunku.
- ManazmentVL – toto je čisto vyhradená sieť pre nastavenie manažment IP aktívnych sieťových zariadení.
- BkancelVL a BvyrobaVL – sú siete používané v druhej budove B. Použitie majú identické s KancelVL a VyrobaVL.
- MPLS – slúži na prepojenie medzi pobočkami firmy.
- DMZ – do tejto siete bude umiestnený verejne dostupný webserver.

Všetky siete ktoré majú svoj adresný priestor ho majú pridelený pomocou DHCP servera. Zariadenie v DMZ a aktívne sieťové prvky mali IP adresy pridelené administrátorom. Bezdrôtové zariadenia sa s ohľadom na svoje zaradenie pripájajú do rovnakej VLAN ako by sa pripájali v prípade použitia káblového pripojenia.

8.2 Zásady pre pomenovanie zariadení na sieti

Pomenovanie zariadení na sieti bolo vytvorené tak, aby administrátor vedel určiť funkciu daného zariadenia z jeho názvu. Hostiteľský názov by mal byť ľahko zapamätateľný. Ak tomu tak nie je a názov je horšie zapamätateľný ako IP adresa, tak takéto pomenovanie je kontraproduktívne. Ak používame FQDN názvy, tak nie je rozumné používať dlhé pomenovania, aby sa po pripojení názvu domény celkový názov zbytočne neskomplikoval [6]. Firemná politika už mala zavedenú konvenciu pre pomenovanie sieťových zariadení a vychádzala z myšlienky čo najlepšie identifikovať dané zariadenie. Názov zahŕňa lokáciu, typ zariadenia a jeho číslo. Podrobnejšie informácie o danom zariadení je možné získať z internej dokumentácie podniku. Len pripomeniem, že pri pomenovaní zariadení je potrebné si uvedomiť obmedzenia týkajúce sa systému DNS.

8.3 Návrh topológie LAN

8.3.1 Prenosové média

Prepojenie medzi jednotlivými prepínačmi bolo uskutočnené buď pomocou optického kábla, alebo metalickej kabeláže. S ohľadom na budúci trend v oblasti zvyšovania prístupovej rýchlosti bola pre prepojenie aktívnych prvkov siete použitá výlučne gigabitová technológia. Použitá metalická kabeláž bola kategória šesť a kategória päť. Všetky káble kategórie šesť boli tienené typu FTP, alebo STP. Kabeláž kategórie päť môže byť s ohľadom na miesto použitia tienená, alebo netienená. Materiál použitý na opláštenie bol z PVC, alebo LSOH kvôli obmedzeniu vzniku spalín v prípade, ak nastane jeho horenie. Optická kabeláž pozostávala z viacvidového kábla o priemere 50/125 μm .

8.3.2 Aktívne prvky siete

Niektoré aktívne sieťové prvky nachádzajúce sa vo firemnej sieti nespĺňali funkčné kritéria kladené na budovanú sieť. Ako najväčší nedostatok bolo možné pokladať nemožnosť vzdialenej správy zariadenia, či už pomocou webového rozhrania, alebo aspoň vzdialeného spojenia pomocou Telnetu. Takýmto zariadením bol napríklad prepínač Allied Telesyn AT-FS724i a AT-8026FC, ktorý obsahoval aj optické rozhranie. Ako hlavné prepínače boli zvolené Catalyst 3560G-24TS a Catalyst 3750G-24TS, oba o veľkosti 1U. Toto sú viacvrstvové prepínače a okrem prepínania rámcov dokážu pracovať aj na vyšších vrstvách, vrátane tretej sieťovej vrstvy.

Pre budovu A bol pre vrstvu jadra zvolený súčasný Catalyst 3560G-24TS :

- Pracuje na vrstve L2 a L3.
- Podporuje rýchlosti 100 a 1000 Mbps.
- Možnosť pripojenia 4x 1Gbps SFP.
- IP Unicast a Multicast smerovanie.
- STP:
 - UplinkFast, BackboneFast, PortFast, 802.1s/w .
- Združovanie portov:
 - EthernetChannel podporujúci 100 Mbps a 1 Gbps.
 - 802.3ad, PAgP a LACP.

- L2 PVST , L3 ECR, CEF.
- DTP, VTP, CDP.
- Podpora DHCP.
- Zabezpečenie:
 - ACL, SSH, Kerberos, SNMPv1-3, HTTPS.
 - DHCP Snooping, port security, 802.1x, SPAN.
- QoS:
 - Priorita fronty.
 - 802.1p COS a DSCP.
 - Ochrana pred zahltením.
 - Auto QoS.

Pre budovu B tvorí jadro Catalyst 3750G-24TS. Je to nástupca 3560 a parametricky je s ním podobné, ale má určité vylepšenia oproti svojmu predchodcovi.

- Umožňuje až deväť prepínačov 3750 ukladať do stohu (stack).
 - Cisco StackWise umožňuje prepojenie rýchlosťou 32 Gbps.
 - Pripojenie zariadení spôsobom Plug-and-Play.
- Obsahuje múdre porty (smartports), ktoré aplikujú makrá.
- Podporuje Tacacs+ a Radius.
- Podpora pre Jumbo frames.

Distribučná vrstva spolu s prístupovou vrstvou pozostáva zo zariadení Catalyst 2950 a modelu 2960. Dôraz sa kladie na uplinkové porty, ktoré musia umožňovať minimálnu rýchlosť prenosu 1 Gbps a v prípade distribučných prepínačov umiestnených vo výrobní hale musia obsahovať optické pripojenie.

Základné vlastnosti Prepínača Catalyst 2960:

- Pomocou Cisco FlexStack, môžeme umiestniť až štyri prepínače do stohu.
- Podpora SFC modulov 1 Gbps.
- Podpora PoE.
- Security:
 - 802.1x, RADIUS, TACASC.
 - Bezpečnosť portov, inšpekcia ARP, IP zdrojová ochrana.
- QoS:
 - Auto QoS.

- Cross-stack QoS.
- Makrá:
 - Smart porty.
 - Inteligentný riešiteľ problémov.
- STP, MSTP, RSTP.

Cisco svoju radu prepínačov Catalyst rozdeľuje do viacerých podskupín. Každá z týchto podskupín obsahuje určité technické riešenia, ponúkajúce nastaviť výkonnosť siete podľa rôznorodých požiadaviek a výšky dostupných finančných prostriedkov. Rada 2960 je navyše rozdelená na dva modely. Základný model je prepínač s IOS LAN Base (-L). Jeho výkonnosťne obmedzenejšia verzia je model označovaný ako LAN Lite (s modelovou píponou -S).

Postup obmeny zariadení bol vykonávaný nasledovne:

- Pokazené zariadenia.
- Zariadenia, ktoré nemali možnosť vzdialenej správy.
- Zariadenia, ktorých zostávajúca voľná kapacita pre pripojenie koncových zariadení bola nedostačujúca.
- Zariadenia s nedostatočným výkonom, alebo technickým vybavením.

Všetky prepínače nachádzajúce sa vo firemnej sieti poskytujú maximalný výkon, odolnosť voči chybám, vysokú spoľahlivosť a centralizovanú správu. Zariadenia, ktoré spĺňajú minimálne výkonnosťné požiadavky, sa vymieňajú priebežne.

Firewally ASA sú nástupcom firewallov rady PIX. Pre malé a stredne veľké spoločnosti je určená ASA 5505. Stredne veľké až väčšie spoločnosti by sa mali zamerať na model 5510 a viac. Oba modely podporujú funkcionality IPS, ktorá ale nepatrí do základnej výbavy. Ďalšou doplnkovou výbavou je kontrola obsahu, ktorá ale nie je podporovaná v najnižšom modeli 5505. Nastavovanie firewallu môže byť vykonávané v dvoch prostrediach. Prvý spôsob je použitie príkazového riadku. Druhý spôsob predstavuje používateľsky intuitívne grafické rozhranie ASDM (Adaptive Security Device Manager).

Tab. 6. Porovnanie firewallov ASA 5505 a 5510.

	ASA 5505	ASA 5510
max priepustnosť	150 Mb/s	300 Mb/s
IPS priepustnosť	75 Mb/s	150 - 300 Mb/s
max počet spojení	10 000 / 25 000	50 000 / 130 000
Max počet spojení	4 000	9 000
paket / s (64 byte)	85 000	190 000
3DES/AES VPN priepustnosť	100 Mb/s	170 Mb/s
site-to-site VPN spojenie	25	250
VPN užívateľských spojení	25	250
VLANy	20	50 / 100
HA podpora	nie	nie, A/A a A/S
porty	8 (2 s PoE) - FE	5 / 5(2) - FE
USB 2.0	3	2
RAM	512 MB	1 GB
Min. veľkosť pamäte Flash	128 MB	256 MB

Nevýhodou týchto zariadení je licenčná politika. Základná verzia licencie pre 5505 obsahuje rôzne obmedzenia napríklad pre počet tunelov VPN, VLAN, alebo flexibility pre DMZ. Zariadenia ASA dokážu smerovať pakety medzi jednotlivé VLAN a vystupovať ako DHCP server. Pomocou týchto zariadení dokážeme vytvoriť tunel medzi dvoma rôznymi lokálnymi sieťami a využívať ich služby. Používatelia môžu na prístup do firemnej siete použiť protokol IPSec, alebo SSH. Všetky firewally rady 5500 predstavujú kvalitné zariadenia pre ochranu vnútorných sietí.

8.3.3 Základné ovládanie zariadení Catalyst

Operačný systém prepínačov spoločnosti Cisco je IOS (Internetwork Operation System). Samotné konfigurácie sa vykonávajú v niekoľkých užívateľských režimoch.

- Interaktívny režim – je to konfiguračný dialóg, ktorý pomáha administrátorovi pri konfigurácii zariadenia.
- Užívateľský režim – zobrazuje sa ihneď po prihlásení do zariadenia. Je obmedzený len na základné kontrolné použitie.
- Privilegovaný režim – v tomto režime je možné kontrolovať všetky nastavenia a je povolený prístup na vykonávanie monitorovacej činnosti. Okrem toho je z neho možné ukladať a spravovať konfiguráciu.

- Globálny režim konfigurácie – využívaný na konfiguráciu systémových nastavení a služieb.
- Režim rozhrania – v tomto režime sa konfiguruje konkrétne rozhranie zariadenia.

Každý z týchto režimov je špecifický a vždy umožňuje vykonávať len určité nastavenia. Každá zmena a nastavenie je v prípade príkazového riadka CLI (Command Line Interface) vykonávaná postupnosťou príkazov zadávaných v príslušných režimoch. Skúsený administrátor by mal mať jasno, čo sa v ktorom režime konfiguruje a aké jednotlivé príkazy sa pri tom používajú. Väčšina týchto zariadení má možnosť základné nastavenia vykonať pomocou webového rozhrania. Klasická konfigurácia je vykonávaná pomocou konzolového pripojenia, SHH, prípadne Telnet, alebo iným dostupným rozhraním špecifickým pre dané zariadenie.

8.4 Topológia budovy A

Táto budova pozostáva z viacerých oddelení charakteristickými svojou pracovnou činnosťou. Ako základné delenie môžeme budovu rozdeliť na nasledujúce časti:

- Kancelárske priestory.
- Výrobné priestory.
- Sklad.
- Konferenčné miestnosti.

Nie každý zamestnanec potrebuje využívať všetky služby poskytované sieťou a preto nie je vždy na každom mieste v budove umožnený prístup do každej siete. Základná myšlienka topológie vychádzala z modelu trojúrovňovej architektúry. Trojvrstvová architektúra pozostáva z vrstvy prístupovej, distribučnej a jadra. Z praktických dôvodov bola distribučná vrstva zlúčená s prístupovou vrstvou a teda slúži aj na pripájanie koncových zariadení. Takto riešená topológia sa nazýva architektúra so zrútením jadrom. Chrbticové prepojenia sú dvojitého druhu. Na štyri miesta vo výrobe bol uplink uskutočnený pomocou optickej kabeláže. Pre optické prepojenia je typické, že kvôli duplexnému spojeniu bolo treba natiahnuť až dve vlákna. Už pri prvotnom návrhu a implementácii bol natiahnutý aj druhý záložný pár optických vodičov, ktorý momentálne nie je využitý. Ako kritické miesta boli pre implementovanie optických vodičov vybraté výrobné a skladové priestory. Vzhľadom na imunitu optického vlákna voči okolitému rušeniu a vzdialenosť týchto

prepínačov bol optický kábel ideálne prenosové médium. Optickým káblom boli prepojené len prepínače na úrovni distribučnej vrstvy. Všetky ostatné prepínače boli prepojené pomocou krútenej dvojlinky CAT 6. Kábel rovnakej kategórie bol použitý aj v prípade vzájomného prepojenia jednotlivých prepínačov umiestnených priamo v racku.

8.4.1 Základné nastavenie prepínačov

Princíp konfigurácie bol pre jednotlivé prepínače rovnaký. Základným pravidlom pre nastavenie zariadenia bolo priradiť mu názov, banner, heslo do privilegovaného režimu, IP adresu zariadenia a predvolenú bránu.

```
hostname [meno zariadenia]
banner motd ###*** Pre pracu sa je nutne PRIHLASIT !!! ***###
enable secret [heslo]
interface vlan [číslo manažovacej vlan]
ip address 172.30.44.12 255.255.254
ip default-gateway 172.30.44.1
```

Konfigurácia zariadenia je možná viacerými spôsobmi a preto bolo dobré nastaviť prístupové heslá aj na ne. Konkrétne na konzolu, telnet a AUX.

```
line {console 0, aux 0, vty [číslo, alebo rozsah od 0 do 15]}
password [heslo]
login
```

Pre spravovanie zariadenia na diaľku nepredstavuje telnet bezpečný spôsob pripojenia a preto bolo lepšie použiť SSH (Secure Shell).

```
aaa new-model
ip domain-name [názov domény (firma.sk)]
crypto key generate rsa general-keys modulus [360, ..., 1024, 2048, 4096]
ip ssh time-out [1 až 120 sec]
ip ssh authentication-retries [1 až 5]
line vty [číslo, alebo rozsah od 0 do 15]
transport input ssh
```

Generovanie RSA kľúča nie je v nových zariadeniach potrebné, pretože sa automaticky generuje pri prvom nastavení prepínača. Ako prednastavené SSH je verzia 2 a ak je

potrebné zmeniť to na prvú verziu, tak iba nasledujúcim príkazom *ip ssh version 1*. V nastaveniach vty namiesto telnet sa nastavilo SSH. Na to, aby sa administrátori mohli prihlásiť pomocou SSH, bolo potrebné vytvoriť pre každého z nich používateľa a heslo.

```
username [meno] password [heslo]
```

Takto vytvorené heslo bolo uložené v čitateľnej podobe. Ak by sme ho chceli uložiť šifrované, museli sme namiesto *password* použiť príkaz *secret*. V globálnom konfiguračnom režime je možné automaticky šifrovať všetky čitateľné heslá pomocou príkazu *service password-encryption*. Nastavenia boli uložené pomocou príkazu:

```
copy running-config startup-config
```

Alebo aj príkazom *write memory*. Lokálne uložené prihlasovacie údaje sú náročné na udržiavanie. Na to, aby sme nemuseli pre každého administrátora vytvárať zvlášť účet, postačilo pre istotu vytvoriť záložný lokálny účet a pre všetkých administrátorov požadovať prihlásenie pomocou autentifikačného servera.

```
aaa new-model
```

```
aaa authentication login MojRADIUS group radius local
```

```
radius-server host IP-RADIUSu auth-port 1645 acct-port 1646 key nejakeHeslo
```

```
line vty 0 15
```

```
login authentication MojRADIUS
```

```
transport input SSH
```

V každom prepínači boli podľa potreby nastavené jednotlivé virtuálne siete.

```
vlan [číslo]
```

```
name [nejaké meno]
```

Prepoje medzi zariadeniami sa nazývajú trunk, na ktorých sa povolila premávka z vybraných VLAN. Prepínače catalyst majú preddefinovaný automatický mód pre zostavenie trunku. Niekedy je lepšie napevno nastaviť trunk a natívnu VLAN. Konfigurácia sa vykonávala pre daný interface. Nie je potrebné zadávať enkapsuláciu, prednastavená je dot1q (802.1Q).

```
switchport mode trunk
```

```
switchport trunk native vlan [číslo vlan (40)]
```

```
switchport trunk allowed vlan [all, číslo, rozsah]
```

Po priradený portu do niektorej VLAN by bolo možné nastaviť akceptovanie pripojenia len zariadeniu so špecifickou MAC adresou. Použil by sa na to príkaz *switchport port-security MAC adresa* plus akcia, ktorá sa vykoná pri neoprávnenom pokuse pripojiť sa. V našej sieti nie je takáto politika zavedená. Ak je potrebné zamedziť používaniu takéhoto portu, je možné ho vypnúť, alebo priradiť do VLAN, ktorá sa potom deaktivuje. Príkaz na nastavenie prístupového portu a priradenie do VLAN sa vykonával priamo na danom rozhraní.

switchport mode access

switchport access vlan [číslo VLAN]

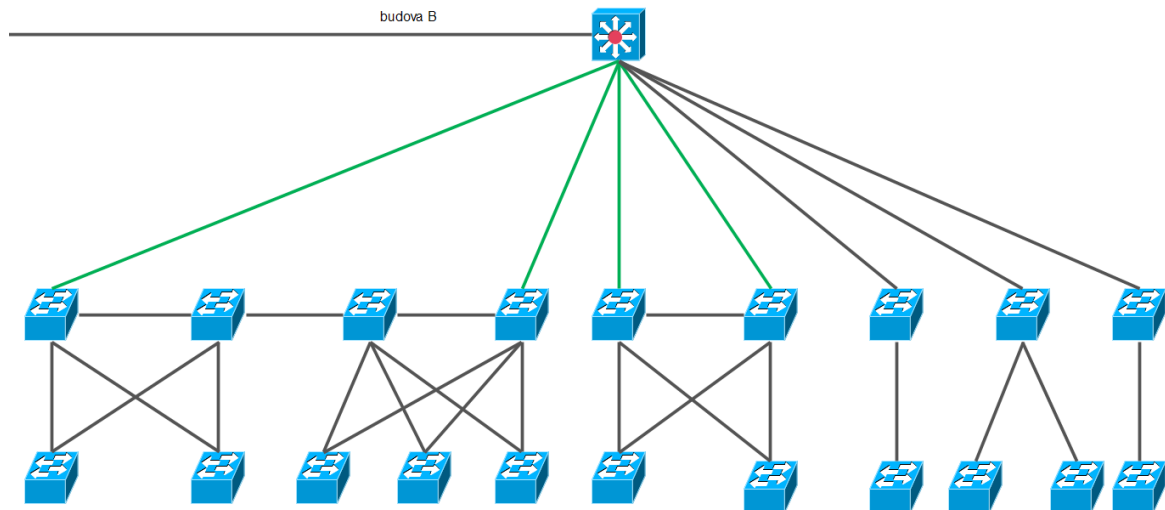
Na to, aby mohol DHCP server pridelovať adresy na inej VLAN, sa muselo na smerovači povoliť smerovanie týchto požiadaviek a odpovedí.

ip helper-address [IP adresa DHCP servera]

Na prepínačoch bola nastavená kvalita služieb pre VoIP. Cisco ponúka automatické nastavenie pomocou automatického QoS, ktoré sa konfigurovalo na rozhraní, pre ktoré sa predpokladala daná prevádzka.

auto qos voip [trust...]

Vybrala sa možnosť trust, pretože ostatné voľby boli určené pre originál Cisco telefóny. Po nastavení auto QoS sme uvideli doplnenie CoS nastavení vo výpise konfigurácie. Viacvrstvová architektúra poskytuje možnosti zálohovať trasy smerom do vrstvy jadra v prípade výpadku aktuálne aktívnej trasy. A to aj v prípade zariadenia nachádzajúce sa v smere do hlavného prepínača. Využitie záložnej trasy bude mať v našej sieti zmysel iba v prípade, ak nezhavaruje hlavný prepínač, ale preruší sa kábel, alebo port spájajúci dané zariadenia.



Obr. 7. Počítačová sieť v budove A.

Ako je vidieť na obrázku 7, dôležité časti majú vytvorené redundantné cesty pre prípad náhleho výpadku hlavných liniek. Prvé štyri racky boli s hlavným prepínačom prepojené pomocou optického kábla. Tieto racky mali potom medzi sebou vytvorené záložné cestym vždy po dva. Na vzájomné prepojenie boli použité tienené káble kategórie šesť. O zabezpečenie bezslučkovej topológie sa stará STP v režime PVST. Je dôležité, aby hlavný prepínač bol vždy vyhlásený za primárny spanning-tree prepínač a teda mal najmenšiu prioritu. To bolo možné docieľiť viacerými spôsobmi.

spanning-tree vlan [č. VLAN] priority [číslo (24576)]

Manuálne zadaná priorita sa udávala v násobkoch 4096. V prípade využitia makra sa namiesto priority použil príkaz *root primary*. Niekedy sa stalo, že nami požadovaná cesta vytvorená pomocou STP nevyzerala presne podľa našich predstáv. Pre prispôbenie trasy sme museli upraviť nejaký parameter ovplyvňujúci proces výberu portov. Najvhodnejšie bolo zmeniť prioritu portov.

spanning-tree port-priority [číslo]

Priorita portov sa udávala v násobkoch 16. Iná možnosť bolo zmeniť cenu portu. Každé Cisco zariadenie v určitých intervaloch vysiela BPDU rámce, na ktoré sa dá nastaviť ochrana pred nechcením pripojením, napríklad prepínača do prístupového portu. Pre každý prístupový port bolo umožnené po jeho aktivovaní okamžite začať prenos dát a teda preskočiť všetky jeho inicializačné stavy.

spanning-tree portfast

spanning-tree bpduguard enable

Portfast sa nastavil buď priamo na rozhraní, alebo globálne pre všetky prístupové porty. Prepnutie portu do stavu err-disabled po prijatí BPDU rámca spôsobí funkcia bpduguard. V prípade náhleho preťaženia siete spôsobeného všesmerovým, viacsmerovým, alebo jednosmerovým vysielaním, sa na uplink portoch uplatní funkcia kontrola búriek.

storm-control broadcast level 90.00 75.00

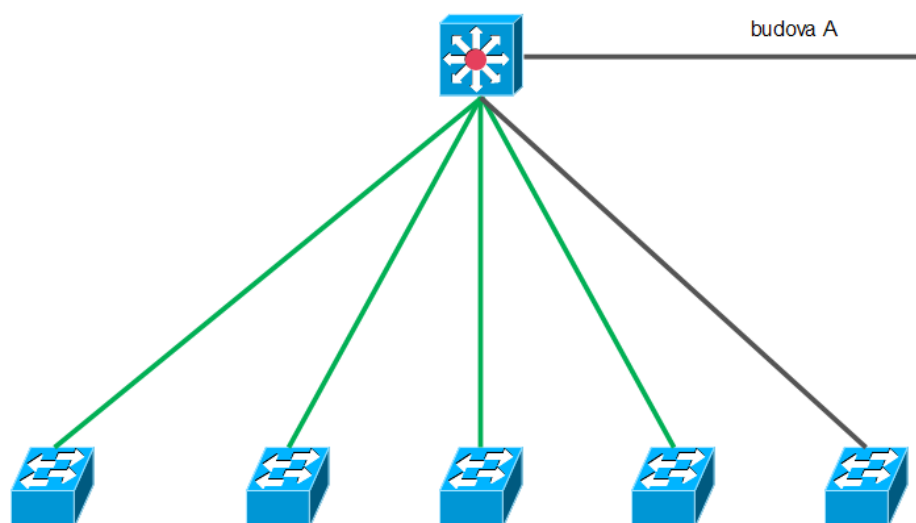
storm-control multicast level 90.00 75.00

storm-control unicast level 90.00 75.00

Prepínač každých 200 ms kontroluje prevádzku a porovnáva ju s nastavenou prahovou hodnotou. Všetky presahujúce pakety sú na nasledujúcich 200 ms zahodené. Ak na konci ďalšieho časového okna prevádzka neklesla pod druhú nastavenú hodnotu, tak prepínač naďalej prichádzajúce pakety zahadzuje. Prahové hodnoty sa dajú konfigurovať ako počet bitov za sekundu, paketov za sekundu, alebo ako v našom prípade percentuálna hodnota z celkovej dostupnej šírky pásma.

8.5 Topológia budovy B

Topológia druhej budovy vychádzala z rovnakého základu ako má prvá budova. Kritické pripojenia budú mať vzájomne prepojené záložné cesty.



Obr. 8. Počítačová sieť v budove B.

Momentálne boli vo všetkých rackoch umiestnené minimálne distribučné prepínače, ktoré zabezpečujú dátové spojenie pre nevyhnutné systémy umiestnené v tejto budove. Návrh počítal s dvoma prepínačmi Catalyst 3750, ktoré mali predstavovať vrstvu jadra. Nakoniec sa tam dočasne umiestnil len jeden MLS prepínač 3750. Distribučné a prístupové prepínače boli Catalyst 2960. S ohľadom na vzdialenosť boli štyri racky prepojené optickou kabelážou, pričom dva budú mať v budúcnosti priame duplicitné optické spojenie do vrstvy jadra. Redundantné linky pre zvyšné racky a prepínače sa vzájomne prepoja pomocou tienenej metallickej kabeláže CAT 6. Distribučná vrstva bude pozostávať z dvoch prepínačov 2960 a každý z nich bude mať priamu cestu do hlavných prepínačov. Aktívne zariadenia boli už pripravené na používanie a v prípade potreby rozšírenia kapacity stačí pripojiť vhodne nakonfigurovaný prepínač.

8.6 Vzájomné prepojenie budov

Obe budovy boli spolu priamo spojené a preto nebolo potrebné kabeláž ťahať a vystavovať vonkajším podmienkam. V každej budove sa nachádzala serverovňa s lokálnou vrstvou jadra. Tieto serverovne boli vzájomne prepojené pomocou optickej kabeláže.

V budove A sa nachádzal jeden aktívny MLS prepínač, ktorý už mal všetky optické porty obsadené. Aby sme mohli používať ďalšie optické pripojenie, bolo potrebné použiť médium konvertor. Medzi serverovňami boli natiahnuté dve optické linky o rýchlosti 1 Gbps a plánujú sa použiť ako ethernet-channel.

8.7 Smerovanie v sieti

8.7.1 Smerovanie v rámci budovy

Vo firemnej sieti sa používa statické smerovanie. DHCP server vždy nastaví aj bránu pre danú VLAN. Kancelárska sieť má ako bránu nastavený MLS prepínač. Ostatné virtuálne siete majú ako bránu nastavený firewall určený pre danú VLAN. Komunikácia medzi jednotlivými virtuálnymi sieťami je zakázaná, alebo obmedzená iba pre nutné protokoly. Takto obmedzená komunikácia prebieha medzi výrobnou a kancelárskou VLAN. Tieto dve siete sú od seba oddelené pomocou firewallu. Na hlavnom prepínači je nastavená statická cesta smerom do firewallu predstavujúceho bránu pre výrobnú sieť. Pravidlá nastavené na firewallle umožňujú smerovanie len na potrebné servery. Prístup na Internet a iné

nepotrebné služby poskytované sieťou boli zakázané. Z kancelárskej siete je možné pristupovať k zariadeniam vo výrobnjej sieti a to hlavne pre protokoly umožňujúce vzdialený prístup. Ďalšie dve virtuálne siete určené pre návštevníkov spoločnosti a pre pripojenie inteligentných telefónov boli medzi sebou úplne oddelené a nie je možnosť medzi nimi vykonávať smerovanie. NavstevaVL a PushVL má neobmedzený prístup do Internetu, ale smerovanie medzi nimi a ostatnými virtuálnymi sieťami používanými vo firme nebolo povolené.

```
ip route 0.0.0.0 0.0.0.0 [IP FW]
```

Smerovanie smerom do Internetu majú povolené len dve virtuálne siete určené pre administratívnu časť zamestancov. Štandardne bola na hlavnom prepínači nastavená statická cesta do firewallu určená pre každú komunikáciu, ktorej cieľová adresa sa nenachádza v smerovacej tabuľke.

8.7.2 Smerovanie medzi budovami

Každá budova mala pridelený svoj vlastný adresný rozsah pre každú virtuálnu sieť. Komunikácia medzi nimi sa riadi podľa rovnakých kritérií ako v prvej budove. Na oboch MLS prepínačoch sa nastavili statické cesty do jednotlivých VLAN.

```
ip route 172.30.64.0 255.255.252.0 192.168.100.2
```

```
ip route 172.30.45.0 255.255.255.0 192.168.100.2
```

```
ip route 172.30.60.0 255.255.252.0 192.168.100.2
```

```
ip route 0.0.0.0 0.0.0.0 192.168.100.1
```

Pretože obe budovy majú svoj vlastný adresný priestor, bolo potrebné, aby oba MLS prepínače mali svoje IP adresy, na ktoré sa môžu odkazovať počas smerovania medzi budovami. Prepínač v budove A má IP adresu 192.168.100.1 a prepínač v budove B má 192.168.100.2. Je dôležité si uvedomiť, že tieto pridelené IP adresy sa nevzťahujú na fyzické rozhranie smerovača, ale iba pre na ňom vytvorené SVI. Prevádzkovať návštevnícku sieť aj v druhej budove bolo možné pomocou povolenia komunikácie tejto VLAN na linke spájajúcej budovy. Virtuálne siete priamo pripojené na MLS prepínač majúce svoje SVI nepotrebujú smerovanie, ale pre všetku ostatnú komunikáciu bola nastavená statická cesta do MLS prepínača v budove A.

8.8 Bezdrôtová sieť

V tejto dobe je využívanie bezdrôtových technológií skoro nutnosťou. Vo firme, v ktorej pracuje veľa mobilných pracovníkov, je potrebné zabezpečiť spoľahlivé pripojenie, ktoré bude v maximálnej miere umožňovať využívanie služieb poskytovaných sieťou. Pri návrhu bolo treba zohľadniť jednotlivé zóny, ktoré sme chceli pokryť signálom. Nie všetky prístupové body budú umožňovať prístup do všetkých podsietí podniku. Dôležitou požiadavkou bolo zabezpečiť spoľahlivú službu, kde by v prípade výpadku jedného AP nezostalo veľa zariadení odpojených od siete a mohli by napríklad spôsobiť prerušenie výroby, čo je vo výrobnom podniku vážny problém. Bezdrôtové pripojenie by nemalo vytlačiť fyzické pripojenie pomocou sieťového kábla. Bezdrôtová sieť je ovplyvňovaná veľkým množstvom faktorov, ktoré sa nie vždy dajú odstrániť a administrátori by nemali na ne zabúdať. Jej použitie by malo byť iba ako predĺženie fyzickej siete a nasadenie na miestach, kde použitie klasickej kabeláže nie je z nejakého dôvodu možné.

8.8.1 Prístupový bod

V celom areáli firmy boli použité rovnaké prístupové body. Zjednotenie hardvéru uľahčuje spravovanie jednotlivých prvkov a hlavne v prípade pokazenia zariadenia je možné ho rýchlo nahradiť a konfiguráciu nahráť zo zálohy. Ako prístupové body boli vybrané zariadenia od firmy Cisco a to konkrétne model Aironet 1140.

Základné vlastnosti prístupového bodu sú nasledovné:

- Šírka kanála 20 a 40 MHz.
- PHY až do 300 Mbps.
- Podporuje CSD multiplex pre viacero antén.
- Maximálny výkon 20 dBm pre dve antény.
- Ethernet 10/100/1000Base-T.
- 128 MB RAM.
- 32 MB flash.
- Môže byť napájané cez PoE.
- Štandardy IEEE 802.11a/b/g/n, 802.11h/d.
- Podpora 802.11i WPA a WPA2.
- EAP TLS/TTLS, PEAPv0 a EAP-MSCHAPv2, PEAPv1.

- Podporuje 13 kanálov.
- Frekvencia 2,4 GHz a 5 GHz.
- 802.11a: 6, 9, 12, 18, 24, 36, 48, a 54 Mbps.
- 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, a 54 Mbps.
- 802.11n rýchlosť prenosu (2.4 GHz and 5 GHz) – závisí od nastavenia.

Rýchlosť prenosu pri použití 802.11n závisí od nastavenej modulačnej schémy MCS (Modulation Coding Scheme).

Aironet 1140 je prístupový bod, ktorý dokáže pracovať v dvoch režimoch:

- Autonómne AP – nastavenia sa robia priamo na AP.
- Odlahčené AP – ide o tzv. LWAP.

Nevýhodou autonómneho AP je fakt, že každé jedno nastavenie sa muselo vykonávať na všetkých AP zvlášť. Ak požadujeme rovnaké služby na všetkých AP, tak nastavenia musia byť vždy identické. Druhá možnosť bolo použiť LWAP a tým centralizovať manažment bezdrôtovej siete na jedno miesto. Najčastejšie sa používa WLC, ktoré má vytvorené špeciálne komunikačné kanály, pomocou ktorých poskytuje svoje služby. Použitie tohto riešenia má mnohé výhody, ktoré bez centralizovania nie je možné dosiahnuť a ak áno, je nutné použiť viacero technických riešení od tretích strán.

8.8.2 Požiadavky na bezdrôtovú sieť

Budova sa skladá z viacerých zón a pre každú boli špecifické zariadenia, ktoré sa tam nachádzali a používatelia, ktorí sa po danom priestore budú pohybovať. Na začiatok si bolo treba povedať, aké zariadenia sa budú na danú sieť pripájať a aké služby pre ne chceme poskytovať.

Zariadenia pripájajúce sa na sieť:

- Laptopy.
- Počítače typu All in One.
- Mobilné telefóny a smartfóny.
- Stolové počítače za použitia Wifi karty, alebo USB Wifi modulu.
- Bezdrôtové skenery.

Služby poskytované bezdrôtovou sieťou sú identické so službami na pevnej sieti. Bezdrôtová sieť musela podľa možností pokryť čo najväčšiu časť budovy. Konfigurácia siete musela minimalizovať riziko výpadkov a súčasne používateľom garantovať určitý stupeň komfortu. AP muselo byť dostatočne výkonné, aby dokázalo zabezpečiť súčasnú komunikáciu zariadení umiestnených v rôznych podsieťach. Okrem pripojenia na Internet bola dôležitá komunikácia so servermi umiestnenými v lokálnej sieti. V budove sa budú nachádzať používatelia, ktorí sa budú často premiestňovať a pre tých bolo potrebné zabezpečiť v každom čase bezproblémové pripojenie do siete.

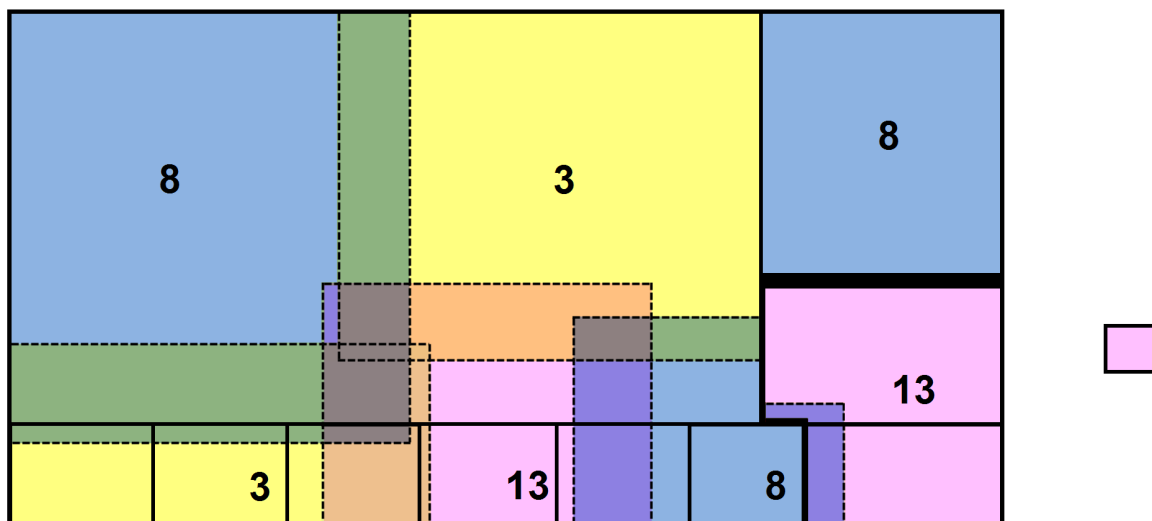
Klienti pripájajúci sa k sieti:

- Zamestnanec firmy.
- Návštevník.
- Výrobný stroj.

Na bezpečnosť pri používaní bezdrôtových sietí bol obzvlášť kladený dôraz. Bolo dôležité oddeliť jednotlivých používateľov a umožniť im prístup len tam, kde to naozaj potrebujú. Pri návrhu sa počítalo aj s prenikaním signálu mimo budovu a areál spoločnosti. Preto bolo nutné umiestniť prístupové body tak, aby bol dosah siete čo najviac obmedzený. Vedenie spoločnosti sa v záujme najvyššej bezpečnosti rozhodlo používať výlučne WPA2 a zariadeniam nepodporujúcim tento typ pripojenia neumožniť prístup na sieť. V tomto čase nie sú na bezdrôtovej sieti používané VoIP telefóny.

8.8.3 Realizácia bezdrôtovej siete

Aj keď použité prístupové body umožňujú centralizovanú správu v režime LWAP, tak v tomto návrhu sa zameriavalo iba na autonómne riešenie. Pri návrhu rozloženia aktívnych prvkov bolo dôležité uvedomiť si rozdielnosť prostredia, v ktorom boli jednotlivé AP inštalované. Budovu si môžeme rozdeliť na dve časti. Prvá časť je administratívna, kde sa nachádzajú kancelárie a mítingové miestnosti. Druhá časť sú výrobné priestory a sklad. Najväčším problémom v bezdrôtových sieťach bolo rušenie spôsobené prekryvaním kanálov jednotlivých AP. Toto bol problém aj v pôvodnom riešení, pretože prístupové body boli nastavené na automatickú voľbu kanála. To fungovalo tak, že AP vykonalo skenovanie jednotlivých kanálov a pokiaľ našlo voľný kanál, začalo na ňom vysielat'.



Obr. 9. Dosah jednotlivých AP.

Štandardne na pokrytie priestoru stačí vybrať tri kanály, ktoré sa neprekrývajú. Vo väčšine literatúry sa uvádza použitie kanálov 1,6,11. V našom prípade to nebolo možné, pretože mimo budovy sa nachádzal ešte jeden špecifický priestor, pre ktorý bolo potrebné zabezpečiť bezdrôtové spojenie. Išlo tam o projekt, v ktorom sa testovanie uskutočňovalo na otvorenom priestranstve mimo budovu. Na začiatku nebola deklarovaná nutnosť spojenia do siete a preto bolo IT oddelenie vynechané z prípravného procesu. Do priestoru, v ktorom bolo zariadenie umiestnené, nebolo možné dotiahnuť kabeľ a preto jediný spôsob bolo použiť WLAN. Pri obhliadke prostredia bolo zistené veľké množstvo bezdrôtových sietí a prepojov. Výhodou bola priama viditeľnosť na firemné AP umiestnené v miestnosti oproti. Zistilo sa, že dosah tohto AP je dostatočne silný na to, aby bolo možné naše zariadenie naň pripojiť. Meranie pomocou aplikácie InSSIDer preukázalo husté obsadenie jednotlivých kanálov, ale kanál číslo 13 nebol využitý vôbec. A preto sa celý návrh odvíjal od nutnosti použitia kanálu číslo 13 na tomto AP. Aby sme priestor pokryli a vyhli sa vzájomnému rušeniu, vybrali sa kanály číslo 3, 8 a 13. AP boli pripojené STP, alebo FTP káblom Cat. 6 na 1000Base-T port. V sieťovej hierarchii sa pripájali do distribučnej vrstvy. Medzi prístupovým bodom a prepínačom bol zostavený trunk. Na obrázku číslo 9 je vidieť umiestnenie prístupových bodov a nastavenie ich kanála. Na kritických miestach sa pomocou aplikácie inSSIDer vykonala kontrola kvality signálu. To, prečo vzniklo takéto pokrytie, je výsledkom požiadavky celú budovu pokryť bezdrôtovým signálom. Vyhovieť takejto žiadosti je bolo náročné a často sa ani nedalo

úplne splniť. Na WLAN vplýva veľké množstvo faktorov, ako sú elektromagnetický smog z prístrojov, materiál z ktorého sú steny postavené, úmyselné tienenie a iné okolité vplyvy rušenia. Pre mobilných používateľov je dôležité byť pokiaľ možno stále pripojený a preto Cisco doporučuje prekrytie minimálne 15 až 20 percent [11].

8.8.4 Konfigurácia prístupových bodov

S ohľadom na hore uvedené rozmiestnenie prístupových bodov bol výkon niektorých AP upravený a to takým spôsobom, aby sa splnila podmienka prekrytia a minimalizovala sa možnosť vzájomného rušenia kanálov. Nastavovanie prístupových bodov je možné pomocou webového rozhrania a teda veľmi jednoducho a intuitívne. Pretože toto je prechodné riešenie pre bezdrôtovú sieť, tak prihlasovanie na jednotlivé AP je pomocou lokálneho užívateľa a hesla. Pokiaľ chceme vytvoriť nejaké SSID, tak sa musela najskôr definovať VLAN, na ktorú sa bude dané SSID viazať.

Ethernetové spojenie sa muselo nastaviť v dvoch krokoch. Prvý krok bolo nastavenie komunikácie a rýchlosti. IP adresa sa tu nenastavovala:

```
interface GigabitEthernet0
```

```
no ip address
```

```
duplex auto
```

```
speed auto
```

V druhom kroku bolo pre každú VLAN nutné nastaviť podinterfejs, v ktorom sa definovalo zapuzdrenie do správnej VLAN:

```
interface GigabitEthernet0.číslo VLAN
```

```
encapsulation dot1Q číslo vlan
```

Keď pripájame prístupový bod do káblovej siete LAN, tak na komunikáciu s AP sa používa BVI interfejs. Je to virtuálny premost'ovací interfejs a vďaka nemu sme nemuseli zvlášť zadávať IP adresu pre NIC a pre radiové rozhranie.

```
interface BVII
```

```
ip address IP MASKA
```

WLAN pozostáva zo štyroch sietí s nasledujúcimi SSID:

- Kancelarie – je štandardná firemná sieť.
- Navsteva – určená pre firemných návštevníkov.
- Push – poskytuje firemné služby.
- Vyroba – určená pre výrobné použitie.

Prvá Wifi sieť Kancelarie je v podstate hlavná firemná sieť, nachádzajúca sa aj v rovnakej VLAN 31. Poskytuje identické služby pre používateľov, ako sú e-mail, prístup na Internet, komunikáciu s ostatnými pobočkami cez MPLS, tlačové a súborové služby. Prístup do siete bol povolený len zamestnancom, ktorí majú doménový účet. Autentifikácia je vykonávaná Radius serverom, bezpečnostný štandard je WPA2 Enterprise a šifrovacia metóda je AES. Autentifikačný model je PEAP-MSCHAPv2.

Nastavenie autentifikácie klientov pomocou Radius servera:

```
aaa new-model
aaa group server radius rad_eap
server 172.33.28.12 auth-port 1645 acct-port 1646
aaa authentication login eap_methods group rad_eap1
```

Zabezpečenie spojenia s autentifikačným serverom pomocou hesla:

```
radius-server host 172.33.28.12 auth-port 1645 acct-port 1646 key 7 123AB546CD
```

Definovanie novej VLAN a jej čísla:

```
dot11 vlan-name KancelVL vlan 31
```

Vytvorenie nového SSID pre danú VLAN a nastavenie zabezpečenia:

```
dot11 ssid Kancelarie
vlan 31
authentication open eap eap_methods1
authentication network-eap eap_methods1
authentication key-management wpa version 2
mbssid guest-mode
```

Nastavenie interfejsu antény. Pozostávalo z pripojenia SSID na daný interfejs a nastavenia šifrovania pre danú VLAN:

```
interface Dot11Radio0
ssid Kancelarie
encryption vlan 31 mode ciphers aes-ccm
```

Pretože AP má iba jednu anténu, ale podporuje súčasne viacero SSID, bolo nutné použiť virtuálny podinterfejs, v ktorom sa definovalo zapuzdrenie prenášaných dát do danej VLAN:

```
interface Dot11Radio0.31
encapsulation dot1Q 31
```

SSID Navsteva je určená pre návštevníkov, ktorí navštívili firmu a potrebujú mať prístup na Internet. Klienti pripojení na túto sieť nemajú žiaden prístup do firemnej siete a ani nemôžu využívať žiadne služby štandardne poskytované zamestnancom. Do tejto siete sa je možné pripojiť len pomocou WIFI. Použitý štandard je WPA2 Personal a šifrovacia metóda je AES. Pripojenie do tejto siete bolo obmedzené len na kancelársku oblasť.

Vytvorenie VLAN:

```
dot11 vlan-name kancelarievl vlan 31
```

Vytvorenie SSID :

```
dot11 ssid Navsteva
vlan 32
authentication open
authentication key-management wpa version 2
mbssid guest-mode
wpa-psk ascii 7 7515400
```

Nastavenie podinterfejsu pre dané SSID spolu s zapuzdrením:

```
interface Dot11Radio0
encryption vlan 32 mode ciphers aes-ccm
```

interface Dot11Radio0.32

encapsulation dot1Q 32

SSID Push slúži pre pripojenie inteligentných telefónov. Tieto telefóny majú niektorí zamestnanci a môžu využívať pripojenie na Internet výhradne cez túto sieť. Službu Push Email mali sprístupnenú práve cez túto bezdrôtovú sieť. Push Email je služba umožňujúca mať svoje e-maily stále pri sebe, synchronizovať kalendár a podobne. Nastavenie je identické ako pre návštevnícku sieť. Rozdiel je iba v tom, že táto sieť nevysiela svoje SSID a to bolo docielené príkazom, ktorý sa zadal v nastaveniach pre SSID:

no mbssid guest-mode

SSID Vyroba je určená na pripojenie zariadení, ktoré sú určené na používanie v procese výroby. Sú to napríklad výrobné stroje, ktoré potrebujú komunikovať s databázovým serverom a podobne. Nastavenie je WPA2 Personal so šifrovaním AES. Postup vytvorenia tejto siete bol identický ako pri Navsteve.

Kvôli nastaveniu dosahu bol na niektorých AP upravený výkon príkazom:

power local (hodnota{-1 | 2 | 5 | 8 | 11 | 14 | 15 | 17 | maximum })

Použitý štandard bol 802.11g a prenosová rýchlosť bola nastavená až na maximum 54Mbps a v prípade potreby zostali povolené aj záložné rýchlosti:

speed basic-1.0 basic-2.0 basic-5.5 basic-11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Podľa umiestnenia bol na každom AP napevno nastavený prenosový kanál. Konkrétne bolo možné zadať číslo, alebo frekvenciu. Bol zadaný kanál 8 = 2447:

channel (2447 | 8)

Toto bola ukážka základného nastavenia pre prístupové body. Bolo vhodné ešte nastaviť predvolenú bránu pomocou príkazu *ip default-gateway IPadresa*. Konfigurácia sa uložila príkazom *copy running-config startup-config*. Po uložení bolo možné si nastavenia pozrieť pomocou webového rozhrania, kde sa našiel textový dokument s konfiguráciou, alebo pomocou príkazu *show startup-config*. Aktuálne aktívne nastavenia sa dajú pozrieť príkazom *show running-config*.

8.9 Ochrana siete

8.9.1 Ochrana vo vnútornej sieti

Každá virtuálna sieť je už z princípu oddelená od ostatných. Pretože je medzi nimi vykonávané smerovanie, je potrebné kontrolovať komunikáciu a povoliť len to čo naozaj potrebujeme. Flexibilnú kontrolu nám umožňuje virtuálny firewall umiestnený medzi výrobnou a kancelárskou sieťou. Pretože v druhej budove nie je veľká dátová prevádzka, na oddelenie sietí bolo možné použiť MLS prepínač umiestnený v serverovni. Nastavením ACL sa potom povolil príchod len pre vybrané protokoly.

```
permit tcp 172.30.64.0 0.0.3.255 172.30.28.0 0.0.3.255 eq www
```

```
permit tcp 172.30.64.0 0.0.3.255 172.30.60.0 0.0.3.255 eq www
```

```
permit icmp any any echo
```

```
permit icmp any any echo-reply
```

MLS smerovače nemajú vytvorené SVI virtuálnych sietí určených pre návštevníkov a push email. Ale aby mohli byť tieto VLAN súčasťou podnikovej siete, museli byť vytvorené pre každý prepínač na ktorom sa daná komunikácia predpokladala.

8.9.2 Ochrana vnútornej siete

Ochranu vnútornej siete zabezpečujú firewally ASA 5505 a 5510. Spoločnosť má niekoľko prenajatých liniek pomocou ktorých uskutočňuje pripojenie do Internetu. Ako už bolo spomenuté vnútorná sieť pozostáva z viacerých virtuálnych sietí a nie každá má povolený prístup do Internetu. Každé rozhranie na firewalle bolo zaradené do nejakej pomenovanej VLAN.

```
interface Vlan1
```

```
nameif NavstevaVL
```

```
security-level 100
```

```
ip address [IP adresa][maska]
```

```
interface Ethernet0/0
```

```
switchport access vlan 1
```

Každá virtuálna sieť mala pridelený takzvaný bezpečnostný identifikátor, ktorý je využívaný jedným základným pravidlom firewallu a to, že je zakázané smerovať dáta zo siete s nižšou hodnotou identifikátora do siete s vyššou hodnotou. Rozhranie na ktorom je pripojená nedôveryhodná sieť Internet má štandardne hodnotu nula. Dôveryhodnejšie siete potom môžu mať hodnotu identifikátora v intervale jeden až sto. Obe vnútorné siete mali nastavenú hodnotou 100. Rovnaká hodnota pre rôzne siete ešte neznamená vzájomné smerovanie, pretože ak je ho potrebné vykonávať, tak na firewalloch ASA sa to muselo explicitne povoliť. Takáto vlastnosť firewallu v našom prípade spĺňala požiadavku úplného izolovania týchto sietí. Celá komunikácia mimo firemnú sieť prechádza hlavným prepínačom nachádzajúcim sa v budove A. Virtuálne siete NavstevaVL a PushVL mali každá osobitne dotiahnutú linku z hlavného prepínača do ich spoločného firewallu. Tieto linky nie sú trunkové a porty na prepínači boli nastavené čisto ako prístupové porty. Aj keď v rámci firmy sú to dve oddelené siete, tak z pohľadu Internetu zdieľajú jednu verejnú IP adresu nastavenú na vonkajšom interfejsu. Firewall vykonáva preklad vnútorných adries na jednu verejnú pomocou funkcie PAT. Ako prvé sa musel definovať objekt siete a až potom na sa tento objekt aplikovalo PAT. Zariadenie už malo niektoré objekty preddefinované, ale pre lepšiu orientáciu bolo lepšie vytvoriť si vlastné.

```
object network siet-navsteva-obj
```

```
subnet 192.168.32.0 255.255.255.0
```

```
description toto je objekt vnutorna siet NavstevaVL, ktora ma povoleny PAT
```

```
object network siet-navsteva-obj
```

```
nat (NavstevaVL,outside) dynamic interface
```

Toto nastavenie sa muselo spraviť pre všetky siete pre ktoré sa vykonáva preklad adries. IP adresy prideliuje firewall a preto sa musela DHCP služba aktivovať a povoliť len pre daný port. Spolu s ňou sa nastavil aj DNS server.

```
dhcpd address 192.168.32.10- 192.168.32.254 NavstevaVL
```

```
dhcpd dns 192.168.32.1 interface NavstevaVL
```

```
dhcpd enable NavstevaVL
```

Firewall sám seba nastavil ako bránu pre danú sieť. Nastavením statickej cesty pre všetky neznáme adresy sa zabezpečilo správne smerovanie paketov do Internetu.

```
route outside 0.0.0.0 0.0.0.0 [IP ISP] 1
```

Podobne sa nastavilo smerovanie aj na firewalle chrániacom kancelársku sieť. Pretože budova B má spojenie s Internetom cez tento firewall bolo nutné zapísať aj túto sieť do smerovacej tabuľky.

```
route inside 172.30.60.0 255.255.252.0 172.30.28.1 1
```

Číslo jedna zadané na konci oznamuje metriku, ktorá vyjadruje prioritu cesty do siete pokiaľ by existovalo viacero možných ciest. Statické smerovanie do siete budovy B sa nastavovalo na firewalle oddelujúceho Internet a kancelárske siete a nie na firewalle určenom pre návštevníkov. Overenie prihlasovacích údajov sa môže vykonávať lokálne, ale aj pomocou autentifikačného servera. Prihlasovať sa na firewally budeme doménovým účtom za pomoci RADIUS servera, ale pre istotu bol vytvorený aj lokálny účet a prideliť sa mu najvyššie práva.

```
username michal password [HESLO] encrypted privilege 15
```

Keď sa už vytvoril lokálny účet, nastavil sa aj RADIUS server, ktorý sa bude používať pri overovaní doménových prihlasovacích údajov.

```
aaa-server AAA-SERVER-Skup protocol radius
```

```
aaa-server AAA-SERVER-Skup (inside) host 172.33.28.12
```

```
key [heslo]
```

```
radius-common-pw [heslo]
```

```
aaa authentication enable console LOCAL
```

```
aaa authentication http console AAA-SERVER-Skup LOCAL
```

```
aaa authentication ssh console AAA-SERVER-Skup LOCAL
```

Prihlasovanie pomocou Radius servera je vykonávané iba na firewalle 5510. Na firewalle 5505 oddelujúceho návštevníkov je prihlasovanie pomocou lokálneho mena a hesla.

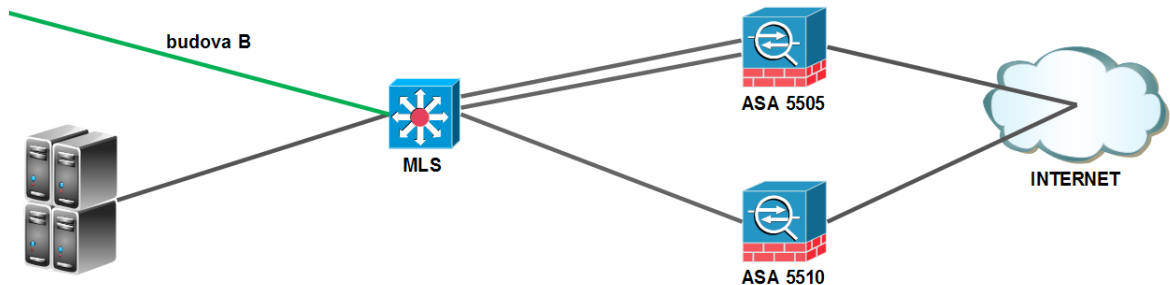
Prístup na Internet pre používateľov nachádzajúcich sa v kancelárskej sieti bol na firewalle zakázaný. Táto služba spolu so službou FTP je poskytovaná pomocou proxy servera, ktorý má prístup na Internet povolený. Okrem proxy boli povolené aj niektoré protokoly využívané niektorými aplikáciami pracujúcimi na niektorých zariadeniach.

```
object-group network sietova-skupina-NET
```

```
network-object object mojPC-obj
```

```
network-object object testServer10-obj
```

access-list inside_access_in extended permit ip object-group sietova-skupina-NET any



Obr. 10. Umiestnenie firewallov.

Ako je vidieť z návrhu, tak pre používateľov na dvoch virtuálnych sieťach nie je prístup na Internet žiadnym spôsobom obmedzovaný. Zariadenia a používatelia nachádzajúci sa v sieťach určených pre kancelárie majú tiež prístup na Internet, len sa vždy musia autentifikovať voči proxy serveru. Aj keď majú oba MLS prepínače pre neznáme IP adresy nastavenú statickú cestu smerujúcu do hraničného firewallu aj tak zariadeniam a používateľom vo výrobnjej sieti nebude umožnený prístup na Internet a tiež ani z Internetu smerom do týchto sietí. Toto bolo ošetrené prvýkrát na hraničnom firewallle a druhýkrát na firewallle umiestnenom medzi výrobnou a ostatnou podnikovou sieťou.

8.10 Prístup do DMZ

Nutnosť vytvorenia demilitarizovanej zóny bolo z dôvodu umiestnenia verejného servera poskytujúceho webové služby dostupné z Internetu. Aby nebola narušená ochrana vnútornej siete, tak bolo nutné tento server umiestniť do priestoru kde bude umožnený prístup z dôveryhodnej a súčasne aj s nedôveryhodnej siete.

Aj keď by sme mohli do demilitarizovanej zóny umiestniť aj iné servery, tak v súčasnosti sa tam nachádza iba jeden webový server. E-mailové služby a teda aj server je spravovaný v inej firemnej pobočke s ktorou je naša prevádzka prepojená pomocou MPLS tunela. Ako prvé bolo nutné zvoliť vhodný firewall. Bolo zvolené použitie jedného firewallu, ktorý obsahuje viacero portov. Pre vytvorenie “trihomed DMZ“ boli potrebné minimálne tri porty, ktoré sa spolu s tromi VLAN pomenovali a pridelil sa im bezpečnostný identifikátor.

```
interface Vlan150
nameif dmz
security-level 50
ip address 192.168.150.1 255.255.255.0
```

V tomto prípade sa použilo pomenovanie pre vonkajšie a vnútorné rozhranie pridelené výrobcom firewallu. Pomenovala sa len tretia virtuálnu sieť DMZ a pridela sa jej hodnota 50. To firewallu hovorí, že môže smerovať pakety smerom do Internetu, ale do vnútornej siete nemôže. Boli vytvorené pomenované sieťové objekty a povolil sa im preklad adres PAT na verejnú adresu priradenú rozhraniu pripojenému do Internetu.

```
object network dmz-obj
subnet 192.168.150.0 255.255.255.0
description objekt predstavujuci siet dmz
```

Vytvoril sa jeden špecifický sieťový objekt predstavujúci náš webový server a nastavil sa mu statický preklad adresy.

```
object network webserver-obj
host 192.168.150.10
description objekt webovy server
```

```
object network webserver-obj
nat (dmz,outside) static interface
```

Teraz bol povolený statický preklad pre všetky protokoly. Keďže sa jedná o webový server, vonkajším klientom sa povolil prístup iba pre protokoly http a https.

```
access-list outside_access_in extended permit tcp any object webserver-obj object-
group outside-inside-sl
```

Outside-inside-sl je skupina služieb v ktorej sa zadefinovali protokoly pracujúce na portoch 80 a 443. Pre korektnú komunikáciu sa musel nastaviť aj statický preklad pri prechode z dmz do vnútornej siete podniku.

```
object network webserver-do-inside
nat (dmz,inside) static webserver-do-inside
```

V podstate bol nastavený preklad samého seba na svoju vlastnú IP adresu. Aj v takomto prípade bude zakázaná komunikácia do vnútornej siete. Zariadenia ktoré chcú pristupovať na webový server musia byť povolené. Opäť bolo potrebné rozdeliť ich do skupín a povoliť im prístup iba tam kde potrebujú.

```
object-group network sietova-skupina-DMZ
```

```
description skupina ktora bude mat povoleny plny pristup do dmz web servera
```

```
network-object object mojPC-obj
```

```
network-object object testServer10-obj
```

```
access-list inside_access_in remark sluzi na povolenie plneho pristupu pre urcite  
pocitace z inside do web servera dmz
```

```
access-list inside_access_in extended permit ip object-group sietova-skupina-DMZ
```

```
object webserver-obj
```

```
object-group network sietova-skupina-do-dmz-web
```

```
description skupina ktora bude mat povoleny obmedzeny pristup do dmz web servera
```

```
network-object object Bkancel-do-dmz-obj
```

```
network-object object kancel-do-dmz-obj
```

```
access-list inside_access_in remark povolenie obmedzeneho pristupu na web server  
pre kancelarske skupiny
```

```
access-list inside_access_in extended permit tcp object-group sietova-skupina-do-
```

```
dmz-web 192.168.150.0 255.255.255.0 object-group inside-dmz-sl
```

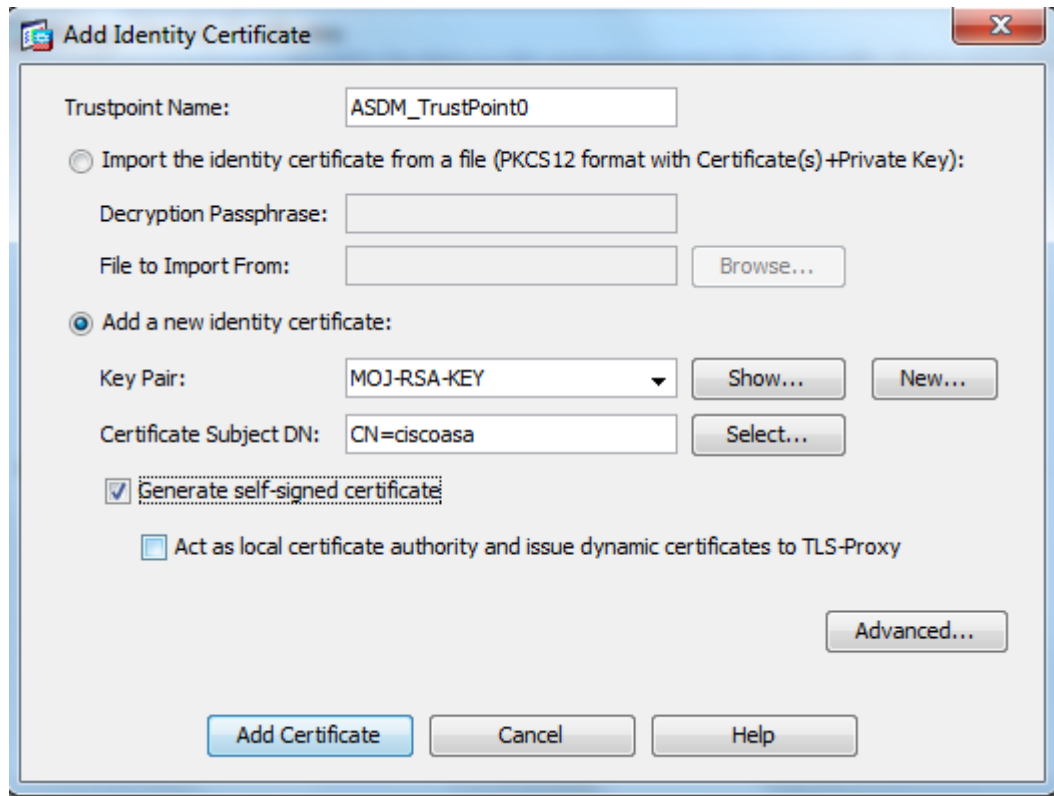
Aj keď pre prístup z vnútornej siete na webový server boli povolené rovnaké protokoly aj tak bolo vhodné vytvoriť novú skupinu služieb pre prípad, ak by sme potrebovali dodatočne doplniť aj iné protokoly. Je dôležité dať si pozor na poradie ACL pravidiel, aby sa nestalo, že povolíme niečo čo by malo zostať zakázané. Takýmto spôsobom bol umožnený externý prístup na firemný webový server a súčasne bola zabezpečená vnútorná podniková sieť pred neoprávneným prístupom z Internetu.

8.11 VPN

Možnosť vzdialeného prístupu do firemnej siete je veľkou výhodou pre zamestnancov, ale aj pre samotnú firmu. Zamestnanci ktorým bol povolený prístup do vnútornej siete môžu využívať služby poskytované sieťou ktoré im aj na veľkú vzdialenosť umožnia pracovať tak ako keby boli priamo pripojení do firemnej siete. Na druhú stranu prenos informácií cez Internet a zároveň umožnenie prístupu do vnútornej siete predstavuje určité bezpečnostné riziko. VPN sa bude v našej sieti zavádzané v dvoch fázach. V prvej fáze sa povolil prístup len pre IT oddelenie. Neskôr v druhej fáze sa povolí prístup vybraným zamestnancov. Prístupovať do vnútornej podnikovej siete sa bude cez rozhranie firewallu, ktoré bolo umiestnené smerom do Internetu. Firewall ASA poskytuje dve možnosti pripojenia VPN. Prvý je pomocou protokolu SSL, pri ktorom sa klienti dokážu prihlásiť pomocou webového prehliadača. Druhý spôsob je pomocou IPSec klienta. V našom prípade budeme na tunelovanie používať klient aplikáciu Cisco AnyConnect. Na firewalle bolo nutné vytvoriť VPN profil ktorý sa následne pri prvom pokuse o spojenie nahrá do koncového zariadenia na ktorom beží klient AnyConnect. Ako tunelovací protokol sa nastavil IPSec, ale prvé spojenie bude vždy vykonané pomocou protokolu SSL. Komplikovaná konfigurácia VPN sa dala uľahčiť pomocou ASDM , ktoré má v sebe implementovaného sprievodcu nastavenia VPN.

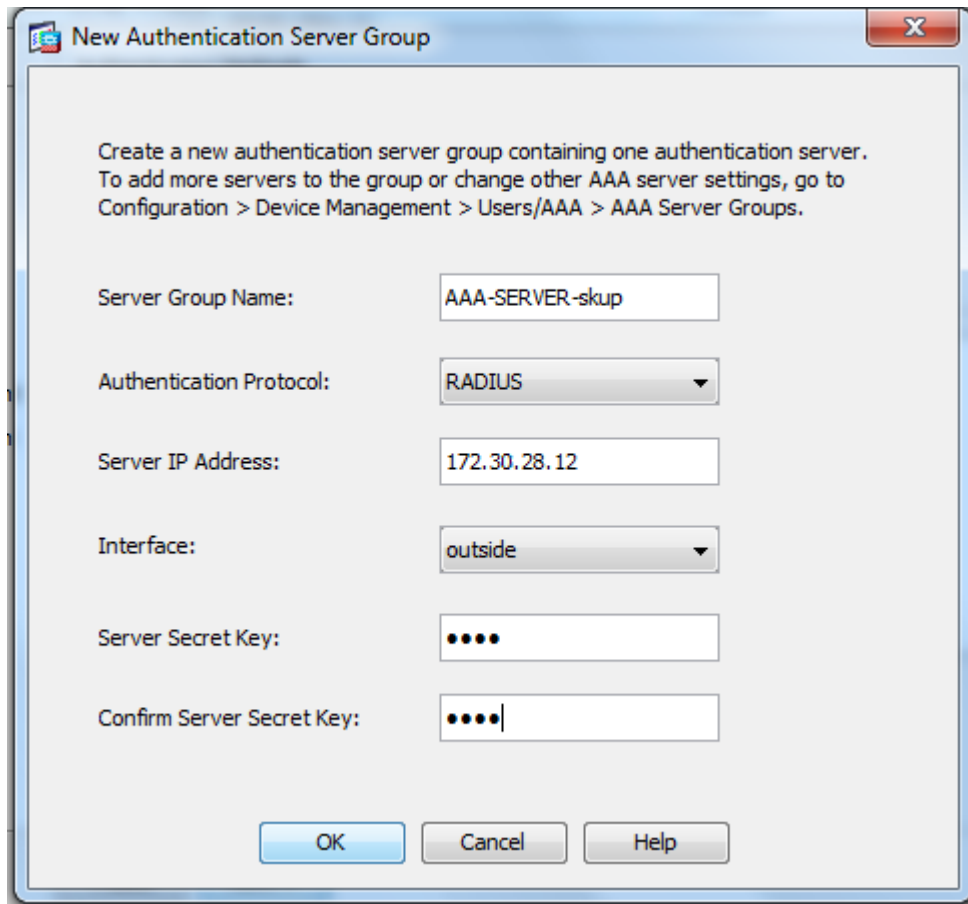
Po prihlásení sa do ASDM bolo nutné v hornom menu vybrať položku Wizards -> VPN Wizards -> AnyConnect VPN Wizard. Následne sa zobrazil sprievodca vytvorenia VPN profilu.

1. V prvom kroku sa musel vytvoriť a pomenovať profil pre dané VPN spojenie a označiť interfejs na ktorom bude tunel ukončený.
2. Boli vybrané protokoly VPN spojenia. Na výber boli SSL, IPSec, alebo kombinácia oboch. Vybral sa protokol IPSec.
3. Pre spojenie bolo potrebné vytvoriť certifikát ktorým sa ASA bude identifikovať VPN klientom. Ak už bol certifikát vytvorený môžeme ho importovať, alebo vytvoriť si nový. Nový certifikát mal vytvorenú identitu zadaním RSA kľúča. Bolo kliknuté na Add -> vybralo sa Add a new identity certificate -> New -> do okienka Enter new key pair name sa zadal náš názov -> vybrala sa veľkosť kľúča a bolo to potvrdené stlačením tlačidla Generate Now. Týmto sa vytvorila identita pre náš certifikát, ktorá sa následne skontrolovala v nasledujúcom okne.



Obr. 11. Vytvorenie certifikátu pomocou ASDM.

4. V ďalšom kroku bol nahratý zdrojový súbor klienta AnyConnect. Pri pokuse o pripojenie sa skontroluje jeho verzia a ak je nižšia ako nami požadovaná, ASA ponúkne inštaláciu novej verzie klienta AnyConnect.
5. V piatom kroku boli definovaní používatelia ktorý budú môcť vytvoriť VPN spojenie do vnútornej siete podniku. Autentifikácia používateľov bola nastavená pomocou lokálnej databázy, alebo použitím autentifikačného servera.



Obr. 12. Nastavenie autentifikačného serveru pomocou ASDM.

6. Pretože na vzájomnú komunikáciu medzi sieťami je potrebné smerovať pakety, bolo nutné pripojením klientom vytvoriť adresný rozsah z ktorého bude DHCP server priradzovať IP adresy.
7. V tomto kroku bol určený DNS server a doména pre virtuálne spojenie.
8. Počas komunikácie medzi vnútornou sieťou a Internetom prebieha preklad adres pre adresy prichádzajúce z inside do outside interfejsu. Pretože tunel je ukončený na outside interfejsu, tak vnútorná sieť by zostala skrytá aj pre vytvorený tunel a preto bolo potrebné zaškrtnúť vyčlenenie VPN komunikácie z prekladu adres a definovať sieť pre ktorú sa to týka.
9. Nakoniec sa nám zobrazilo zosumarizovanie nastavení, ktoré sa aj následne potvrdilo.

9 MONITOROVANIE SIETE

Monitorovanie poskytuje správcovi siete informácie a prehľad o sieti. Vďaka týmto informáciám dokážeme správne a rýchlo reagovať na udalosti, ktoré by mohli obmedziť, alebo úplne prerušiť poskytovanie služieb. Správne nakonfigurované Cisco zariadenie dokáže pri chybe vygenerovať udalosť, ktorú následne odošle podľa nastavených pravidiel. Efektívny spôsob prístupu ku sieťovým zariadeniam je možné vykonávať pomocou protokolu SNMP (Simple Network Management Protocol), ktorý komunikuje pomocou TCP/IP. Riadené objekty sú sieťové karty, smerovače a podobne. Tento protokol využíva aj takzvaných agentov, ktorý predstavujú modul zbierajúci informácie o objektoch. Databáza MIB obsahuje informácie o riadených objektoch. Konzola slúži na vizuálne zobrazenie a správu jednotlivých zariadení. Administrácia siete pomocou tohto protokolu funguje na princípe odosielania SNMP príkazov na zariadenia. Na tieto príkazy potom odpovedajú SNMP agenti. Fungovanie je založené na všesmerovom vysielaní a operuje na aplikačnej vrstve sieťového modelu. Udalosti ktoré vzniknú na zariadení sú následne vysielané do siete ako SNMP trap správa. Týmto spôsobom preskočíme operáciu žiadosti o stav. Zariadenia ktoré počúvajú na sieti môžu túto informáciu zachytiť a nastaveným spôsobom to oznámiť správcovi siete. Súborny MIB majú stromovú štruktúru a každý uzol je identifikátor objektu OID má hodnotu ktorú môžeme čítať (read), zmeniť ju (set), alebo oboje naraz. MIB je nezávislý na platforme a je popisovaný pomocou sady SMI (Structure of Management Information).

9.1 Aplikácia OpenNMS

Je bezplatná aplikácia určená na správu počítačovej siete a zariadení na nej nachádzajúcich sa. Podporuje automatické a manuálne objavovanie siete. OpenNMS obsahuje veľké množstvo nastavení, filtrovacích a oznamujúcich mechanizmov vďaka ktorým je ideálnym monitorovacím prostriedkom v sieti. Ovládanie aplikácie je možné pomocou skriptov, alebo použitím webového GUI. Veľké množstvo data kolektorov podporuje SNMP a jemu podobné protokoly. Okrem chybových stavov je možné graficky zobrazovať aj výkonnostné informácie a tým zjednodušiť vyhľadávanie možných problémov na sieti.

SNMP Attributes	
Name	SWITCHDA1
Object ID	.1.3.6.1.4.1.9.1.717
Location	KontaktLok
Contact	KontaktJA
Description	Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(1)SE3, RELEASE SOFTWARE (fc1)...Technical Support: http://www.cisco.com/techsupport...Copyright (c) 1986-2012 by Cisco Systems, Inc...Compiled Wed 30-May-12 14:26 by prod_rel_team

Availability		
Availability (last 24 hours)	59.274%	
172.30.44.2	Overall	28.729%
	HTTP	4.972%
	ICMP	4.972%
	SNMP	100.000%
	SSH	4.972%
	StrafePing	Not Monitored
	Telnet	Not Monitored
	Overall	100.000%
	HTTP	100.000%
	ICMP	100.000%
SSH	100.000%	
StrafePing	Not Monitored	
Telnet	Not Monitored	

Node Interfaces			
IP Interfaces	Physical Interfaces		
IP Address	IP Host Name	IfIndex	Managed
172.30.44.2	SWITCHDA1	10	M

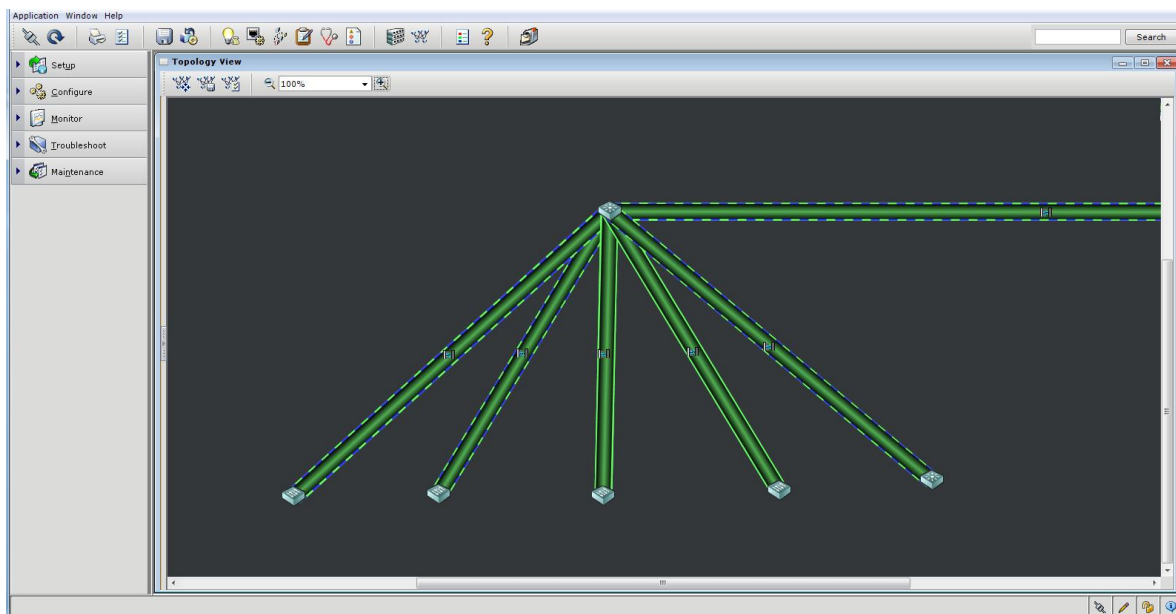
General (Status: Active)				
View Node Link Detailed Info				
Surveillance Category Memberships (Edit)				
This node is not a member of any categories.				
Notification				
You: Outstanding: (Check)				
You: Acknowledged: (Check)				
Recent Events				
<input type="checkbox"/>	229	5/14/13 06:58:53	Normal	Node #4's label was changed from 172.30.44.2 to SWITCHDA1
<input type="checkbox"/>	228	5/14/13 06:58:53	Warning	Node information has changed for 4.
<input type="checkbox"/>	227	5/14/13 06:58:53	Normal	A services scan has been completed on this node.
<input type="checkbox"/>	226	5/14/13 06:58:53	Warning	Primary SNMP interface for node 4 has changed from to 172.30.44.2
<input type="checkbox"/>	225	5/14/13 06:58:53	Warning	The SSH service has been discovered on interface
More...				
Recent Outages				
Interface	Service	Lost	Regained	Outage ID
172.30.44.2	HTTP	5/8/13 05:06:30	5/14/13 06:54:45	7
172.30.44.2	ICMP	5/8/13 05:06:30	5/14/13 06:54:45	6
172.30.44.2	SSH	5/8/13 05:06:30	5/14/13 06:54:45	5

Obr. 13. Podrobný popis služeb bežiacich na zariadení.

Podľa nastavenia aplikácie je možné pri zachytení trap správy vykonať niekoľko akcií. OpenNMS môže automaticky vyslať príkaz na inkriminované zariadenie a následne skontrolovať jeho stav. Pokiaľ toto nepomôže nasledujúca akcia bola nastavená odoslanie e-mailu o vzniknutej chybe, alebo ak je nainštalovaná GSM brána odoslať SMS správu na predvolené čísla. Toto má výhodu v prípade ak monitorovaná sieť zlyhaním prestala preposielať dáta a tento stav by následne nedovolil vykonať prvé dve spomínané akcie.

9.2 Aplikácia Cisco Network Assistant

Táto aplikácia je priamo od spoločnosti Cisco a umožňuje jednoduché monitorovanie siete. Aplikácia komunikuje výhradne so zariadeniami patriacej do portfólia tejto spoločnosti. Vo všeobecnosti je to voľne dostupná aplikácia umožňujúca monitorovanie a nastavovanie aktívnych prvkov siete pomocou grafického rozhrania. Použitie CNA je intuitívne a so zariadeniami komunikuje automaticky. Pri prvom prihlásení sa do aplikácie bolo potrebné vytvoriť profil predstavujúci komunitu zariadení a zaradiť tam jedno zariadenie. V našom prípade tam bol zaradený hlavný MLS prepínač v budove A. Na vzájomnú komunikáciu medzi zariadeniami používa CDP protokol. Aplikácia so zariadeniami komunikuje pomocou protokolu HTTPS a ak to nie je možné použije HTTP.



Obr. 14. Zobrazenie počítačovej siete v budove B pomocou CNA.

Okrem automatického mapovania siete pomocou ICMP a CDP je možné pridať zariadenie manuálne a to najmä v prípade ak sú na ňom tieto protokoly zakázané. Podobne ako OpenNMS dokáže zobrazovať vytázenie zariadení a identifikovať na nich vzniknuté chyby. Výhodou oproti OpenNMS je schopnosť CNA vybrať a zobrazit' jednotlivé zariadenia a kliknutím myši vykonať zmenu nastavenia. Umožňuje zálohovať jednotlivé konfigurácie a v prípade potreby ich kedykoľvek obnoviť. Dokáže kontrolovať jednotlivé verzie IOSu, požadovať jeho aktualizáciu a nakoniec ju aj vykonať. Nevýhodou CNA sú možnosti jeho využitia. Aplikácia beží lokálne na počítači a nie je možné sa na ňu prihlásiť inak ako lokálne. Aj keď predstavuje silný nástroj na správu siete, nemožnosť pripojiť sa pomocou webového rozhrania a limitované možnosti oznamovania chýb túto aplikáciu predurčuje len na individuálne použitie pre administrátora.

ZÁVER

Cieľom práce bolo navrhnúť spôsob inovácie podnikovej počítačovej siete. V prvej časti boli popísané fyzické zariadenia operujúce na sieti a metódy ich vzájomného prepojenia. Je dôležité aby čitateľ, alebo správca počítačovej siete rozumel jednotlivým segmentom, ktoré pri vhodnom prepojení dokážu zabezpečiť vysokú dostupnosť služieb a pohodlie pre používateľov. Okrem fyzických zariadení boli popísané niektoré najčastejšie používané protokoly. Hodnota prenášaných dát má pre firmu nevyčísliteľnú hodnotu a preto bol do práce uvedený aj spôsob ich ochrany pred nezainteresovanými osobami a prostredím mimo firmu. Obmedzenie rozsahu práce neumožňovalo podrobné rozobratie každej kapitoly a preto bolo nutné zamerať sa len na najnutnejšie informácie oboznamujúce čitateľa o danej problematike.

V praktickej časti bol opísaný pôvodný stav firemnej počítačovej siete a nedostatky ktoré takáto počítačová sieť obsahuje. Ako najzložitejšiu časť sa považuje problém finančného škrtania výdavkov a nemožnosť ucelenej obmeny všetkých zariadení, tak ako to bolo pôvodne naplánované. Počas písania práce sa podarilo vymeniť a nakonfigurovať všetky kriticky dôležité časti siete a teda doceliť stav kedy má administrátor pod kontrolou každé zariadenie nachádzajúce sa v sieti. Okrem toho sa zvýšila dostupnosť služieb aj na miesta na ktorých to nebolo z technických príčin možné. Za najväčší úspech sa považuje vyriešenie problému záložných ciest do hlavného prepínača vytvorením viacnásobných redundantných prepojov medzi najkritickejšími prepínačmi v sieti. V pôvodnom modeli neboli cesty vôbec zálohované a v prípade výpadku by až do okamihu odstránenia chyby nebolo možné zasiahnutý segment siete používať. Rozšírením bezdrôtovej siete sa otvorili možnosti využívania takejto technológie aj v procese výroby. Druhou veľkou výzvou bolo pripojenie vedľajšej budovy a jej príprava na budúce rozširovanie. Poslednou uskutočnenou zmenou bola výmena firewallov a umiestnenie webového servera do DMZ. Pre administrátorov bola vytvorená možnosť priameho vzdialeného prístupu na podnikovú sieť pomocou technológie VPN.

Do budúca ak to finančná situácia dovoľí, sa plánuje dokončiť obmena zariadení a to hlavne dokúpením MLS prepínačov pre vrstvu jadra a WLC kontroléra pre podnikovú WLAN. Okrem toho umožniť používateľom využívanie nášho VPN a rozšírenie služieb umiestnených v demilitarizovanej zóne.

CONCLUSION

The aim of this thesis was innovation of corporate computer network. In the first section I described all network equipments what are essential for innovation process. It is very important to understand what all network segments do if administrator must resolve some kind of problem. Good configuration offer reliable and comfortable network services for end user. Company data contain private informations what should be unavailable for external access. Network protection and protocol review is described in network security chapter.

Original condition of corporate network and old devices didn't support new features and this negatives were described before they had been replaced. Only necessary devices were replaced because of company financial limitation didn't allow made it as I proposed. All network devices were configured and administrator has all this parts under his control via real time network monitoring tool. Wireless technology overcome technical limitations how connect devices situated on places where physical connection is not available. Redundant paths provide reliable connection between all critical switches in the topology. In old layout the were not redundant paths and if network interruption occurred the connection was lost until the issue was resolved. Second building was connected to major corporate network and if it is needed we are able extend or connect new network devices immediately. I have replaced all firewalls and company web server is now available from Internet. This server is situated on special network called demilitarized zone. Only administrators have access to company network via our VPN, but this feature will be available in near future for all employees.

Forecast for future is to continue in the exchange of old equipments and buy new MLS switches for core layer and WLC for smarter management of corporate WLAN.

ZOZNAM POUŽITEJ LITERATURY

- [1] PC-networks:TIA-568-A-B. *PC-networks* [online]. 2010 [cit. 2013-05-01]. Dostupné z: <http://pc-networks.info/sk/wp-content/uploads/2010/10/obr8.jpeg>
- [2] TRULOVE, James. *Sítě LAN: hardware, instalace a zapojení*. Vyd. 1. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.
- [3] SOSINSKY, Barrie. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: Computer Press, 2010, 840 s. Mistrovství (Computer Press). ISBN 978-80-251-3363-7.
- [4] Helix84:Osi-model-sk.png. *Wikipedia* [online]. 2005 [cit. 2013-03-20]. Dostupné z: <http://upload.wikimedia.org/wikipedia/commons/f/fb/Osi-model-sk.png>
- [5] CASAD, Joe. *Sams teach yourself TCP/IP in 24 hours* [online]. 5th ed. Indianapolis, Ind.: Sams, c2012, xiii, 529 p. [cit. 2013-05-09]. ISBN 06-723-3571-9. Dostupné z: <http://it-ebooks.info/book/1004/>
- [6] DONAHUE, Gary A. *Kompletní průvodce síťového experta*. Vyd. 1. Brno: Computer Press, 2009, 528 s. ISBN 978-80-251-2247-1.
- [7] 56cto:802.11b_g.jpg 56cto [online]. 2008 [cit. 2013-04-28]. Dostupné z: <http://www.56cto.com/html/Center/fenxi/Cisco/40655.html>
- [8] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.
- [9] Pbroks13:DMZ_network_diagram_1_firewall.svg. *Wikipedia* [online]. 2008 [cit. 2013-03-20]. Dostupné z: [http://upload.wikimedia.org/wikipedia/commons/6/6f/DMZ_network_diagram_1_firewall .svg](http://upload.wikimedia.org/wikipedia/commons/6/6f/DMZ_network_diagram_1_firewall.svg)
- [10] CISCO. *Cisco Systems* [online]. 2013 [cit. 2013-02-04]. Dostupné z: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch3_WLAN.html
- [11] CISCO. *Cisco Systems* [online]. 2013 [cit. 2013-02-07]. Dostupné z: <http://www.cisco.com/en/US/hmpgs/index.html>
- [12] NORTHCUTT, Stephen a Lenny ZELTSER. *Bezpečnost sítí: velká kniha*. Vyd. 1. Brno: CP Books, 2005, 589 s. ISBN 80-251-0697-7.

-
- [13] FRAHIM, Jazib a Omar SANTOS. *Cisco ASA: all-in-one firewall, IPS, Anti-X, and VPN adaptive security appliance*. 2nd ed. Indianapolis, IN: Cisco Press, c2010, xxv, 1119 p. Cisco Press networking technology series. ISBN 15-870-5819-7.
- [14] KÁLLAY, Fedor a Peter PENIAK. *Počítačové siete a ich aplikácie*. Žilina: EDIS, 1998. ISBN 80-7100-380-8.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
ASA	Adaptive Security Appliances
ASDM	Adaptive Security Device Manager
BID	Bridge ID
BPDU	Bridge Protocol Data Unit
BSS	Basic Service Set
CAM	Content-addressable memory
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
DCE	Data Communications Equipment
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized zone
DTE	Data Terminal Equipment
DTP	Dynamic Trunk Protocol
EAP	Extensible Authentication Protocol
EIA/TIA	Electronic Industries Alliance / Industry Association
ESS	Extended Service Set
FIB	Forwarding Information Base
FTP	File Transfer Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers

IGRP	Internal Gateway Routing Protocol
IP	Internet Protocol
IPS	Intrusion Prevention Systems
ISL	Cisco Inter-Switch Link
ISO	International Organization for Standardization
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
LLC	Logical Link Control
LWAP	Lightweight Access Point
LWAPP	Lightweight Access Point Protocol
MAC	Media Access Control address
MIC	Message Integrity Code
MLS	Multilayer Switch
MPDU	MAC Protocol Data Unit
MSK	Master Session Key
MSS	Maximum Segment Size
MSTP	Multiple Spanning Tree Protokol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NIC	Network Interface Card
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAT	Port Address Translation
PEAP	Protected Extensible Authentication Protocol
PHY	Physical layer of the OSI model

PIX	Private Internet eXchange
PVST	Per VLAN Spanning Tree
QoS	Quality of Services
RFC	Request for Comment
RIB	Routing Information Base
RIP	Routing Information Protocol
RSTP	Rapid Spanning Tree Protocol
SFF	Small Form Factor
SIP	Session Initiation Protocol
SSID	Service Set Identifier
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
SVI	Switched Virtual Interface
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time to Live
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Masking
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTP	VLAN Trunking Protokol
VLAN	Virtual Local Area Network
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller

ZOZNAM OBRÁZKOV

Obr. 1. Schéma zapojenia podľa TIA [1].....	14
Obr. 2. Referenčný model OSI [4].....	23
Obr. 3. Porovnanie referenčných modelov.	27
Obr. 4. Zobrazenie kanálov pre 802.1b a 802.1g [7].	48
Obr. 5. Logika použitia ACL.	55
Obr. 6. Model DMZ [9].	56
Obr. 7. Počítačová sieť v budove A.	73
Obr. 8. Počítačová sieť v budove B.	74
Obr. 9. Dosah jednotlivých AP.	80
Obr. 10. Umiestnenie firewallov.....	88
Obr. 11. Vytvorenie certifikátu pomocou ASDM.....	92
Obr. 12. Nastavenie autentifikačného serveru pomocou ASDM.....	93
Obr. 13. Podrobný popis služieb bežiacich na zariadení.	95
Obr. 14. Zobrazenie počítačovej siete v budove B pomocou CNA.....	96

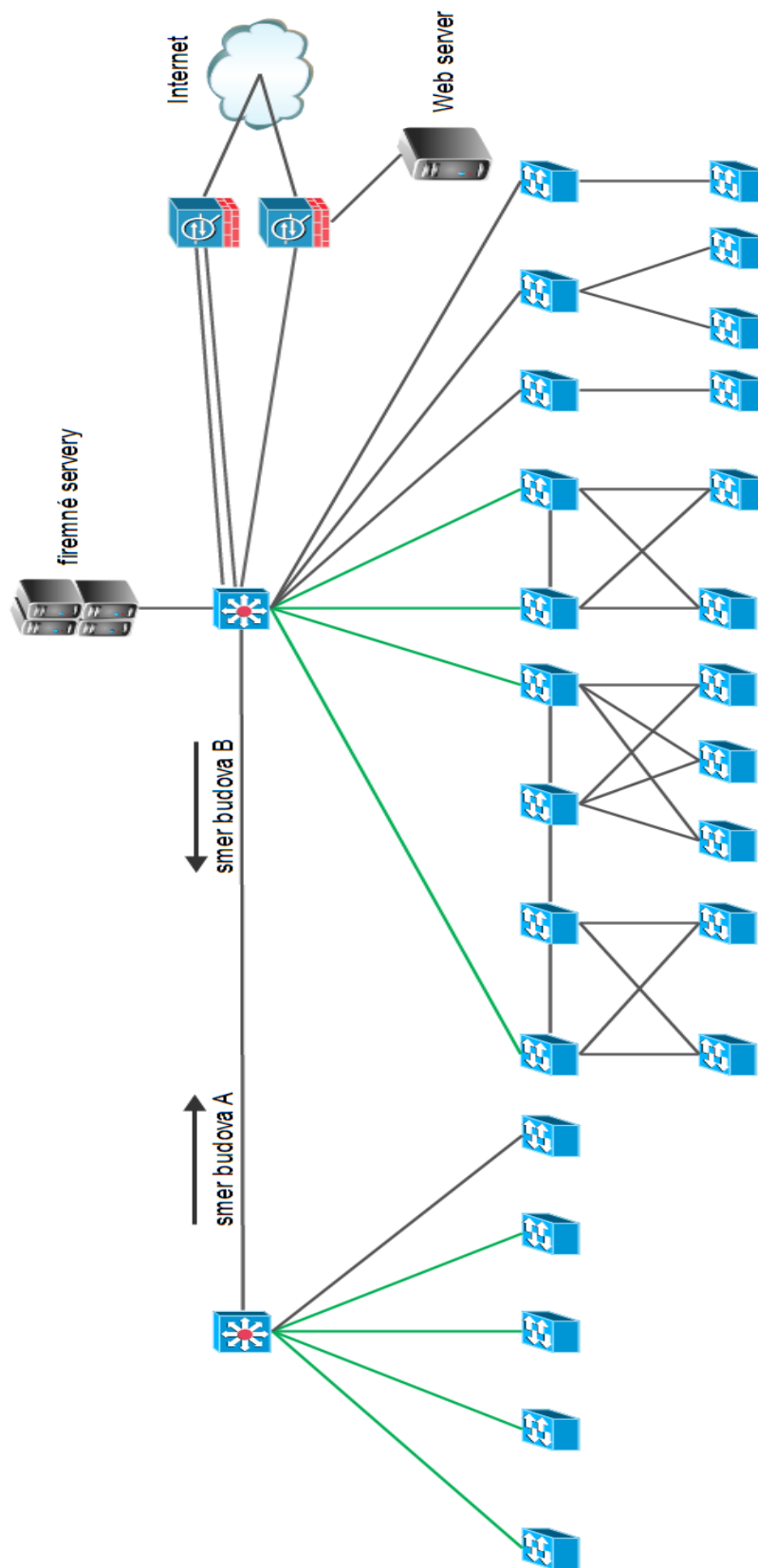
ZOZNAM TABULIEK

Tab. 1. Šírka pásma pre viacvidové vlákna [2].....	17
Tab. 2. Adresné bloky podľa triedy.	31
Tab. 3 Cena jednotlivých portov.....	40
Tab. 4. Prehľad štandardov 802.11.	47
Tab. 5. Adresovanie v sieti.	63
Tab. 6. Porovnanie firewallov ASA 5505 a 5510.....	68

ZOZNAM PRÍLOH

- P I Topológia siete
- P II Štruktúra zložiek disku uložená na CD

PRÍLOHA P I: TOPOLOGIA SETE



PRÍLOHA P II: ŠTRUKTÚRA ZLOŽIEK DISKU ULOŽENÁ NA CD

\Config_mls\	- konfigurácia MLS
\Config_2960\	- konfigurácia distribučného prepínača
\Config_ap\	- konfigurácia AP
\Config_pushfw\	- konfigurácia push firewallu
\Config_mainfw\	- konfigurácia hlavného firewallu