Mendelova univerzita v Brně
Provozně ekonomická fakulta

Návrh inovácie počítačovej siete pre strednú školu a školský internát

Bakalárska práca

Vedúci práce:
Ing. Ludmila Kunderová

Lukáš Duban

Brno 2014

Poďakovanie patrí hlavne Ing. Ludmile Kunderovej, vedúcej mojej bakalárskej práce za vedenie a rady, za pomoci ktorých som mohol vypracovať túto bakalársku prácu. Taktiež by som chcel poďakovať vedeniu Strednej priemyselnej školy elektrotechnickej v Piešťanoch za poskytnutie podkladov potrebných pre túto prácu.

Čestné prehlásenie

Prehlasujem, že som túto prácu: **Návrh inovácie počítačovej siete pre strednú školu a školský internát**
vypracoval samostatne a všetky použité pramene a informácie sú uvedené v zozname použitej literatúry. Súhlasím, aby moja práca bola zverejnená v súlade s § 47b zákona č. 111/1998 Sb., o vysokých školách v znení neskorších predpisov, a v súlade s platnou *Smernicou o zverejňovaní vysokoškolských záverečných prácach.*
Som si vedomý, že sa na moju prácu vzťahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzatvorenie licenčnej zmluvy o užití tejto práce ako školského diela podla § 60 odst. 1 autorského zákona.
Ďalej sa zaväzujem, že pred spísaním licenčnej zmluvy o využití diela inou osobou (subjektom) si vyžiadam písomné stanovisko univerzity o tom, že predmetná licenčná zmluva nie je v rozpore s oprávnenými záujmami univerzity, a zaväzujem sa uhradiť prípadný príspevok na úhradu nákladov spojených so vznikom diela, a to až do ich skutočnej výšky.

Brno 2014 .....

Abstract

Citácia práce v anglickom jazyku

Bachelor thesis is focused to evaluate computer network in school and college from the functional and safety point of view. It is processed theoretical basis which is used to make innovative resolution. This solution is verified in simulation application and then evaluated from functional, safety and financial point of view.

Abstrakt

Citácia práce v slovenskom jazyku

Práca je zameraná na zhodnotenie počítačovej siete v škole a školskom internáte z hľadiska funkčnosti a bezpečnosti. Spracované su v nej teoretické východiská pre vytvorenie inovatívneho riešenia, ktoré je súčasťou práce. Toto riešenie je overené simulačným programom a následne vyhodnotené z funkčného, bezpečnostného a finančného hľadiska.

Obsah

Zoznam tabuliek

1 Úvod a cieľ práce

1.1 Úvod do problematiky

Počítačová sieť na školách je v dnešnej dobe súčasťou života každého žiaka či študenta. Preto sa na školách snažia zlepšiť podmienky aj po stránke informačných technológií. Nie každá škola však má dostatok finančných prostriedkov na inováciu a správu takýchto sietí. Preto je dôležité poukázať na výhody, ktoré prinesie zavedenie novších technológií nielen vo výuke, ale hlavne bezpečnosti, ktorá je na nižších úrovniach školstva zanedbávaná. Každá takáto škola by teda mala dbať aspoň na zabezpečenie počítačovej siete. Ak sa na problematiku pozrieme z hľadiska užívateľov, zistíme že čoraz viac z nich používa sieťové služby a nahrádza tak bežné prostriedky. Užívatelia, ktorí bežne používali USB flash disky prešli na rýchlejší a pohodlnejší spôsob ukladania informácií na zdieľané disky, ku ktorým majú prístup iba oni. Avšak to zo sebou prináša aj zvyšovanie množstva dát, ktoré sieťou prechádzajú, čím sa zvyšuje zaťaženie sietí. Preto je potrebné tieto siete neustále inovovať a zrýchľovať.

1.2 Cieľ práce

Cieľom práce je analyzovať a popísať súčasný stav počítačovej siete na Strednej priemyselnej škole elektrotechnickej v Piešťanoch. Zistiť jej nedostatky a navrhnúť nové riešenia s finančnou analýzou, ktoré budú overené pomocou aplikácie pre modelovanie počítačových sietí.

1.3 Literárne zdroje

V práci je využitých množstvo informácií, ktoré sú pôvodom iných autorov, ktorí už popísali množstvo technologických a funkčných postupov. Tieto infromácie pomáhajú lepšie pochopiť fungovanie počítačovej siete, a preto v tejto časti budú uvedené literárne zdroje, ktoré boli v práci použité.

Jedna z najväčších firiem, ktorá sa zaoberá tematikou počítačových sietí a dominuje na poli sieťových prvkov, je Cisco Systems, Inc. Wendel Odom vydal niekoľko publikácií, ktoré rozoberajú všetky technológie Cisca a aplikujú ich v rôznych sektoroch použitia, ako aj postupy pri tvorbe počítačových sietí.

Ďalšia kniha je trochu staršia, avšak mnoho zo štandardov, ktoré táto kniha popisuje, stále platí a aktívne sa používajú. Ide o knihu Velký průvodce protokoly TCP/IP a systémem DNS, od Libora Dostálka a Aleny Kabelovej, ktorá popisuje základné protokoly, sieťové architektúry, prácu s aplikačnými protokolmi a ďalšie.

Ďalším významným zdrojom je Wikipedia, kde sa dá nájsť mnoho informácií, a to hlavne v anglických článkoch, ktoré sú z hľadiska dôveryhodnosti lepšie.

Všetky spomínané zdroje popisujú technologické a hardvérové vlastnosti v sieťových technológiách. Softvérové nástroje, ktoré budú požité v práci sú popísané na

stránkach výrobcov. Ide o voľne šíriteľný simulačný nástroj GNS 3 a preto je popísaný iba formou návodov a tipov ako aplikáciu používať a tak isto aj test bezpečnosti IPA Benchmark.

Určite je treba spomenúť, že niektoré podobné témy už boli spracované v predošlých prácach, a teda je možné nahliadnuť a použiť tieto spracované informácie tak, aby zapadli do kontextu tejto práce.

1.4 Metodika práce

Pre správny postup pri tvorbe práce je najdôležitejšie vybrať a naštudovať správne literárne zdroje, z ktorých je potrebné získať potrebné informácie. V teoretickej časti sú následne tieto informácie použité a doplnené o vlastné vedomosti a skúsenosti nodobudnuté počas štúdia.

V časti zameranej na vlastnú prácu sa aplikujú vhodné praktiky pre vytvorenie inovatívneho riešenia, ktoré analyzujú súčasný (IPA test informačnej bezpečnosti) stav a zistia nedostatky. Na základe nájdených nedostatkov budú vytvorené opatrenia.

Tieto opatrenia budú implementované do nového riešenia, ktoré tvorí hlavnú časť vlastnej práce. Vytvorené riešenie bude následne overené v simulačnom programe, ktorý zistí, či je možné riešenie použiť v reálnej sieti.

V záverečnej časti bude navrhované riešenie vyhodnotené z hľadiska zabezpečenia, funkčnosti a finančných nákladov na realizáciu.

2 Teoretický úvod

Počítačová sieť je systém vzájomne prepojených sieťových prvkov a uživateľských staníc. Pomocou siete je teda možné prenášať informácie. Hardvér siete zahŕňa fyzické prostriedky, ktoré sú pomocou káblového spojovacieho vedenia pospájané a tým tvoria sieť na fyzickej úrovni. Sú to napríklad sieťové karty (NIC), ktoré pre uživateľské stanice sprostredkúvajú komunikáciu v sieti, sieťové tlačiarne, tlačové servery, ktoré slúžia na tlač z nesieťových tlačiarní po sieti, webové, súborové a iné servery. Sieťový softvér je programové vybavenie, ktoré v spolupráci s hardvérom siete zabezpečuje funkcie siete.

V tejto kapitole budú popísané všeobecne potrebné štandardy pri vytváraní počítačovej siete. Ďalej tu budú popísané zásady, ktoré by mali byť dodržiavané pri návrhu siete pre vzdelávacie a školské zariadenia.

2.1 Switched Ethernet

Nie je samostatným protokolom, avšak jeho použitím sa sieť rozdeľuje na menšie segmenty, ktoré sa dajú ľahšie kontrolovať, čím je zaistená minimálna vnútorná priepustnosť každého segmentu, a tak nedochádza ku kolíziám. Umožňuje tiež manipuláciu s dátami na úrovni 2. vrstvy. Prepínané sú vnútorné spoje siete, avšak ak je v segmente hub, nie je možné používať obojsmernú komunikáciu v tejto časti siete. Od prepínača do serveru vedie obvykle priama krútená dvojlinka, čiže určuje oddelený segment, a teda je možné používať obojsmernú komunikáciu. Pri obojsmernej komunikácii je však potrebné zabezpečiť, aby toto vysielanie nebolo považované za kolíziu. Systém kolízií zamedzuje garanciu, ako často bude umožnená komunikácia k prenosovému médiu.

- **802.3** – pre sieť 10 BASE 5
- **802.3a** – pre sieť 10 BASE 2
- **802.3i** – pre sieť 10 BASE T
- **802.3j** – pre sieť 10 BASE FX
- **802.3u** – pre sieť 100 BASE T
- **802.3z** – pre sieť 1000 BASE (gigabitový ethernet, backbone siete)

10Base-T Tvorí rozvod z krútených (z ang. twisted) vodičov. Systém popisuje norma IEEE 802.3 a vytvára sieť s mnohonásobným prístupom CSMA/CD.

FastEthernet

Používa sa len na krútených pároch alebo optických vláknach. Zvýšená rýchlosť je na úkor vzdialenosti, ktorá je zvyčajne 210m. Môže pracovať aj v režime full duplex, čo

je 2x100Mb/s. Využitie full duplexu je však vhodné iba na spoje medzi prepínačmi, pretože prenosy klient-server bývajú veľmi často nesymetrické.

100BASE-T je štandard, ktorý používa rovnakú metódu prístupu ako 10BASE-T, ale tiež podporuje hviezdicovú topológiu a káble typu STP (Shiled Twisted Pair), čo znamená, že kábel je upravený tienením, a tým znižuje mieru žiarenia. Odvodené štandardy:

Tabuľka 1: Tabuľka prenosových médií pre FastEthernet a ich dosah

Norma	**Prenosové médium**	**Dosah v m**
100BASE-TX	2 páry STP alebo UTP kategórie 5	100
100BASE-FX	2 vlákna optického kabelu	412
100BASE-T4	UTP kategórie 3 a 4 s voľnými všetkými pármi	100

GigabitEthernet

Prenosová rýchlosť zvyšuje na 1Gbit/s. Opäť využíva prvky pôvodného Ethernetu. V praxi sa využíva iba prepínane s full duplexom. Dôležité je použitie rovnakého rámca. Pôvodne vytvorený pre optické vlákna (IEEE 802.3z), neskôr bol doplnený aj štandard pre krútenú dvojlinku (IEEE 802.3ab). Hlavné využitie je teda pre prepojovanie FastEthernet prepínačov, centrálnych Gigabitových prepínačov alebo servery s Gigabitovým adaptérom.

Tabuľka 2: Tabuľka prenosových médií pre GigabitEthernet a ich dosah

Norma	**Prenosové médium**	**Dosah v m**
1000 Base SX	mnoho vidové optické vlákno (850 nm)	500
1000 Base LX	mnoho vidové optické vlákno (1300 nm)	500
	mnoho vidové optické vlákno (130 nm)	2000
1000 Base CX	koaxiálny kábel STP (twinax)	25
1000 Base T	krútené páry UTP	

10 GigabitEthernet

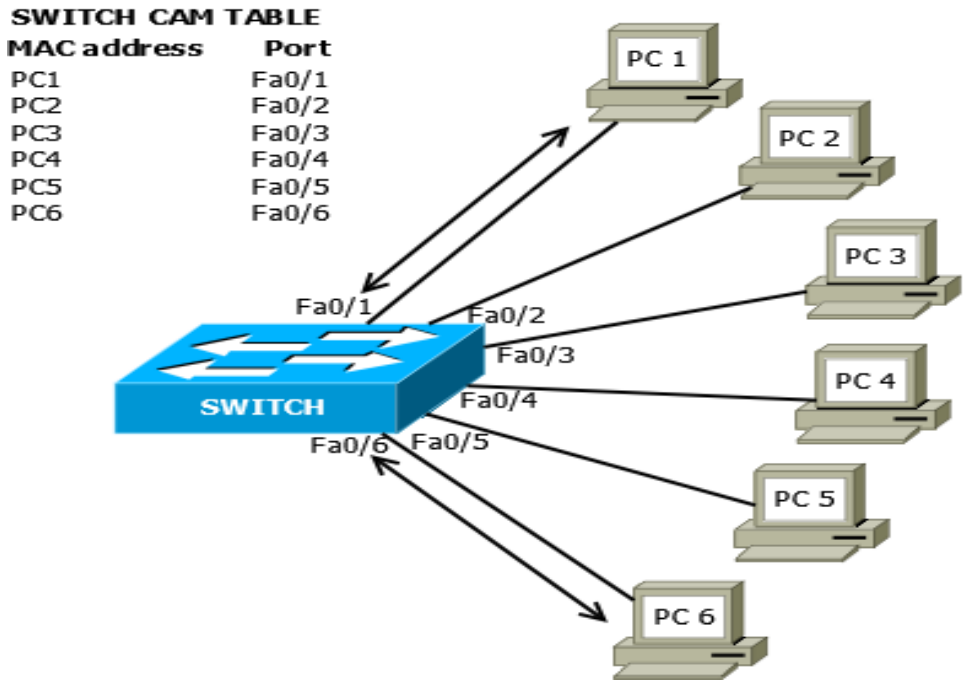
Je poslednou štandardizovanou normou IEEE 802.3ae prijatou v roku 2003. Prenosová rýchlosť bola zvýšená na 10Gb/s. Na prenos dát využíva optické vlákna a rovnaký formát rámca ako pôvodný Ethernet. Avšak jedna zásadná zmena sa udiala, a to že sa upustilo od algoritmu CSMA/CD. Pracuje vždy v režime full-duplex. Špecifikácie pre prenosové médium je určené CAT7 pre 100m, na kratšie vzdialenosti je však možné použiť i nižšiu kategóriu.

2.2 Aktívne prvky

Sú hlavnou časťou počítačovej siete. Slúžia na riadenie toku dát v sieti, určujú ako budú klienti komunikovať a sprostredkúvajú samotnú komunikáciu. Tri hlavné tvoriace počítačovú sieť sú switch (prepínač), router (smerovač) a Wifi Acess Point (bezdrôtový prístupový bod).

Prepínač

Je prvok pracujúci na linkovej vrstve modelu OSI, kde slúži k prepojeniu jednotlivých prvkov v rámci jednej siete. Funguje na základe MAC adries CAM[1] tabuľky. Ako je vidieť na obrázku č. 1, pri komunikácii PC1 s PC6 prepínač zistí z eternetového rámca cieľovú MAC adresu čo je MAC adresa PC6 a porovná ju so záznamami v CAM tabuľke. Ak sa cieľová MAC adresa zhoduje s niektorým záznamom, odošle paket na príslušný port. Ak by sa zhoda nenašla, prepínač odošle paket na všetky porty okrem portu, z ktorého bola komunikácia iniciovaná, počká na odpoveď od PC, pre ktorý bola komunikácia určená a pridá nový záznam do CAM tabuľky na základe tejto odpovede.

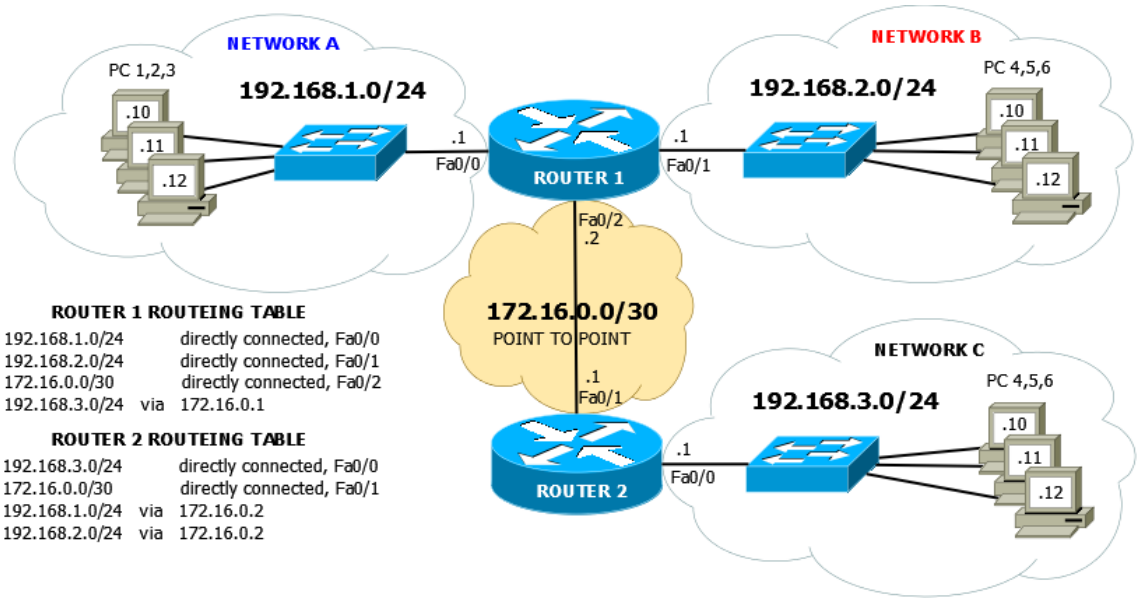


Obr. 1: Princíp fungovania prepínača, zdroj: vlastný

[1] Contetn Addressable Memory je dynamická tabuľka prepínača, ktorá obsahuje porty prepínača a MAC adresy zariadení pripojených k týmto portom

Smerovač

Tento prvok pracuje o vrstvu vyššie, a to na sieťovej vrstve. Smerovač slúži na prepojenie komunikácie medzi sieťami, ak teda potrebujeme aby komunikovali zariadenia v rôznych sieťach medzi sebou, musí byť medzi nimi smerovač. Pracuje s IP adresami a smerovacou tabuľkou. V tabuľke sú uvedené cieľové siete a k nim IP adresy alebo porty, cez ktoré sú tieto siete dostupné. Na obrázku č. 2 sú zapojené dva smerovače a štyri rôzne siete. Ak bude chcieť niektorý počítač komunikovať zo siete A alebo C, odošle dáta na predvolenú bránu, čo je IP adresa smerovača v sieti, v ktorej sa počítač nachádza. Smerovač otvorí paket na sieťovej vrstve a zistí cieľovú IP adresu a teda cieľovú sieť. Tú porovná zo sieťami vo svojej smerovacej tabuľke. Pri zhode môžu nastať dve situácie, a to buď ide o sieť priamo pripojenú k smerovaču a paket bude odoslaný na port, kde je sieť pripojená, alebo je určená nexthop IP adresa, cez ktorú je táto adresa siete dostupná. Ak bude teda počítač zo siete A komunikovať s počítačom zo siete B, počítač zo siete A odošle dáta na smerovač jedna, ten zistí podľa smerovacej tabuľky, že ide o sieť priamo pripojenú na porte Fa0/1 a odošle dáta na tento port. Ak by však išlo o komunikáciu do siete C, smerovač jedna odošle dáta na základe smerovacej tabuľky na smerovač dva pomocou nexthop IP. Smerovač dva zasa skontroluje svoju smerovaciu tabuľku, kde zistí priamo pripojenú sieť, pre ktorú je komunikácia určená a odošle dáta na port Fa0/0.

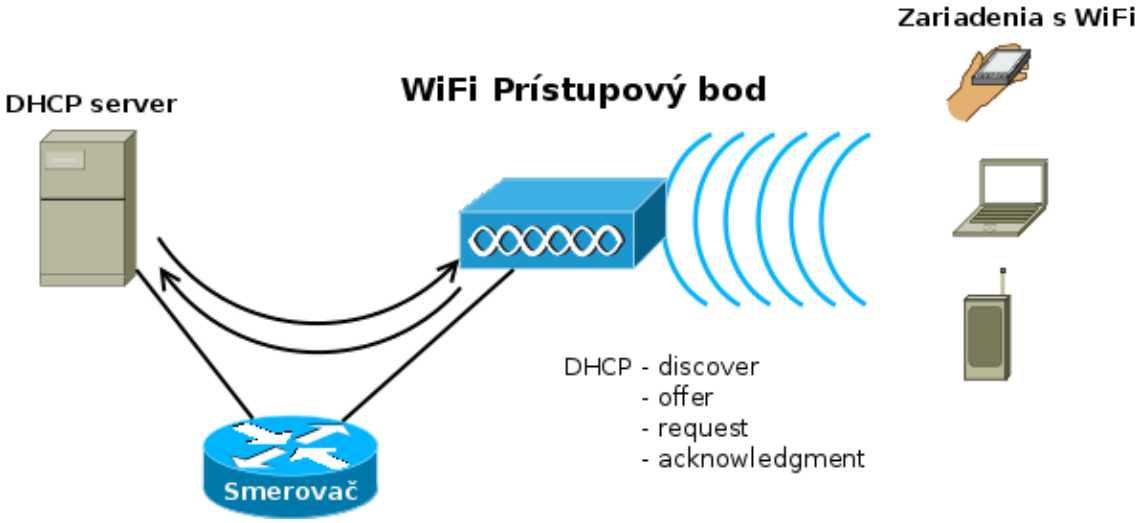


Obr. 2: Princíp fungovania smerovača, zdroj: vlastný

WiFi Bezdrôtový prístupový bod

Hlavné využitie bezdrôtovej siete je pri vytváraní počítačovej siete v domácnostiach, firmách alebo školách, kde často znemožňujú prístup sieti steny alebo iné prekážky.

S vytvorením bezdrôtových Access Pointov (AP), je užívateľom umožnený prístup k sieti aj v takýchto podmienkach iba pomocou pár alebo aj žiadnych káblov. AP je priamo pripojené do siete pomocou káblového Eternetového spojenia, kde je ďalej toto spojenie šírené využitím rádiofrekvenčnej linky. Zariadenie môže poskytovať vlastný DHCP server, ktorý poskytne konečnému užívateľovi informácie potrebné pre pripojenie do siete. Ďalším dôležitým faktorom je zabezpečenie a zamedzenie prístupu nepovoleným užívateľom, čo bude popísané v časti zabezpečenie počítačovej siete.



Obr. 3: Princíp fungovania WiFi Prístupového bodu, zdroj: vlastný

2.3 Zásady pri tvorbe siete pre vzdelávacie zariadenia

V tejto časti sa oboznámime zo zásadami, ktoré by mali byť dodržané pri tvorbe siete pre školy a školské zariadenia, aby nedošlo k narušeniu alebo znehodnoteniu informácií prenášaných počítačovými sieťami. Vzdelávacie zariadenia by mali poskytovať všetky výhody siete, tak aby bolo umožnené užívateľom, v našom prípade žiakom a študentom, plnohodnotné vzdelávanie. Narušením informácií v škole môžeme považovať zmenu, pridanie alebo vymazanie informácií súvisiacich so štúdiom, ktoré sú vykonané neautorizovanou osobou alebo osobou, ktorá nie je k týmto akciám oprávnená. Musí byť teda zamedzené študentom meniť alebo nejak ovplyvňovať výsledky štúdia. Pri vytváraní siete je teda potreba vytvoriť pravidlá pre používanie siete. Ďalej by mala byť oddelená sieť pre administratívu od školskej siete určenej pre výuku. Ak sa v škole nachádzajú laboratória pre výuku počítačových sietí, mala by byť táto sieť taktiež oddelená alebo samostatne vytvorená sieť pre účely výučby alebo výskumu. Pri laboratórnych cvičeniach často dochádza k úkonom, ktoré by mohli narušiť školskú sieť alebo by mohlo dôjsť k porušeniu zákonov o ochrane osobných údajov. Aby bolo možné kontrolovať prácu s koncovými zariadeniami, pretože v prostredí školy je vysoká možnosť pravdepodobnosť narušenia

alebo poškodenia zariadení slúžiacich pre výuku, je potrebné vytvoriť pre užívateľov prihlasovacie práva, podľa ktorých bude možné identifikovať narušiteľa.

Zabezpečenie siete z teoretického hľadiska

Pri zabezpečovaní siete je potreba dbať na tzv. CIA[2] trojicu bezpečnostných cieľov, jedny z hlavných princípov informačnej bezpečnosti. (Wikipedia, 2014). Dosiahnutie týchto cieľov je možné využitím moderných technológií v počítačových sieťach. Aby bolo možné tieto technológie použiť, najskôr je nutné určiť bezpečnostné hrozby pomocou analýzy rizík alebo penetračných testov, ktoré by mali odhaliť tieto hrozby. Následne po odhalení je potreba vytvoriť návrh opatrení, ktorými by sa tieto hrozby dali obmedziť alebo trvale odstrániť. Všetky tieto úkony sú riadené systémom ISMS[3]. Hlavné časti ISMS:

Analýza rizík je kľúčová aktivita v procese riešenia bezpečnosti. Jej cieľom je stanoviť možné hrozby a aká je vysoká pravdepodobnosť zraniteľnosti aktív voči týmto hrozbám. V analýze rizík sa riešia nasledujúce pojmy:

- **aktívum** - dôležité informácie s nejakou hodnotou týkajúce sa spoločnosti
- **hrozba** - úkony, ktoré by mohli narušiť dôveryhodnosť alebo integritu aktív
- **zraniteľnosť** - miera zneužitia hrozieb na fyzickej, logickej alebo administratívnej úrovni bezpečnosti
- **útok** - uskutočnenie hrozby
- **riziko** - pravdepodobnosť, že hrozba zneužije zraniteľnosť
- **typ dopadu** - môže byť finančného alebo nefinančného charakteru
- **protiopatrenia** - opatrenia, ktoré môžu viesť k zníženiu zraniteľnosti a ochrane aktíva pred hrozbou

Hrozby sa identifikujú podľa katalógu hrozieb ISO/IEC TR13335. Najskôr je však potrebné identifikovať a ohodnotiť aktíva. Potom nasleduje posúdenie hrozieb, pri ktorých je potrebné určiť pravdepodobnosť výskytu, ktorých výstupom je zoznam zraniteľných miest s určeným stupňom zraniteľnosti (vysoký/stredný/nízky). V ďalšom kroku sa určia zraniteľné miesta s popisom možnosti využitia týchto miest. Výstupom je zoznam zraniteľných miest a stupňom zraniteľnosti (rizikové/havarijne). Z týchto výstupov sa následne odvodia protiopatrenia a zoznam prijateľných rizík. Analýza rizík teda hovorí, čo všetko sa môže stať, prečo sa to tak môže stať, ako sa to môže stať, kde sa to môže stať(Čermák, 2010).

Fyzické zabezpečenie je dôležitou súčasťou bezpečnosti informačných systémov a siete. Je potrebné, aby bola serverová miestnosť dobre zabezpečená proti

[2] Confidentiality, Integrity, Availability(dôveryhodnosť integrita dostupnosť)

[3] Information security management system je súbor bezpečnostných politík zaoberajúcich sa informačnými systémami a súvisiacimi IT rizikami

Obr. 4: Analýza rizík, zdroj: vlastný

vniknutiu cudzích osôb. K hlavným prvkom siete a serverom by mali mať prístup iba osoby poverené ich administráciou. Ďalej by malo byť zabezpečené dobre odvetrávanie alebo chladenie, ktoré bude udržovať v miestnosti stálu prevádzkovú teplotu. V organizáciách, v ktorých je potrebné predísť výpadkom prúdu, je taktiež treba zaistiť záložné zdroje energie ako sú UPS[4] zdroje, veľkokapacitné batérie alebo motorové agregáty.

Zabezpečenie siete z praktického hľadiska

Po zistení možných hrozieb alebo zraniteľných miest siete sú následné protiopatrenia, ktoré boli označené ako dôležité, aplikované na rizikové časti systému. Implementácia týchto protiopatrení závisí od technologických možností systému, čo znamená, že aby mohli byť niektoré z nich aplikované, bude nutné inovovať niektoré časti tohoto systému. V nasledujúcom zozname sú uvedené najbežnejšie možné napadnutia počítačových sietí a ich protiopatrenia.

- **CAM overflow** - Port Security
- **MAC address spoofing** - Port Security

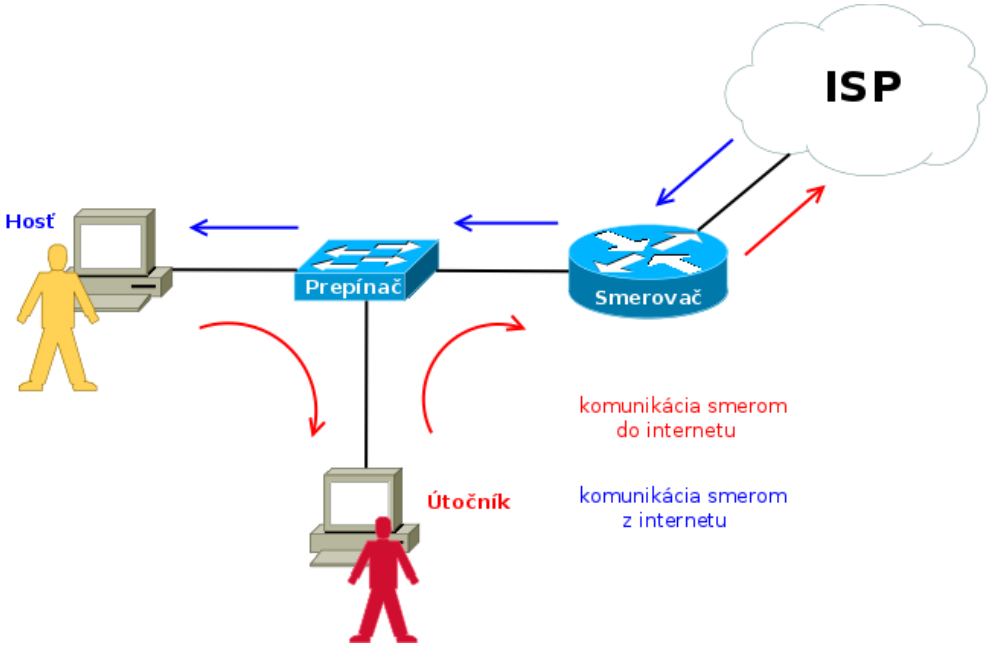
[4]Uninterruptible Power Supply - neprerušiteľný zdroj energie je zariadenie, ktoré zaisťuje nepretržitú dodávku elektrickej energie.(Wikipedia, 2014)

- **DHCP server spoofing** - DHCP Snooping
- **ARP spoofing** - Dynamic ARP Inspection
- **L2 loop, storm** - Strom Control
- **Unautorized access** - IEEE 802.1x, EAP, RADIUS, X.509

CAM overflow - preplnenie CAM tabuľky - ide o útok, pri ktorom útočník nageneruje veľké množstvo MAC adries, a tým vlastne preplní CAM tabuľku prepínača, čo znamená, že ak útočník následne zmení svoju MAC adresu na MAC adresu hosťa, na ktorého je útok cielený, bude komunikácia hosťa posielaná na port útočníka. Doba záznamu je obecne nastavená na 300 sekúnd, čo dáva útočníkovi možnosť uskutočniť tento útok.

Obrana: Port Security - ide o nastavenie prepínača, pri ktorom sa povolí iba jedna MAC adresa na port. MAC adresu je možné zadať staticky alebo dynamicky, čím sa vylúči možnosť nagenerovať veľké množstvo MAC adries z jedného portu.

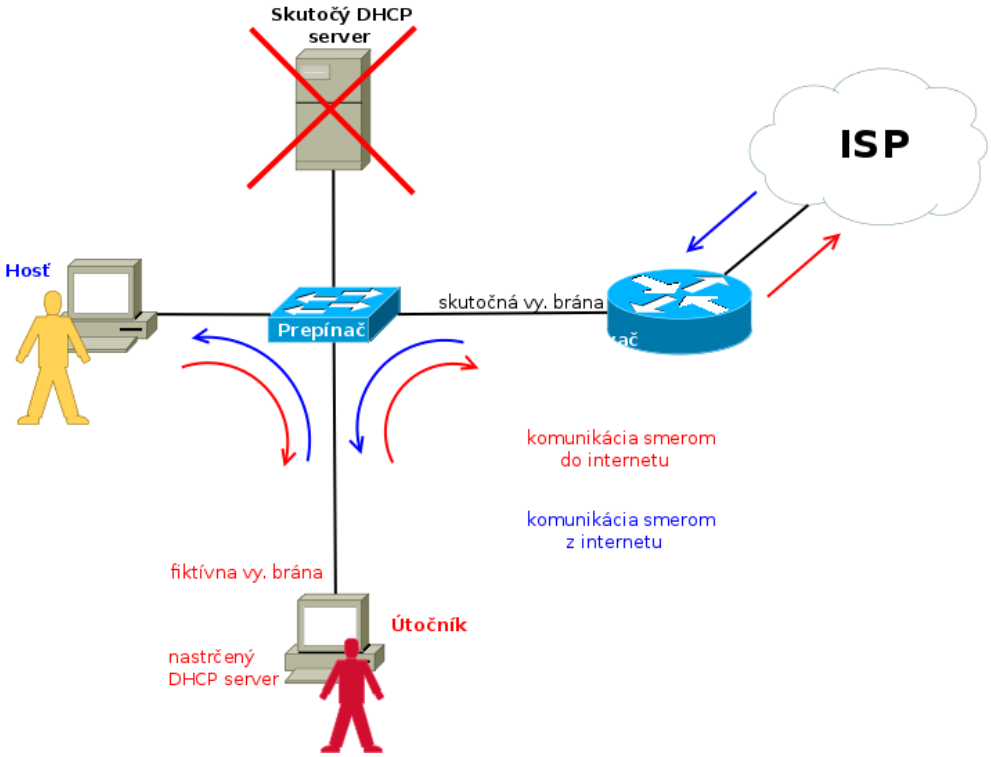
MAC address spoofing - nastrčenie MAC adresy - tento útok súvisí s CAM overflow, avšak tu si útočník zmení MAC adresu na MAC adresu predvolenej brány, a teda všetka odchádzajúca komunikácia ostatných hostov v sieti smerujúca mimo sieť bude posielaná na port útočníka. Ďalšie detaily sú vidieť na obrázku č. 5.



Obr. 5: MAC address spoofing, zdroj: vlastný

Obrana: Port Security - obrana je rovnaká ako pri CAM overflow

DHCP server spoofing - nastrčenie DHCP serveru - je útok, pri ktorom útočník zaberie všetky IP adresy poskytované skutočným DHCP serverom a následne poskytne cez nastrčený DHCP server IP adresu, predvolenú bránu a DNS informácie, pomocou ktorých dokáže presmerovať komunikáciu na svoje zariadenie, ktoré sa tvári ako smerovač, a teda komunikáciu preposiela ďalej do skutočného cieľa. Útočník má teda možnosť kontrolovať celú komunikáciu. Ďalšie detaily sú vidieť na obrázku č. 6.



Obr. 6: DHCP spoofing, zdroj: vlastný

Obrana: DHCP Snooping - nakonfigurovanie prepínača tak, aby rozoznával dôveryhodné (správy DHCP offer, DHCP Ack/Nack) a nedôveryhodné (správy DHCP discover, DHCP request, DHCP release) porty.

ARP spoofing - nastrčenie IP adresy - pri nadväzovaní komunikácie s neznámym cieľom v rámci siete vysiela počítač správu ARP request, v ktorej zisťuje MAC adresu cieľa broadcastom všetkým počítačom v sieti. Počítač, pre ktorý je správa určená, odpovedá správou ARP reply, v ktorej oznamuje svoju MAC. Následne si uložia obaja MAC adresy do ARP tabuľky, komunikujú na základe MAC adresy. To isté funguje aj v prípade, ak počítač nepozná MAC adresu predvolenej brány. Ak je ale v sieti útočník, ktorý vygeneruje správu GARP reply a oznámi, že MAC adresa

predvolenej brány je MAC adresa útočníka, tak hosť, ktorý komunikáciu iniciuje, bude všetku komunikáciu určenú mimo svoju sieť posielať na PC útočníka.

Obrana: DHCP Snooping - ide o podobný útok ako je DHCP spoofing, a teda obrana je podobná vo forme DHCP snooping table na prepínači, ktorá obsahuje záznamy s portom, MAC adresou a IP adresou každého hosta.

Unauthorized access to network - neoprávnený prístup do siete - je možný ak sieť nie je zabezpečená autentizačným mechanizmom. Útočník má tak prístup do siete bez toho, aby vedel alebo musel zadať informácie pre prístup do siete.

Obrana: Autentizácia užívateľa - aby bolo možné kontrolovať, kto má prístup do siete, je potrebné, aby sa každý uživateľ autentizoval. Najčastejšie je potrebné kontrolovať prístup do bezdrôtovej siete, kde sa najčastejšie využívajú autentizačné mechanizmy WEP, WPA, WPA2. Aby sa užívateľ pripojil do bezdrôtovej siete, bude potrebné zadať kľúč. Tento kľúč je však pre všetkých užívateľov rovnaký. Pre ešte lepšiu kontrolu je možné tieto autentizačné mechanizmy použiť v kombinácii s RADIUS[5] serverom. Táto forma autentizácie je potom riadená autentizačným protokolom 802.1x[6]. Postup autentizácie 802.1x:

Komunikácia medzi pripojovacím zariadením(AUTHENTICATOR) a klientom(SUPPLICANT) prebieha pomocou EAP[7] rámca. Pri pripojení klienta do siete dôjde k nadviazaniu komunikácie s pripojovacím zariadením, ktorý požiada klienta o identifikačné údaje (EAP Request Identity) podľa použitého typu autentizačného mechanizmu[8]. Klient následne na výzvu odošle odpoveď s ID (EAP Response Identity), ktoré pripojovacie zariadenie odošle prostredníctvom RADIUS protokolu na RADIUS server (RADIUS Access Request). Ten na základe ID požiada klienta o jeho tajný autentizačný kľúč (RADIUS Challenge Request - EAP Challenge Request). Klient odošle šifrovanú odpoveď s jeho tajným kľúčom (EAP Challenge Response - RADIUS Challenge Response). RADIUS server má taktiež tento údaj, ktorý zašifruje a porovná s zašifrovaným klúčom prijatým od klienta, čím overí pravosť, a teda autenticitu klienta. Ak bude autentizácia schválená, odošle RADIUS server správu (RADIUS Acess Accep) pripojovaciemu zariadeni, ktoré povolí komunikáciu do siete na porte autentizovaného klienta. Celý postup je zobrazený na obrázku č. 7

Základné delenie ako autentizovať užívateľa je:

a. **Niečo viem** - heslo, PIN

b. **Niečo mám** - certifikát, čipová karta

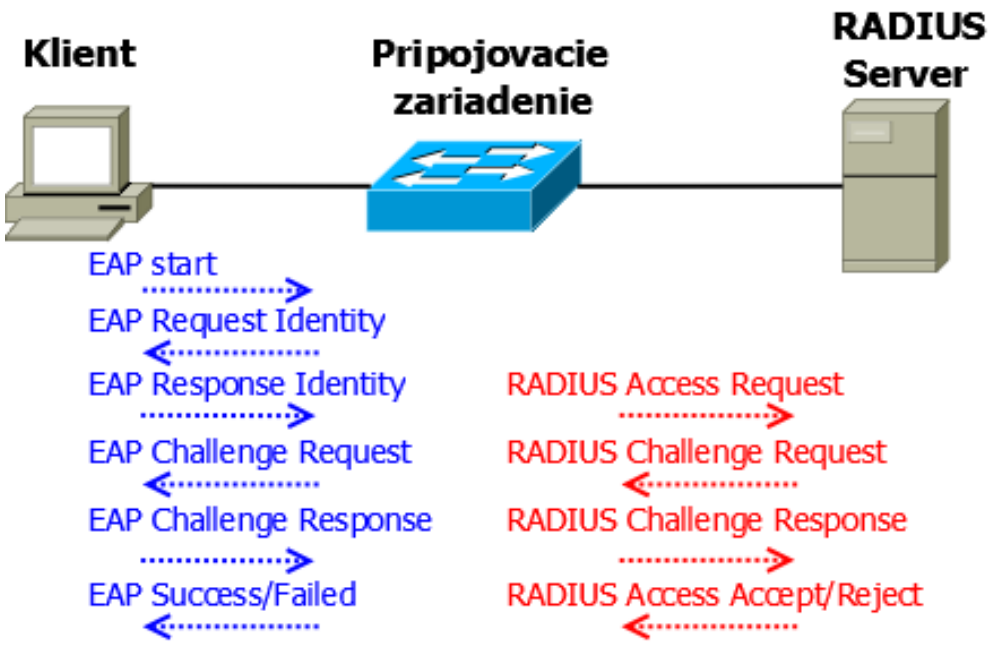
c. **Niečo som** - biometrika

[5]Remote Authentication Dial In User Service - autentizačný, autorizačný a účtový server

[6]IEEE 802.1x je autentizačný protokol, ktorý umožňuje zabezpečenie prístupu do siete

[7]Extensible Authentication Protocol je autentizačný rámec sprostredkujúci prenos autentizačných dát

[8]Autentizačné mechanizmy sú metódy autentizácie klienta, ktorých je definovaných okolo 40.



Obr. 7: Priebeh autentizácie, zdroj: vlastný

Unauthorized access to PC - neoprávnený prístup do operačného systému PC - k narušeniu môže dôjsť aj z počítača, ktoré je súčasťou podnikovej alebo školskej siete, napríklad počítače v laboratóriách určené pre výučbu študentov. Nekontrolovaný prístup do systému počítača je teda možnou hrozbou, z ktorého je možné uskutočniť útok.

Obrana: Autentizácia užívateľa - keďže väčšina počítačov má operačný systém Windows, je možné použiť technológiu Active Directory(AD), ktorá môže byť použitá k centralizovanej správe užívateľských účtov a autentizácii a autorizácii užívateľov systému. Ak je v sieti nasadená technológia AD, je tiež možné na všetky počítače súčasne inštalovať nový alebo aktualizovať nainštalovaný softvér.

2.4 Redundancia a loadballancing

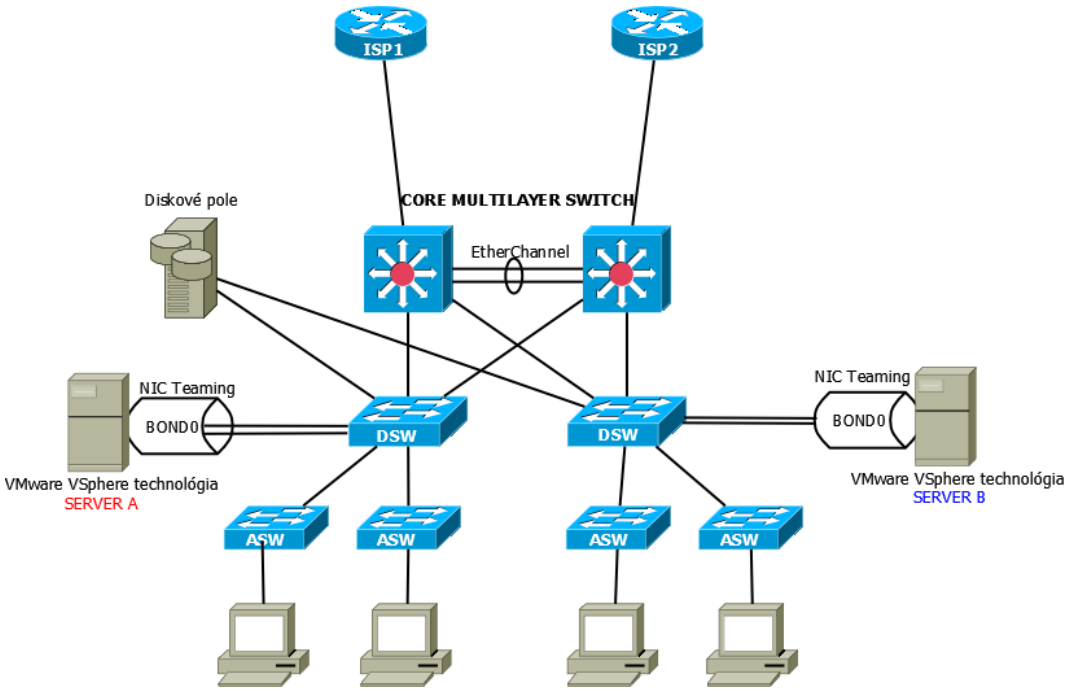
V sieti, kde je vyžadovaný nepretržitý prístup do siete, je potrebné zaviesť redundantné spoje a zariadenia v hlavných častiach siete. Ide vlastne o záložné prvky siete, ktoré sú rovnako nakonfigurované, a v prípade zlyhania jedného z nich sieť nespadne, ale bude ďalej fungovať s jedným zariadením. Aby však boli zariadenia využité aj v prípade, že všetko funguje, je využitá funkcia loadballancingu, čo znamená, že sa komunikácia v sieti rozdeľuje vždy na oba prvky siete.

Použité technológie:

- *EtherChannel* - je agregácia dvoch až ôsmich fyzických portov do jedného logického portu, používaná primárne na Cisco prepínačoch. V prípade vypadnutia

jedného z týchto portov, či už vplyvom poškodenia portu alebo sieťového kábla, logické rozhranie nič nespozná a pokračuje v komunikácii. Aby však boli využité všetky fyzické rozhrania, je opäť zavedená aj funkcia loadballancingu.

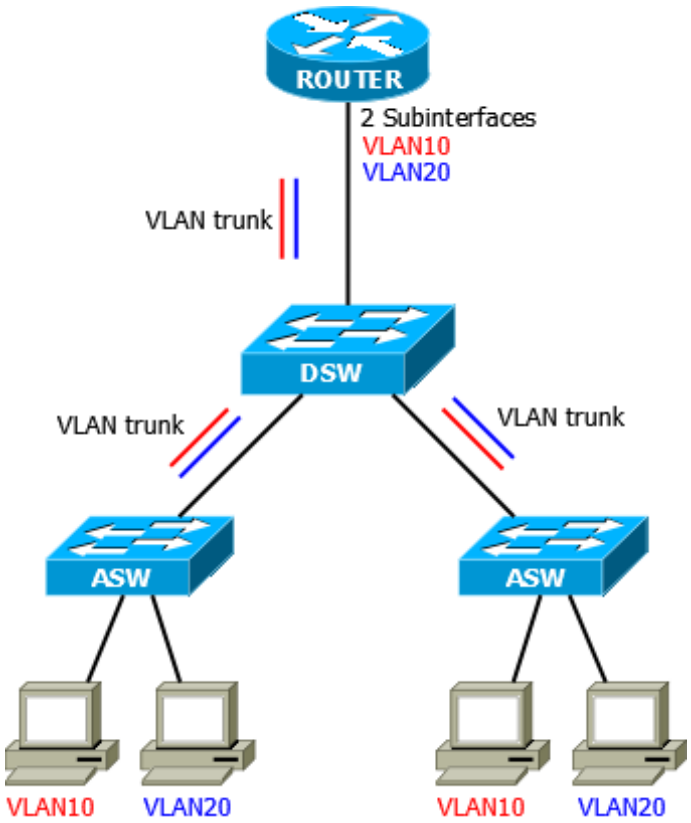
- *VMware vSphere a NIC Teaming* - tieto dve technológie súvisia so serverovými zariadeniami. NIC Teaming je podobná technológia ako EtherChannel. Server má dve fyzické rozhrania agregované do jedného logického, ktoré je nakonfigurované pre komunikáciu v sieti. VMware vSphere je virtualizačná technológia, ktorá slúži k redundancii a loadballancingu serverových zariadení.(Wendell, 2013)



Obr. 8: Redundancia a Loadballancing, zdroj: vlastný

Rozdelenie siete do Virtual LAN počítačových sietí

Slúži na logické rozdelenie sietí podľa portu, MAC adresy, protokolu alebo autentizácie. Pretože je táto technológia implementovaná na prepínači, ide o logické delenie už na úrovni druhej vrstvy sieťovej architektúry. Prepínač zaistí komunikáciu v sieti s klientami v rovnakej VLANe. Najrozšírenejšou normou VLAN je tagovací protokol IEEE 802.1Q. Pre umožnenie komunikácie medzi VLAN sieťami je potrebné do siete pridať smerovač, ktorý bude pripojený k prepínaču. Port smerovača bude nastavený subinterfacemi jednotlivých VLAN a komunikačným protokolom 802.1Q. Toto nastavenie umožní smerovanie medzi jednotlivými VLAN sieťami. Spoje medzi prepínačmi a smerovačom a prepínačom sú v tomto prípade označované ako trunk spoje.(Wendell, 2013)



Obr. 9: VLAN: Router on a stick, zdroj: vlastný

2.5 Simulačná aplikácia GNS3

GNS3 je voľne šíriteľná aplikácia pre simulovanie komplexných sietí, tak ako reálna sieť. Táto aplikácia poskytuje intuitívne grafické rozhranie pre dizajnovanie a konfiguráciu virtuálnych sietí. Beží na bežnom počítačovom hardvéri a je možné ho spustiť na viacerých operačných systémoch, zahrňujúcich Windows, Linux, MacOS X.

Pre vytvorenie simulácií používa GNS3 nasledovné emulátory pre spustenie operačných systémov, aké sa používajú v reálnych počítačových sieťach:

- **Dynamips** - Cisco IOS emulátor
- **VirtualBox** - používa sa pre spustenie rôznych virtuálnych operačných systémov
- **Qemu** - emulátor pre Cisco zariadení ASA, PIX a IPS
- **Virtual PC Simulator** - jednoduchý simulátor, ktorý dokáže vytvoriť až 9 počítačov

Aplikácia sa používa ako alternatíva alebo náhrada skutočného sieťového laboratória. Pomocou aplikácie je teda možné testovať a overovať nové nastavenia, ktoré

budú neskôr použité na reálnych zariadeniach.

Umožňuje tiež prepojenie virtuálnej a reálnej siete, čím je možné overiť nastavenia prvkov v reálnych sieťach. Pre diagnostiku je využívaná aplikácia Wireshark pre odchyt prenášaných dát v sieti a následnú analýzu.

Aby bolo možné využívať všetky funkcie programu je nutné správne nainštalovať aplikáciu so všetkými potrebnými súčasťami.

Jednou z nevýhod aplikácie je, že nedokáže emulovať prepínače Cisco Catalyst rady 2600. Vhodnou náhradou sú prepínače vyššej rady s podporou smerovania Cisco Catalyst 3750. V simulačnom programe je vytvorený zo smerovača Cisco rady 3700 a to tak, že je do neho pridaný modul so šestnástimi portmi pre podporu prepínania.(GNS3 team, 2014)

Druhou z nevýhod je, že aplikácie nepodporuje emuláciu bezdrôtových zariadení.

Ovládanie aplikácie GNS3

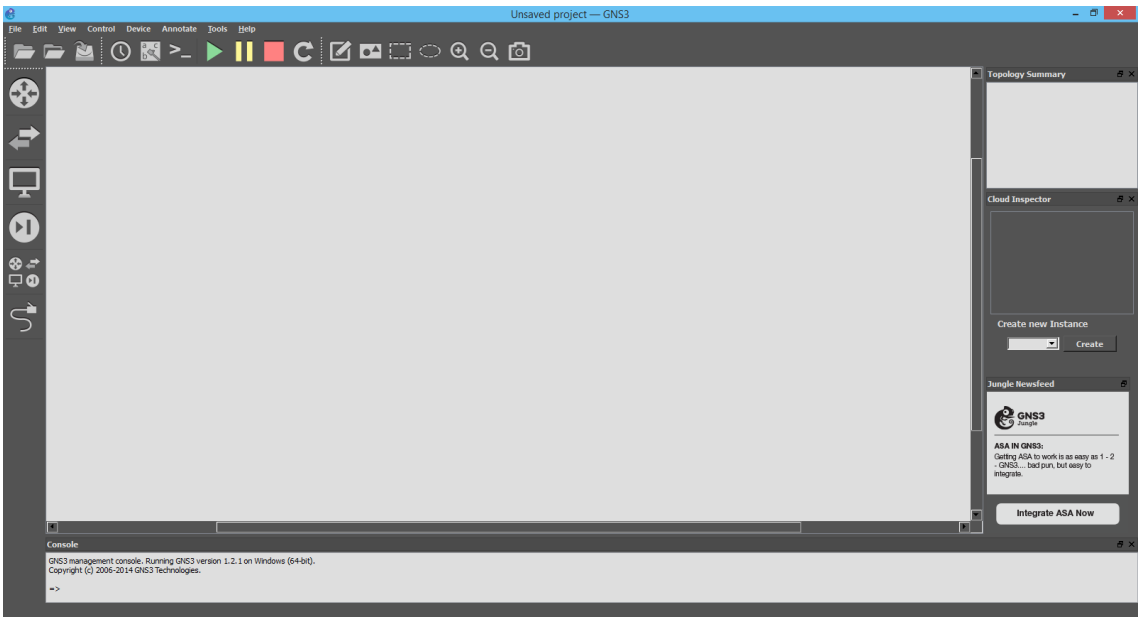
Aplikácia má jednoduché grafické rozhranie rozdelené na päť častí. Hlavnú časť tvorí pracovná plocha, kde sa umiestňujú sieťové prvky. V ľavej postrannej lište je zoznam použiteľných prvkov siete rozdelený podľa kategórií:

- **Smerovače**
- **Prepínače**
- **Koncové zariadenia**
- **Bezpečnostné zariadenia**
- **Všetky zariadenia**
- **Vytvorenie linku medzi prvkami**

V spodnej časti je manažment konzola, ktorou je možné alternatívne ovládať prvky a informuje tiež o chode aplikácie. Vpravo dole sa nachádza prehľad topológie, kde je uvedený zoznam prvkov použitých pre vytvorenie virtuálnej siete. Vpravo hore je zoznam zahájených odchytov, kde je uvedený názov zariadenia a rozhranie, na ktorom je odchyt zahájený. Vrchná lišta obsahuje nástroje pre správu aktívnych prvkov siete a nástroje pre poznámky a kreslenie.

Hlavné okno aplikácie je zobrazené na obrázku č. 10.

Pridanie sieťových prvkov do pracovnej plochy aplikácie je možné presunutím vybraného prvku na pracovnú plochu, kde sa vytvorí ikona, ktorá reprezentuje daný prvok. V ďalšom kroku bude potrebné zariadenia prepojiť prostredníctvom ikony konektoru v ľavej postrannej lište. Po kliknutí na hociktorý prvok v pracovnej ploche aplikácie sa zobrazí menu s dostupnými portmi daného zariadenia, kde stačí už len vybrať potrebný port a potvrdiť kliknutím. Taký istý postup je ešte potrebné použiť na druhom prvku a spojenie sa automaticky vytvorí.



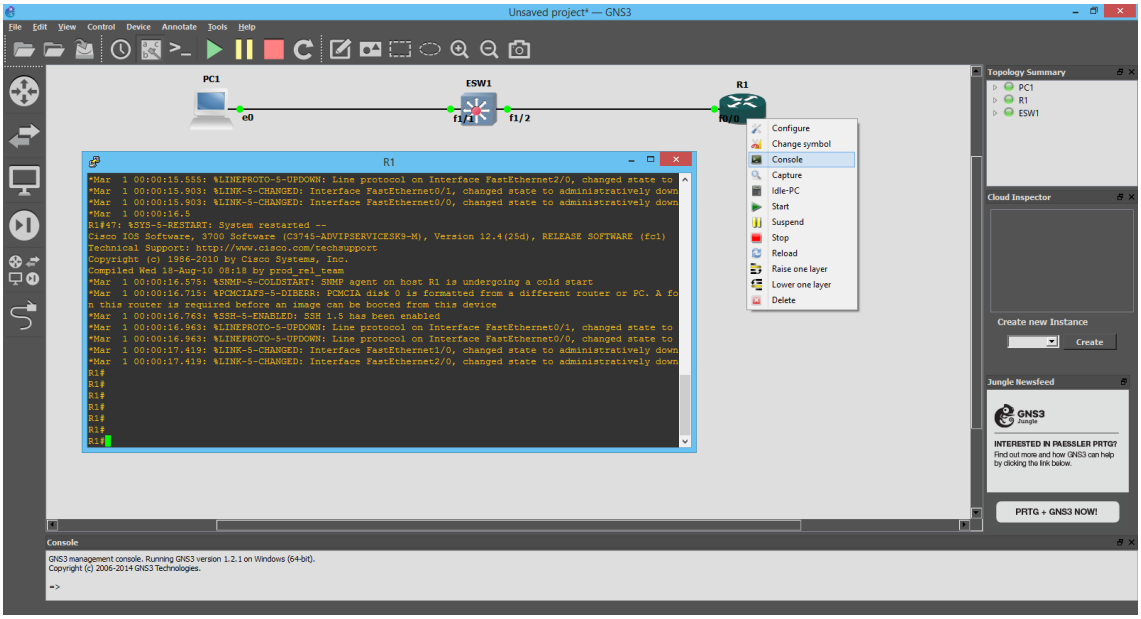
Obr. 10: Graphical Network Simulator 3, zdroj: vlastný

Po kliknutí ľavým tlačítkom na jednotlivé prvky sa zobrazí menu s ovládacími prvkami zariadenia (spustenie, zastavenie, pozastavenie, konzola...). Po spustení a otvorení konzoly je zariadenie pripravené na konfiguráciu viď. obrázok č. 11. Na obrázku je vidieť všetky popísané ovládacie prvky a tiež konzolové okno smerovača R1. V pravej hornej časti je vidieť zahájený odchyt na SW1 port fa1/1 čo je spoj medzi R1 a SW1.

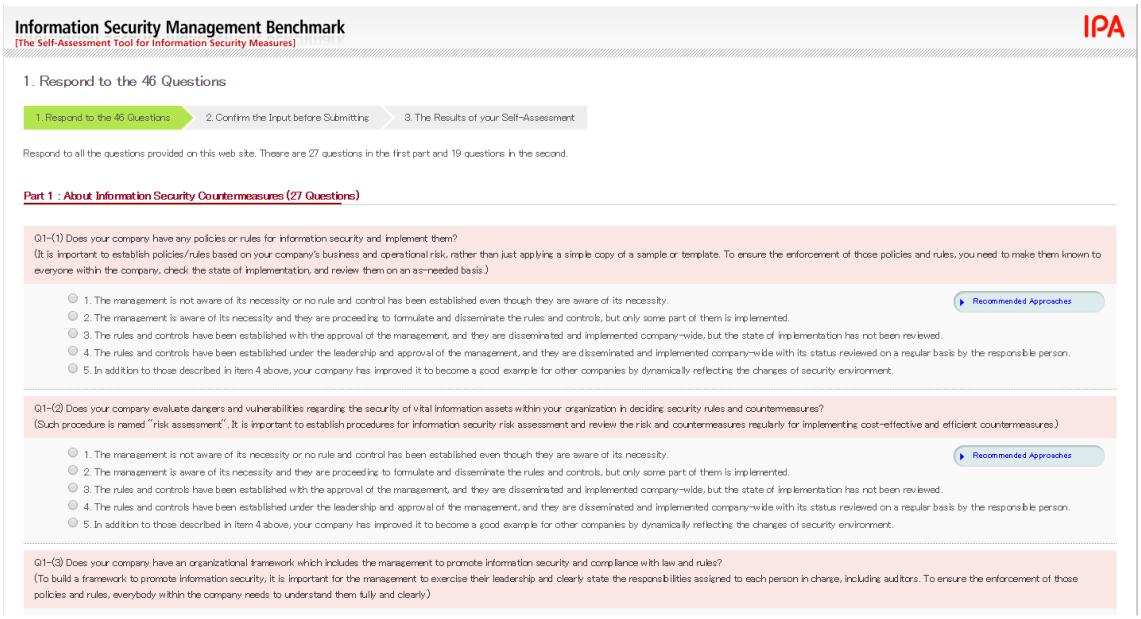
2.6 Aplikácia pre vyhotovenie analýzy rizík IPA - Information Security Management Benchmark

Aplikácia slúži k vytvoreniu správy o bezpečnosti organizácie z IT hľadiska. Pre vytvorenie správy je potrebné vyplniť 46 otázok na webovej stránke IPA Japan viď. obrázok č. 12. Tieto otázky sú rozdelené na dve časti. Prvá časť skúma organizáciu z hľadiska bezpečnostných rizík organizácie. Kde, kedy a ako by mohlo dôjsť k bezpečnostnému incidentu. Druhá časť sa zaoberá profilom organizácie. Čiže o akú organizáciu ide, čím sa zaoberá a aký druh činnosti vykonáva atď.

Po vyplnení všetkých otázok sa vytvorí analýza súčasného stavu bezpečnosti a poravnáva sa s priemerom organizácií rovnakého typu. Na základe tejto analýzi je možné identifikovať kritické miesta, kde by mohlo dôjsť k potenciálnemu bezpečnostnému riziku. Ak zistíme nejaké riziká, je možné ľachšie vytvoriť protiopatrenia, ktoré zamedzia alebo znemožnia, aby k bezpečnostnému incidentu došlo.



Obr. 11: GNS 3 - ovládanie a prvky, zdroj: vlastný



Obr. 12: Information Security Management Benchmark

3 Analýza problému a návrh riešenia

V tejto kapitole bude zhodnotený stav súčasného riešenia počítačovej siete, z ktorého bude na základe nájdených problémov vypracovaný návrh inovatívneho riešenia, kde budú tieto problémy odstránené. Sieť v Strednej priemyselnej škole elektrotechnickej v Piešťanoch je obmedzovaná hlavne z finančného hľadiska, a preto nezodpovedá nárokom, ktoré by mala sieť v školskom vzdelávacom zariadení a školskom internáte spĺňovať.

Analýza bude skúmať hlavne kritické časti siete, ktoré predstavujú potenciálne najväčšiu hrozbu. Stanovuje aktíva školy, ktoré by mohli byť zneužité alebo inak znehodnotené využitím zraniteľných miest, popisuje súčasné vybavenie školskej siete, logickú a fyzickú štruktúru siete. Súčasťou analýzy je výstup z webovej aplikácie IPA[9] IT Secturity, ktorá slúži k vyhodnoteniu bezpečnostnej situácie v podniku alebo iných zariadeniach.

3.1 Popis školy

Názov: Stredná priemyselná škola elektrotechnická
Sídlo: Piešťany, nám. SNP č.8
Zameranie: Elektrotechnika, Informatika

Ide o školu kde sú hlavné vyučovacie predmety zamerané na informatiku, a teda je potrebné, aby v škole fungoval informačný systém, ktorý zlepšuje kvalitu výuky a napomáha študentom pri štúdiu.

3.2 Popis súčasného stavu

Fyzické prostredie školy

Škola je situovaná v centre mesta, kde má z hľadiska infraštruktúry dobré podmienky pre prístup k rôznym technológiám. Budova bola postavená v roku 1934 pre administratívne účely, kde pracovali štátny úradníci. Neskôr v roku 1969 sa po krátkej rekonštrukcii už začala budova využívať pre študijné účely. V budove bola postupne vybudovaná počítačová sieť, ktorá slúžila iba učiteľom a administratíve. Nástupom novších technológií sa sieť rozšírila aj do laboratórií a začali sa vyučovať aj informatické predmety.

Budova má tri podlažia, kde prebieha výuka. V prízemí sa nachádzajú triedy, laboratória a administratíva. V suteréne budovy sú umiestnené špeciálne laboratória pre výuku elektrotechniky a tiež technologická miestnosť, kde je umiestnená chrbticová(backbone) časť siete. V areáli školy sú tiež školské dielne, ktoré slúžia k výuke študentov a školské garáže.

[9] Information-technology Promotion Agency

Do budovy školy je možné vstúpiť hlavným vchodom alebo zadným vchodom, ktorý je však prístupný iba v skorých ranných a poobedných hodinách po skončení výuky.

K škole patrí aj školský internát, kde majú študenti, ubytovaný v tomto zariadení, prístup k internetu v rámci školskej siete, ktorá je prepojená. Školské výpočtové stredisko(ŠVS) je samostatná časť budovy školy a nebude predmetom analýzy.

Použitie siete a aktíva školy

Využívaná je primárne pre študijné účely či už pre študentov, kde majú prístup k študijným materiálom, alebo špeciálnym sieťovým aplikáciám k výučbe webových technológií. Sekundárne využitie majú administratívny pracovníci školy, ktorí používajú sieť k prístupu do databáze študentov a ich informáciám a do účtovníckej aplikácie a jej detabází. Sieť je teda rozdelená do dvoch uživateľských skupín. Jednu skupinu tvoria študenti a učitelia a druhú administratívny pracovníci školy. Druhú časť siete tvorí WiFi sieť, ktorá slúži študentom a zamestnancom školy k prístupu na internet z ich bezdrôtových WiFi zariadení. Prepojenie školskej siete na internát slúži k pokrytiu budovy WiFi signálom a prepojenie administratívnej časti internátu a školy.

V sieti sú pripojené tiež periférne zariadenia, ktoré využívajú k práci učitelia a administratívny pracovníci, ako sú tlačiarne. Ďalej je k sieti pripojený školský server, na ktorom sú spustené služby pre web, dáta, poštu a vzdialený prístup.

Aktíva školy, ktoré by mohli byť zneužité, môžeme rozdeliť do dvoch skupín, a to na aktíva administratívy (mzdový systém, financie školy, databáza školských zariadení) a aktíva výuky (testy, známky jednotlivých študentov, materiály týkajúce sa výuky). K týmto aktívam by mali mať prístup iba osoby, ktoré majú povolené s týmito aktívami nakladať.

Hardvérové vybavenie

Stanice v jednotlivých učebniach sú vždy vybavené rovnakou hardvérovou konfiguráciou, aby bolo možné vytvoriť jeden inštalačný image pre všetky stanice v učebni. Ak by došlo ku kritickej chybe v operačnom systéme na niektorej stanici, je možné iba obnoviť systém z inštalačného image aj so všetkými potrebnými aplikáciami. K školskej sieti je pripojených 96 staníc pre výuku, 10 staníc pre administratívu a 9 staníc pre kabinety pripojené do siete výuky. Rozpis jednotlivých učební je v tabuľke č. 3. Väčšina počítačov prešla obmenou, aby spĺňala nároky potrebné pre plynulý chod aplikácií, avšak s ukončením podpory pre Windows XP niektoré stratili podporu, a preto by mali byť v blízkej dobe vymenené. Ku každej učiteľskej stanici je priamo pripojená tlačiareň, ktorú využívajú učitelia pre výukové účely. V administratívnej časti sú dve zdieľané tlačiarne pripojené k sieti.

Tabuľka 3: Počet staníc v jednotlivých učebniach

Učebňa	**Zariadenie**	**Počet**
U114	PC	10
U117	PC	12
U120	PC	14
U411	PC	16
U412	PC	10
U413	PC	12
U414	PC	10
U420	PC	12
Kabinety	PC	9
Administratíva	PC	10

Súčasný stav siete

Počítačová sieť školy je tvorená jediným manažovateľným prepínačom, ktorý tvorí hlavnú časť siete (Core Switch). Tento prepínač rozdeľuje sieť na dve virtuálne siete. Sieť študentskú, kde sú pripojené študentské a učiteľské stanice a administratívy, kde sú pripojené stanice administratívnych pracovníkov školy. Z tohoto prepínača sú vedené linky do jednotlivých prístupových prepínačov v počítačových učebniach a kanceláriách administratívy. Prístup do internetu poskytuje školské výpočtové stredisko, ku ktorému je tento hlavný prepínač pripojený gigabitovým pripojením, a ktoré je ďalej pripojené na poskytovateľa internetu.

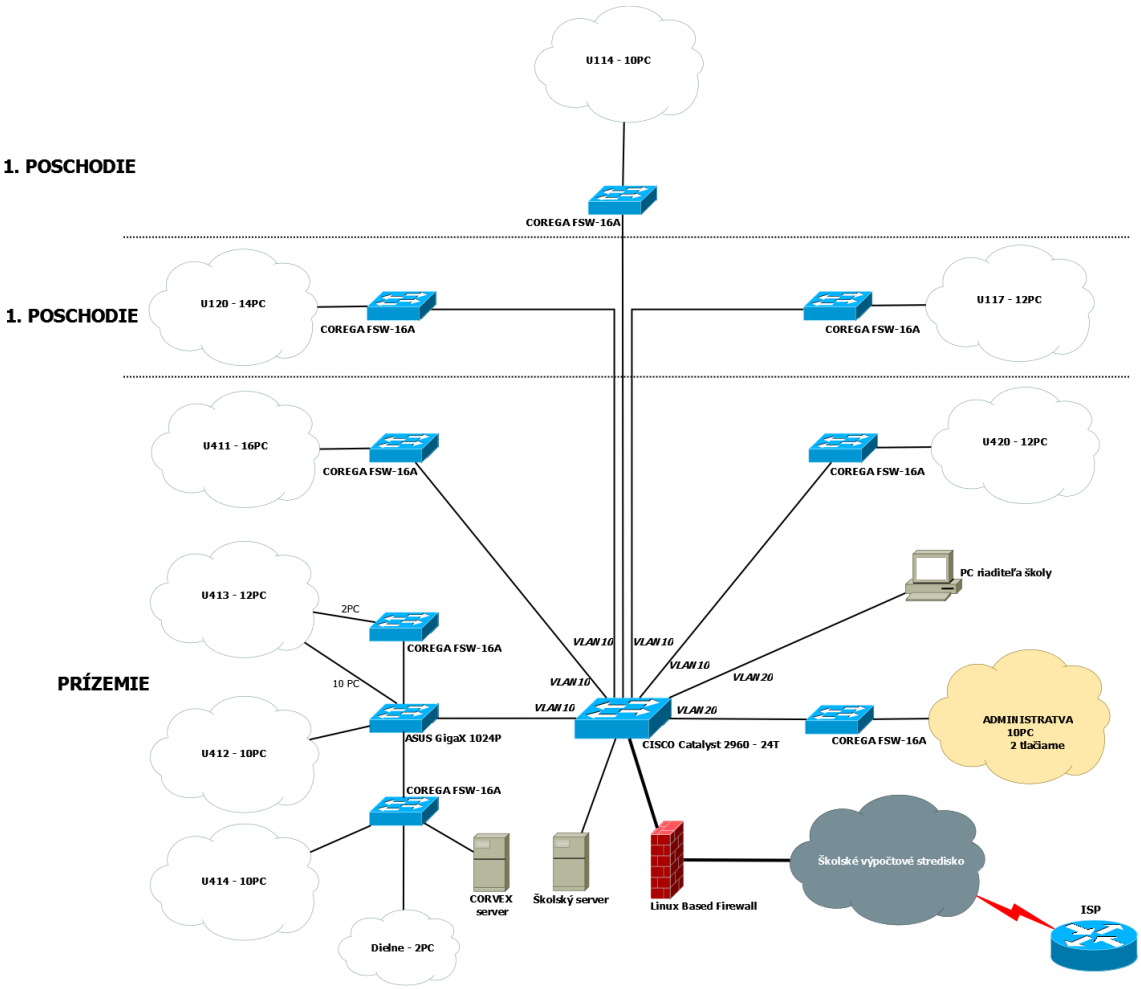
Ďalšiu časť siete tvorí WiFi sieť, ktorá bola v roku 2004 vybudovaná, aby mali študenti prístup k internetu aj zo svojich prenosných zariadení. Aby bolo možné túto sieť rozšíriť aj na internát, bolo potrebné vytvoriť bezdrôtové spojenie medzi týmito dvomi budovami. Aby to bolo možné, museli byť nainštalované na obe budovy antény s priamym výhľadom jednej na druhú. Keďže školský internát je postavený tak, že nie je nan priamy výhľad, tak do úvahy prišla najbližšia budova s priamym výhľadom, čo bola budova nemocnice. Z budovy nemocnice bol potom už len natiahnutý sieťový kábel priamo do prístupového WiFi bod na povale internátu. V škole na povale bol nainštalovaný taktiež prístupový WiFi bod, ktorý má slúžiť k pokrytiu celej školy. Tento prístupový bod je priamo pripojený ku Core Switch v suteréne budovy.

Filtrovanie komunikácie je prevádzané na samostatnom linuxovom firewalle, ktorý je pripojený medzi školskou sieťou a sieťou školského výpočtového strediska.

Do školskej siete je spolu pripojených 120 koncových zariadení, zhruba ďalších 100 klientov je pripojených pomocou WiFi siete, školský server, server určený pre výuku a dva print servery.

Sieť na školskom internáte je určená pre ubytovaných študentov, ktorým poskytuje pripojenie k internetu pomocou WiFi prístupového bodu. Sieť využívajú aj dva počítače administratívy internátu, ktoré sú pripojené k prístupovému bodu sieťovým káblom.

Celá sieť je zobrazená na obrázku č. 13. Väčší obrázok je možné nájsť v prílohe.



Obr. 13: Topológia súčasnej siete, zdroj: vlastný

Bezpečnosť IS/IT

Z hľadiska bezpečnosti je sieť v niektorých častiach nevyhovujúca a bolo by možné zneužiť niektoré slabé miesta. V nasledujú cej časti budú tieto zraniteľné miesta podrobnejšie popísané z rôznych hľadísk.

1. **Fyzická bezpečnosť** - kontrola vstupu osôb do budovy je pri vrátnici, ktorá je umiestnená v strede budovy pri hlavnom vchode, odkiaľ má vrátnik pod kontrolou všetky osoby vchádzajúce do laboratórií, administratívnej časti a na ďalšie podlažia. Vstup študentov do laboratórií a špecializovaných učební, kde by mohli byť ohrozené aktíva školy, je možný iba v sprievode učiteľa, ktorý by mal mať pod kontrolou fyzickú bezpečnosť učebne, v ktorej prebieha výuka. Do

Tabuľka 4: Sieťové zariadenia a ich počet

Zariadenie	**Počet**	**Popis**
Cisco Catalyst 2960	1	24-portový manažovateľný prepínač
ASUS GigaX 1024	1	24-portový nemanažovateľný prepínač
COREGA FSW-16A	7	16-portový nemanažovateľný prepínač
AP BOX	1	WiFI prístupový bod školy
ASUS 500GL	1	WiFI prístupový bod školského internátu
Pacific Wireless PAWDC24-HD	2	smerová WiFi anténa
ConnectGear PS	2	1-port USB 10/100 Print Server
HP Compaq dc5100 Microtower	1	Linux based Firewall-PC
HP ProLiant ML310e	1	školský server

administratívnej časti je prístup študentov voľný, avšak vstup do jednotlivých kancelárií už nie.
Zabezpečenie jednotlivých hardvérových komponentov siete proti prístupu neautorizovanou osobou je vyhovujúce skoro v celej budove. Existujú však aj miesta, kde by mohli mať prístup k prístupovým prepínačom aj neautorizované osoby. V prízemí sú prepínače určené pre výuku informačných technológií umiestnené v samostatnej miestnosti spolu so serverom pre výuku, kde má prístup iba autorizovaná osoba. Ostatné prístupové prepínače sú už však umiestnené priamo v učebniach na učiteľskom stole, kde by mohli mať prístup k týmto zariadeniam žiaci, a teda potenciálny útočníci. Keďže ide o nemanažovateľné prepínače, je jednoduché sa do siete pripojiť iba prostredníctvom sieťového kábla. Hlavný prepínač a školský server sú umiestnené v technologickej miestnosti suterénu budovy, kde majú prístup iba administrátori siete.

2. **Bezpečnosť siete:**

   a) **Prístup k aktívam** je dôležité zabezpečiť sieť tak, aby neboli ohrozené prenášané informácie, alebo aby nedošlo k narušeniu integrity, a teda zmene prenášaných informácií. Sieť je teda rozdelená na dve virtuálne siete VLAN - administratíva a výuka. Tým je zamedzený prístup k informáciám z výukovej časti, kde je riziko útoku vyššie, do administratívy (aktíva administratívy). Avšak keďže stanice v kabinetoch a stanice výuky sú v jednej virtuálnej sieti, vzniká riziko neoprávneného prístupu k aktívam výuky. Riziko zvyšuje ešte aj možnosť napadnutia z WiFi siete, pretože aj táto sieť je vo virtuálnej sieti spolu s výukovou časťou a stanicami kabinetov.

   b) **Školský server** je pripojený priamo k hlavnému prepínaču, v základnej VLAN 1, čo predstavuje ďalšie zraniteľné miesto.

   c) **Prístup do LAN siete** nie je nijak obmedzený, a teda ak by sa potenciálny útočník pripojil do siete, má možnosť vykonať útok. Tu vzniká vysoké riziko napadnutia a je potrebné vytvoriť protiopatrenia. Zoznam možných útokov

a ich protiopatrení je uvedený v sekcii Zabezpečenie siete z praktického hľadiska.

d) **Prístup do siete WiFi** je zabezpečený pomocou WPA autentizačného mechanizmu a filtrovania MAC adries, čo je dostačujúce, avšak ak by došlo k útoku po pripojení, je ťažké identifikovať útočníka.

e) **Jednotný prihlasovací účet** do operačného systému počítača je pre všetkých študentov rovnaký. Identifikácia narušiteľa systému alebo útočníka je prakticky nemožná.

f) **Zabezpečenie siete proti výpadku** - aby bol zabezpečený plynulý a nepretržitý chod, sú hlavné prvky siete pripojené na UPS zariadenia, ktoré slúžia k nepretržitej dodávke elektrickej energie počas jej menšieho výpadku. Ak by však vypadol sieťový spoj medzi hlavným prepínačom a školským výpočtovým strediskom, stratí škola prístup k internetu. Tým bude ohrozená výuka, ktorá podlieha predpokladu pripojenia k internetu. Ďalší zo zásadných výpadkov nastane ak vypadne spojenie so školským serverom. To bude mať za následok vypadanutie viacerých služieb (web, pošta, databáza školy…).

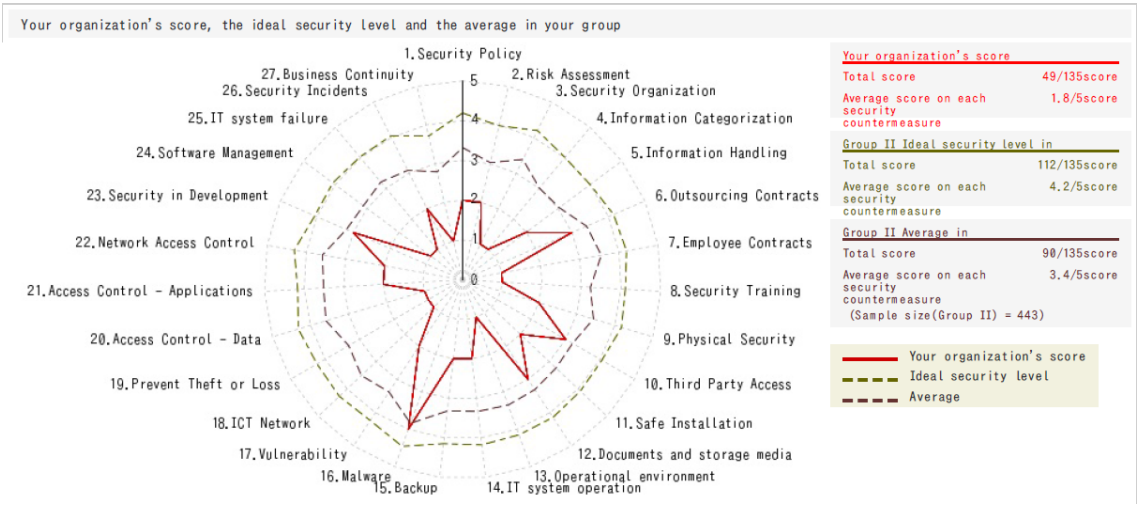
Tabuľka 5: Hrozby a stupeň zraniteľnosti

Hrozby	**Stupeň zraniteľnosti**
Jednotná komunikácia v rámci výukovej siete	4
Nezabezpečený prístup do siete LAN	7
Umiestenie servera v sieti	5
Jednotné prihlasovacie údaje k výukovým staniciam	5
Výpadky siete z dôvodu absencie redundantných spojov	3

Pre vyhodnotenie riadenia bezpečnosti informačného systému je možné použiť nástroj, ktorý obsahuje 27 otázok týkajúcich sa bezpečnostných protiopatrení. Výsledkom tohto testu je grafické zobrazenie úrovne bezpečnostných opatrení v 27 oblastiach. Tento test vyhodnotil bezpečnostnú situáciu vo väčšine oblastí ako nevyhovujúce, a preto je potrebné vytvoriť nové pravidlá, ktoré by mali zvýšiť bezpečnosť informačného systému. Grafické vyhodnotenie testu je na obrázku č. 14.

3.3 Návrh inovatívneho riešenia

Na základe vyhodnotenia hrozieb nájdených v analýze bude vypracovaný návrh inovatívneho riešenia súčasnej siete. Aby bolo možné použiť nové technológie, bude potrebné vymeniť niektoré aktívne prvky siete. Ďalej bude musieť sieť prejsť celkovou prestavbou, čo zahŕňa aj výmenu stávajúcej zastaralej kabeláže. Následne budú vytvorené nové pravidlá pre prístup do siete, tak aby sa znížili možnosti napadnutia



Obr. 14: Grafické zobrazenie IPA testu, zdroj: IPA Benchmark test

útočníkom zvnútra siete. Pre prípad napadnutia budú vytvorené lepšie autentizačné mechanizmy, podľa ktorých bude možné lepšie určiť útočníka.

Výber vhodných aktívnych prvkov siete

Aktívne prvky školskej siete tvoria prístupové prepínače, ktoré sú v súčasnosti nemanažovateľné, čiže nie je možné vytvoriť bezpečnostné pravidlá pre prístup do sieťe. Jediný manažovateľný prepínač je určený ako Core prepínač, ktorý však nesplňuje podmienky pre prenos vysokého množstvá dát z celej siete. Preto je potrebné tento prepínač tiež nahradiť viacvrstvovým prepínačom Cisco Catalyst rady 3750-X, ktorý disponuje dvomi redundantnými napájacími zdrojmi. Prístupové prepínače bude potreba nahradiť manažovateľnými, aby bolo možné lepšie kontrolovať prístup do LAN siete. Pre tento účel budú potrebné prístupové prepínače rady 2600. Alternatívnou náhradou Cisco technológie je Juniper. Ako Core prepínač je možné použiť Juniper rady EX4200 a prístupové prepínače rady EX2200. Pre vyššiu bezpečnosť a ochranu proti napadnutiu zvonku je možné nahradiť linuxový firewall Cisco smerovačom s podporou firewall funkcií alebo bezpečnostné zariadenie Juniper rady SRX240.

Vytvorenie novej topológie vyžaduje presun stávajúcej technologickej miestnosti na prízemie, kde budú vytvorené lepšie prístupové možnosti. Miestnosť bude zabezpečená s lepším odvetrávaním. Bude v nej umiestnený rack[10], kde budú upevnené hlavné prvky siete (core prepínač, servery, zálohovacie zariadenia, dátové centrum ...) a prístupové prepínače pre prízemie. Prístupové prepínače prvého a druhého podlažia budú umiestnené v kabinete na prvom podlaží v menšom jednodielnom racku.

Pre širšie pokrytie budovy WiFi sieťou, či už školy alebo internátu, bude potrebné vybudovať novú WiFi sieť. Na každé podlažie budú umiestnené dva prístu-

[10]Štandardizovaný systém pre montáž elektrických a elektronických zariadení

pové body, ktoré budú tvoriť jednu centrálnu WiFi sieť. Prístupové body musia zvládnuť vysoký tok dát, pretože ide o veľké množstvo zariadení, ktoré do siete pristupujú a lepšie zabezpečovacie mechanizmy. Na tento účel sú vhodné zariadenia Cisco Aironet rady 700i alebo Juniper rady WLA322. Zariadenia môžu byť napájané sieťovým káblom, čo je výhodou pri inštaláciách, kde nie je v blízkosti WiFi prístupového bodu elektrická zásuvka.

Pre zvyšujúcu sa záťaž servera bude stávajúci server nahradený novším a rýchlejším, aby nedochádzalo k vysokým odozvám. Súčasný server bude slúžiť ako zálohovací server pre administratívu, čím sa zvýši bezpečnosť uchovávaných informácií. Dáta budú ukladané do diskového poľa, ktoré disponuje vysokorýchlostným pripojením, čím bude zabezpečený rýchly prístup k dátam zo strany servera.

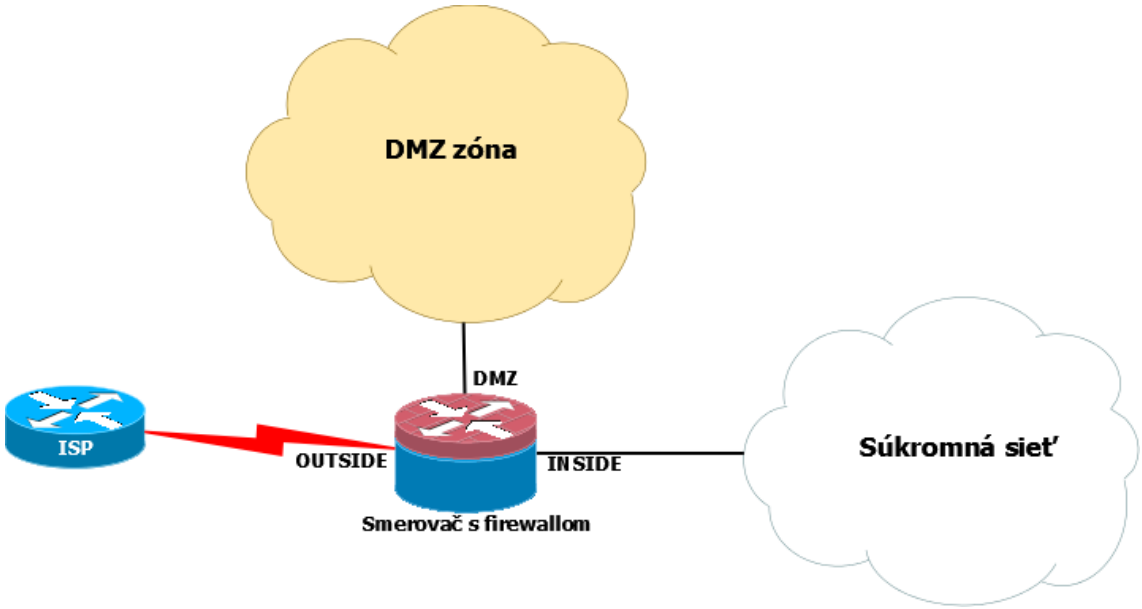
Zabezpečenie siete

Pôvodné riešenie malo hlavné nedostatky v zabezpečení LAN siete. V tejto časti budú na základe jednotlivých hrozieb navrhnuté riešenia, ktoré budú znižovať riziko napadnutia.

- **Jednotná komunikácia v rámci výukovej siete** - pre zamedzenie prístupu študentov k aktívam výuky na učiteľských staniciach, bude potrebné vytvoriť ďalšie dve viruálne siete, v jednej budú umiestnené stanice učiteľov v kabinetoch a v druhej bude tvoriť WiFi sieť školy. Riadenie prístupu medzi VLAN sieťami budú riešiť jednoduché pravidlá vytvorené na smerovači.
- **Nezabezpečený prístup do siete LAN** - zavedenie manažovateľných prístupových prepínačov, ktoré umožňujú kontrolovať pripojené zariadenia k prepínaču na základe MAC adresy pripojeného zariadenia. Táto funkcia sa nazýva Port Security. Táto funkcia umožňuje nastaviť jednu alebo viacero adries, ktoré môžu byť pripojené na port prepínača. Tieto adresy je možné buď nastaviť staticky, alebo dynamicky s prvým pripojeným zariadením automaticky. Po pripojení zariadenia, ktoré nie je v zozname povolených adries, sa port prepínača vypne alebo zablokuje. V prípade školských staníc bude port nastavený na jednu statickú MAC adresu. To zamedzí pripojeniu iných zariadení do výukovej siete LAN. Týmto opatrením sú vyriešené aj ďalšie dva z možných útokov a to *MAC address spoofing* a CAM overflow. Ak by sa však podarilo útočníkovi obísť tento zabezpečovací prvok, je potrebné zaviesť protiopatrenia pred ďalšími možnými útokmi:
  - *DHCP server spoofing* - obranou je funkcia DHCP server snooping, ktorú je potrebné zapnúť na smerovači
  - *ARP spoofing* - funkcia DHCP server snooping rieši aj problém ARP spoofingu (DHCP snooping table)
  - *L2 loop storms* - pri zaplnení celej šírky pásma nie je možné kontrolovať prepínače, preto je potrebné nastaviť maximum, aby bolo možné aj v prí-

pade vytvorenia slučky pristúpiť vzdialene k zariadeniam siete. Druhou variantou je vytvorenie Out of band managementu, čo je samostatná sieť pre manažment zariadení.

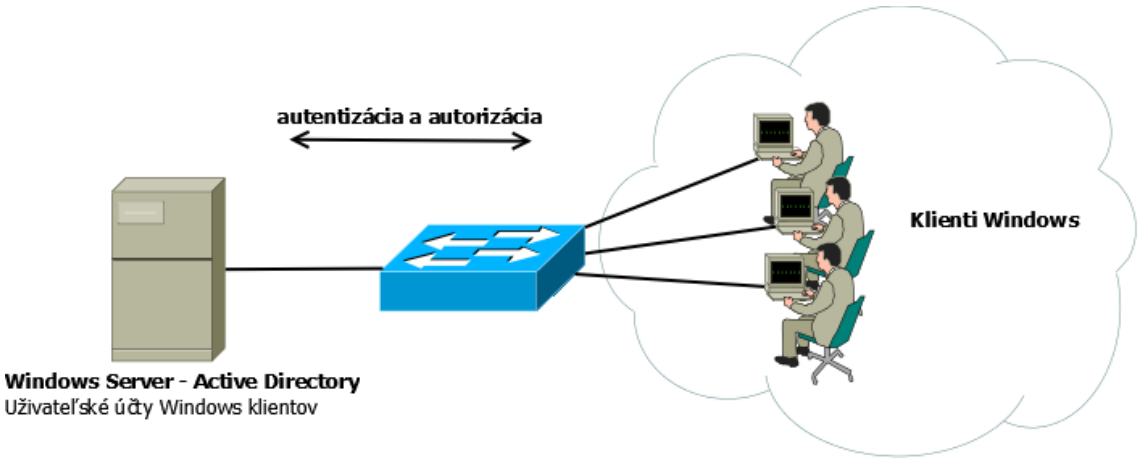
- **Umiestnenie servera v sieti** - v súčasnosti je server nechránený proti útokom zvonku (mimo lokálnu sieť), pretože je umiestnený v sieti spolu s ostatnými zariadeniami. Pre server je nutné vytvoriť samostatnú sieť, ktorá sa nazýva DMZ[11]. Hlavnou výhodou DMZ zóny je vytvorenie bezpečnostnej zóny, do ktorej sa vytvoria pravidlá pre prístup. Napríklad ak webový server komunikuje s databázou, nie je potrebné, aby k tomuto databázovému serveru mal prístup bežný užívateľ prezerajúci si iba webové stránky, preto sa povolí iba komunikácia s webovým serverom na bežnom porte. Zapojenie je zobrazené na obrázku č. 15.



Obr. 15: Demilitarizovaná zóna, zdroj: vlastný

- **Jednotné prihlasovacie údaje k výukovým staniciam** - aby bolo možné kontrolovať, kedy a kto bol prihlásený na ktorej stanici, musí byť vytvorený centralizovaný systém pre prihlasovanie užívateľov. Pre operačný systém Windows je vytvorená služba Active Directory, ktorá je implementovaná vo väčšine Windows serverových operačných systémoch. Na serveri sa vytvoria užívateľské účty, prostredníctvom ktorých sa užívatelia môžu prihlasovať do operačného systému na ktorejkoľvek stanici v škole v rámci výukovej časti siete. Študenti budú mať teda vlastné prihlasovacie údaje, ktorými sa budú autentizovať a autorizovať do operačného systému.

[11] DeMilitarized Zone - fyzická alebo logická podsieť, ktorá je z bezpečnostných dôvodov oddelená od ostatných zariadení(Wikipedia, 2014)



Obr. 16: Centralizovaná správa účtov, zdroj: vlastný

- **Výpadky siete z dôvodu absencie redundantných spojov** - niektoré časti výuky si vyžadujú prístup na internet, čiže by nemalo dochádzať k výpadkom, ktoré by mohli spôsobiť prerušenie výuky. Preto by mali mať hlavné časti záložové zariadenia, ktoré by v prípade výpadku zastúpili toto zariadenie. V navrhovanej topológii ide o core prepínač, ktorým prechádza vysoký tok dát, a teda ak by vypadol tento hlavný prvok, dôjde k výpadku celej siete. Vybraný prepínač disponuje tiež dvomi redundantnými zdrojmi.
  V sieti budú vybudované tiež redundantné spoje, ktoré sú podstatné hlavne v chrbticovej časti siete (backbone). A to od core prepínača k smerovaču, od smerovača do školského výpočtového strediska, ktoré poskytuje pripojenie k internetu. Potrebné je ešte zaistiť neustálu komunikáciu so serverom, čiže spojenie servera a prepínača v DMZ a tiež prepínača DMZ a smerovača. Tu všade budú vybudované dva a viac fyzických spojov, ktoré budú fungovať ako jeden logický spoj. V prípade výpadku jedného z fyzických pripojení je stále v zálohe ďalšie spojenie. Vďaka tejto technológii je výpadok siete iba minimálny a bežný užívateľ chvíľkové oneskorenie ani nespozná. Spolu s redundanciou funguje aj loadballancing, čo sa v sietí prejaví rýchlejším prístupom či už do internetu, alebo k školskému serveru.
  Ďalšími zabezpečovacími prvkami budú UPS zdroje, pre zabezpečenie neustálej dodávky energie. UPS zdroje budú napájať prepínače a servery, čo by malo zabezpečiť po skončení výpadku ihneď plnú komunikáciu v sieti.

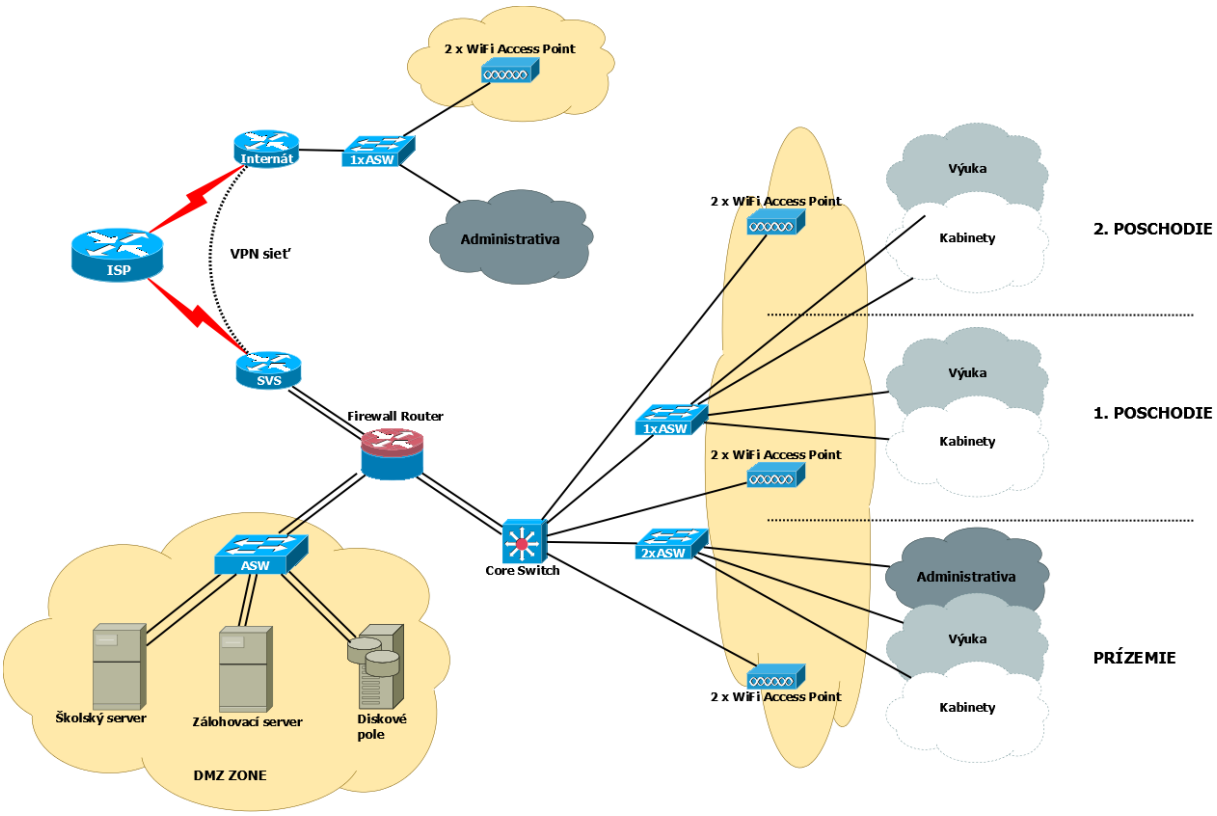
Vytvorenie nového prepojenia školskej a internátnej siete

Pre komunikáciu školy so školským internátom je vytvorené bezdrôtové spojenie, ktoré podlieha možnému napadnutiu. Pre prepojenie budov, kde nie je možné fyzické prepojenie, je lepšie použiť zabezpečené virtuálne spojenie prostredníctvom internetu. Takáto sieť sa nazýva Virtuálna privátna sieť(VPN). Je to prepojenie, ktoré vytvára tunelové spojenie medzi dvomi smerovačmi. Tunelové spojenie je možné za-

bezpečiť technológiou IPsec, čo je bezpečnostné rozšírenie IP protokolu založené na autentizácii a šifrovaní každého IP datagamu (Wikipedia, 2013). Predpokladom vytvorenia takéhoto prepojenia je zavedenie samostatného pripojenia internátu k internetu.

Topológia inovatívneho riešenia

Návrh novej topológie je vytvorený tak, aby spĺňal všetky predošlé podmienky a pravidlá, ktoré budú vytvárať kvalitnejšie zabezpečenie, rýchlejšiu konvergenciu a neprerušený chod siete. Návrh zobrazuje obrázok č. 17.



Obr. 17: Návrh novej topológie, zdroj: vlastný, viz. prílohy

3.4 Realizácia návrhu

Teória overenia návrhu spočíva v otestovaní funkčnosti návrhu simulačným programom, v ktorom by mala byť vytvorená topológia nového riešenia za použitia funkcií, ktoré zvyšujú bezpečnosť a rýchlosť prenášaných dát v sieti. Pre tento účel bola použitá aplikácia pre simuláciu počítačovej siete Graphical Network Simulator 3 (GNS3).

Simulácia novej topológie a overenie návrhu

Pre vytvorenie simulácie boli použité tieto virtuálne sieťové zariadenia:

- 10 x Cisco Catalyst 3750 - dva z týchto prepínačov zastávajú úlohu Core prepínačov školskej siete. Ďalšie tri nahrádzajú prístupové prepínače, ktoré nemajú v aplikácii podporu. Jeden je použitý ako prepínač serverovej časti a ostatné štyri ako prístupové prepínače WiFi siete pre overenie zabezpečenia pomocou 802.1X
- 3 x Cisco Router 7200 - smerovač s firewall funkciami pripojený k internetovému poskytovateľovi
- 9 X Virtuálny PC (VPCS) - nahrádza počítače v učebniach, administratíve a kabinetoch
- 3 X Server - simulovaný virtuálnym rozhraním na PC pripojeným do virtuálnej siete

Po vytvorení celkovej topológie boli nakonfigurované všetky zariadenia tak, aby spĺňali podmienky zabezpečenia tak, ako určuje nové riešenie. Bolo potrebné nastaviť všetky rozhrania, smerovanie, atď. Všetky funkcie a prevedené akcie na jednotlivých prvkoch sú popísané v nasledujúcej časti. Obrázok návrhu je v prílohe.

CORE SWITCH 1 a 2

- *IP adresy L3 rozhraní* - základné nastavenie pre komunikáciu na úrovni L3 s firewall smerovačom, ktorý smeruje do internetu.
- *OSPFv2* - smerovací protokol pre propagovanie priamo pripojených sietí medzi smerovačmi.
- *Trunk rozhrania* - pre komunikáciu na L2 medzi prvkami siete, kde existujú VLAN siete, je potrebné nastaviť trunkovanie.
- *VLAN a VTP server* - vytvorenie VLAN v rámci návrhu a VTP severu, ktoré tieto VLAN siete propaguje ostatným prvkom v sieti.
- *VLAN rozhrania* - VLAN rozhrania slúžia ako predvolená brána do ostatných častí siete pre koncové prvky.
- *ACL pravidlá* - pravidlá pre komunikáciu v sieti a obmedzenie komunikácie v sieti.
- *DHCP server* - server, ktorý poskytuje IP adresy pre koncových užívateľov vo WiFi sieti.
- *OOB manažment* - nastavenie rozhrania pre OOB manažment a vytvorenie prístupu ku konzole.

- *Per VLAN Spanning Tree (PVST)* - rozdelenie záťaže siete pre jednotlivé VLAN siete.

Prístupové prepínače

- *Access rozhrania* - priradenie rozhraní k jednotlivým VLAN sieťam a nastavenie MAC adresy koncového zariadenia.
- *VTP client* - nastavenie VTP klienta, ktorý preberie a vytvorí VLAN siete propagované VTP serverom.
- *OOB manažment* - nastavenie rozhrania pre OOB manažment a vytvorenie prístupu ku konzole.
- *Overenie 802.1x* - zabezpečenie prístupových rozhraní pre prístup do siete po úspešnom prihlásení.

Firewall smerovač

- *IP adresy L3 rozhraní* - základné nastavenie pre komunikáciu na úrovni L3 s firewall routerom, ktorý smeruje do internetu.
- *OSPFv2* - smerovací protokol pre propagovanie priamo pripojených sietí medzi smerovačmi.
- *OOB manažment* - nastavenie rozhrania pre OOB manažment a vytvorenie prístupu ku konzole.
- *VPN tunel* - vytvorenie virtuálnej siete pre prepojenie školy a administratívnej časti internátu.

Po nastavení a uvedení do chodu všetkých prvkov siete, sa sieť chovala ako je uvedené v návrhu. Otestovaná bola konvergencia siete pri výpadku linkov a celých zariadení v rôznych variantach. Sieť sa vždy dokázala do pár sekúnd skonvergovať do stavu, kedy všetko fungovalo. Výpadok nikdy nebol dlhší ako pár sekúnd. Túto funkčnosť siete zabezpečujú redundantné spoje a zariadenia. Rýchlosť konvergencie je možné ešte zrýchliť zapnutím funkcie Rapid Spanning Tree Protocol +, ktorá zrýchľuje proces konvergencie, avšak je potrebné mať vyššiu licenciu.

Ďalej bolo otestovnané prihlasovanie do siete pomocou RADIUS serveru, na úrovni MD5 šifrovania. Funkčnosť bola overená a do siete sa bolo možné prihlásiť až po zadaní hesla. Keďže ide o zabezpečenie portu, súvisí s tým aj povolenie určitej MAC adresy zariadenia, ktoré môže byť na port pripojené, aby nedošlo k pripojeniu neznámeho zariadenia. Po pripojení zariadenia s inou MAC adresou ako je nastavená, sa port prepínača zmenil do stavu vypnutý.

Virtuálne siete rozdelili sieť do štyroch skupín. Pre tieto skupiny sú vytvorené pravidlá prístupu medzi nimi tak, ako určuje návrh. Testovanie prebehlo pred a po nastavení pravidiel. Pred nastavením mali zariadenia zo všetkých skupín prístup všade. Avšak po nastavení už tento prístup stratili a umožnený bol iba tam, kam

dovoľujú pravidlá. S virtuálnymi sieťami sa spája aj rozdeľovanie záťaže do siete, a teda funkcia Per VLAN Spanning Tree (PVST), čo umožňuje rozdeliť záťaž na jednotlivá zariadenia a linky v sieti tak, aby všetka komunikácia netiekla iba jedným spojom a jedným zariadením. Odchytom paketov pomocou programu Wireshark bolo zistené, že táto funkcia funguje správne a pakety z VLAN 10 a 20 tečú cez CORE SWITCH 1 a VLAN 30 a 30 tečú cez CORE SWITCH 2.

Tomuto dopomáha aj ďalšia funkcia a to Hot Standby Routing Protocol (HSRP). Aby bolo možné nastaviť na 2 a viac prvkov rovnakú predvolenú bránu, je potrebné použiť protokol, ktorý dokáže vytvoriť jeden virtuálny prepínač. Je možné použiť aj novšiu a lepšiu funkciu StackWise[12] avšak to simulačný program neumožňuje. Po vytvorení VLAN sietí a nakonfigurovaní HSRP vznikol jeden virtuálny prepínač, ktorý vyvažoval tok v sieti tak, ako bolo popísané v časti vyššie.

Vytvorenie komunikácie na L3 medzi Core vrstvou a firewall smerovačom zabezpečuje OSPF smerovací protokol. Ten propaguje medzi L3 prvkami ich priamo pripojené siete. Firewall router je priamo pripojený do internetu, a teda propaguje ostatným smerovačom aj predvolenú bránu. Týmto je zabezpečená kompletná komunikácia medzi týmito prvkami. Pre overenie boli použité príkazy show ip ospf neighbor, výstup tohoto príkazu je na obrázku č. 18.

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           1   FULL/BDR        00:00:35    172.16.0.10     GigabitEthernet2/0
2.2.2.2           1   FULL/BDR        00:00:32    172.16.0.6      GigabitEthernet1/0
FW_TO_NET#

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/DR         00:00:32    172.16.0.5      FastEthernet1/0
3.3.3.3           1   FULL/DR         00:00:37    172.16.0.2      FastEthernet1/1
CORE_SWITCH_1#

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/DR         00:00:38    172.16.0.9      FastEthernet1/0
2.2.2.2           1   FULL/BDR        00:00:32    172.16.0.1      FastEthernet1/1
CORE_SWITCH_2#
```

Obr. 18: OSPF neighbors, zdroj: GNS3

Aby bolo možné vytvoriť komunikáciu z vnútornej siete do internetu, je potrebná funkcia Network Address Translation. NAT je preklad adries privátnych na verejnú adresu a späť. Pre overenie funkčnosti bol použitý príkaz show ip nat translations, ktorý zobrazuje tabuľku prekladaných adries na obrázku č. 19

```
FW_TO_NET#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 198.80.2.2:40889  172.16.10.10:40889 198.80.2.1:40889   198.80.2.1:40889
icmp 198.80.2.2:41145  172.16.10.10:41145 198.80.2.1:41145   198.80.2.1:41145
icmp 198.80.2.2:41401  172.16.10.10:41401 198.80.2.1:41401   198.80.2.1:41401
icmp 198.80.2.2:41657  172.16.10.10:41657 198.80.2.1:41657   198.80.2.1:41657
icmp 198.80.2.2:42169  172.16.10.10:42169 198.80.2.1:42169   198.80.2.1:42169
```

Obr. 19: Tabuľka NAT, zdroj: GNS3

Nakoniec bolo požiadavkou tiež možnosť ovládať prvky vzdialene, avšak mimo bežnej prevádzky. Na to slúži virtuálna sieť 99, ktorá je nastavená na každom prvku

[12] **StackWise** - technológia pre vytvorenie jedného virtuálneho zariadenia z dvoch a viacerých fyzických zariadení

siete a každý tento prvok má na tejto VLAN sieti vytvorený manažovací port. Tieto porty sú pripojené jedným prepínačom, kde je pripojené aj koncové zariadenie, z ktorého je možné ovládať všetky prvky.

Všetky popísané funkcie boli do zariadení naimplementované a odskúšané. Do konfiguračných súborov je možné nahliadnuť v prílohe.

3.5 Finančné vyhodnotenie

Na trhu sieťových technológií je množstvo firiem, ktoré sa touto tematikou zaoberajú. Pre finančnú analýzu boli vybraté dve najrozšírenejšie firmy v oblasti sieťových technológií a to Juniper a Cisco Systems. Tieto firmy sú dodávateľmi hlavne priemyselných a business riešení. Pre serverovú časť siete sú to firmy HP, DELL a IBM.

V nasledujúcich tabuľkách č. 6 a č. 7 budú vypísané nové prvky siete a ich cena pre Cisco a Juniper.

Tabuľka 6: Cisco Systems

Zariadenie	Typ	Cena bez DPH	Cena s DPH
Cisco Catalyst 2960	prepínač	38 079 Kč	46 075 Kč
Cisco Catalyst 3750X	prepínač	70 496 Kč	85 300 Kč
Cisco Router 1921	smerovač	21 731 Kč	26 294 Kč
Cisco Aironet 702i	Wi-fi AP	5 959 Kč	7 210 Kč

Tabuľka 7: Juniper

Zariadenie	Typ	Cena bez DPH	Cena s DPH
JUNIPER EX 2200	prepínač	25 636 Kč	31 019 Kč
JUNIPER EX 4200	prepínač	48 081 Kč	58 179 Kč
JUNIPER SRX 220	smerovač	20 280 Kč	24 540 Kč
JUNIPER WLA422	Wi-fi AP	10 072 Kč	12 187 Kč

Ďalej je potrebné uvážiť výber vhodnej sieťovej kabeláže. Pre účely vytvorenia uplinkov, čo sú spoje medzi hlavnými prvkami siete, je potrebný kabel s vyššou prenosovou rýchlosťou CAT6 a pre pripojenie koncových zariadení je možné použiť aj nižšiu kategóriu s dobrými prenosovými vlastnosťami CAT5e. V tabuľke č. 8 sú uvedené typy kabeláže a nákupné ceny.

Tabuľka 8: Sieťová kabeláž

Zariadenie	Typ	Cena bez DPH	Cena s DPH
Gamebird 1000m	FTP kabel Cat5e	8 191 Kč	9 912 Kč
InLine 100m	SSTP kabel Cat6	2 903 Kč	3 513 Kč

Návrh novej siete v neposlednej rade počíta aj s výmenou stávajúceho servera a doplnenie serverovej časti o diskové pole. Pre serverovú časť boli vybrané kvalitné a rýchle zariadenia s najmodernejšími technológiami. Srdce tvorí server HP

Cisco Catalyst 2960S-F48TS-S - špecifikácie prepínača

- *Typ zariadenia* : prepínač - 48 portov - riadený
- *Prevedenie* : montovateľné do 1U
- *Porty* : 48 x 10/100 + 2 x SFP
- *Výkon* : Prepojovacia kapacita : 176 Gbps ¦ Výkon presmerovania : 88 Gbps
- *Napájanie* : AC 120/230 V (50/60 Hz)
- *Rozmery (ŠxHxV)* : 44.5 x 31.4 x 4.5 cm

Obr. 20: Cisco Catalyst 2960, zdroj: www.markit.eu

ProLiant DL360p Gen8 Base, čo je výkonný server business triedy a je dostatočný pre navrhovanú školskú sieť. Ako voliteľné zariadenie bolo vybrané diskové pole HP StoreVirtual 4130, ktoré disponuje rýchlymi prenosovými vlastnosťami a najmodernejšou technológiou VMware. Aby však bola aj v tomto prípade dodržaná redundancia, boli by potrebné aspoň 2 servery. Táto vlastnosť je však tiež voliteľná z dôvodu vysokých finančných nákladov. Ceny týchto zariadení sú uvedené v tabuľke č. 9.

Tabuľka 9: Server a diskové poľe

Zariadenie	Typ	Cena bez DPH	Cena s DPH
HP ProLiant DL360p	Server - inštalovateľný na regál	48 181 Kč	58 299 Kč
HP StoreVirtual 4130	pole pevných diskov	94 924 Kč	114 858 Kč

Aby bolo kam tieto všetky zariadenia namontovať, je potreba rozvádzacia skrinka s upevnením pre rack patent. Pre tento účel postačí skrinka pre upevnenie osemnástich zariadení. Zároveň je potreba počítať aj s dobrým odvetrávaním, čiže do skrinky bude namontované ventilačné zariadenie, ktoré má tiež uchytenie do rack patentu. Vybrané prvky sú v tabuľke č. 10.

Tabuľka 10: RACK a ventilačný panel

Zariadenie	Typ	Cena bez DPH	Cena s DPH
19”RACK jednodielny 18U	RACK skriňa	3742 Kč	4528 Kč
Ventilačný panel do RACK	ventilácia	1650 Kč	1996 Kč

Toto vyhodnotenie spracováva dve riešenia, ktoré sú z hľadiska funkčnosti, bezpečnosti a spoľahlivosti najlepšie na trhu. Do analýzy boli zahrnuté iba tie prvky,

Cisco Catalyst 3750X-12S-S - špecifikácie L3 prepínača

- *Typ zariadenia* : prepínač - 12 portov - riadený - stohovateľný
- *Prevedenie* : montovateľné do 1U
- *Porty* : 12 x Gigabit SFP
- *Smerovací protokol* : RIP-1, RIP-2, HSRP, statické smerovanie IP, RIPng
- *Výkon* : Prepínanie štruktúry pásma : 160 Gbps ¦ Výkon presmerovania : 35.7 Mpps
- *Napájanie* : AC 120/230 V (50/60 Hz)
- *Rozmery (ŠxHxV)* : 44.5 x 46 x 4.5 cm

Obr. 21: Cisco Catalyst 2960, zdroj: www.markit.eu

ktoré si vyžadujú výmenu, a teda nákup nových zariadení pre splnenie návrhu nového riešenia. V predošlých častiach boli spomenuté aj ďalšie zariadenia, avšak to sú už koncové zariadenia (PC) a nemajú vplyv na celkovú bezpečnosť a spoľahlivosť.

Cenové vyhodnotenie riešení

V konečnom návrhu vyšli dve riešenia, ktoré sú cenovo odlišné, avšak funkčnosťou a bezpečnosťou rovnaké. V tabuľke č. 12 bude drahšie riešenie, ktoré zahrňuje Cisco zariadenia, HP server a HP diskové poľe, v tabuľke č. **??** budú Juniper zariadenia a HP server.

Tabuľka 11: Riešenie č. 1

Zariadenie	Cena bez DPH	Cena s DPH	Počet
Cisco Catalyst 2960	38 079 Kč	46 075 Kč	3
Cisco Catalyst 3750X	70 496 Kč	85 300 Kč	2
Cisco Router 1921	21 731 Kč	26 294 Kč	2
Cisco Aironet 702i	5 959 Kč	7 210 Kč	4
HP ProLiant DL360p	48 181 Kč	58 299 Kč	2
HP StoreVirtual 4130	94 924 Kč	114 858 Kč	1
Gamebird 1000m	8 191 Kč	9 912 Kč	2
InLine 100m	2 903 Kč	3 513 Kč	2
19”RACK jednodielny 18U	3742 Kč	4528 Kč	1
Ventilačný panel do RACK	1650 Kč	1996 Kč	1
Spolu	541 393 Kč	655 085 Kč	20

Cisco 1921 - špecifikácie smerovača

- *Typ zariadenia* : smerovač
- *Sieťový / prenosový protokol* : IPSec, L2TPv3
- *Prevedenie* : montovateľné do 1U
- *Porty* : 2 x 10Base-T/100Base-TX/1000Base-T - RJ-45
- *Smerovací protokol* : OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, statické smerovanie IP, IGMPv3, GRE, PIM-SSM, statické smerovanie IPv4, statické smerovanie IPv6, smerovanie PBR (policy-based routing), MPLS
- *Charakteristiky* : Ochranná brána firewall, podpora VPN, Quality of Service (QoS)
- *Napájanie* : AC 120/230 V (50/60 Hz)
- *Rozmery (ŠxHxV)* : 34.3 x 29.2 x 4.4 cm

Obr. 22: Cisco Router 1921, zdroj: www.markit.eu

3.6 Diskusia

V nasledujúcej časti budú porovnané obe riešenia, čo sa týka ich funkčnosti, zabezpečenia a finančnej náročnosti.

Prvé riešenie je drahšie, pretože používa Cisco zariadenia, ktoré sú rádovo drahšie, ale funkciami sú rovnaké ako konkurenčné Juniper zariadenia približne rovnakej rady. Toto riešenie obsahuje veľmi kvalitné zariadenia, ktoré svojou spoľahlivosťou a prevedením dokážu vytvoriť veľmi rýchlu a vysoko zabezpečenú sieť. Sieť je natoľko robustná, že funguje aj po výpadku jedného z hlavných zariadení. Toto riešenie je rozšírené o jeden ďalší server, ktorý nielenže dokáže veľmi rýchlo nahradiť stávajúci server v prípade výpadku, ale aj spolupracovať s druhým serverom, a tým vyvažovať zaťaženie oboch serverov. Toto funguje len za spolupráce diskového poľa, ktoré je súčasťou tohto riešenia. Finančná náročnosť tohto riešenia je asi dva krát väčšia, ale to je vyvážené vyššou mierou spoľahlivosti vďaka redundantnému riešeniu servera.

Druhé riešenie je lacnejšie, avšak zabezpečením a spoľahlivosťou nezaostáva. Ako bolo už v predošlej časti spomenuté, zariadenia od Juniper a Cisca sú veľmi porovnateľné, a teda ich úlohu v sieti spĺňajú rovnako. Asi iba s jediným rozdielom, že zariadenia od Cisca sú drahšie s lepšou podporou. Naopak Juniper poskytuje otvorené riešenie, a tým umožňuje nahliadnuť do fungovania zariadení. Toto riešenie

Cisco Aironet 702i Standalone Access Point - špecifikácie Wifi AP

- *Typ zariadenia* : bezdrôtový prístupový bod
- *Prevedenie* : externý
- *Rozhrania* : 1 x 1000Base-T - RJ-45 + 1 x management - RJ-45
- *Frekvenčné pásmo* : 2.4 GHz, 5 GHz
- *Prenosová rýchlosť dát* : 300 Mbps
- *Podpora PoE* : Áno
- *Výkon* : Prepínanie štruktúry pásma : 160 Gbps ¦ Výkon presmerovania : 35.7 Mpps
- *Rozmery (ŠxHxV)* : 17.76 x 17.76 x 5.04 cm

Obr. 23: Cisco Aironet 702i AP, zdroj: www.markit.eu

však neobsahuje dva servery a ani diskové poľe, a teda čo sa týka výpadku serveru nie je sieť chránená. To však nemá vplyv na celkovú funkčnosť siete.

Obe riešenia tvoria dobrý základ pre rozširovanie siete o nové technológie i čo sa týka množstva koncových zariadení. V serverovej časti siete je možné vytvoriť dátové centrum, ktoré by zvýšilo kvalitu obsluhy koncových užívateľov a rozšírilo možnosti použitia. Riešenia sú taktiež zohľadnené z dlhodobého hľadiska, aby nedošlo k tomu, že bude po roku opäť potreba zariadenia inovovať, pretože by boli zastaralé.

Prínosy

Návrh novej siete je hlavným prínosom pre školu, ktorá tieto riešenia môže použiť pri inovácii a hlavne pri rozhodovaní, aké prvky siete je vhodné využiť a v akej cenovej hladine.

Osobný prínos je dôložitý, pretože som sa naučil mnoho nových informácií, ale taktiež som zúročil informácie nadobudnuté počas štúdia. Hlavným prínosom pre mňa je naučenie sa pracovať v simulačnom programe GNS3, kde je možné využiť

Zariadenia od firmy Juniper majú podobné parametre ako konkurenčné Cisco zariadenia, preto nie je potrebné popisovať špecifické vlastnosti znova.

Obr. 24: Juniper zariadenia, zdroj: www.markit.eu

HP ProLiant DL360p - špecifikácie serveru

- Procesor : Intel Xeon E5-2640 / 2.5 GHz (3 GHz) (6-jádrový)
- RAM : 16 GB (inštalovaný) / 384 GB (max.) - DDR3 SDRAM - 1333 MHz - PC3-10600
- Externé rozhranie poľa HDD : iSCSI (1GbE)
- Rozhrania : 1 x sériový vstup ¦ 1 x VGA ¦ 4 x LAN (Gigabit Ethernet) ¦ 1 x HP iLO ¦ 6 x USB 2.0 (2 vpredu, 4 vzadu)
- HDD: Bez HDD

Obr. 25: HP ProLiant DL360p, zdroj: www.markit.eu

a natrénovať teoretické znalosti zo sieťových technológií. Mojím hlavným cieľom teda bolo využiť všetky znalosti a priučiť sa niečomu novému.

HP StoreVirtual 4130 - špecifikácie diskového poľa

- Procesor : Xeon 2.4 GHz
- RAM : 8 GB
- Externé rozhranie poľa HDD : iSCSI (1GbE)
- Rozhrania : 4 x Ethernet 1000 ¦ 1 x sériový ¦ 1 x VGA ¦ 1 x management - RJ-45 ¦ 4 x USB
- HDD: 4 x 600GB
- Celková kapacita poľa: 2,4 TB

Obr. 26: HP StoreVirtual 4130, zdroj: www.markit.eu

Tabuľka 12: Riešenie č. 2

Zariadenie	Cena bez DPH	Cena s DPH	Počet
JUNIPER EX 2200	25 636 Kč	31 019 Kč	3
JUNIPER EX 4200	48 081 Kč	58 179 Kč	2
JUNIPER SRX 220	20 280 Kč	24 540 Kč	2
JUNIPER WLA422	10 072 Kč	12 187 Kč	4
HP ProLiant DL360p	48 181 Kč	58 299 Kč	1
Gamebird 1000m	8 191 Kč	9 912 Kč	2
InLine 100m	2 903 Kč	3 513 Kč	2
19”RACK jednodielny 18U	3742 Kč	4528 Kč	1
Ventilačný panel do RACK	1650 Kč	1996 Kč	1
Spolu	329 679 Kč	398 911 Kč	18

19”RACK jednodielny 18U - špecifikácie RACK skrine

- Konštrukcia : jednodielna, odnímateľná bočnica
- Určené pre : zriadenia 1U
- HĺbkA : 500 mm
- Materiál : bezpečnostné kalené sklo, ocelový plech
- Hmotnosť : 30kg
- Vonkajšie rozmery : 900 x 600 x 495 mm

Obr. 27: 19”RACK jednodielny 18U, zdroj: www.alza.cz

Ventilačný panel do RACK (1U, 3 ventilátory) - špecifikácie

- Počet ventilátorov : 3
- Napätie : 230V
- Výška a uchytenie : 1U

Obr. 28: Ventilačný panel do RACK, zdroj: www.t-cz.com

4 Záver

Cieľom práce bolo vytvoriť inovatívne riešenie počítačovej siete na Strednej priemyselnej škole elektrotechnickej v Piešťanoch a školskom internáte. Jednou z hlavných častí práce je analýza súčasnej siete, ktorá mala za úlohu zistiť, aké bezpečnostné riziká sieť obsahuje, čo ich spôsobuje a vytvoriť ochranné opatrenia, ktoré nové riešenie bude obsahovať.

Analýza bola teda akýmsi návodom pre vytvorenie nového riešenia a vyobrazila kritické miesta, ktoré sú v práci popísané. Tieto kritické miesta boli zistené vo viacerých oblastiach:

- Fyzické zabezpečenie
- Systémové zabezpečenie
- Riadenie prístupu k logickým i fyzickým dátam

Ako už bolo spomenuté, v týchto oblastiach boli nájdené bezpečnostné riziká. Následne boli, v časti venovanej návrhu, vytvorené inovatívne riešenia, ktoré tieto riziká odstraňujú. Návrh obsahuje všetky protiopatrenia, a tým spĺňa stanovené bezpečnostné zásady určené analýzou. Každé protiopatrenie teda popisuje, aké kritické miesto odstraňuje alebo do akej miery znižuje možnosť využitia tohto miesta a technológiu alebo systémový postup, ako je treba postupovať k vyriešeniu tohto problému.

Kvalitné a spoľahlivé prvky novej siete zaručujú bezproblémový chod, vysokú bezpečnosť a vďaka redundancii aj funkčnosť v prípade vypadnutia hlavných prvkov siete či už zariadenia, alebo fyzických linkov medzi prvkami.

Ďalšia časť práce bola simulácia prevádzky v aplikácii GNS3. Tá mala za úlohu overiť funkčnosť navrhnutej topológie a technológie, ktoré boli navrhnuté v časti analýza a majú odstrániť nedostatky v pôvodnej sieti. Výsledkom boli konfiguračné súbory jednotlivých zariadení, ktoré je možné použiť na reálnych prvkoch v reálnej sieti.

V poslednej časti bola vyhotovená finančná analýza a prehľad jednotlivých vybraných prvkov. Výsledkom tejto analýzy boli 2 riešenia, ktoré boli následne okomentované a popísané z funkčnej, bezpečnostnej a finančnej stránky.

Tuto prácu je možné použiť, ako štúdiu pri vytváraní projektu pre získanie financí z európskych fondov v rámci inovácie a zvyšovania bezpečnosti a prístupu študentov k potrebným informáciám pri každodennom štúdiu. Taktiež môže byť využitá, ako podklad pre ďalšie práce alebo iné články zaoberajúce sa podobnou tématikou.

5 Literatúra

WIKIPEDIA *Uninterruptible Power Supply*. online, 2014. Dostupné z: http://cs.wikipedia.org/wiki/UPS.

WIKIPEDIA *Twisted pair*. online, 2010. Dostupné z: http://en.wikipedia.org/wiki/Twisted_pair.

WIKIPEDIA *Information security*. online, 2014. Dostupné z: http://en.wikipedia.org/wiki/Information_security.

WIKIPEDIA *DMZ (Computing)*. online, 2014. Dostupné z: http://en.wikipedia.org/wiki/DMZ_(computing).

WIKIPEDIA *IPsec*. online, 2014. Dostupné z: http://en.wikipedia.org/wiki/IPsec.

MIROSLAV ČERMÁK *Analýza rizik: Jemný úvod do analýzy rizik*. online, 2014. Dostupné z: http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik.

GNS3 TEAM *Úvod do GNS3*. online, 2014. Dostupné z: https://community.gns3.com/docs/DOC-1750.

ODOM, WENDELL *Cisco CCENT/CCNA ICND1 100-101: official cert guide*. Indianapolis: Cisco Press, 2013. 899 s. ISBN 1-58714-385-2..

ODOM, WENDELL *Cisco CCNA routing and switching ICND2 200-101: official cert guide*. Indianapolis: Cisco Press, 2013. 717 s. ISBN 1-58714-373-9..

Prílohy

A Infromation Security Management Benchmark

IPA INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Information Security Management Benchmark

This page shows the result of your self-assessment for your security measures.
Based on your answer to 27 questions regarding your company profile, you will be classified into one of the 3 groups, Low, Medium or High. Based on your answer to 20 questions asking the information security countermeasures, your score is calculated. In the result, you can see your security level, the ideal security level and the average, along with recommended security approaches.

Data : 2014/04/01 20:13:56
Organization : SPSE PN (Slovakia)
The scope of your self-assessment :Administrative
Login ID : 7016545

Information Security Management Benchmark Ver.4.2

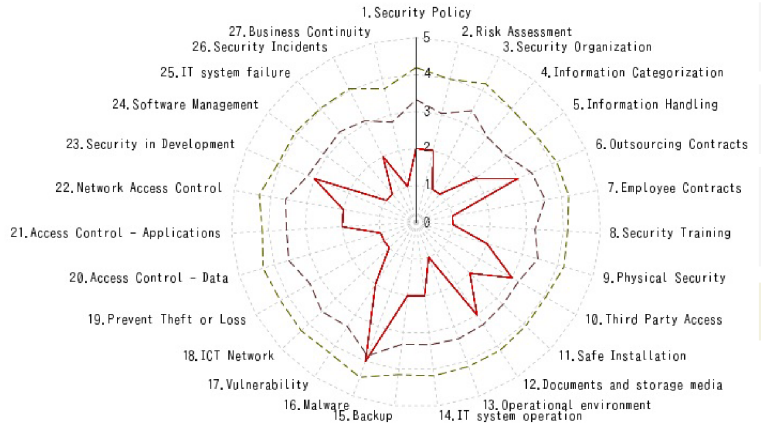
The Result of your Self-Assessment

Group II where medium level IT security measures are required.
Among Group II, your company is in the position of 91 - 100% from the top.
(Among all the 3 groups, your company is in the position of 91 - 100% from the top.)

The radar chart below shows your company's score on each security countermeasure, the ideal security level and the average in the group you belong to.

The ideal security level indicates the level to be targeted which is average of the top 1/3 organizations in your group. If your score doesn't reach the average score shown below, your organization shall target the average score in the first stage.

Your organization's score, the ideal security level and the average in your group



Your organization's score	
Total score	49/135score
Average score on each security countermeasure	1.8/5score

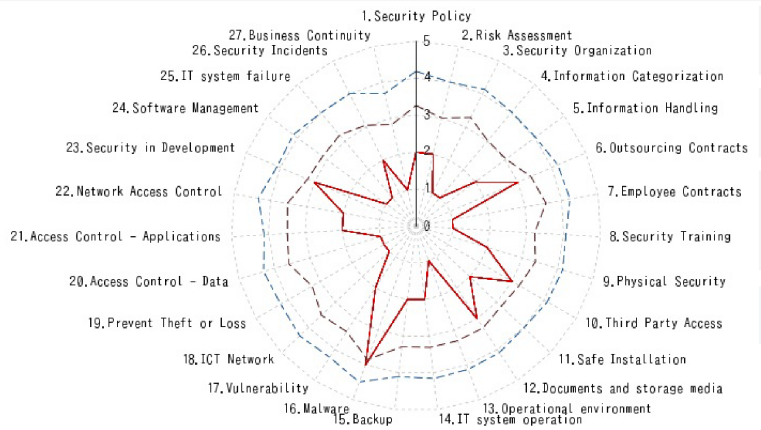
Group II Ideal security level in	
Total score	112/135score
Average score on each security countermeasure	4.2/5score

Group II Average in	
Total score	90/135score
Average score on each security countermeasure (Sample size(Group II) = 443)	3.4/5score

Your organization's score
Ideal security level
Average

According to your answer about the number of your employees, you are categorized into the group of small and medium size companies.

Your organization's score, the ideal security level and the average in the group of small and medium size companies (employee number less than 300)



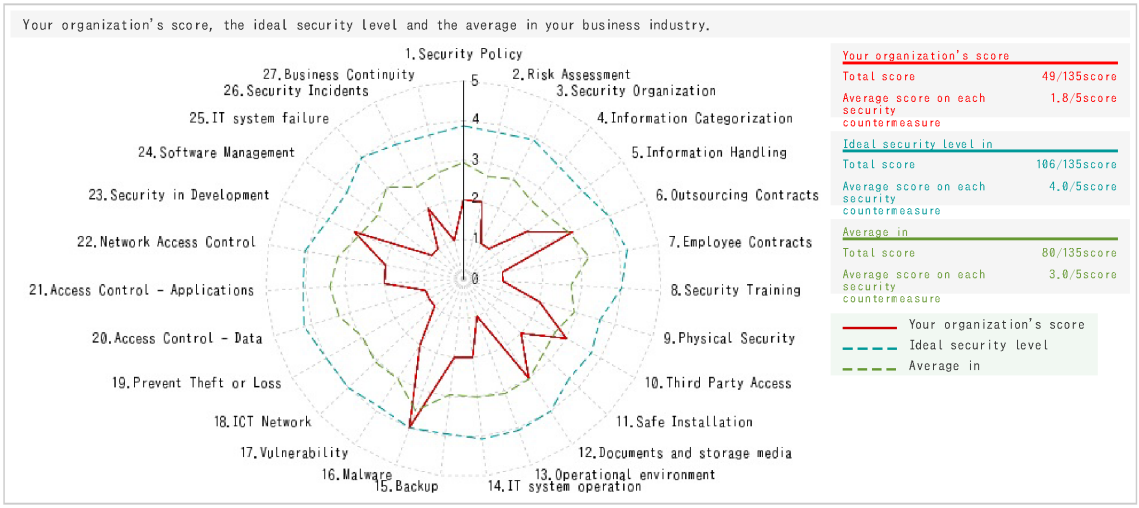
Your organization's score	
Total score	49/135score
Average score on each security countermeasure	1.8/5score

Company size Ideal security level in	
Total score	112/135score
Average score on each security countermeasure	4.2/5score

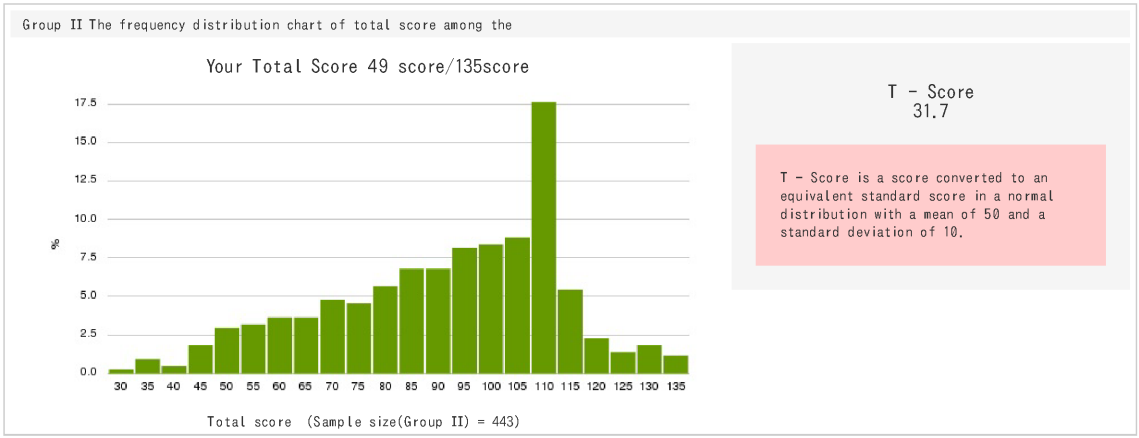
Company size Average in	
Total score	89/135score
Average score on each security countermeasure (Sample size(300) = 241)	3.3/5score

Your organization's score
Ideal security level
Average

Here the radar chart below shows your score, the ideal security level and the average in the same business industry.:



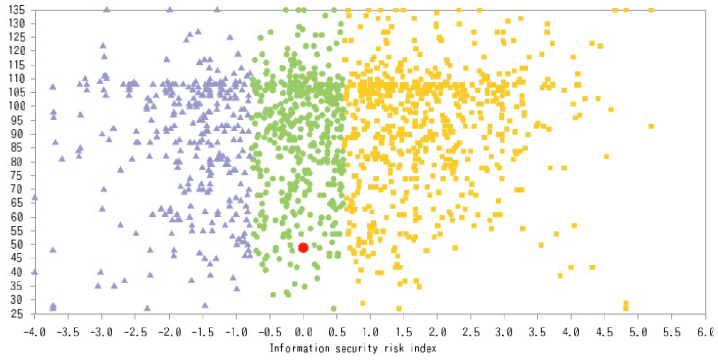
Group II Among the , the frequency distribution chart of total score and the T-score of your organization are as follows:



The result shown in scatter chart

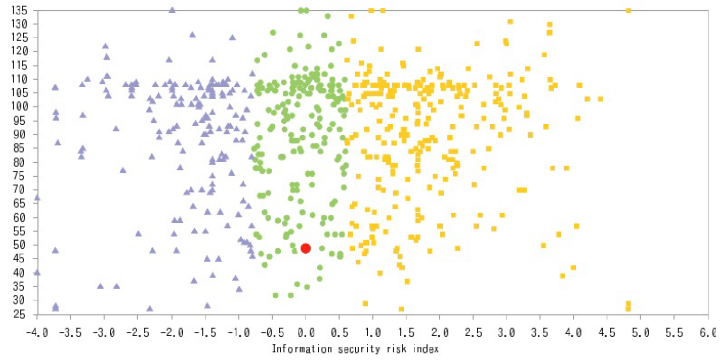
Group II where medium level IT security measures are required.
From your answer about company profile "the information security risk index" is calculated.The scatter chart shows the distribution of all the companies and your position in the chart.The vertical axis shows "total score"and horizontal axis shows "Information security risk index".

Scatter chart of all the companies



▲ Group III: Not thorough IT security measures are required.
● Group II : Medium level IT security measures are required.
■ Group I : High level IT security measures are required.
● This time's position
● The previous position
● The last but one's position
(Sample size(all) = 1403)

Scatter chart of the group small and medium size companies (employee number less than 300)



▲ Group III: Not thorough IT security measures are required.
● Group II : Medium level IT security measures are required.
■ Group I : High level IT security measures are required.
● This time's position
● The previous position
● The last but one's position
(Sample size(300) = 665)

Classification Based on Information Security Levels Required

Social Influence Index

Organizational Value
- Sales figures
- Brand image

Social Responsibility
- Public utility in businesses (national, social, economical)
- Influence to consumers (lives, physical, financial, honorable, etc.)

Information Assets
- Quantity of Important Information Possessed (national/operational secrets, privacies, etc.)

1. Group I
High level
IT security measures are required.

2. Group II
Medium level
IT security measures are required.

3. Group III
Not thorough
IT security measures are required.

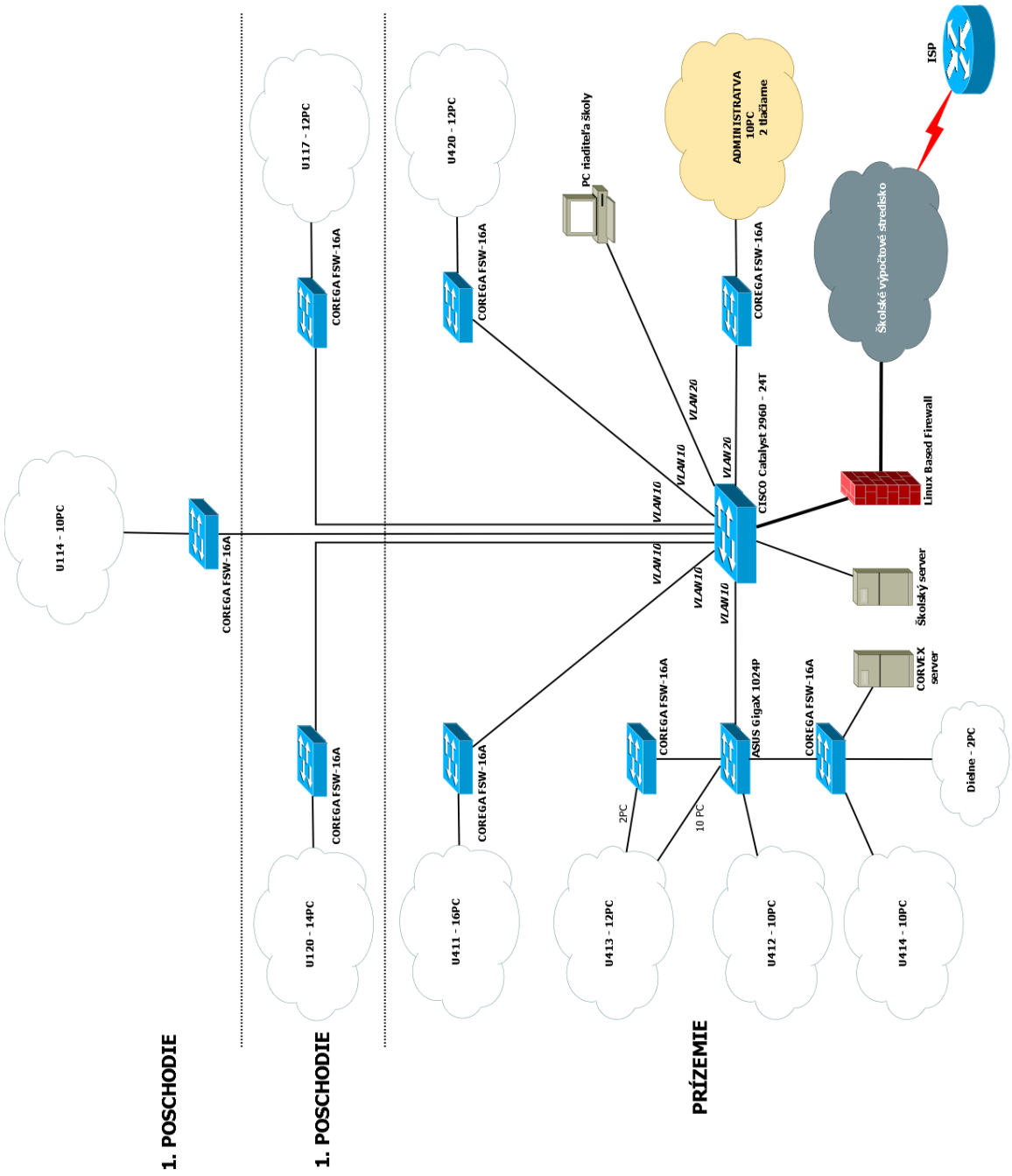
Vulnerability Index on Business Structures

Dependency to Information System in Operation
- Features in category of business
- Dependency to information System in mission-critical tasks

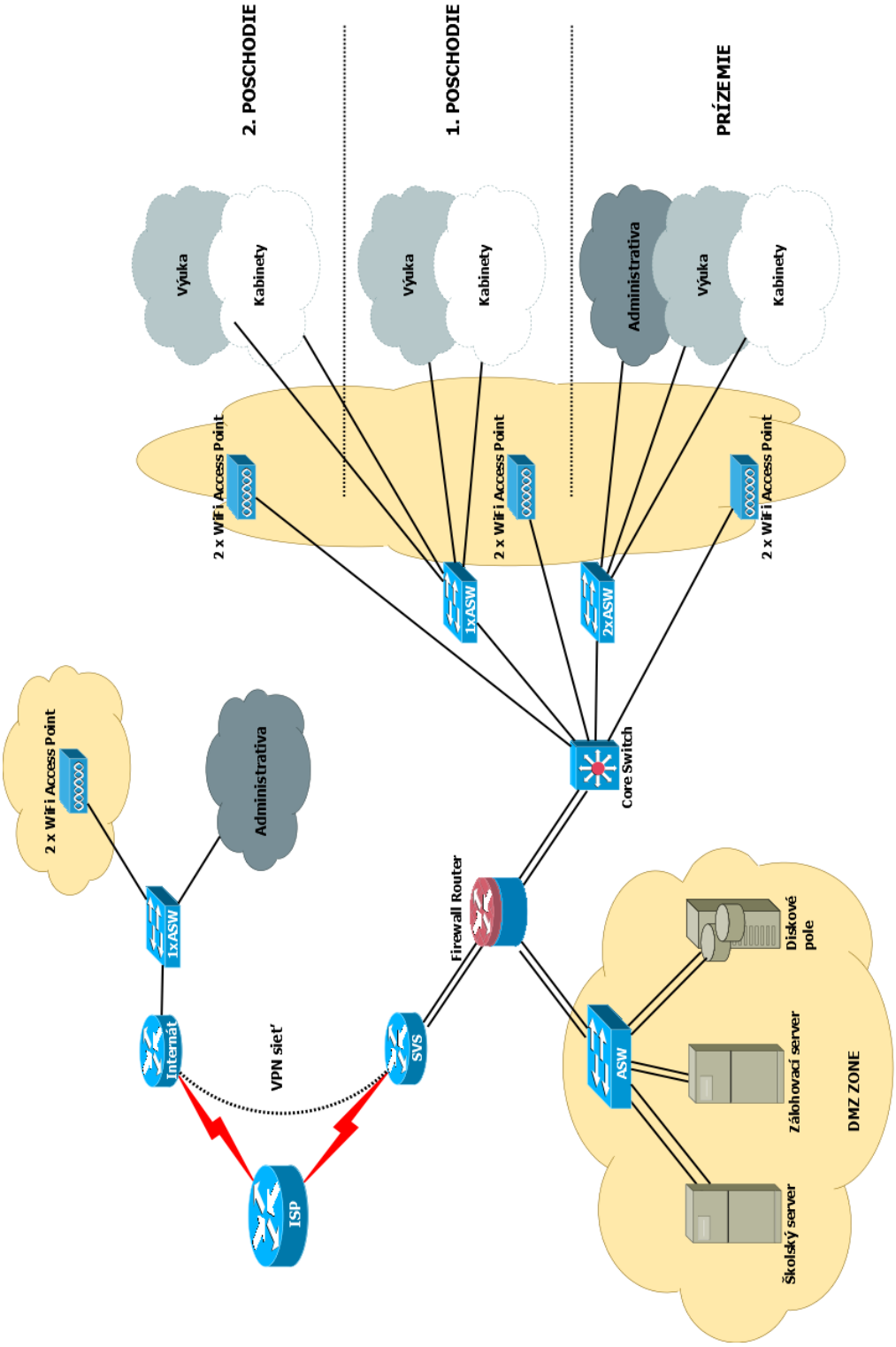
Operational Dependency to Outsource
- Dependency to agencies, etc.
- Dependency to the Internet
- Ratio in permanent employees: nonpermanent employees

Extent of Concerned Parties/Personnel
- Number of bases, with/without of the bases in overseas
- Job separation rate

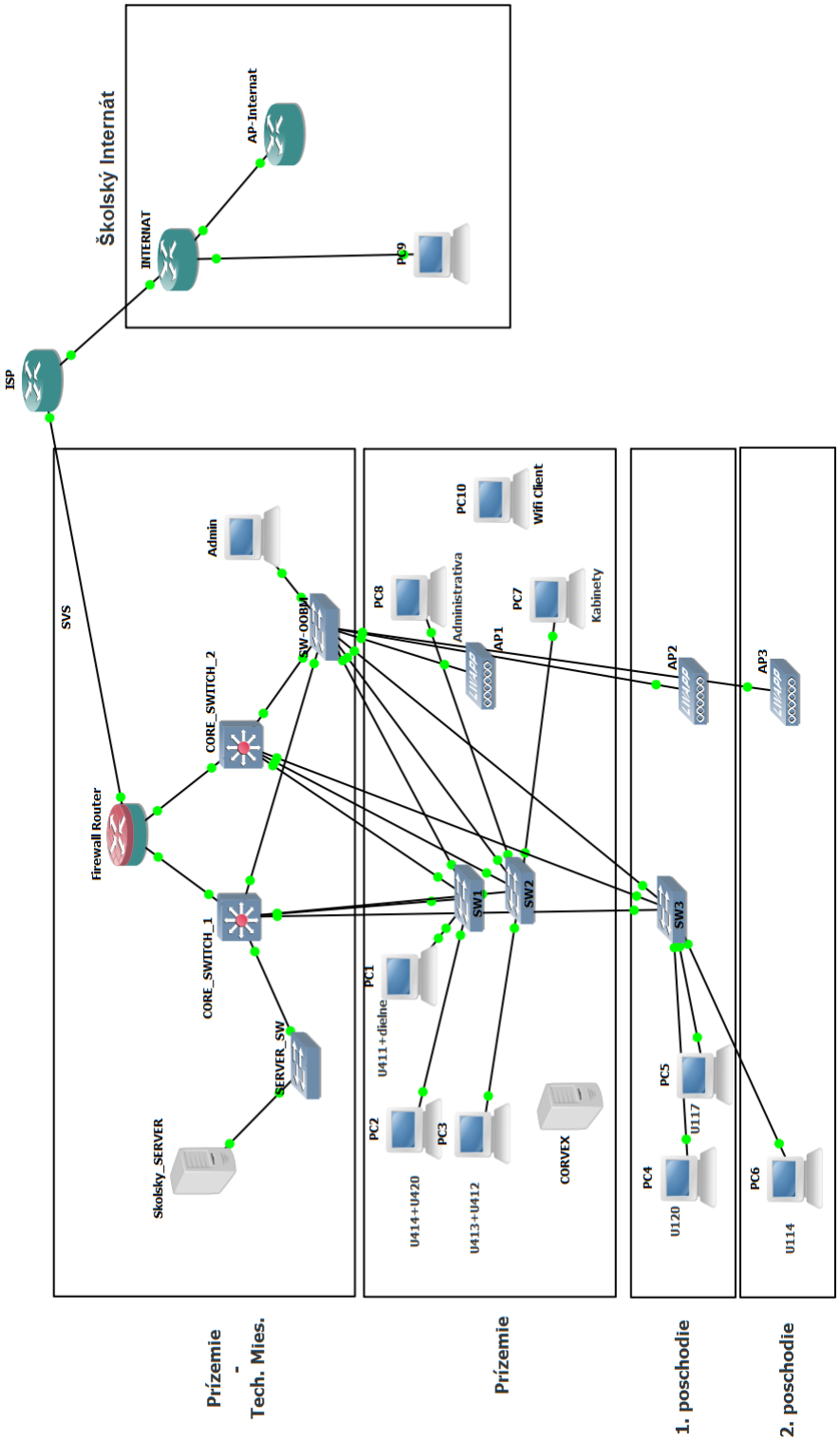
B Topológia súčasnej siete



C Návrh novej topológie siete



D Návrh siete v GNS3



E Konfiguračný súbor prepínača SW1-SW

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service dhcp
!
hostname SW1-SW
!
boot-start-marker
boot-end-marker
!
enable secret 5 1/yKWrhZGGh0OcYc5k9uXHkl6x0
!
aaa new-model
!
!
aaa authentication dot1x default group radius
!
aaa session-id common
memory-size iomem 5
no ip routing
no ip icmp rate-limit unreachable
no ip cef
!
no ip domain lookup
ip domain name spsepn.edu.sk
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
dot1x system-auth-control
vtp file nvram:vlan.dat

username admin password 0 spse
!
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 description *** Unused for Layer2 SW ***
 no ip address
```

```
 no ip route-cache
 shutdown
 speed auto
 full-duplex
!
interface FastEthernet0/1
 description *** Unused for Layer2 SW ***
 no ip address
 no ip route-cache
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/1
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/2
 duplex full
 speed 100
!
interface FastEthernet1/3
 duplex full
 speed 100
!
interface FastEthernet1/4
 duplex full
 speed 100
!
interface FastEthernet1/5
 switchport access vlan 10
 dot1x port-control auto
 duplex full
 speed 100
 dot1x port-control auto
 switchport port-security maximum 1
 switchport port-security violation shutdown
```

```
 switchport port-security mac-address 00:50:79:66:68:01
!
interface FastEthernet1/6
 switchport access vlan 10
 dot1x port-control auto
 duplex full
 speed 100
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security mac-address 00:50:79:66:68:02
!
interface FastEthernet1/7
 switchport access vlan 10
 dot1x port-control auto
 duplex full
 speed 100
 dot1x port-control auto
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security mac-address 00:50:79:66:68:03
!
interface FastEthernet1/8
 switchport access vlan 20
 duplex full
 speed 100
 dot1x port-control auto
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security mac-address 00:50:79:66:68:04
!
interface FastEthernet1/9
 switchport access vlan 20
 duplex full
 speed 100
 dot1x port-control auto
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security mac-address 00:50:79:66:68:05
!
interface FastEthernet1/10
 switchport access vlan 20
 duplex full
 speed 100
```

```
 dot1x port-control auto
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security mac-address 00:50:79:66:68:06
!
interface FastEthernet1/11
 switchport access vlan 30
 duplex full
 speed 100
 dot1x port-control auto
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security mac-address 00:50:79:66:68:07
!
interface FastEthernet1/12
 switchport access vlan 30
 duplex full
 speed 100
 dot1x port-control auto
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security mac-address 00:50:79:66:68:08
!
interface FastEthernet1/13
 switchport access vlan 30
 duplex full
 speed 100
 dot1x port-control auto
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security mac-address 00:50:79:66:68:09
!
interface FastEthernet1/14
 duplex full
 speed 100
!
interface FastEthernet1/15
 switchport access vlan 99
 duplex full
 speed 100
!
interface Vlan1
 no ip address
```

```
 no ip route-cache
 shutdown
!
interface Vlan99
 ip address 172.16.99.11 255.255.255.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
radius-server host 192.168.0.5 auth-port 1812 acct-port 1813
radius-server host 192.168.0.5 key CISCO
!
control-plane
!
banner exec
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password spse
 login local
!
!
end
```

F Konfiguračný súbor CORE-SWITCH1 prepínača

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service dhcp
!
hostname CORE_SWITCH_1
!
boot-start-marker
boot-end-marker
!
enable secret 5 1/yKWrhZGGh0OcYc5k9uXHkl6x0
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 172.16.40.1 172.16.40.10
!
ip dhcp pool WiFi
   network 172.16.40.0 255.255.255.0
   default-router 172.16.40.1
   dns-server 192.168.0.1
   domain-name spsepn.edu.sk
!
!
no ip domain lookup
ip domain name spsepn.edu.sk
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
spanning-tree vlan 10 priority 8192
spanning-tree vlan 20 priority 8192
spanning-tree vlan 30 priority 16384
spanning-tree vlan 40 priority 16384
vtp file nvram:vlan.dat
```

```
username admin password 0 spseadmin
!
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 description *** Unused for Layer2 SW ***
 no ip address
 shutdown
 speed auto
 full-duplex
!
interface FastEthernet0/1
 description *** Unused for Layer2 SW ***
 no ip address
 shutdown
 speed auto
 full-duplex
!
interface FastEthernet1/0
 no switchport
 ip address 172.16.0.6 255.255.255.252
 duplex full
 speed 100
!
interface FastEthernet1/1
 no switchport
 ip address 172.16.0.1 255.255.255.252
 duplex full
 speed 100
!
interface FastEthernet1/2
 duplex full
 speed 100
!
interface FastEthernet1/3
 duplex full
 speed 100
!
interface FastEthernet1/4
 duplex full
 speed 100
!
```

```
interface FastEthernet1/5
 duplex full
 speed 100
!
interface FastEthernet1/6
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/7
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/8
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/9
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/10
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/11
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/12
 duplex full
 speed 100
!
interface FastEthernet1/13
 duplex full
 speed 100
!
interface FastEthernet1/14
```

```
 duplex full
 speed 100
!
interface FastEthernet1/15
 switchport access vlan 99
 duplex full
 speed 100
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 172.16.10.3 255.255.255.0
 ip access-group STUDENTI_DENY in
 no ip redirects
 standby 1 ip 172.16.10.1
 standby 1 priority 150
 standby 1 preempt
!
interface Vlan20
 ip address 172.16.20.3 255.255.255.0
 no ip redirects
 standby 2 ip 172.16.20.1
 standby 2 priority 150
 standby 2 preempt
!
interface Vlan30
 ip address 172.16.30.3 255.255.255.0
 standby 3 ip 172.16.30.1
!
interface Vlan40
 ip address 172.16.40.3 255.255.255.0
 standby 4 ip 172.16.40.1
!
interface Vlan99
 ip address 172.16.99.1 255.255.255.0
!
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.4 0.0.0.3 area 0
```

```
 network 172.16.10.0 0.0.0.255 area 0
 network 172.16.20.0 0.0.0.255 area 0
 network 172.16.30.0 0.0.0.255 area 0
 network 172.16.40.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ip access-list extended STUDENTI_DENY
 deny   ip 172.16.10.0 0.0.0.255 172.16.20.0 0.0.0.255
 deny   ip 172.16.10.0 0.0.0.255 172.16.30.0 0.0.0.255
 deny   ip 172.16.10.0 0.0.0.255 172.16.40.0 0.0.0.255
 permit ip 172.16.10.0 0.0.0.255 any
!
control-plane
!
banner exec
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login local
 transport input ssh
!
!
end
```

G Konfiguračný súbor firewall smerovača

```
upgrade fpd auto
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname FW_TO_NET
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
!
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki trustpoint TP-self-signed-4279256517
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4279256517
 revocation-check none
 rsakeypair TP-self-signed-4279256517
!
!
crypto pki certificate chain TP-self-signed-4279256517
 certificate self-signed 01 nvram:IOS-Self-Sig#1.cer
username admin privilege 15 password 0 svsadmin
!
redundancy
!
!
ip tcp synwait-time 5
!
```

```
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 2
 encr aes 256
 authentication pre-share
crypto isakmp key spsepn address 198.80.2.6
!
!
crypto ipsec transform-set SPSE_PN esp-aes 256 esp-sha-hmac
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to198.80.2.6
 set peer 198.80.2.6
 set transform-set SPSE_PN
 match address 100
!
interface Loopback0
 ip address 172.16.20.2 255.255.255.0
 shutdown
 !
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
 !
!
interface GigabitEthernet1/0
 ip address 172.16.0.5 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 negotiation auto
 !
!
interface GigabitEthernet2/0
 ip address 172.16.0.9 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 negotiation auto
```

```
 !
!
interface GigabitEthernet3/0
 ip address 198.80.2.2 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 negotiation auto
 crypto map SDM_CMAP_1
!
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface default
 no passive-interface GigabitEthernet1/0
 no passive-interface GigabitEthernet2/0
 network 172.16.0.4 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
 default-information originate
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
ip nat inside source list 101 interface GigabitEthernet3/0 overload
ip route 0.0.0.0 0.0.0.0 198.80.2.1
!
access-list 100 remark CCP_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 172.16.20.0 0.0.0.255 172.16.50.0 0.0.0.255
access-list 101 deny   ip 172.16.20.0 0.0.0.255 172.16.50.0 0.0.0.255
access-list 101 permit ip 172.16.0.0 0.0.255.255 any
!
control-plane
!
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
```

```
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 privilege level 15
 login
 transport input telnet ssh
!
end
```